
Escalation of Privileges
(…I've got the power)
http://www.JasonDion.com

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Escalation of Privilege Phase

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Escalation of Privilege Phase

Step 4 - Escalation of Privilege

- Gain administrative, system or root access by escalating the account's privileges
- After privilege escalation, attackers have full control over the system and/or network
- Gain administrator access over the workstation, then expand to domain administrator (if possible)

Escalation Methods

- Exploit admin or “system”
- Steal password with keylogger
- Steal and crack SAM database

SAM Database

- Stores passwords as a binary encrypted hash

Stealing SAM

- Physical access
  - Copy SAM with NT Emergency Repair Disk
  - Reset user passwords using NTFSDOS or LINNT
- Logical access
  - Copy SAM (hashdump) and crack with Pwdump, LCP, Ophcrack, or John the Ripper

Authentication Types

- LM authentication
- NTLM authentication
- NTLM v2
- Kerberos

LM Authentication

- LANMAN
- Used by Windows 95/98/ME
- Based on DES (easy to crack)
- Used for backward compatibility

NTLM Authentication

- NT LANMAN
- Used in Windows NT (<SP3)
- Based on DES and MD4
- Now only used for backward compatibility

NTLM v2

- NT LANMAN Version 2
- Used in Windows NT (SP3+)
- Based on MD4 and MD5

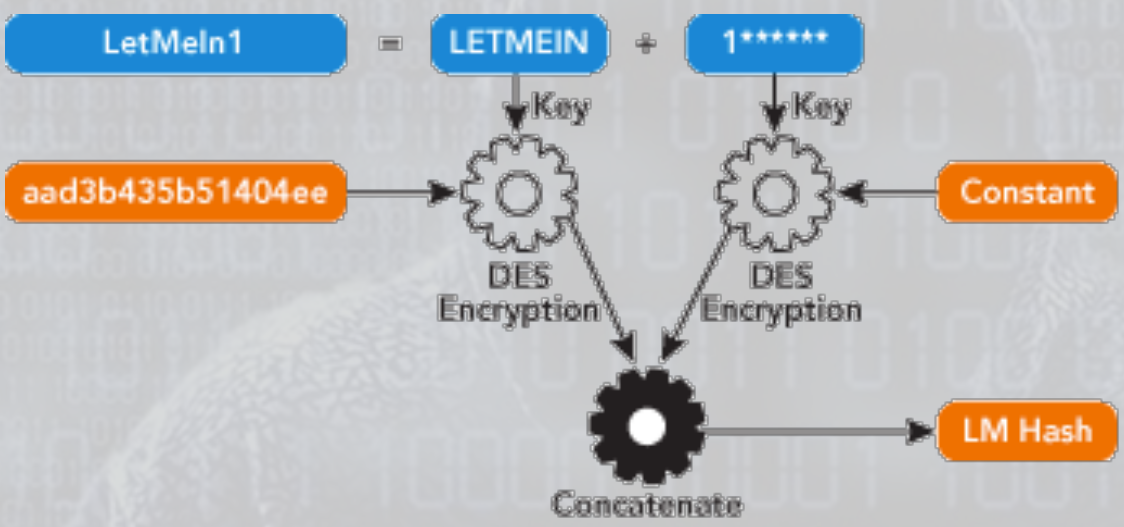
Kerberos

- Updated authentication which started in Windows 2000

- Still used in Windows 8 and Windows 2012

How LM Hashes Works

1) Password is converted to all uppercase (LETMEIN)
2) Password is padded with null (blanks) to make it 14 characters long (LETMEIN1……)
3) String is broken into two 7 character parts (LETMEIN and 1……)
4) Each part is then encrypted separately and put back together



Collecting Hashes (Hashdump)

- Command in meterpreter
- Part of Metasploit Framework
- Collects hashes from remote machines with interactive shell

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 00a29affc07173e032c00a50a74197ba...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...
```

Hashdump (example)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:8e21a23181ac4c37d65b1078c0dfbf1b:65794c60b55dafd2e0783e8a6e4fac98:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8c91347da95093b16772c42a93c50f68:::
Bazinga:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
track:1004:eb498aa66abdd32aaad3b435b51404ee:34b23d452077f6dd6e097a722bb5223a:::
troll:1005:aebd4de384c7ec43aad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
```

Hashdump (example)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:50[illegible]:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssi[illegible]ant:1000:8e21a23181ac4c37d65b1078c0dfbf1b:65794c60b55dafd2e0783e8a6e4fac98:::
SUPPORT_[illegible]8945a0:1002:aad3b435b51404eeaad3b435b51404ee:8c91347da95093b16772c42a93c50f68:::
Bazinga:1[illegible]03:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
track:100[illegible]eb498aa66abdd32aaad3b435b51404ee:34b23d452077f6dd6e097a722bb5223a:::
troll:100[illegible]aebd4de384c7ec43aad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
```

User

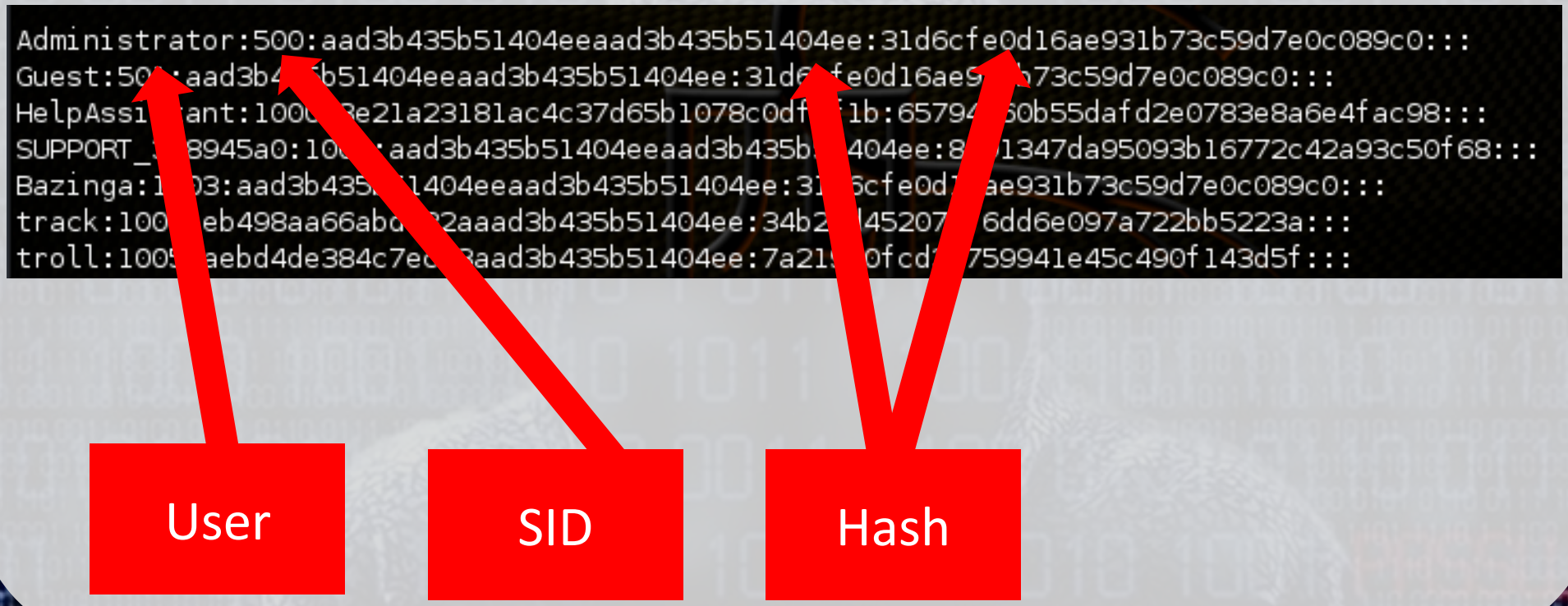
Hashdump (example)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:50[illegible]:aad3b4[illegible]b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssi[illegible]tant:100[illegible]8e21a2318lac4c37d65b1078c0dfbf1b:65794c60b55dafd2e0783e8a6e4fac98:::
SUPPORT_[illegible]8945a0:10[illegible]:aad3b435b51404eeaad3b435b51404ee:8c91347da95093b16772c42a93c50f68:::
Bazinga:1[illegible]03:aad3b435[illegible]1404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
track:100[illegible]eb498aa66abd[illegible]2aaad3b435b51404ee:34b23d452077f6dd6e097a722bb5223a:::
troll:100[illegible]aebd4de384c7ec[illegible]3aad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
```

User

SID

Hashdump (example)



Collecting Hashes (L0phtcrack)

- Extracts hashes from local or remote machines
- Sniffs passwords from local network (if used with an admin account)

Collecting Hashes (Pwdump)

- Command-line tool that can bypass SYSKEY encryption of the SAM (if you have admin rights)
- Collects hashes and can store as text file

Password Cracking

- Dictionary
- Brute Force
- Hybrid

Dictionary Attack

- Uses a dictionary or word list to crack password
- Quickest attack method
- Only as good as your dictionary
- Rainbow Tables

Brute Force Attack

- Uses random numbers and characters

- Crack can take hours, years, or decades depending on password length and complexity
- 100% successful method

Hybrid Attack

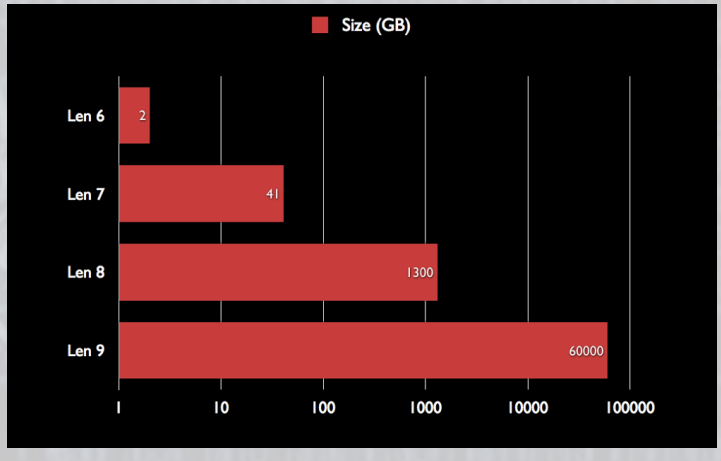
- Uses dictionary or word list and prepends or appends characters and numbers to a base word

- More time than dictionary, less than brute force

- Example:
  - password, 1password, password123, p@ssw0rd, …

Password Cracking (Cane and Able)

- Multipurpose tool to perform password cracking, Windows enumeration, and VOIP sniffing

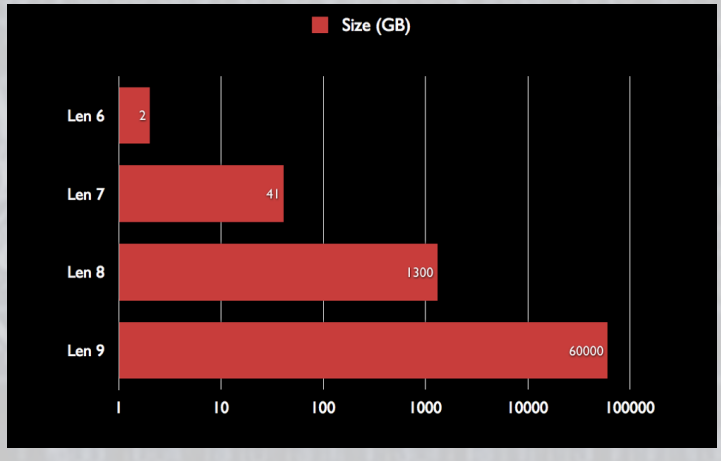


- Uses:
  - Dictionary
  - Brute Force
  - Rainbow Tables

Password Cracking (John the Ripper)

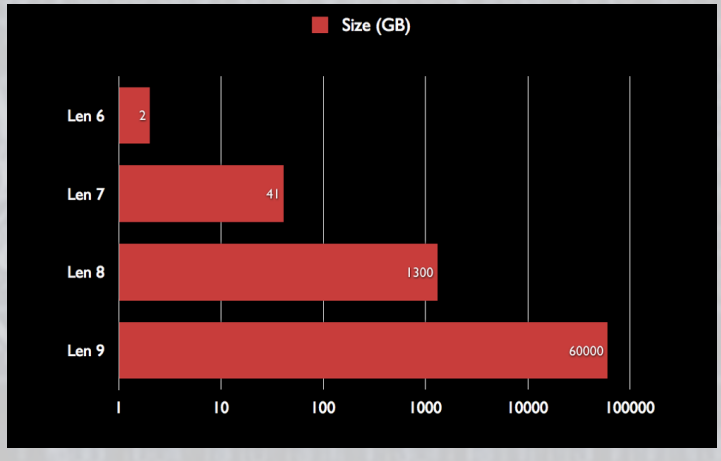
- Can crack Kerberos AFS, LM Hashes, and more

- Passwords cracked are not case-sensitive
  - Password = PASSWORD



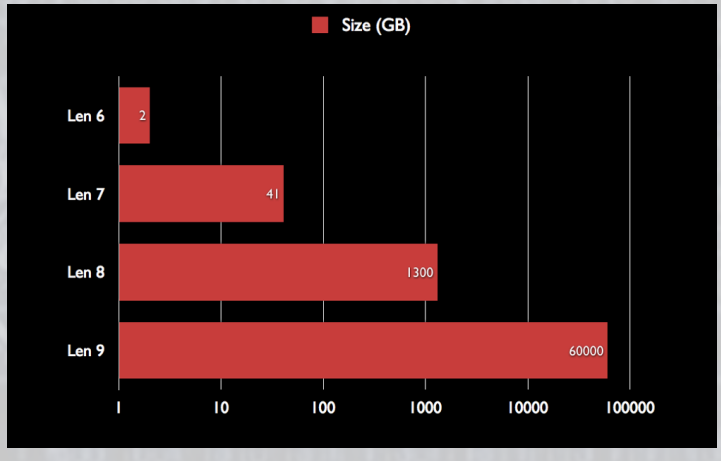
Password Cracking (Ophcrack)

- Uses rainbow tables for very fast password cracking
- Rainbow tables can be very large files, though
- All passwords from 0 to 9 characters takes 60 TB!



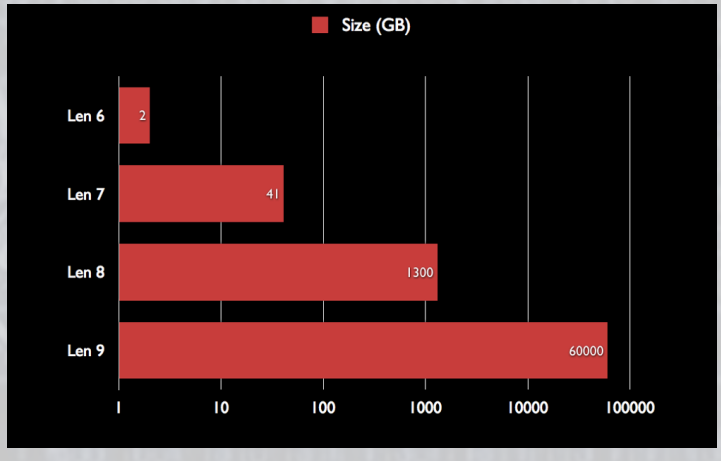
Password Cracking (Crackstation)

- Crackstation.net
- Uses rainbow tables for very fast password cracking
- All rainbow tables are loaded on their servers
- Example LM: 855c3697d9979e78ac404c4ba2c66533



Password Cracking (Crackstation)

- Crackstation.net



- Uses rainbow tables for very fast password cracking

- All rainbow tables are loaded on their servers

passphrasefloppy

- Example LM: 855c3697d9979e78ac404c4ba2c66533

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Escalation of Privilege Phase


Escalation of Privileges
(…I've got the power)
http://www.JasonDion.com