NETWORK SCANNING

presented by,

A.THILAGAVATHI
THE KAVERY ENGINEERING COLLEGE
BE.COMPUTER SCIENCE ENGINEERING

Introduction

- Scanning can be compared to a thief checking all the doors and windows of a house he wants to break into.
- Scanning- The art of detecting which systems are alive and reachable via the internet and what services they offer, using techniques such as *ping sweeps*, *port scans* and *operating system identification*, is called *scanning*.

The kind of information collected here has to do with the following:

1) TCP/UDP services running on each system identified.

2) System architecture (Sparc, Alpha, x86)

3) Specific IP address of systems reachable via the internet.

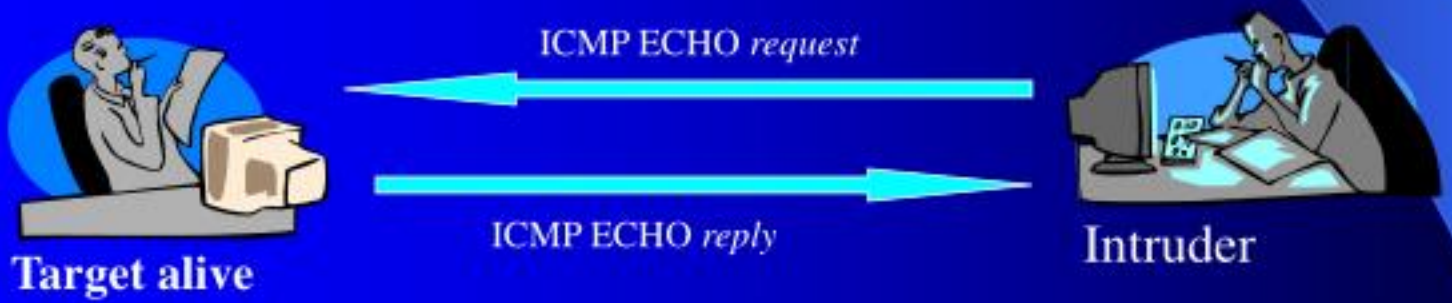
4) Operating System type.

Ping Sweeps

- ICMP Sweeps (ICMP ECHO requests)
- Broadcast ICMP
- Non Echo ICMP
- TCP Sweeps
- UDP Sweeps

PING SWEEPS

ICMP SWEEPS

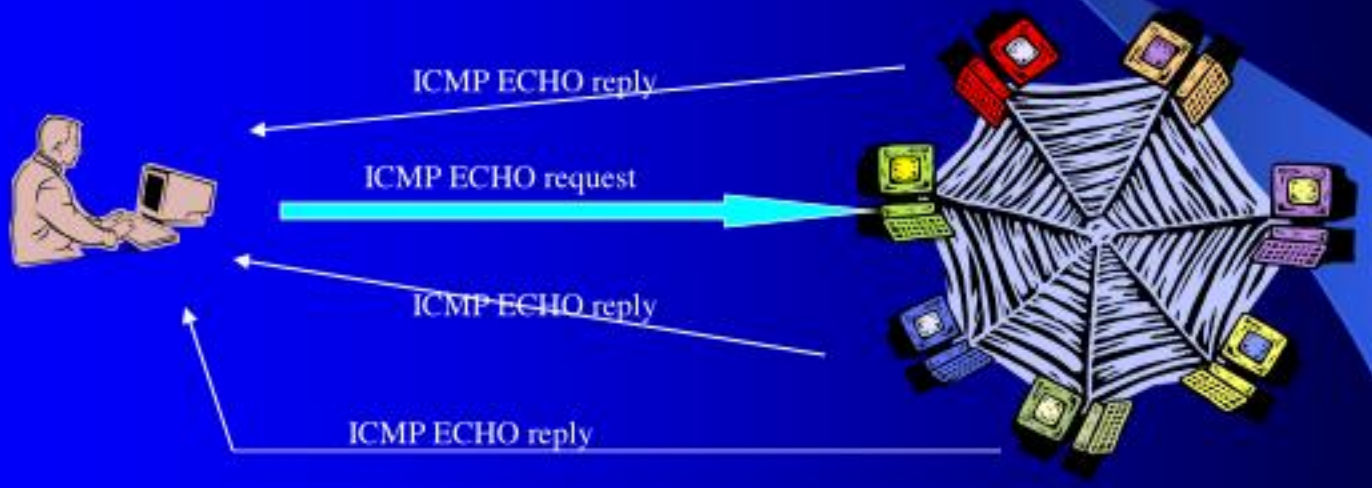


Querying multiple hosts – Ping sweep is fairly slow

Examples UNIX – *fping and gping*

WINDOWS - *Pinger*

Broadcast ICMP



Can Distinguish between UNIX and WINDOWS machine

UNIX machine answers to requests directed to the network address.

WINDOWS machine will ignore it.

PING SWEEPS

NON – ECHO ICMP

Example ICMP Type 13 – (Time Stamp)

- Originate Time Stamp
  - The time the sender last touched the message before sending
- Receive Time Stamp
  - The echoer first touched it on receipt.
- Transmit Time Stamp
  - The echoer last touched on sending it.

PING Sweeps

TCP Sweeps

When will a RESET be sent?

When RFC does not appear correct while appearing.

RFC = (Destination (IP + port number) & Source(IP & port number))

PING Sweeps

Depends on ICMP PORT UNREACHABLE message.

Unreliable because

- Routers can drop UDP packets
- UDP services may not respond when correctly probed
- Firewalls are configured to drop UDP
- Relies on fact that non-active UDP port will respond

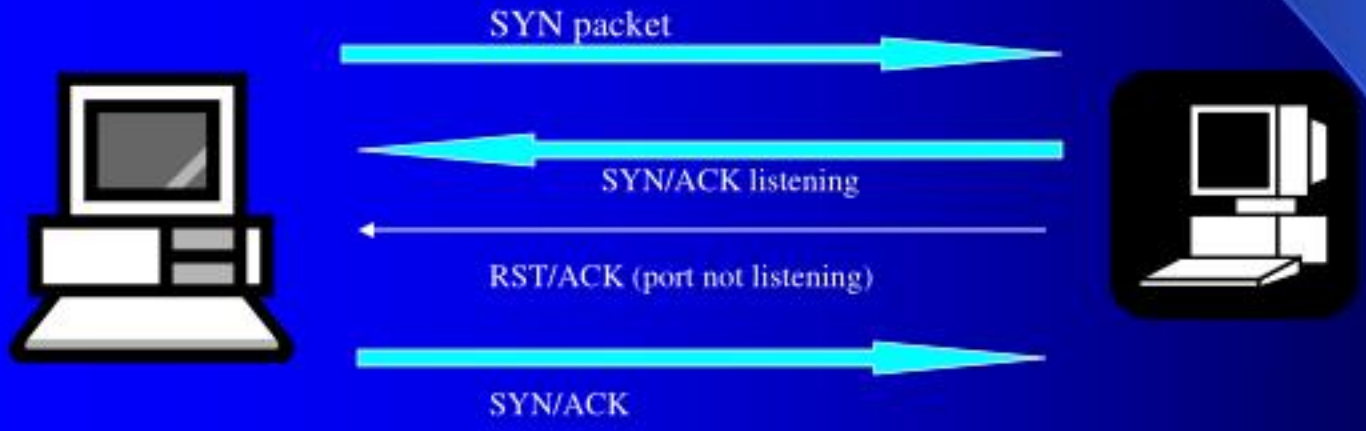
PORT SCANNING

Types:

- TCP Connect() Scan
- TCP SYN Scan(Half open scanning)
- Stealth Scan
- Explicit Stealth Mapping Techniques
  SYN/ACL , FIN, XMAS and NULL
- Inverse Mapping
  Reset Scans, Domain Query Answers
- Proxy Scanning / FTP Bounce Scanning
- TCP Reverse Ident Scanning

Port Scanning Types

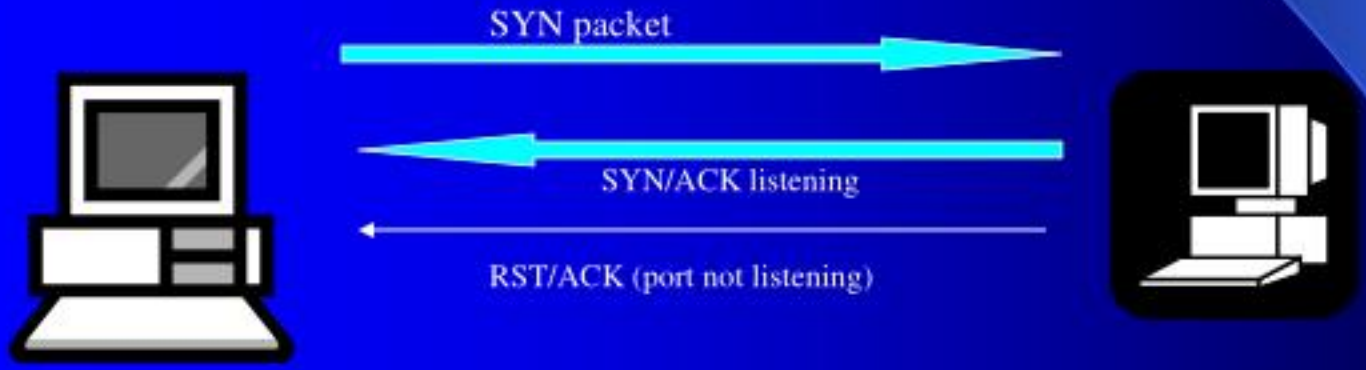
- TCP Connect() Scan



A connection is terminated after the full length connection establishment process has been completed

PORT SCANNING

- TCP SYN Scan (half open scanning)



We immediately tear down the connection by sending a RESET

Port Scanning

Stealth Scan

A scanning technique family doing the following

- Pass through filtering rules.
- Not to be logged by the targeted system logging mechanism
- Try to hide themselves at the usual site / network traffic.

The frequently used stealth mapping techniques are.

- SYN/ACK scan
- FIN scans
- XMAS scans
- NULL scans

PORT Scanning

Techniques:

- Random Port scan
- Slow Scan
- Fragmentation Scanning
- Decoy
- Coordinated Scans

PORT Scanning

"Random" Port Scan

Randomizing the sequence of ports probed may prevent detection.

Slow Scan

Some hackers are very patient and can use network scanners that spread out the scan over a long period of time. The scan rate can be, for example, as low as 2 packets per day per target site.

Fragmentation scanning

In case of TCP the 8 octets of data (minimum fragment size) are enough to contain the source and destination port numbers. This will force the TCP flags field into the second fragment.

Decoy

Some network scanners include options for Decoys or spoofed address in their attacks.

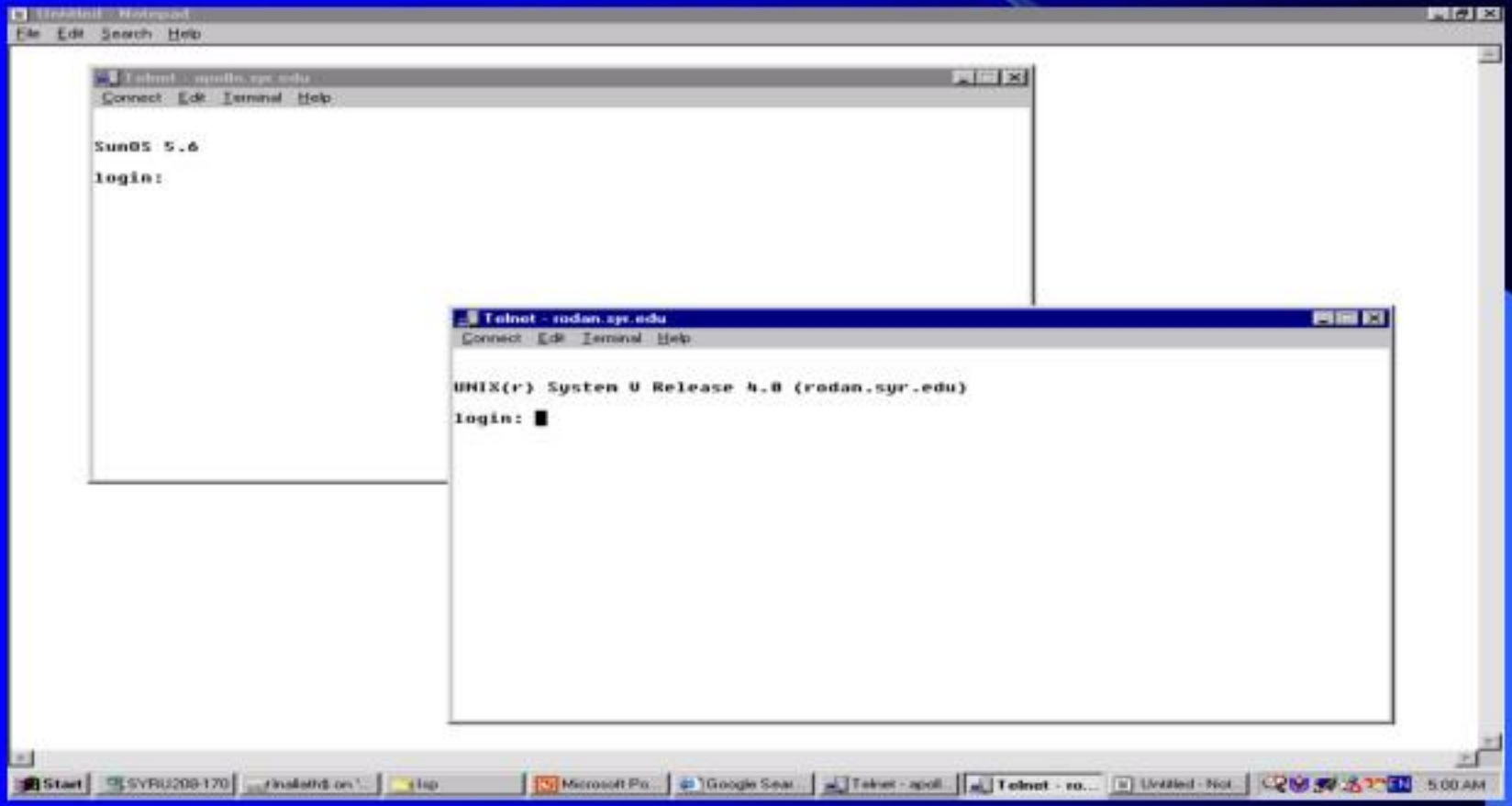
Coordinated Scans

If multiple IPs probe a target network, each one probes a certain service on a certain machine in a different time period, and therefore it would be nearly impossible to detect these scans.

Operating System Detection

- Banner Grabbing
- DNS HINFO Record
- TCP/IP Stack Fingerprinting

Operating System Detection



Operating System Detection

- DNS HINFO Record

The host information record is a pair of strings identifying the host's hardware type and the operating system

www IN HINFO "Sparc Ultra 5" "Solaris 2.6"

One of the oldest technique

Operating System Detection

- TCP/IP Finger Printing

The ideas to send specific TCP packets to the target IP and observe the response which will be unique to certain group or individual operations.

Types of probes used to determine the OS type

The FIN Probe, The Bogus Flag Probe, TCP initial sequence number sampling, Don't Fragment bit, TCP initial window, ACK value, ICMP error Message Quenching, ICMP message quoting, ICMP error message Echoing Integrity, Type of service, fragmentation handling, TCP options

Firewalking

- Gather information about a remote network protected by a firewall
- Purpose
  - Mapping open ports on a firewall
  - Mapping a network behind a firewall
    - If the firewall's policy is to drop ICMP ECHO Request/Reply this technique is very effective.

How does Firewalking work?

- It uses a traceroute-like packet filtering to determine whether or not a particular packet can pass through a packet-filtering device.

- Traceroute is dependent on IP layer(TTL field), any transport protocol can be used the same way(TCP, UDP, and ICMP).

What Firewalking needs?

- The IP address of the last known gateway before the firewall takes place.
  - Serves as WAYPOINT
- The IP address of a host located behind the firewall.
  - Used as a destination to direct packet flow

Getting the Waypoint

- If we try to traceroute the machine behind a firewall and get blocked by an ACL filter that prohibits the probe, the last gateway which responded(the firewall itself can be determined)
- Firewall becomes the waypoint.

Getting the Destination

- Traceroute the same machine with a different traceroute-probe using a different transport protocol.
- If we get a response
  - That particular traffic is allowed by the firewall
  - We know a host behind the firewall.
- If we are continuously blocked, then this kind of traffic is blocked.
- Sending packets to every host behind the packet-filtering device can generate an accurate map of a network's topology.

How to identify/avoid threats?

- Long-standing rule for Unix System administrators to turn off any services that aren't in use
- For personal workstations!
  - Hackers have access to utilities to scan the servers but so do you!.
  - Hackers look in for open ports. So we can our servers first and know what the hackers will see and close any ports that shouldn't be open.

Some tools to help us

- Nmap
  - It is a utility that scans a particular server and informs us which ports are open.
- Ethereal
  - It is a utility that will scan the network and help us decode what is going on.
  - We can watch the network traffice and find out if hackers can see anything that will help them break into our systems.

Resources

- www.onlamp.com
- www.nfr.net
- www.sys-security.com
- www.insecure.org
- www.ietf.org/rfc
- www.kyuzz.org/antirez
- www.netsys.com

Conclusion

- We have reviewed some scanning types with hard-to-detect or even non-detectable scanning techniques.
- Understanding the importance of detecting these scan can prevent, in some case, intrusion.
- Detection can be partly achieved by IDS.
- Second part is maintenance of the system, getting info on new and wicked scanning techniques, understanding their signatures, and implementing new filter to detect them
- Tighten your security to the maximum.
- Identifying these probing attempts will give you an indication that an upcoming attack might be on the way!

THANK YOU