Network Scanning Phases and Supporting Tools

Joseph Bugeja
Information Security Manager/Architect
November 24, 2013
Scanning Phase Goals

- **Overall:** Learn more about targets and find openings by interacting with the target environment
  - Determine network addresses of live hosts, firewalls, routers, etc. in the network
  - Determine network topology of target environment
  - Determine operating system types of discovered hosts
  - Determine open ports and network services in target environment
  - Determine list of potential vulnerabilities
  - Do these in a manner that minimizes risk of impairing host or service
Scan Types

- **Network Sweeping**
  - Send a series of probe packets to identify live hosts at IP addresses in the target network

- **Network Tracing**
  - Determine network topology and draw a map

- **Port Scanning**
  - Determine listening TCP and UDP ports on target systems

- **OS Fingerprinting**
  - Determine the target operating system type based on network behaviour
Scan Types

- **Version Scanning**
  - Determine the version of services and protocols spoken by open TCP and UDP ports

- **Vulnerability Scanning**
  - Determine a list of potential vulnerabilities (misconfigurations, unpatched services, etc.) in the target environment
Scanning Tip: While Scanning Run a Sniffer

• Whenever you run a scan, run a sniffer so that you can monitor network activity
  – You do not have to capture all packets in the file system
    • That would likely require huge storage space
  – Instead, display them on the screen so you can visualize what is happening in the scan

• Which sniffer to use?
  – Any sniffer that shows packet headers will do, but you want something small, flexible and fast
  – tcpdump is ideal for this purpose
Scanning Tip: Use TCPDump

- Free, open source sniffer
  - www.tcpdump.org
  - Ported to Windows as WinDump at www.winpcap.org/windump/default.htm
- Supports various filtering rules
- While testing, you will likely have it display all packets leaving from and coming to your scanning machine
- But, for specific issues, you may need to focus on specific packets
- Often, just running tcpdump with no special options while scanning provides the information you need
  
  $ sudo tcpdump
Network Sweep Tools

- Angry IP
  - www.angryip.org
  - GUI-based tool for Windows
    - Ping sweep (via ICMP Echo Request)
    - TCP port scan
    - Gets MAC address for systems on same subnet
    - NetBIOS name and workgroup gathering

- ICMPQuery
  - www.angio.net/security/icmpquery.c
  - Command-line tool for Linux/UNIX
    - Sends ICMP Timestamp (Type 13) and Address Mask Request (Type 17) messages to identify live hosts
    - Useful for identifying hosts in a network that has firewalls which block ICMP Echo Request
Network Sweep Tools

• HPing
  – Inspired by ping, but goes much further
    • Originally Hping, then Hping2...latest is Hping3
    • From man page: “Send (almost) arbitrary TCP/IP packets to networks hosts”
  – Free at www.hping.org, runs on Linux, *BSD, Windows and MacOS X
  – The latest version, Hping3, supports TCL scripting
  – By default, sends TCP packets with no control bits set to target port 0 continuously, once per second
    • Possibly getting RESETs back
  – Example: `# hping3 10.10.10.20`
Network Tracing Tools

- **Traceroute**
  - Discovers the route that packets take between two systems
  - Helps a tester construct network architecture diagrams
  - Included in most operating systems
  - Sends packets to target with varying TTLs in the IP Header

- **Layer Four Traceroute (LFT)**
  - Free at http://pwhois.org/lft
  - Runs on Linux and Unix
  - Supports a variety of Layer Four options for tracerouting
Network Tracing Tools

- **3D Traceroute**
  - Runs on Widows, free at www.d3tr.de
  - Graphical traceroute using ICMP Echo Request, updated/animated in real-time

- **Web-Based Traceroute Services**
  - Instead of tracerouting from your address to the target, various websites allow you to traceroute from them to the target
  - Very useful in seeing if you are being shunned during a test!
Port Scanning Tools

• **Nmap**
  - Written and maintained by Fyodor
    - Very popular, located at www.insecure.org
  - Has been extended into a general-purpose vulnerability scanner via Nmap Scripting Engine (NSE)
  - Run with *--packet-trace* to display summary of each packet before it is sent, with output that includes:
    - Nmap calls to the OS
    - SENT/RCVD
    - Protocol (TCP/UDP)
    - Source IP:Port and Dest IP:Port
    - Control Bits
    - TTL
    - Other header information
OS Fingerprinting Tools

• Nmap
  – Attempts to determine the operating system of target by sending various packet types and measures the response
  – Different systems have different protocol behaviour that we can trigger and measure remotely

• Xprobe2
  – ofirarkin.wordpress.com/xprobe
  – Based on Ofir Arkin ICMP fingerprinting research
  – Applies fuzzy logic to calculate the probabilities of its operating system type

• P0f2
  – Supports passive OS fingerprinting
  – Free
Version Scanning Tools

- **Nmap**
  - Version scan invoked with `-sV`
  - Or use `-A` to for OS fingerprinting and version scan (i.e., `-A = -sV + -O`)

- **THC Amap**
  - Free from http://freeworld.thc.org/thc-amap
  - Amap can do a port scan itself or it can be provided with the output file from Nmap
  - It sends triggers to each open port
  - It looks for defined responses
  - A useful second opinion to the Nmap version scan
Vulnerability Scanning Tools

• Nmap Scripting Engine (NSE)
  – Scripts are written in the Lua programming language
  – May some day rival Nessus and NASL as a general purpose, free, open source vulnerability scanner

• Nessus Vulnerability Scanner
  – Maintained and distributed by Tenable Network Security
    • www.nessus.org
  – Free download
  – Plugins measure flaws in target environment
  – As new vulnerabilities are discovered, Tenable personnel release plugins
Vulnerability Scanning Tools

- **Commercial Solutions**
  - SAINT
  - Retina Network Security Scanner
  - Lumension PatchLink Scanner
  - BiDiBLAH
  - CORE Impact

- **Scanning Services/Appliances**
  - Foundscan
  - Qualys

- **Free Solutions**
  - SARA
  - SuperScan
Thank You!

Thanks for Listening!

Joseph Bugeja
bugejajoseph@yahoo.com