Security +
Software Security Tools

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Terms

Passive tools
- Non-intrusive tools that have little chance of compromising the system

Active tools
- Intrusive tools that can potentially affect the operations of a system

Network Mapping
- Discovering devices on a network relative to connectivity
- Nmap, Netcat, and ping can be used to can IP ranges such as:
  - Scan for all IP on subnet
    - **nmap -sn 192.168.1.0/24**
  - Scan for all IP in range
    - **nmap -sP 192.168.1.***
  - Ping for all IP in range
    - **for ip in $(seq 1 254); do ping -c 1 192.168.1.$ip; done**
  - Netcat scan for all IP in range with specific active port
    - **for i in {1..10}; do nc -v -n -z -w 1 192.168.1.$i 80; done**

Banner Grabbing
- Requesting an HTML banner that provides information about a server
- The banner can contain information about the server OS or server services / applications such as application version, etc.
- Netcat can be used to grab banner information:
  - **nc 192.169.1.1 22**
  - **echo "" | nc -vv -w1 192.168.1.1 443**
  - **echo "" | nc -vv -w1 example.com 443**
    - **echo “”** sends empty string to the server
    - **-vv** is high verbosity mode
    - **-w1** is the timeout wait of one second
- **Nmap** can be used to grab banner information:
  - Grab all banners for all registered ports from specific IP
    - **nmap -sV --script=banner 192.168.1.1**
  - Grab all banners for all registered ports for all IP in range
    - **for i in {1..10}; do nmap -sV --script=banner 192.168.1.$i; done**

Penetration Testing

- Actively assesses deployed security controls of a system, network, or publicly available IP address by simulating an attack on the network
- Can test an organizations attack response
- Can also test policy efficacy in the case of social engineering
- Testing can be done on test environments or live environments
- Activities Include
  - **Passive recon**
    - Collection information about the target but does not engage the target
  - **Active recon**
    - Engages the target with tools to send the target data (nmap, nessus) to scan for ports, services, OS, etc.
  - **Initial exploitation**
    - Scanning for vulnerabilities on the target host and attempting to exploit a vulnerability to gain access
  - **Escalation of privilege**
    - Gaining access to accounts or higher-privilege command execution
  - **Pivot**
    - Mapping the network resources available at the initial point of escalation and attempting to compromise the other network resources
  - **Persistence**
    - Installing software that allows continuous access to the system

Vulnerability Scanning

- Scanner software
  - Nessus
  - WPScan
- Identify vulnerabilities
  - Can run as **credentialed** and **non-credentialed**
- Passively test security controls
- Identify lack of security controls
- Identify misconfigurations
  - Open Ports
  - Weak Passwords
  - Default accounts and passwords
  - Access to sensitive data
  - Security and configuration errors
- Lack of up-to-date patches

Network Scanning

- **Ping scan**
  - ICMP scan of the devices on a network
- **Arp ping scan**
  - ARP ping scan can map a network for MAC addresses
- **Syn stealth scan**
  - Using SYN packets to scan a network for available connections
  - Typically the scanning client will send a reset (RST) packet if the host responds

- **Port scan**
  - Checking for open ports on a host. Typically well-known ports are scanned first for known protocol / services
- **Service scan**
  - Mapping open ports to default services that operate on that port
  - Can identify services running on non-standard ports, which is common in practice
  - Work by sending some probe data to the port, and monitoring the response
- **OS detection**
  - TCP/IP fingerprinting can allow OS detection
  - The TCP receive window length can identify various operating systems
  - For example, Linux uses 5,840 bytes, Cisco routers use 4,128 bytes different Windows versions use sizes of 8,192 and 65,535

Wireless Scanners / Cracker

- **Passive wireless**
  - Scan listens on known channels on the 2.4 and 5 Ghz spectrums
- **Active scans** can send queries to the AP to guess WPS pins
- **SSID**
  - Detection of all APs within range
- **MAC addresses** of all APs
- **Signal Strength**
  - Can help find the source of the AP
- **Channels**
  - Can determine if interference between APs is occurring
- **Channel widths**
  - Usually 20Mhz but APs can use two channels which would be 40Mhz
- Security of the AP depends if the scanner is using **Open mode** or another wireless cryptographic protocol (WEP, WPA, WPA2)

Microsoft Windows

Windows Active Directory

- Manages windows network domains
- Can manage federated logons in a Active Directory forest

MBSA Microsoft Baseline Security Analyzer

GPMC Group Policy Management Console

Ping

- **ping [IP or hostname]**
  - Sends ICMP packets to see if another system can be reached / will respond
  - Microsoft defaults to sending 4 ICMP packets
  - If using the hostname such as domain name, the resolution to IP address

will be shown as well

ipconfig

- **ipconfig**
  - Basic NIC information, IP address, subnet mask, and default gateway
- **ipconfig /all**
  - Shows all NIC's and detailed information such as MAC address, DNS servers, DHCP server address
- **ipconfig /displaydns**
  - Show contents of the DNS cache and hostname to IP mappings

Netstat

- **netstat**
  - Shows all open TCP connections
- **netstat -a**
  - Shows all TCP and UDP ports that a system is listening on
- **netstat -r**
  - Display routing table
- **netstat -e**
  - Network statistics such as RX and TX
- **netstat -n**
  - Addresses and port numbers in numerical order
- **netstat -p *protocol***
  - Show statistics on a specific protocol
- **netstat -anp tcp**
  - Displays the state of a connection such as ESTABLISHED

Tracert

- **tracert [IP address or URL]**
  - Lists routers between the two systems
- **traceert -d [IP]**
  - Do not resolve IP to domain name

Arp

- **arp -a [IP]**
  - Shows arp cache
  - If [IP] is specified, will show only for the specified IP address

DNS

- **displaydns**
  - displays the dns cache on

Route

- See Route in Linux section below

Linux Commands

ping

- **ping [IP or hostname]**
  - Send ICMP packets to see if another system can be reached / will respond
- **-c [int]**
  - Specify number of packets to send, otherwise will not stop
- If using the hostname such as domain name, the resolution to IP address will be shown as well

ifconfig and ip

- **ifconfig /flushdns**
  - Erase the contents of the DNS cache
- **ifconfig eth0**
  - Shows the details of a specific NIC
- **ifconfig etho promisc**
  - Enables promiscuous mode on a NIC
- **ifconfig eth0 allmulti**
  - Enables multicast mode on a NIC (disable ifconfig eth0 -allmulti)
- **ip link show**
  - Shows all NIC and details
- **ip link set eth0 up**
  - Enables a network interface (ip link set eth0 down to disable)
- **ip -s link**
  - Shows statistics on NIC

netstat

- **netstat**
  - Shows all open TCP connections
- **netstat -a**
  - Shows all TCP and UDP ports that a system is listening on
- **netstat -r**
  - Display routing table
- **netstat -e**
  - Network statistics such as RX and TX
- **netstat -n**
  - Addresses and port numbers in numerical order
- **netstat -p [protocol]**
  - Show statistics on a specific protocol
- **netstat -anp tcp**
  - Displays the state of a connection such as ESTABLISHED

traceroute

- **traceroute [IP address or URL]**
  - Lists routers between the two systems
- **traceroute -d [IP]**
  - Do not resolve IP to domain name

arp

- **arp** command shows information related to **ARP Address Resolution**

Protocol

- **ARP protocol** resolves IP (network address) address to MAC address (NIC hardware address)
- **arp** command
  - Shows the arp cache
- **arp -d [IP]**
  - Deletes the current arp entries for a host by IP

nslookup and dig

- **nslookup [domain]**
  - Scans for hostnames or **FQDN**s (fully qualified domain name) using DNS protocol and returns the IP address
- **dig [@server] [name] [type]**
  - **[@server]** is the **IP address** of the target of the query
  - **[name]** is the **domain** of the resource to be looked up
  - **[type]** is the type of the record to look up (**DNS "A" record by default**)
  - Similar to **nslookup** but more information is provided
  - **-f [file]** a batch mode of operation for reading lookup requests from file
  - If no name-server is explicitly set, dig will use the ***/etc/resolv.conf*** DNS settings

netcat

- Netcat is a multi-functional network tool which can be used for:
  - Banner grabbing
  - File transfer
  - Port scanner
  - Remote access

nmap

- Scans hosts for open ports, services, grabs banners, and can guess about OS, and service versions when not explicitly revealed in banner info
- Can also be used to enumerate a network IP range for active hosts

dmesg

- Used to examine or control the kernel ring buffer
- dmesg -kH -l --
  - **-H** = human readable output

route

-

Exploitation Frameworks

- Metasploit
- Beef Browser Exploitation Framework

- W3af Web Application Attack and Audit Framework

Password Cracking Tools

John the Ripper

- Password cracker for Unix, Linux, Windows, and MacOS

L0phtCrack

- A password auditing and recovery application originally produced by Mudge from L0pht Heavy Industries
- It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using:
  - dictionary
  - brute-force
  - hybrid attacks
  - rainbow tables

Network Scanning Tools

Protocol analyzers

- Wireshark / Tshark
- TCPDump
- Nmap / Zenmap

SAINT Security Administrator's Integrated Network Tool

- A computer software used for scanning computer networks for security vulnerabilities, and exploiting found vulnerabilities
- Tools include:
- SAINT Network Vulnerability Scanner
- SAINTexploit Penetration Testing Tool
- SAINTmanager Remote Management Console
- SAINTCloud

SATAN Security Administrator Tool for Analyzing Networks

Log Analysis

- **/var/log/auth.log**
- **/var/log/messages**
- **/var/log/boot.log**
- **/var/log/faillog**
- **/var/log/kern.log**
- **/var/log/httpd/**
- Also some linux distros include utmp, wtmp, btmp or utmpx, wtmpx, btmpx variants
- Other logs may include antivirus log, application logs, performance logs

Forensics Tools

AccessData Forensic Toolkit (FTK)

EnCase Commercial Software

dd - Linux command