TOPIC 8 : PORT SCANNERS AND FIREWALLS

MD ARIFUR RAHMAN

WHAT IS PORT SCANNING

- In TCP/IP, every (network) service on a machine is assigned a port number.
- The process of examining an open port on a computer to determine what services are running on a network.

RELATION WITH OSI AND TCP/UDP

- The Ports are defined in the 5th layer of the OSI model.
- Session layer establishes the Conversation between the source and destination.
- Port numbers are actively used by TCP/UDP for different applications.
- TCP/UDP identify the sender or receiver using unique identifiers called port numbers.

OSI MODEL

- Open Systems Interconnection model
- Established by ISO in 1947
- Seven separate but related layer
- Model for understanding and designing a network

Layer	Name	Encapsulation Units	Devices or Components
7	Application	data	PC
6	Presentation	data	
5	Session	data	
4	Transport	segments	
3	Network	packets	router
2	Data Link	frames	bridge, switch, NIC
1	Physical	bits	repeater, hub, transciever

TCP/IP PROTOCOL SUITE

- TCP/IP protocol suite was developed prior to the OSI model
- The protocol suite which is used for the communication between computer networks
- Most widely used and available protocol suite.
- TCP usually specify a source and destination port number.

OSI COMPARISION WITH TCP/IP PROTOCOL

OSI	OSI Layer Name	TCP/IP	TCP/IP Layer Name	Encapsulation Units	TCP/IP Protocols
7	Application	4	Application	data	FTP, HTTP, POP3, IMAP, telnet, SMTP, DNS, TFTP
6	Presentation			data	
5	Session			data	
4	Transport	3	Transport	segments	TCP, UDP
3	Network	2	Internet	packets	IP(ARP,RARP,ICMP)
2	Data Link	1	Network Access	frames	
1	Physical			bits	

SOME WELL KNOWN PORTS

Port Number	TCP/UDP	Protocol
20	TCP	FTP-Data Connection
21	TCP	FTP-Control Connection
23	TCP	TELNET
25	TCP	SMTP
53	TCP/UDP	DNS
67	UDP	DHCP- Destination Port
68	UDP	DHCP- Client Port
80	TCP	HTTP
110	TCP	POP3

PURPOSE OF PORT SCANNING

- To probe a server or host for open ports
- Find services running on computer
- Find known/ Common vulnerabilities

PORT NUMBER REGISTRY

Port numbers are assigned in various ways, based on three ranges:

- 65535 ports in total
- System Ports (0-1023)
- User Ports (1024-49151)
- Dynamic and/or Private Ports (49152-65535)

PORT CATEGORIES

A scan on a port is usually generalized into one of three categories:

- Open or Accepted: The receiving host receives a packet and reply with ACK.
- Closed or Denied or Not Listening: The receiving host receives a packet and reply with RST.
- Filtered, Dropped or Blocked: There was no reply from the host.

PORT VULNERABLITIES

The most common port numbers are commonly associated with vulnerable services, on a given host.

- Open ports present two vulnerabilities
- Filtered ports do not tend to present vulnerabilities.

TYPES OF PORT SCANNER

1. TCP scanning
2. SYN scanning
3. UDP scanning
4. FIN scanning
5. NULL scan
6. XMAS scan

USING PORT-SCANNING TOOLS

- Hundreds of port-scanning tools are available for both hackers and security testers.
- Not all are accurate, so using more than one port-scanning tool is recommended for security purpose.

SOME WELL KNOWN PORT SCANNER TOOLS

- Nmap
- Unicornscan
- Ping Sweeps
- Fping
- Hping

NMAP

- Network mapper is widely used port scanner.
- It adds new features constantly.
- Nmap is a free and open source tool for network security.
- Nmap 193.145.85.201

  scans every port on the computer with this IP address.

ADVANTAGES OF NMAP

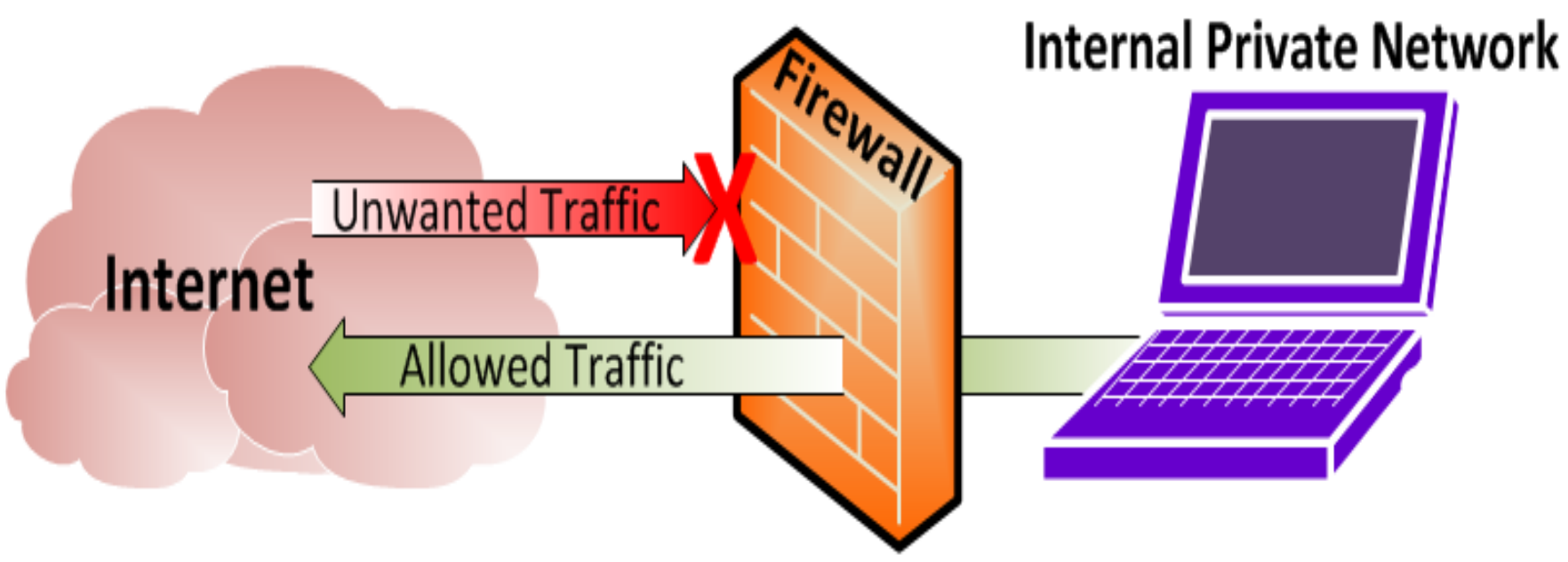
- Easy
- Flexible
- Portable
- Powerful

FIREWALL

- Network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- Imposes restrictions on network services only authorized traffic is allowed.
- A firewall can be installed as a software program on a single computer.
- Three reasons to deploy firewall : ACL, NAT, VPN

FIREWALL FUNCTIONS

- A firewall could be deployed to block all incoming traffic and permit all outgoing traffic.



Source : https://www.howtogeek.com/144269/htg-explains-what-firewalls-actually-do/

CLASSIFICATION OF FIREWALLS

- Packet filters
- Circuit Level gateways
- Application gateways(proxies)
- Stateful inspection firewalls

DEEP PACKET INSPECTION

- Deep packet inspection (DPI) is an advanced method of packet filtering.
- DPI has been used in various forms since the late 1990s.
- Useful to check whether data is in correct format or malware free.
- DPI represents a process in the network technology, data packets to monitor and filter.

DISADVANTGES OF DPI

DPI has at least three significant limitations

- Create new vulnerabilities
- Adds complexity
- Reduce computer speed

Live Demo

Block or Permit a port using ACL with Packet Tracer

REFERENCES

- https://networkengineering.stackexchange.com/questions/16996/what-layer-of-the-osi-model-deals-with-ports
- https://learningnetwork.cisco.com/thread/85693
- https://hackertarget.com/port-scanner/
- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
- Behrouz A Forouzan, "Data Communications and Networking", 4th edition, The MeCraw-Hill Companies.
- https://nmap.org/
- http://resources.infosecinstitute.com/nmap/
- http://resources.infosecinstitute.com/port-scanners/

REFERENCES

- https://www.tunnelsup.com/what-is-a-firewall/
- https://www.howtogeek.com/144269/htg-explains-what-firewalls-actually-do/
- http://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls
- http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
- http://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html
- E. Eugene Schultz, 83-10-41, Types of Firewalls.pdf
- https://advox.globalvoices.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/
- http://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI