Scanning and Enumeration

**Scanning** - discovering systems on the network and looking at what ports are open as well as applications that may be running

**Connectionless Communication** - UDP packets are sent without creating a connection. Examples are TFTP, DNS (lookups only) and DHCP

**Connection-Oriented Communication** - TCP packets require a connection due to the size of the data being transmitted and to ensure deliverability

TCP Flags

| **Flag** | **Name** | **Function** |
| --- | --- | --- |
| SYN | Synchronize | Set during initial communication. Negotiating of parameters and sequence numbers |
| ACK | Acknowledgment | Set as an acknowledgement to the SYN flag. Always set After initial SYN |
| RST | Reset | Forces the termination of a connection (in both directions) |
| FIN | Finish | Ordered close to communications |
| PSH | Push | Forces the delivery of data without concern for buffering |
| URG | Urgent | Data inside is being sent out of band. Example is cancelling a message |

TCP Handshake

* SYN -> SYN-ACK - ACK
* Sequence numbers increase on new communication. Example is computers A and B. A would increment B’s sequence number. A would never increment it’s own sequence.

Port Numbers

* **Internet Assigned Numbers Authority** (IANA) - maintains Service Name and Transport Protocol Port Number Registry which lists all port number reservations
* Ranges
	+ **Well-known ports** - 0 - 1023
	+ **Registered ports** - 1024 - 49,151
	+ **Dynamic ports** - 49,152 - 65,535

| **Port Number** | **Protocol** | **Transport Protocol** |
| --- | --- | --- |
| 20/21 | FTP | TCP |
| 22 | SSH | TCP |
| 23 | Telnet | TCP |
| 25 | SMTP | TCP |
| 53 | DNS | TCP/UDP |
| 67 | DHCP | UDP |
| 69 | TFTP | UDP |
| 80 | HTTP | TCP |
| 110 | POP3 | TCP |
| 135 | RPC | TCP |
| 137-139 | NetBIOS | TCP/UDP |
| 143 | IMAP | TCP |
| 161/162 | SNMP | UDP |
| 389 | LDAP | TCP/UDP |
| 443 | HTTPS | TCP |
| 445 | SMB | TCP |
| 514 | SYSLOG | UDP |

* + A service is said to be **listening** for a port when it has that specific port open
	+ Once a service has made a connection, the port is in an **established** state
	+ Netstat
		- Shows open ports on computer
		- **netstat -an** displays connections in numerical form
		- **netstat -b** displays executables tied to the open port (admin only)

Subnetting

* **IPv4 Main Address Types**
	+ **Unicast** - acted on by a single recipient
	+ **Multicast** - acted on by members of a specific group
	+ **Broadcast** - acted on by everyone on the network
		- **Limited** - delivered to every system in the domain (255.255.255.255)
		- **Directed** - delivered to all devices on a subnet and use that broadcast address
* **Subnet mask** - determines how many address available on a specific subnet
	+ Represented by three methods
		- **Decimal** - 255.240.0.0
		- **Binary** - 11111111.11110000.00000000.00000000
		- **CIDR** - x.x.x.x/12 (where x.x.x.x is an ip address on that range)
	+ If all the bits in the host field are 1s, the address is the broadcast
	+ If they are all 0s, it’s the network address
	+ Any other combination indicates an address in the range
	+ 

Scanning Methodology

* **Check for live systems** - ping or other type of way to determine live hosts
* **Check for open ports** - once you know live host IPs, scan them for listening ports
* **Scan beyond IDS** - if needed, use methods to scan beyond the detection systems
* **Perform banner grabbing** - grab from servers as well as perform OS fingerprinting
* **Scan for vulnerabilities** - use tools to look at the vulnerabilities of open systems
* **Draw network diagrams** - shows logical and physical pathways into networks
* **Prepare proxies** - obscures efforts to keep you hidden

Identifying Targets

* The easiest way to scan for live systems is through ICMP.
* It has it’s shortcomings and is sometimes blocked on hosts that are actually live.
* **Message Types and Returns**

| **ICMP Message Type** | **Description and Codes** |
| --- | --- |
| 0: Echo Reply | Answer to a Type 8 Echo Request |
| 3: Destination Unreachable | Error message followed by these codes:0 - Destination network unreachable1 - Destination host unreachable6 - Network unknown7 - Host unknown9 - Network administratively prohibited10 - Host administratively prohibited13 - Communication administratively prohibited |
| 4: Source Quench | A congestion control message |
| 5: Redirect | Sent when there are two or more gateways available for the sender to use. Followed by these codes:0 - Redirect datagram for the network1 - Redirect datagram for the host |
| 8: Echo Request | A ping message, requesting an echo reply |
| 11: Time Exceeded | Packet took too long to be routed (code 0 is TTL expired) |

* + Payload of an ICMP message can be anything; RFC never set what it was supposed to be. Allows for covert channels
	+ **Ping sweep** - easiest method to identify hosts
	+ **ICMP Echo scanning** - sending an ICMP Echo Request to the network IP address
	+ An ICMP return of type 3 with a code of 13 indicates a poorly configured firewall
	+ **Ping scanning tools**
		- Nmap
		- Angry IP Scanner
		- Solar-Winds Engineer Toolkit
		- Advanced IP Scanner
		- Pinkie
	+ Nmap virtually always does a ping sweep with scans unless you turn it off

Port Scan Types

* **Full connect** - TCP connect or full open scan - full connection and then tears down with RST
	+ Easiest to detect, but most reliable
	+ nmap -sT
* **Stealth** - half-open scan or SYN scan - only SYN packets sent. Responses same as full.
	+ Useful for hiding efforts and evading firewalls
	+ nmap -sS
* **Inverse TCP flag** - uses FIN, URG or PSH flag. Open gives no response. Closed gives RST/ACK
	+ nmap -sN (Null scan)
	+ nmap -sF (FIN scan)
* **Xmas** - so named because all flags are turned on so it’s “lit up” like a Christmas tree
	+ Responses are same as Inverse TCP scan
	+ Do not work against Windows machines
	+ nmap -sX
* **ACK flag probe** - multiple methods
	+ TTL version - if TTL of RST packet < 64, port is open
	+ Window version - if the Window on the RST packet is anything other than 0, port open
	+ Can be used to check filtering. If ACK is sent and no response, stateful firewall present.
	+ nmap -sA (ACK scan)
	+ nmap -sW (Window scan)
* **IDLE Scan** - uses a third party to check if a port is open
	+ Looks at the IPID to see if there is a response
	+ Only works if third party isn’t transmitting data
	+ Sends a request to the third party to check IPID id; then sends a spoofed packet to the target with a return of the third party; sends a request to the third party again to check if IPID increased.
		- IPID increase of 1 indicates port closed
		- IPID increase of 2 indicates port open
		- IPID increase of anything greater indicates the third party was not idle
	+ nmap -sI

Nmap Switches

| **Switch** | **Description** |
| --- | --- |
| -sA | ACK scan |
| -sF | FIN scan |
| -sI | IDLE scan |
| -sL | DNS scan (list scan) |
| -sN | NULL scan |
| -sO | Protocol scan (tests which IP protocols respond) |
| -sP | Ping scan |
| -sR | RPC scan |
| -sS | SYN scan |
| -sT | TCP connect scan |
| -sW | Window scan |
| -sX | XMAS scan |
| -A | OS detection, version detection, script scanning and traceroute |
| -PI | ICMP ping |
| -Po | No ping |
| -PS | SYN ping |
| -PT | TCP ping |
| -oN | Normal output |
| -oX | XML output |
| -T0 through -T2 | Serial scans. T0 is slowest |
| -T3 through -T5 | Parallel scans. T3 is slowest |

* Nmap runs by default at a T3 level
* **Fingerprinting** - another word for port sweeping and enumeration

Hping

* Another powerful ping sweep and port scanning tool
* Also can craft packets
* hping3 -1 IPaddress

| **Switch** | **Description** |
| --- | --- |
| -1 | Sets ICMP mode |
| -2 | Sets UDP mode |
| -8 | Sets scan mode. Expects port range without -p flag |
| -9 | Listen mode. Expects signature (e.g. HTTP) and interface (-I eth0) |
| –flood | Sends packets as fast as possible without showing incoming replies |
| -Q | Collects sequence numbers generated by the host |
| -p | Sets port number |
| -F | Sets the FIN flag |
| -S | Sets the SYN flag |
| -R | Sets the RST flag |
| -P | Sets the PSH flag |
| -A | Sets the ACK flag |
| -U | Sets the URG flag |
| -X | Sets the XMAS scan flags |

Evasion

* To evade IDS, sometimes you need to change the way you scan
* One method is to fragment packets (nmap -f switch)
* **OS Fingerprinting**
	+ **Active** - sending crafted packets to the target
	+ **Passive** - sniffing network traffic for things such as TTL windows, DF flags and ToS fields
* **Spoofing** - can only be used when you don’t expect a response back to your machine
* **Source routing** - specifies the path a packet should take on the network; most systems don’t allow this anymore
* **IP Address Decoy** - sends packets from your IP as well as multiple other decoys to confuse the IDS/Firewall as to where the attack is really coming from
	+ nmap -D RND:10 x.x.x.x
	+ nmap -D decoyIP1,decoyIP2….,sourceIP,…. [target]
* **Proxy** - hides true identity by filtering through another computer. Also can be used for other purposes such as content blocking evasion, etc.
	+ **Proxy chains** - chaining multiple proxies together
		- Proxy Switcher
		- Proxy Workbench
		- ProxyChains
* **Tor** - a specific type of proxy that uses multiple hops to a destination; endpoints are peer computers
* **Anonymizers** - hides identity on HTTP traffic (port 80)

Vulnerability Scanning

* Can be complex or simple tools run against a target to determine vulnerabilities
* Industry standard is Tenable’s Nessus
* Other options include
	+ GFI LanGuard
	+ Qualys
	+ FreeScan - best known for testing websites and applications
	+ OpenVAS - best competitor to Nessus and is free

Enumeration

* Defined as listing the items that are found within a specific target
* Always is active in nature

Windows System Basics

* Everything runs within context of an account
* **Security Context** - user identity and authentication information
* **Security Identifier** (SID) - identifies a user, group or computer account
* **Resource Identifier** (RID) - portion of the SID identifying a specific user, group or computer
* The end of the SID indicates the user number
	+ Example SID: S-1-5-21-3874928736-367528774-1298337465-**500**
	+ **Administrator Account** - SID of 500
	+ **Regular Accounts** - start with a SID of 1000
	+ **Linux Systems** used user IDs (UID) and group IDs (GID). Found in /etc/passwd
* **SAM Database** - file where all local passwords are stored (encrypted)
	+ Stored in C:\Windows\System32\Config
* **Linux Enumeration Commands**
	+ **finger** - info on user and host machine
	+ **rpcinfo and rpcclient** - info on RPC in the environment
	+ **showmount** - displays all shared directories on the machine

Banner Grabbing

* **Active** - sending specially crafted packets and comparing responses to determine OS
* **Passive** - reading error messages, sniffing traffic or looking at page extensions
* Easy way to banner grab is connect via telnet on port (e.g. 80 for web server)
* **Netcat** can also be used to banner grab
	+ nc
* Can be used to get information about OS or specific server info (such as web server, mail server, etc.)

NetBIOS Enumeration

* NetBIOS provides name servicing, connectionless communication and some Session layer stuff
* The browser service in Windows designed to host information about all machines within domain or TCP/IP network segment
* NetBIOS name is a **16-character ASCII string** used to identify devices
* Command on Windows is **nbtstat**
	+ nbtstat (gives your own info)
	+ nbtstat -n (gives local table)
	+ nbtstat -A IPADDRESS (gives remote information)
	+ nbtstat -c (gives cache information)

| **Code** | **Type** | **Meaning** |
| --- | --- | --- |
| <1B> | UNIQUE | Domain master browser |
| <1C> | UNIQUE | Domain controller |
| <1D> | GROUP | Master browser for subnet |
| <00> | UNIQUE | Hostname |
| <00> | GROUP | Domain name |
| <03> | UNIQUE | Service running on system |
| <20> | UNIQUE | Server service running |

* NetBIOS name resolution doesn’t work on IPv6
* **Other Tools**
	+ SuperScan
	+ Hyena
	+ NetBIOS Enumerator
	+ NSAuditor

SNMP Enumeration

* **Management Information Base** (MIB) - database that stores information
* **Object Identifiers** (OID) - identifiers for information stored in MIB
* **SNMP GET** - gets information about the system
* **SNMP SET** - sets information about the system
* **Types of objects**
	+ **Scalar** - single object
	+ **Tabular** - multiple related objects that can be grouped together
* SNMP uses community strings which function as passwords
* There is a read-only and a read-write version
* Default read-only string is **public** and default read-write is **private**
* These are sent in cleartext unless using SNMP v3
* **Tools**
	+ Engineer’s Toolset
	+ SNMPScanner
	+ OpUtils 5
	+ SNScan

Other Enumerations

* **LDAP**
	+ Connects on 389 to a Directory System Agent (DSA)
	+ Returns information such as valid user names, domain information, addresses, telephone numbers, system data, organization structure and other items
	+ **Tools**
		- Softerra
		- JXplorer
		- Lex
		- LDAP Admin Tool
* **NTP**
	+ Runs on UDP 123
	+ Querying can give you list of systems connected to the server (name and IP)
	+ **Tools**
		- NTP Server Scanner
		- AtomSync
		- Can also use Nmap and Wireshark
	+ **Commands** include ntptrace, ntpdc and ntpq
* **SMTP**
	+ VRFY - validates user
	+ EXPN - provides actual delivery address of mailing list and aliases
	+ RCPT TO - defines recipients