Network Security

NAVNEET
Scientist `C`
CERT-In, DIT

Overview

1. **Network security**

1.1 Layered Approach

2. **Network security Threats/Attacks**

3. **Network Vulnerabilities**

4. **Network Security Assessment**

5. **Network configuration Flaws**

6. **Case study of windows Firewalls**

Network & Security

- Network Security is the need to protect one or more aspects of network's operation and permitted use. Security requirements may be Local or Global in their scope, depending upon the network's or internetwork's purpose of design and deployment.

It is impossible to think about a Computer Network without IT Security and Vice Versa.

Vulnerable Organization

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Major Network Security Equipment

1. Routers & Managed Switches
2. Link Load Balancer
3. Firewall
4. VPN
5. Intrusion Prevention System
6. Antivirus and Antimalware Solution
7. Anti spam and email Security
8. Web Security
9. Filters
10. Log Management & Analysis
11. Network Access Control
12. Management System
13. Patch Management
14. Backup Solutions
15. Endpoint Security

Firewall

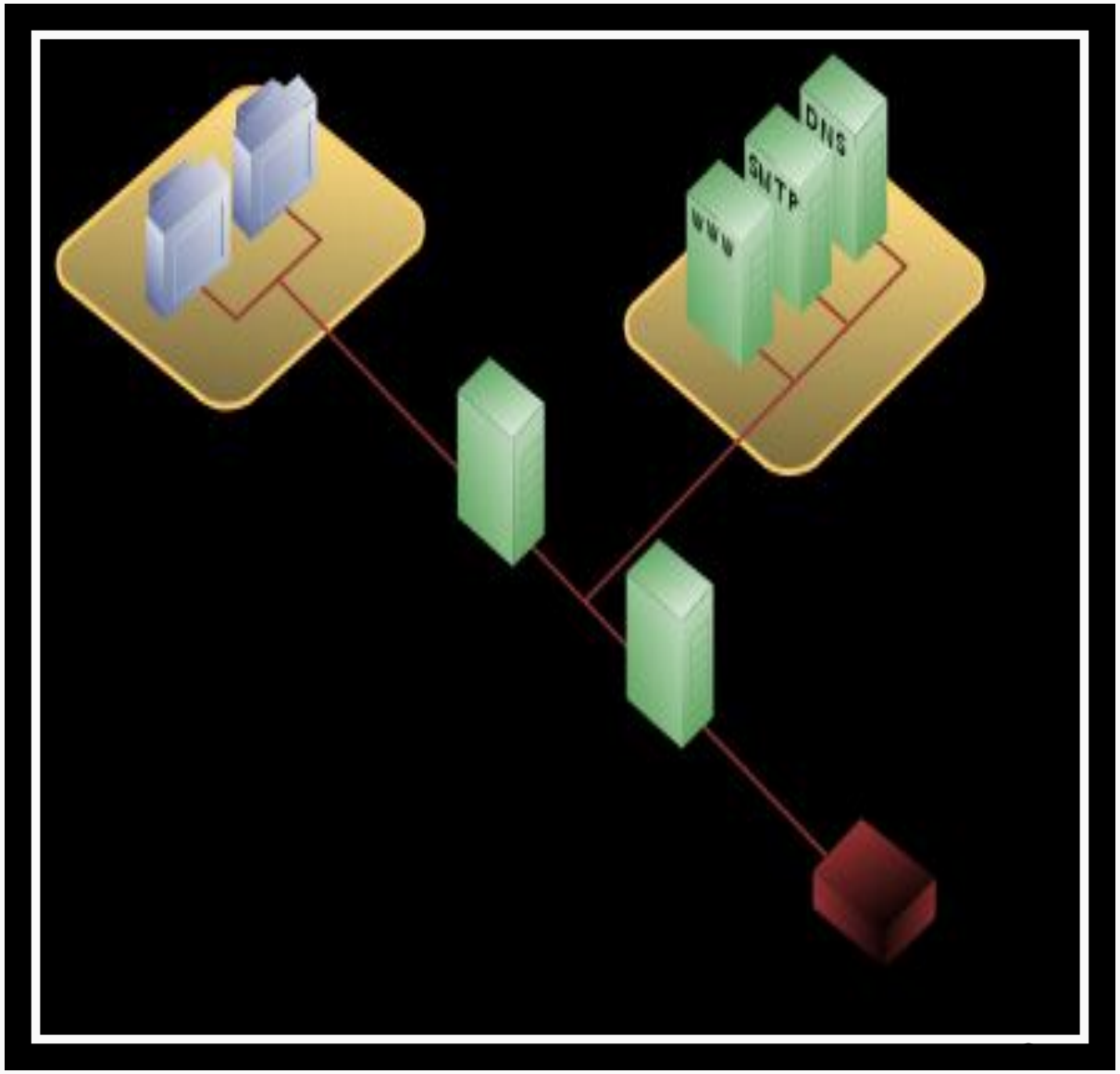
- A firewall is a hardware or software system that prevents unauthorized access to or from a network.
- Implemented in both hardware and software, or a combination of both.
- Sits between two networks
  - Used to protect one network from the other
  - Places a bottleneck between the networks
    - All communications must pass through the bottleneck – this gives us a single point of control

Firewall Functions

- Filtering
- Inspection
- Detection
- Logging
- Alerting
- Allow Address Reuse

Securing DMZ

- Single/ Dual Firewalls is used in creating DMZ



Types of Firewall

- NETWORK LAYER FIREWALLS
- APPLICATION LAYER FIREWALLS (Proxy firewall)
- UNIFIED THREAT MANAGEMENT
- WEB APPLICATION FIREWALL

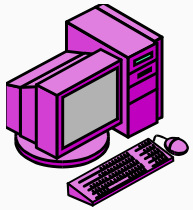
Network layer firewall

- Not allowing packets to pass through the firewall unless they match the established filter rule set.
- Firewall administrator may define the rules
- Filtering rules is based on source and destination address and ports.
- Operates very fast.
- Network layer firewalls generally fall into two sub-categories, stateful and non-stateful.

Stateful Firewall

- State of Connection: Open or Closed
  - State: Order of packet within a dialog
  - Often simply whether the packet is part of an open connection

- Stateful Firewall Operation
  - For TCP, record two IP addresses and port numbers in state table as OK (open)
  - By default, permit connections from internal clients (on trusted network) to external servers (on untrusted network)
    - This default behavior can be changed with an ACL
  - Accept future packets between these hosts and ports with little or no inspection



Internal
Client PC
60.55.33.12

1.
TCP SYN Segment
From: 60.55.33.12:62600
To: 123.80.5.34:80

Note: Outgoing Connections Allowed By Default

2.
Establish Connection

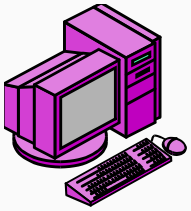
Stateful
Firewall

3.
TCP SYN Segment
From: 60.55.33.12:62600
To: 123.80.5.34:80

External
Webserver
123.80.5.34

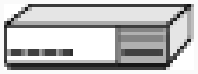
Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK



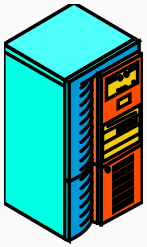
Internal
Client PC
60.55.33.12

6.
TCP SYN/ACK Segment
From: 123.80.5.34:80
To: 60.55.33.12:62600



Stateful
Firewall

4.
TCP SYN/ACK Segment
From: 123.80.5.34:80
To: 60.55.33.12:62600



External
Webserver
123.80.5.34

5.
Check Connection
OK

Connection Table

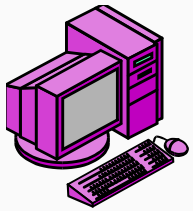
Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

- Stateful Firewall Operation
  - For UDP, also record two IP addresses in port numbers in the state table

Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	1.8.33.4	69	OK

Port-Switching Applications with Stateful Firewalls



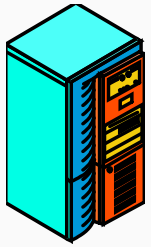
Internal
Client PC
60.55.33.12

1.
TCP SYN Segment
From: 60.55.33.12:62600
To: 123.80.5.34:21

2.
To Establish
Connection

Stateful
Firewall

3.
TCP SYN Segment
From: 60.55.33.12:62600
To: 123.80.5.34:21



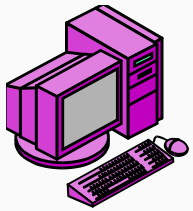
External
FTP Server
123.80.5.34

State Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	21	OK

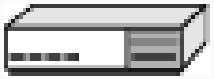
Step 2 →

Port-Switching Applications with Stateful Firewalls



Internal
Client PC
60.55.33.12

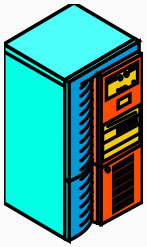
6.
TCP SYN/ACK Segment
From: 123.80.5.34:21
To: 60.55.33.12:62600
Use Ports 20
and 55336 for
Data Transfers



Stateful
Firewall

5.
To Allow,
Establish
Second
Connection

4.
TCP SYN/ACK Segment
From: 123.80.5.34:21
To: 60.55.33.12:62600
Use Ports 20
and 55336 for
Data Transfers



External
FTP
Server
123.80.5.34

State Table

	Type	Internal IP	Internal Port	External IP	External Port	Status
Step 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK
Step 5 →	TCP	60.55.33.12	55336	123.80.5.34	20	OK

Stateful Inspection Firewalls

- Stateful Inspection Access Control Lists (ACLs)
  - Primary allow or deny applications
  - Simple because probing attacks that are not part of conversations do not need specific rules because they are dropped automatically
  - In integrated firewalls, ACL rules can specify that messages using a particular application protocol or server be authenticated or passed to an application firewall for inspection

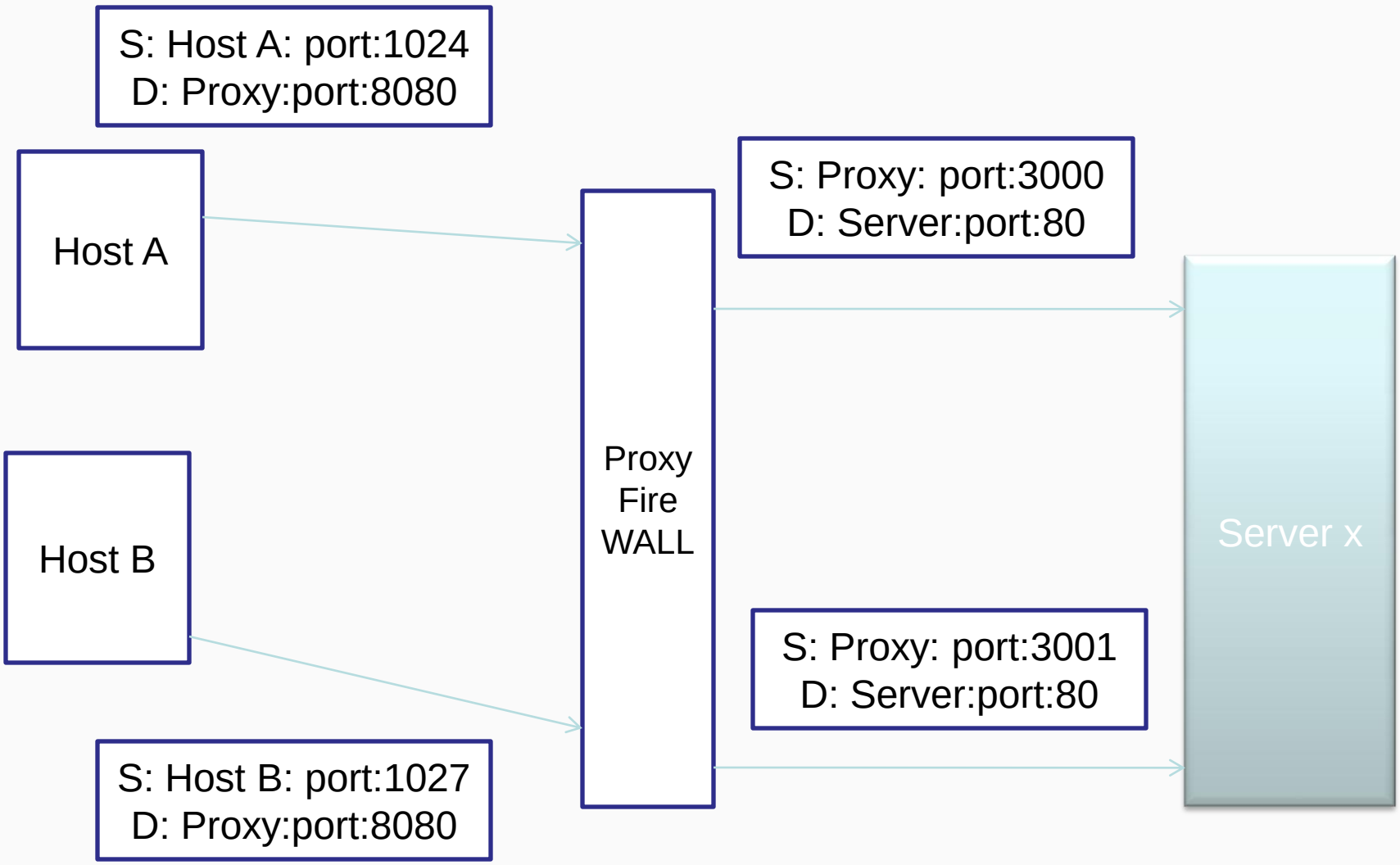
Stateless Firewall

- Stateless firewalls require less memory .
- Faster for simple filters that require less time to filter than to look up a session.
- They may also be necessary for filtering stateless network protocols that have no concept of a session.
- Not good for complex decisions based on what stage communications between hosts have reached.
- less secure.

Application Firewall

- An **application firewall** is a form of firewall which controls input, output, and/or access from, to, or by an application or service.
- It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall.
- Typically built to monitor one or more specific applications or services (such as a web or database service).
- Application firewalls can be in two subcategories
  1. *Network-based application firewall* (Proxy Servers)
  2. *Host-based application firewall*.

Network-based application firewall Proxy Firewall

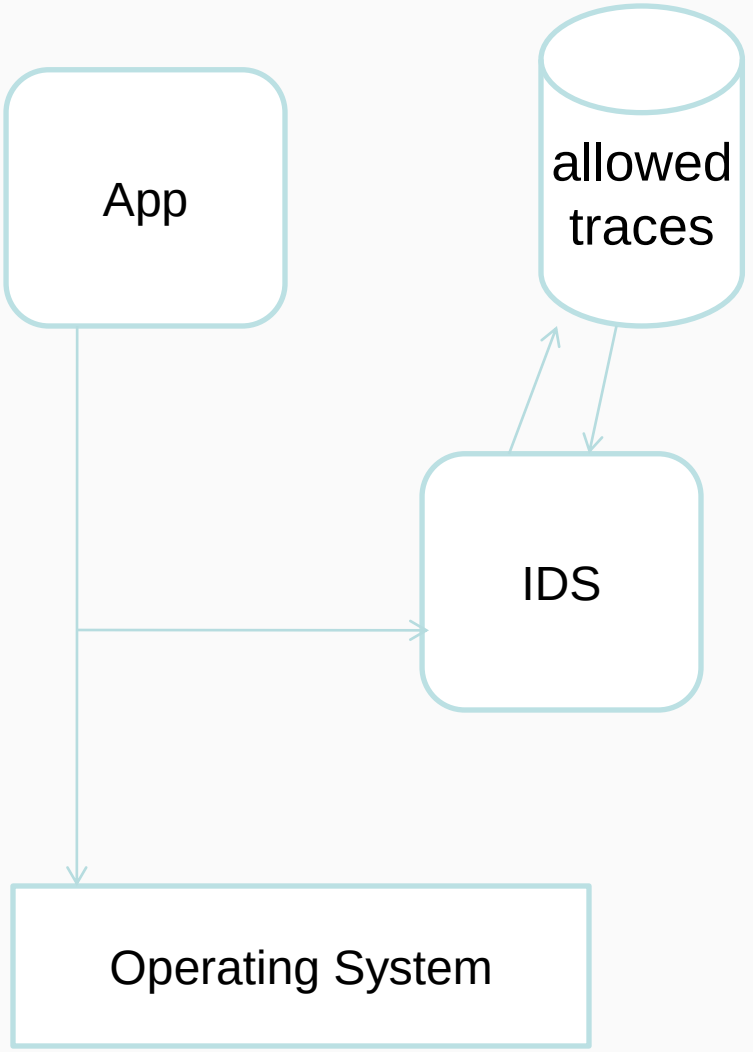


Host based Application Firewall

- Monitors application input/output and system service calls made by/to application.
- Accomplish their function by looking into socket calls to filter the connections between the application layer and the lower layers of the OSI model
- Much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis
- Application Firewall on Solaris can be implemented by mod security.

Anomaly detection:

- IDS monitors system call trace from the app
- DB contains a list of subtraces that are allowed to appear
- Any observed subtrace not in DB sets off alarms



Unified Threat Management (UTM)

- Unified Threat Management is a firewall appliance that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection and anti-virus duties traditionally handled by multiple systems.

Advantages of UTM

- **Reduced complexity**
- **Ease of deployment**
- **Integration capabilities**
- **The black box approach**
- **Troubleshooting ease**

Web Application Firewall

- A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation.
- These rules cover common attacks such as Cross-site Scripting(XSS) and SQL Injection.
- Customizing the rules according to your application.
- Many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

NETWORK SECURITY

Network Threats/Attacks

Network security attacks & their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

NETWORK SECURITY

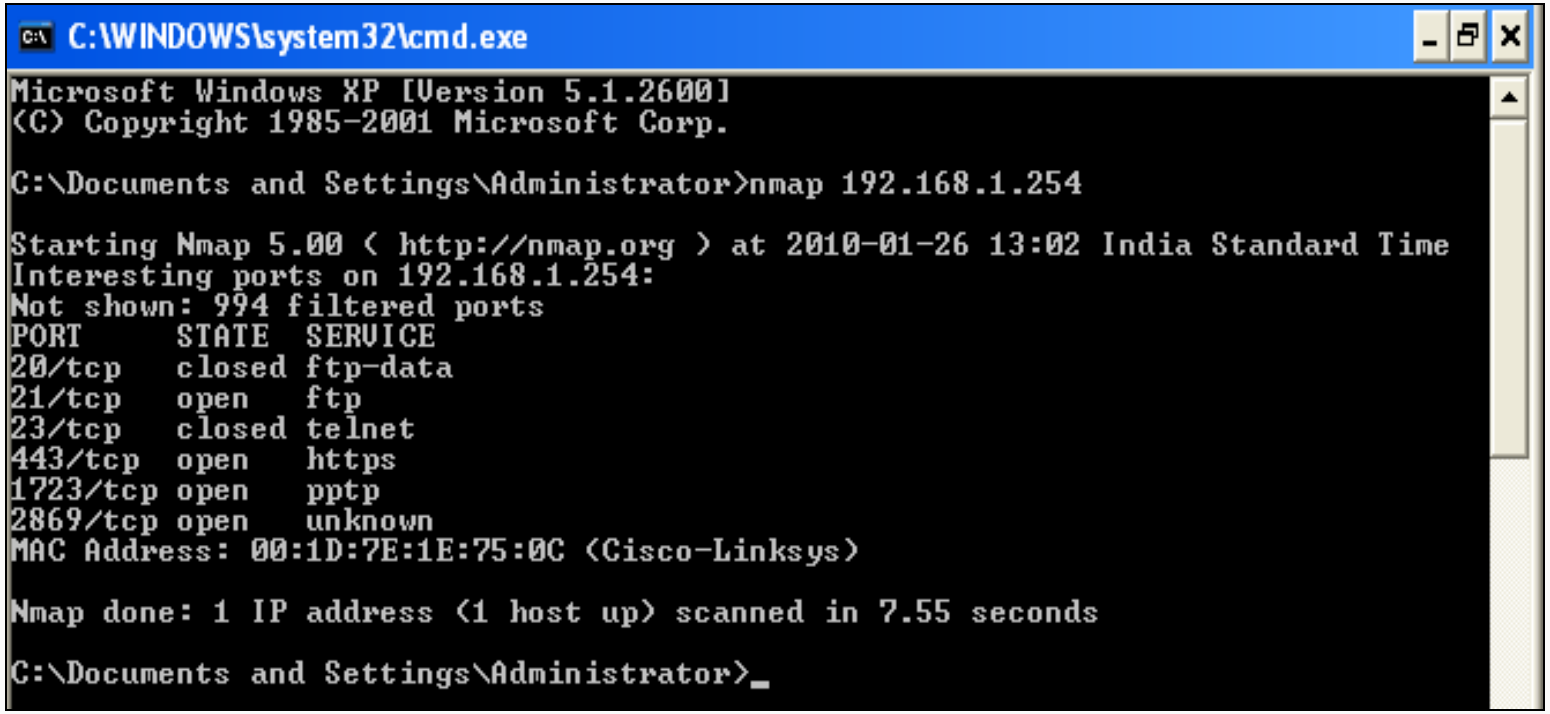
Network vulnerabilities & Assessment

Network Vulnerabilities

- Scanning
- Banner Grabbing
- Sniffing
- Denial of Service
- Session Hijacking

Scanning

- To detect Live machines
- To discover open ports
- To discover services running on the machine
- To discover known Vulnerabilities



Banner Grabbing

- Banner grabbing is the technique used to determine the target Operating system.

Banner Grabbing Using Telnet

C:\> telnet 192.168.2.1 80 (HEAD / HTTP/1.0)

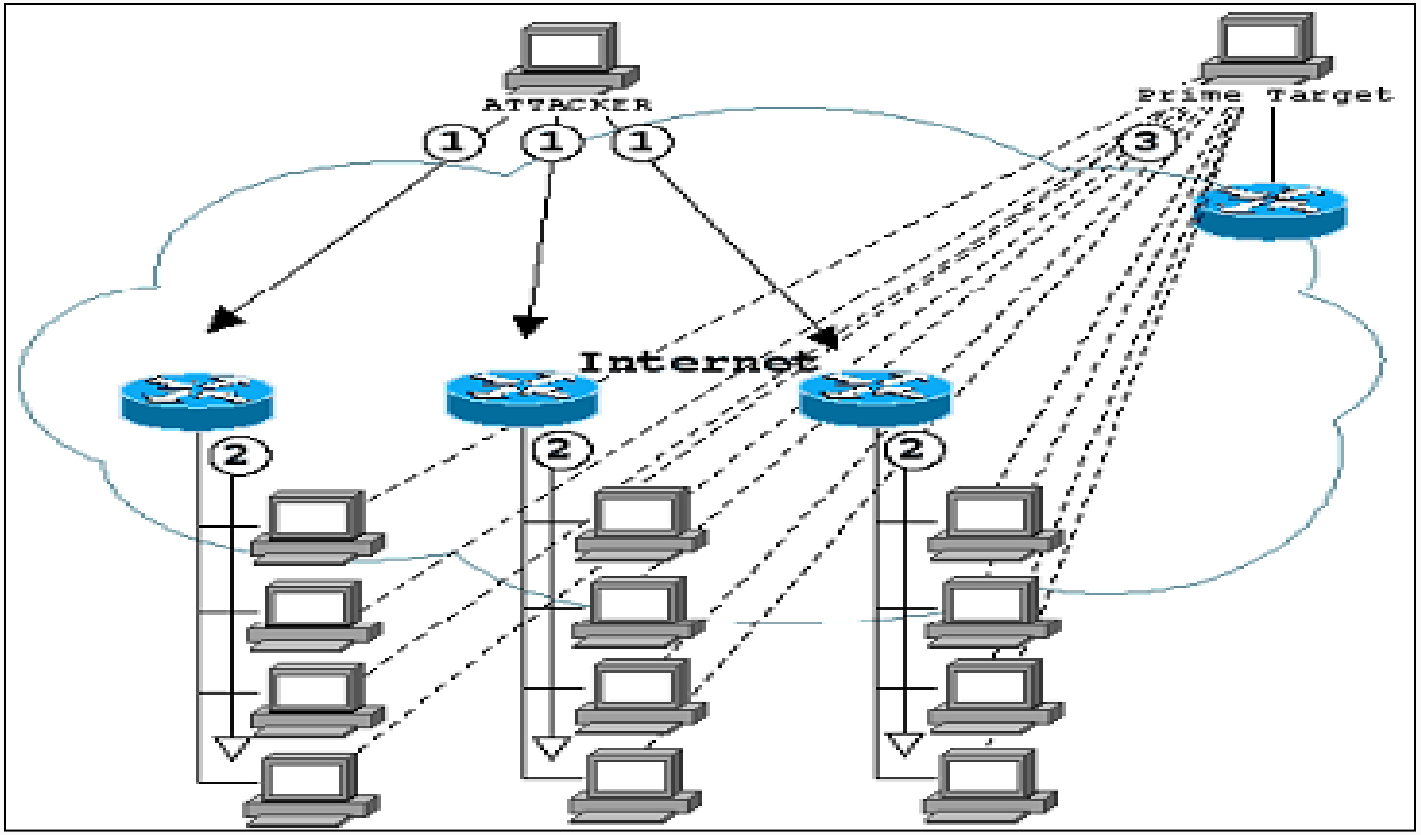
Sniffing

- Sniffing is a data interception technology
- Sniffer is a program or device that captures the vital information from the network traffic specific to a particular network.

  Eg. Wireshark

Denial of Service

- It is the technique used by attackers to make system unusable or significantly slow it down for legitimate users, by overloading its resources.



Session Hijacking

- Session Hijacking is the technique used to hijack an already authenticated session.
- Network level hijacking will be done by guessing the sequence numbers.
- Application level hijacking will occur by stealing a valid session id and which is used to get in to the system.

Network Security Assessment

Why do we need to perform assessment?

- To prevent Hacking, defacement , data integrity, Loss of financial assets and more.
- Computer security professionals know that to defeat malicious intruders, you need to know how to attack like one. Intruders spend much of their time searching for systems with known vulnerabilities: All they need is patience and a chunk of exploit code to succeed in cracking a system. They use Ping or some other utility to locate potential victim machines by IP address or domain name. Then, they find out which OS and applications the hosts are running and run the related exploit code.
- Vulnerability assessment tools automate the intruder exploration process and let network administrators assess the security readiness of their networks. Security policies, ACLs, and signed user agreements mean little if your systems are full of exploitable holes. If you can find the holes before a malicious intruder can, and close them, you've gone a long way toward making your network safer.

List of Tools

Tool Name	Windows Scan	Linux Scan	Network Devices Scan	GUI Support	Free Version	Commercial Cost
Nessus	Yes	Yes	Yes	Yes	Home Usage	$1200 Per year
GFI Languard	Yes	Yes	Yes	Yes	30 Days/5 IP	$4 Per IP Per Year
eEye Retina	Yes	Yes	Yes	Yes	Single IP	$ 575 - 32 Ips
MBSA	Yes	No	No	Yes	Available	NIL
Nipper	Yes	Yes	Yes	Yes	Not Available	$1400 - 100IPs
N-Map	Yes	Yes	Yes	Yes		Free

Network Configuration Flaws

- Weak File system
- Password policy not enforced
- Account Policy not enforced
- Administrator account not renamed
- Antivirus scan engine not updated
- Number of User account existence
- Operating System not updated with proper Service packs and Patches

Free Firewall software packages

- IP Tables
  - comes with most linux distributions
- SELinux (Security Enabled Linux – NSA)
  - comes with some Linux distributions
    - Fedora, Red Hat
- IPCop – specialized Linux distribution

Configuration of Windows Firewall

Question &Answer