4.1

Monday, September 25, 2023 6:12 PM

Cuckoo - sandbox tool to analyze malware as it runs

Nessus - commercial vuln scanner that scans devices and raises alarm if detects vuln

Autopsy - digital forensics platform w/ GUI

FTK Imager - data imaging tool to quickly assess evidence to determine if further anal needed

"help audit server's security settings"

- tcpdump
- tshark - terminal version of wireshark

Wireless scanner - scans for SSIDs, freq band,
channel usage, ...

AirPcap - wireless adapter designed for
packet capture

```
openssl genrsa -out server.key 1024
```

generates RSA key of size 1024

```
nmap -O test.org
```

enable OS detection

Nping & Nmap have packet sniffing
and DoS capabilities

NMap

NSE = DoS

Npcap = packet sniff

Active KillDisk - disk wiping sanitization tool; purge data using 1's and 0's

Nessus compares against known vulns

WinHex - commercial disk editor and hex editor used for data recovery and digital forensics

Volatility - framework for system mem anal; can install pmem kernel driver which gives dd or memdump access to device memory

Metasploit - cybersecurity framework that offers info on security flaws testing and that offers

and assists in pen testing and

creation of IDS sigs

Sn1per - pen test reporting and
evidence gathering

Zed Attack Proxy - scan tools/scripts
for web app and mobile testing

Ping

- -t - send out pings until stop
  like linux

- -c - only send out 4

like windows

-n - sets # of echo requests to

-n - sets # of echo requests to send default 4

-S - specify diff source addr

-r - records rout for count hops IPv4

Select-String requires -Path and -Pattern

theHarvester - OSINT data collection tool

Wireshark

· check for open ports

· eavesdrop on open net comms

moving frames

cant sniff out moving frames

Sniffer tools can

DoD 5220.22-M wipe method
write 1's/0's/random chars

NTDS.DIT - stores domain pwords/creds

Bitlocker keys stored w/ pc account
object in Active Directory

Netstat = ports

ipconfig /all - output detailed net info
for all connected NIC

Meterpreter - exploit module that
uses in memory DLL injection
Stagers - create net connection
attacker/target

Stage(s) —

between attacker/target

Nexpose - vuln scanner

when + w/ metasploit pro, can read and scan report to confirm vulns

FireELF - fileless open source Linux malware framework that can build/manage payloads quickly

Nmap

- -O = OS detection
- -A = OS detection, virus, script scan, traceroute

Sysinternals - suite of tools to assist in troubleshooting Win issues