03 04 05 Scanning, Enumeration & Vulnerability Analysis

What is scanning?

Scanning is the process of gathering additional details about target using highly complex and aggressive reconnaissance techniques.

The main goal of this module is to learn the following:

- Host discovery
- Scanning for open ports
- Service and version detection
- OS detection

Types of Scanning

- Network scanning
- Port scanning
- Vulnerability scanning

Network Scanning

Network scanning is one of the most important phases in intelligence gathering. During the network scanning process you can gather information about specific IP address that can be accessed over internet, the OS running on target, system architecture and services running on each computer. In addition this technique also gathers details about the network and their individual host systems.

Please note that network scanning is illegal in many countries and should not be performed outside the labs without prior authorization.

Network scan or network sweeping

In order to deal with large volume of hosts, or to otherwise try to conserve network traffic, we can attempt to probe these machines using network sweeping techniques. Sweeping indicates it is a network wide action. We do this using ICMP ping requests.

Machines that block or filter ICMP requests may seem down to ping sweep, so it is not a definitive way to identify which machines are up or down.

ICMP stands for Internet Control Message Protocol

List of network scanners

- fping
- netdiscover
- arping
- Angry IP scanner
- Advanced IP scanner

Port Scanning

The port scanning techniques are designed to identify the open ports on a targeted server or host. This is often used by administrators to verify security policiess of their networks and by attackers to identify running services on a host with the intent of compromising it.

Tool used :

NMAP

List of common ports

FTP (File Transfer Protocol)	20/21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name Server)	53
DHCP (Dynamic Host Configuration Protocol)	67/68
Postgresql	5432
HTTP (Hyper Text Transfer Protocol)	80
POP (Post Office Protocol)	110
NTP (Network Time Protocol)	123

NetBIOS	139
IMAP (Internet Message Access Protocol)	143
SNMP (Simple Network Management Protocol)	162
IRC (Internet Relay Chat)	6667
SMB (Server Message Block)	445
HTTPS (Http-secure)	443
MSSQL(Microsoft SQL default Port)	1433
Oracle	1521
MySQL	3306
RDP (Remote Desktop Protocol)	3389

Nmap (network mapping utility)

Nmap is a security scanner used to discover hosts and services on a computer network. To accomplish this goal nmap sends specially crafted packets to the target host and analyzes the responses.

Typical uses:

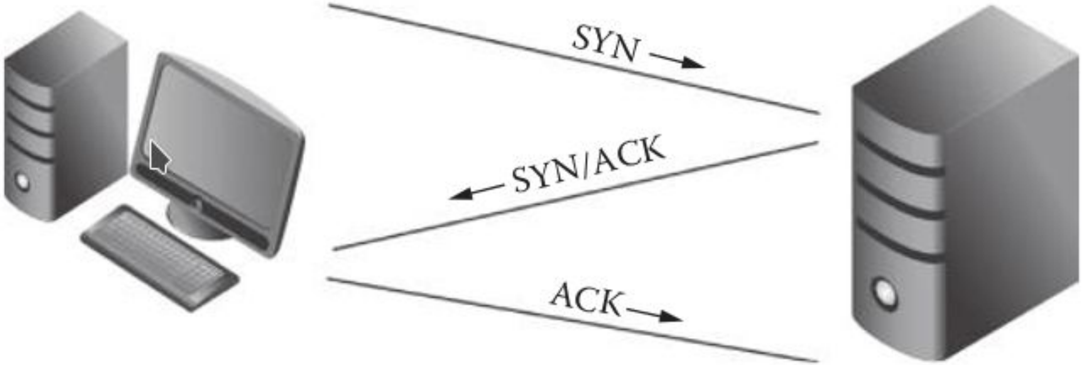
- Auditing the security of device or firewall by identifying network connections which can me made to, or through it.
- Identifying open ports on target host in preparation for auditing.
- Generating traffic to hosts on a network, response analysis and response time management

Understanding the TCP 3 way handshake

The TCP was made for reliable communication. Before understanding how port scanning works, we need to understand how TCP 3 way handshake works.

- The first host SYN packet to second host
- The second host responds with SYN/ACK packet; it indicates the packet was received
- The first host completes connection by sending an acknowledgement ACK packet

TCP 3 way handshake



TCP flags

- SYN (Synchronize) : Initiates a connection between hosts
- ACK (Acknowledgement) : Acknowledges the receipt of packet
- FIN (Finish) : There will be no more transmissions
- URG (Urgent) : Data contained in packet should be processed immediately
- PSH (Push) : Sends all buffered data immediately
- RST (Reset) : Resets a connection

Port Status types

With nmap you would see one of four port status types

- Open : Means that port is accessible and application is listening to it
- Closed : Means that port is inaccessible and no application is listening to it
- Filtered : Means that nmap is not able to figure it out if port is open or closed, as the packets are being filtered, means machine is behind firewall probably
- Unfiltered : Means that ports are accessible by nmap but it is not possible to figure out if they are open or closed

Scanning Techniques

- ICMP Echo scan
- TCP Connect scan/ Full open scan
- TCP Syn scan/ Half open scan
- Null, XMAS and FIN scans
- UDP scan
- Specific ports
- Service Version Detection & OS fingerprinting, both together
- Aggressive Scan
- IDLE scan

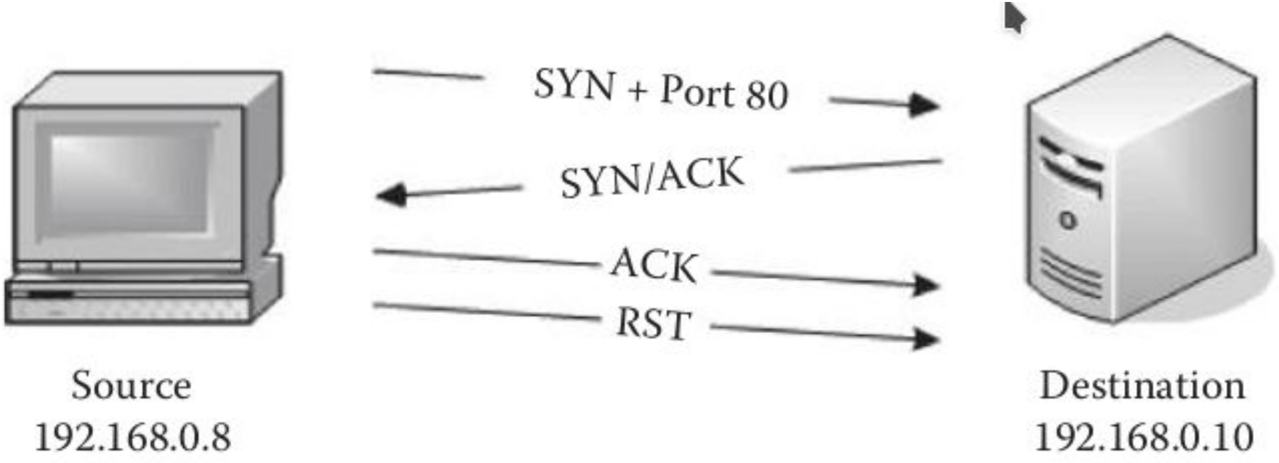
ICMP Echo scan

This is not really a port scanning technique, since ICMP does not have port abstraction. It is useful to determine which hosts in a network are up by pinging them. Attackers send ICMP probe to all hosts in subnet, the live systems will send ICMP echo reply message to source of ICMP echo probe.

Mostly used in Unix/Linux and BSD based machines and not Windows based network because TCP/IP stack implementations.

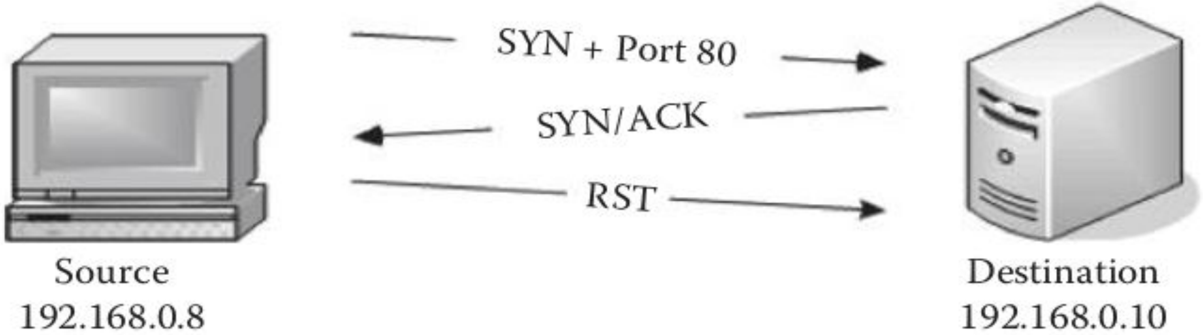
TCP Connect scan/ Full open scan

It detects when a port is open by completing the 3 way handshake. It establishes a full connection and tears it down by sending a RST packet



TCP Syn scan/ Half Open scan

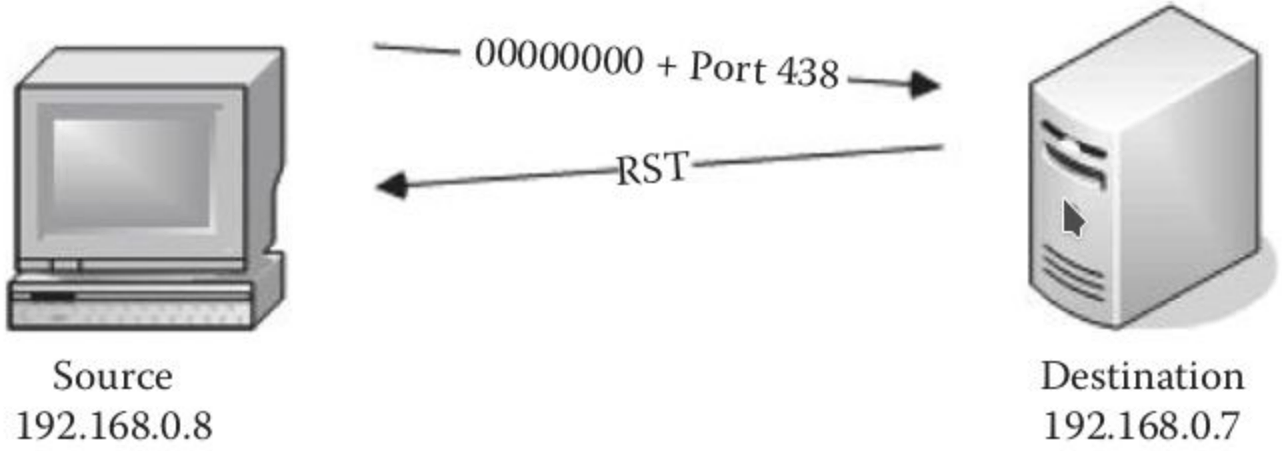
This scan runs default against a target machine if scan type is not provided. It works the same way as connect scan but here 3 way handshake will not be completed. With early and primitive firewalls this method would bypass firewall logging, as logging was limited to completed TCP sessions. This is no longer true with modern firewalls and term stealth is misleading.



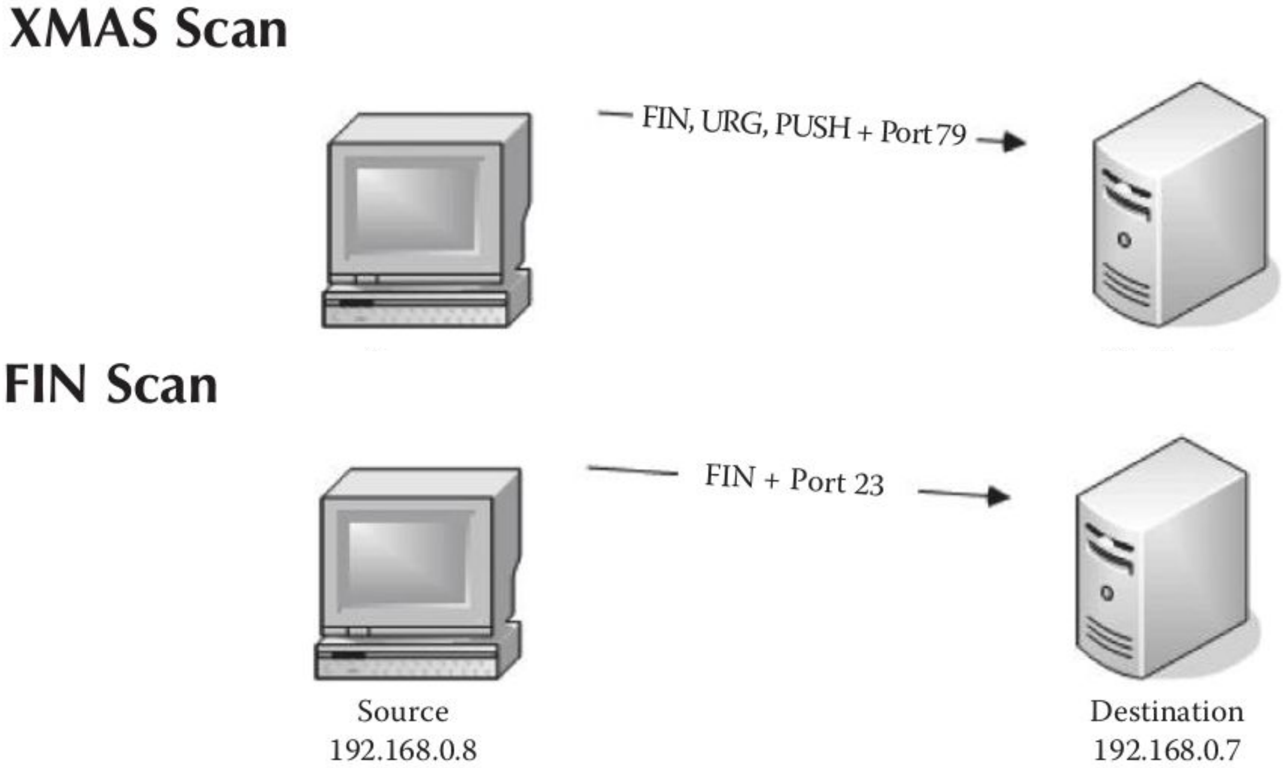
Null, XMAS and FIN scans

These 3 are similar to each other. The advantage is many a times they get past firewalls and IDS. All three of these don't work against Windows OS.

NULL Scan



XMAS and FIN scan



UDP Scan

UDP is stateless and doesn't involve 3 way handshake. An empty UDP packet is sent to specific port. If UDP port is open, no reply is sent back from target machine and If UDP port is closed, ICMP port unreachable should be sent back from target machine

It is often unreliable as firewalls and routers may drop icmp packets and may lead to false positives showing all UDP ports open

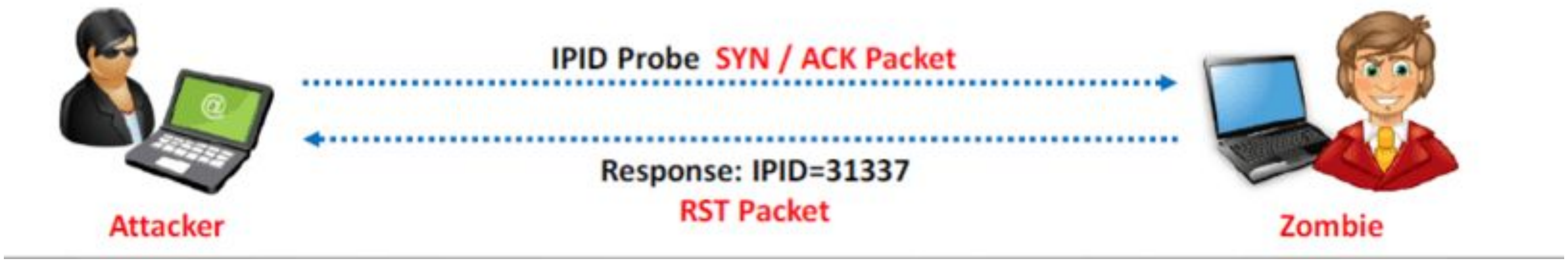
People often forget to scan for UDP services and stick only to TCP scanning, thereby seeing only half the equation

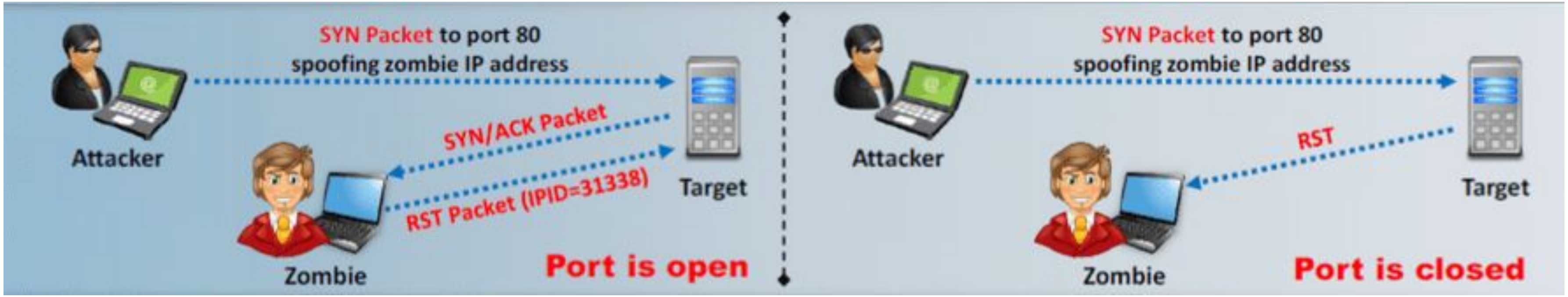
IDLE Scan

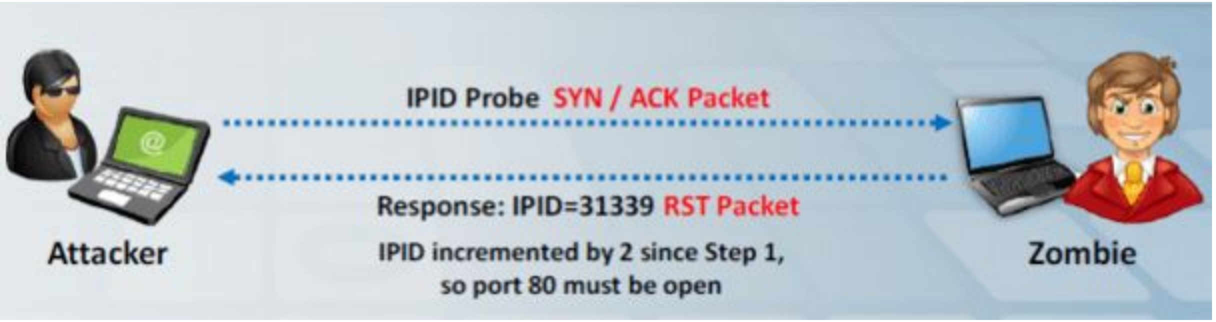
It is a very effective and stealthy scanning technique. The idea behind idle scan is to introduce a zombie to scan another host. This technique is stealthy because the victim would receive packet from zombie host, thus not able to figure out where the scan originated.

Prerequisites

- Finding good candidate whose IP ID sequence is incremental and recording its IP ID
- The host should be idle on the network


IPID Probe SYN / ACK Packet
Response: IPID=31337
RST Packet
Attacker
Zombie


SYN Packet to port 80
spoofing zombie IP address
SYN/ACK Packet
RST Packet (IPID=31338)
Attacker
Zombie
Target
Port is open
SYN Packet to port 80
spoofing zombie IP address
RST
Attacker
Zombie
Target
Port is closed


IPID Probe SYN / ACK Packet
Response: IPID=31339 RST Packet
IPID incremented by 2 since Step 1,
so port 80 must be open
Attacker
Zombie

Enumeration

In the enumeration phase, attacker creates active connections to systems and performs direct queries to gain more information about the target.

Attackers use extracted information to identify system attack points and perform password attacks to go gain unauthorized access to information system resources.

NOTE : Enumeration techniques are conducted in an internal environment

Information we can gather in enumeration phase

- Network resources and share
- Users and groups
- Routing tables
- Machine names
- Applications and banners
- SMTP and DNS details

- NETBIOS enumeration
- SMB enumeration
  - Null session enumeration
  - Nmap SMB NSE scripts
- SSH enumeration

Vulnerability scanning

Vulnerability scanning identifies vulnerabilities and weaknesses of a system and networking order to determine how a system can be exploited.

List of Vulnerability Scanners

- Nessus by Tenable security
- QualysGuard
- OpenVAS
- SAINT vulnerability scanner
- Nexpose

and many more.....

Importance of Scanning

Scanning will give you almost exact outline of target workspace. It is really helpful in hacking attempts on networks, servers and standalone PC’s. Scanning will give the blueprint of the networks and devices, how they are connected to each other and details about OS and service versions etc.