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

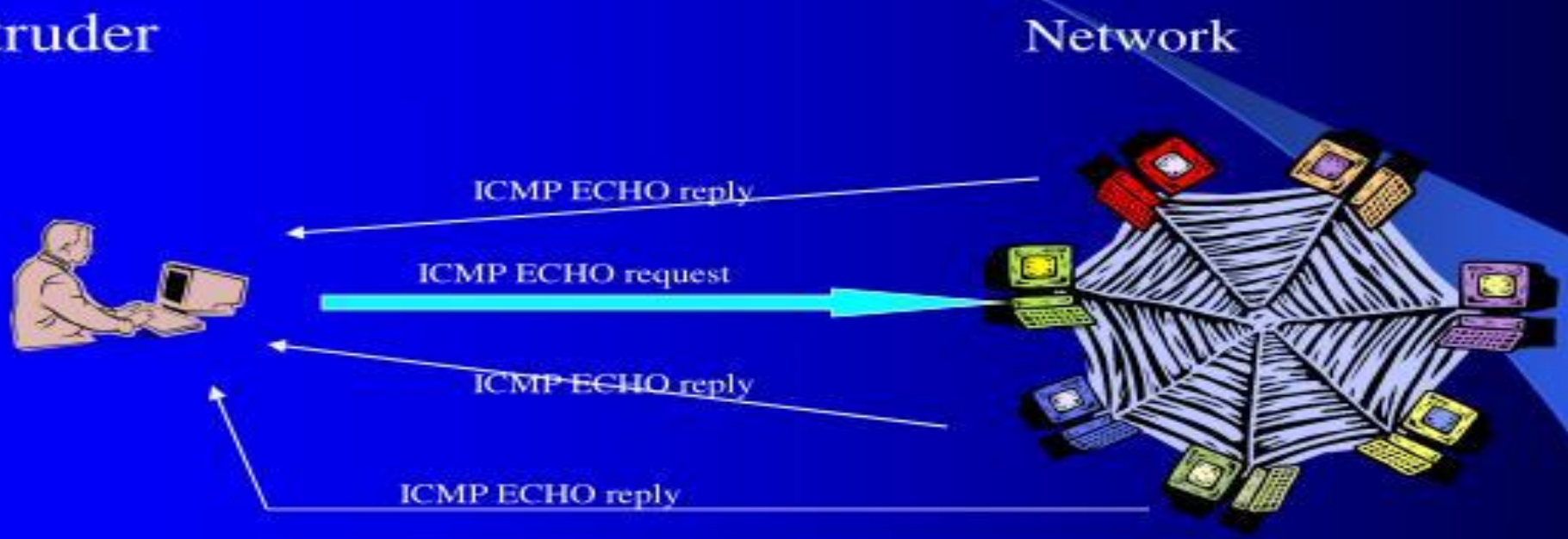
ICMP SWEEPS

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.

UDP data gram

ICMP PORT UNREACHABLE

Target System

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

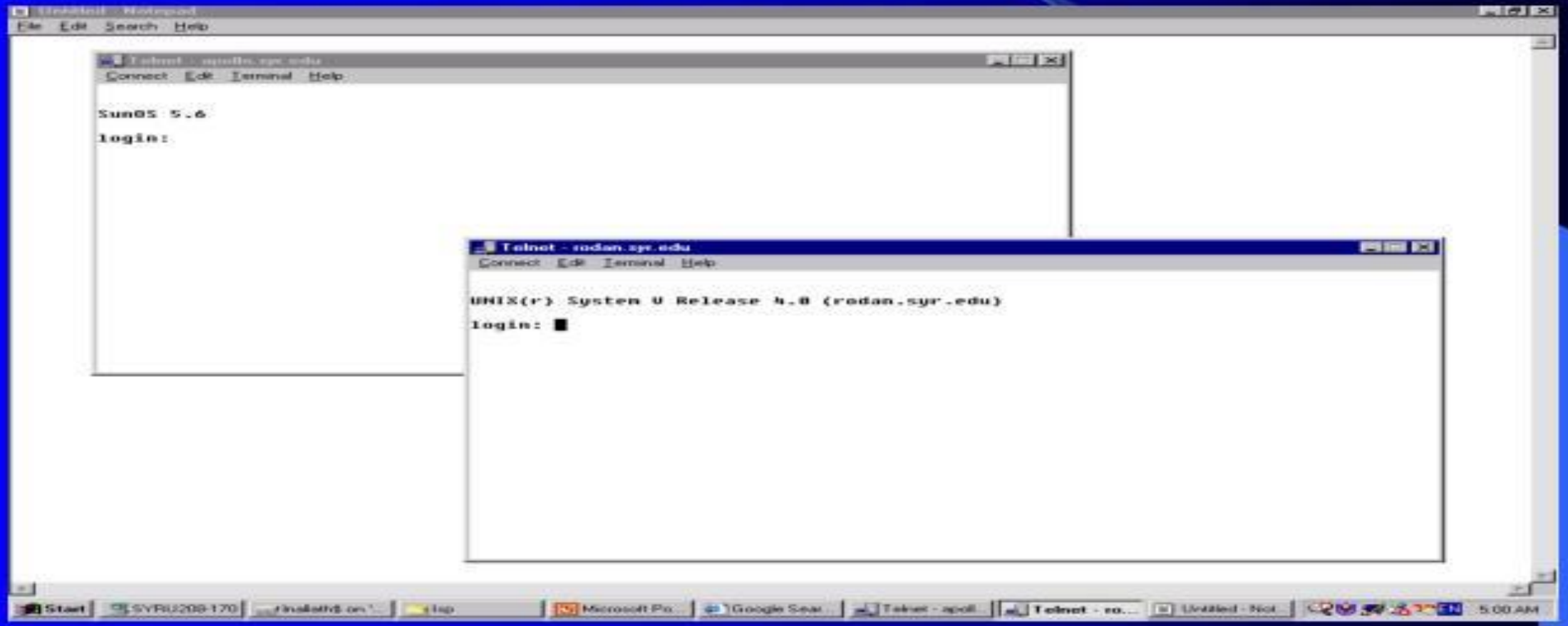
Types:

- 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

Operating System Detection

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

Operating System Detection



SOURCE CODE

```
Import pyfiglet

import sys

import socket

from datetime import datetime
```

```
Ascii_banner = pyfiglet.figlet_format("PORT SCANNER")

print(ascii_banner)


# Defining a target

if len(sys.argv) == 2:
```

```
# translate hostname to IPv4
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Invalid amount of Argument")
# Add Banner
```

```
Print(“-” * 50)

print(“Scanning Target: “ + target)

print(“Scanning started at:” + str(datetime.now()))

print(“-” * 50)
```

Try:

```
    # will scan ports between 1 to 65,535

    for port in range(1,65535):

        s = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)

        socket.setdefaulttimeout(1)
```

```
# returns an error indicator
        result = s.connect_ex((target,port))
        if result ==0:
            print("Port {} is open".format(port))
        s.close()
```

```
Except KeyboardInterrupt:

    print("\n Exiting Program !!!!")

    sys.exit()
```

```
Except socket.gaierror:

    print("\n Hostname Could Not Be Resolved !!!!")

    sys.exit()

except socket.error:

    print("\ Server not responding !!!!")

    sys.exit()
```

Output


PORT SCANNER
Scanning Target: 104.31.85.168
Scanning started at:2020-04-08 17:20:29.777650
Port 80 is open
Port 443 is open

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.

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