
Maintaining Access
(…Hold on tight!)
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

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

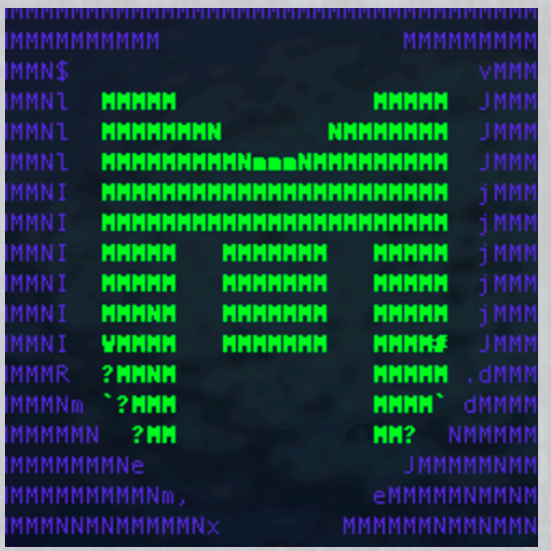
Risk Level

Overview of Maintaining Access

- Attackers use techniques to maintain access:
  - Network sniffers
  - Steal additional passwords
  - Lateral movement to other targets
  - Opening ports and starting services
- Survey the host and understand its posture
  - Look for others on the system…are you alone?
- Goal is keep persistent access
- Now, you are ready for data exfiltration, data compromise, system takeover, ...

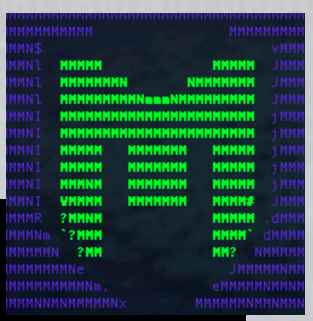
Network Sniffers

- Wireshark
  - Works if you're on same network



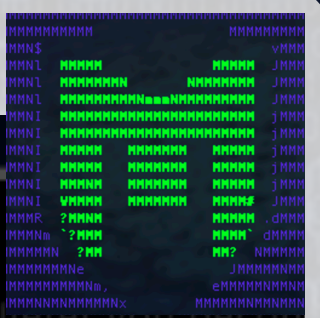
- Meterpreter
  - Has a sniffer built-in

Load Sniffer (meterpreter)



```
meterpreter > load sniffer
Loading extension sniffer...success.
meterpreter > help
```

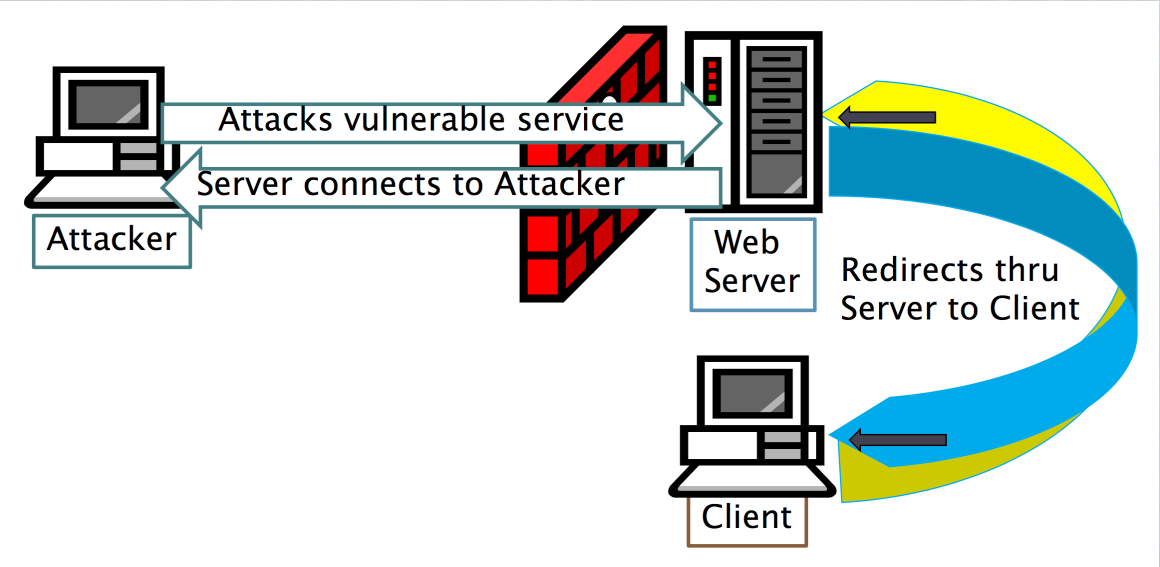
Sniffer Commands



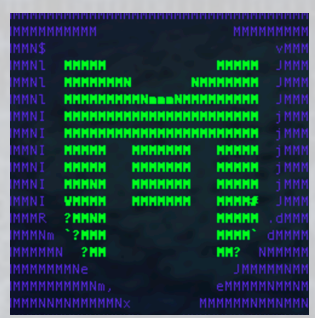
```
Sniffer Commands
================


    Command             Description
    -------             -----------
    sniffer_dump        Retrieve captured packet data to PCAP file
    sniffer_interfaces  Enumerate all sniffable network interfaces
    sniffer_release     Free captured packets on a specific interface instead of downloadin
g them
    sniffer_start       Start packet capture on a specific interface
    sniffer_stats       View statistics of an active capture
    sniffer_stop        Stop packet capture on a specific interface
```

Lateral Movement

- Use another machine as a proxy to exploit other hosts that it can “see”



Lateral Movement



- ARP scan to find a list of potential IPs
  - post/windows/gather/arp_scanner
- Once you have a list of IPs, you can use more focused scanning techniques
  - auxiliary/scanner/portscan/tcp

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


Maintaining Access
(…Hold on tight!)
http://www.JasonDion.com