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.

Banner Grabbing

- Requesting an HTML banner that provides information about a server
- The banner can contain information about the server OS and server application

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
- **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] - send ICMP packets to see if another system can be reached / will respond (-c count : number of packets to send)

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. Shows 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 (-d : do not resolve IP to domain name)

Arp

- arp -a - shows arp cache

DNS

- displaydns - displays the dns cache on

Linux Commands

ping

- ping [IP or hostname] - send ICMP packets to see if another system can be reached / will respond (-c count : number of packets to send)

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 (-d : do not resolve IP to domain name)

arp

- arp - shows the arp cache
- arp -a [IP] -

nslookup and dig

- nslookup [domain] - scans hostnames or **FQDN**s (fully qualified domain name)
- dig [domain] - similar to nslookup but more information is provided

netcat

- echo "" | nc -vv -v w1 [domain]
- file transfer
- portscanner

Exploitation Frameworks

- Metasploit (Linux)
- Beef Browser Exploitation Framework
- W3af Web Application Attack and Audit Framework

Password Cracking Tools

John the Ripper

- Password cracker for *nix, 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