Cyber Security

Subject Code:-102045607

Unit-4 Network Defense and Countermeasures

Automated Security Assessment Tools(OpenVAS, Nessus)

What is Security Testing?

Security testing is the process of testing the security of an information system. The process is intended to identify weaknesses in the system that are exploitable for unauthorized access or cause denial of service to authorized users.

Security testing has two main purposes:

- To find security weaknesses in the system before an attacker does,
- To determine if changes to the system have accidentally created new weaknesses.

What is Security Testing?

Dynamic Application Security Testing

- Dynamic Application Security Testing (DAST) is a method to find security vulnerabilities in an application while in production.
- DAST is conducted in the same way as traditional application security testing, but with the major difference that in DAST, the application is tested in real-time, in production. The testing is conducted using application source code in the same way the application is developed. The application will be tested in the same way customers, or users would use it.
- DAST uses various automated security testing tools that help identify any potential security vulnerabilities in an application known as automated security testing tools.

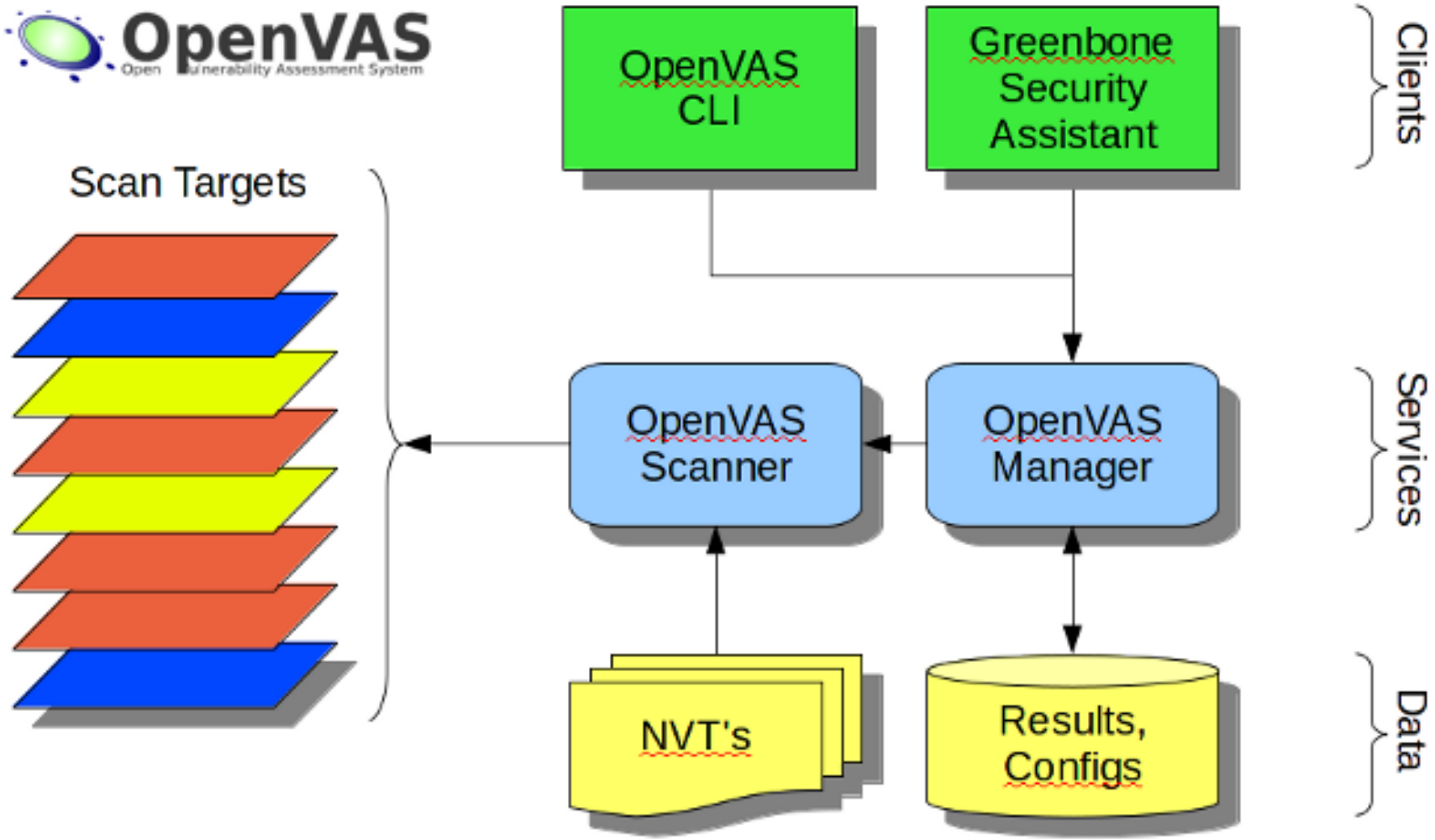
Automated Security Testing

- Automated Security Testing is the process of scanning the application for vulnerabilities using automated tools. This is important because it can help to prevent certain vulnerabilities from being exploited by hackers. With the help of automation scripts or applications, a programmer analyzes the application for potential security holes and fixes these holes automatically.
- Automated security testing is the practice of using software/applications to test a system for security vulnerabilities known as automated security testing tools. The automated security testing tools can be run against any application (e.g., web app) and report back to the user with a list of the vulnerabilities found in the application.

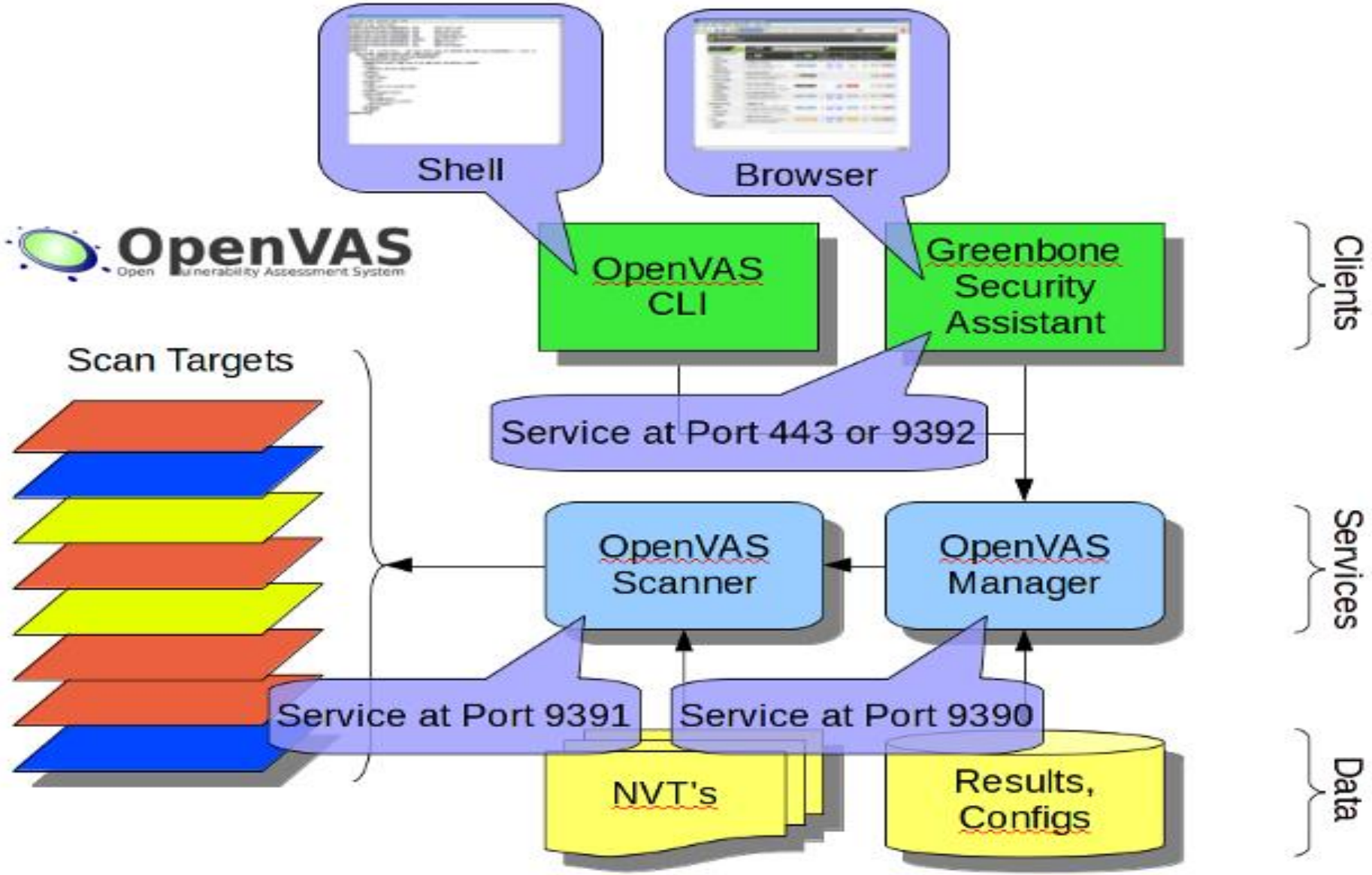
Automated Security Testing – Open VAS (Vulnerability Assessment System)

- The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.
- All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL).
- https://www.openvas.org/index.html

Automated Security Testing – Open VAS (Vulnerability Assessment System)



Automated Security Testing – Open VAS (Vulnerability Assessment System)



Automated Security Testing – Open VAS (Vulnerability Assessment System)

- The OpenVAS Manager is the central service that consolidates plain vulnerability scanning into a full vulnerability management solution. The Manager controls the Scanner via OTP (OpenVAS Transfer Protocol) and itself offers the XML-based, stateless OpenVAS Management Protocol (OMP).
- All intelligence is implemented in the Manager so that it is possible to implement various lean clients that will behave consistently e.g. with regard to filtering or sorting scan results. The Manager also controls a SQL database (sqlite-based) where all configuration and scan result data is centrally stored. Finally, Manager also handles user management including access control with groups and roles.

Automated Security Testing – Open VAS (Vulnerability Assessment System)

- Refer video.
- https://www.youtube.com/watch?v=koMo_fSQGIk

Automated Security Testing - Nessus

- Refer video.
- https://www.youtube.com/watch?v=35a0VhzIO2Y

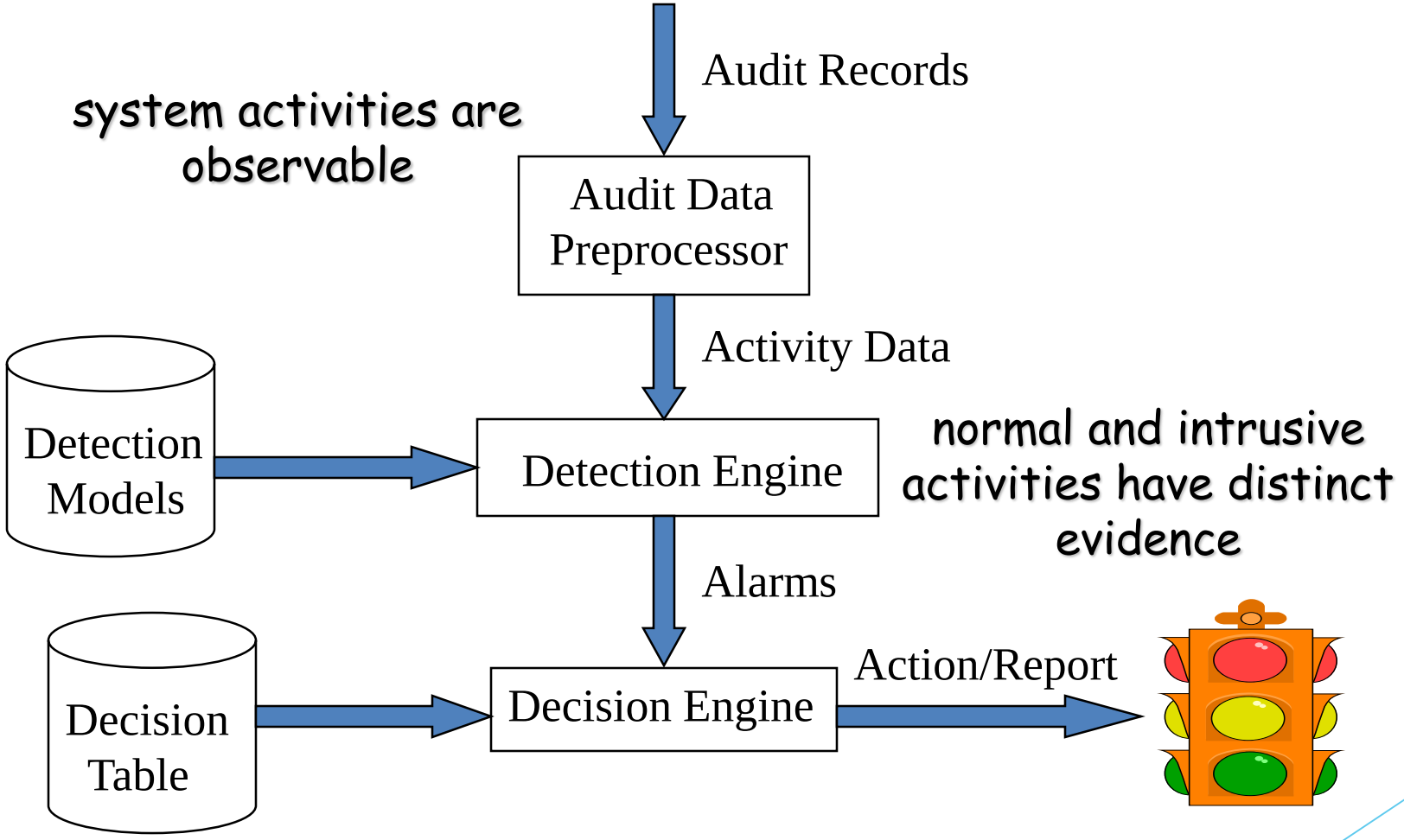
What is an Intrusion Detection System?

- Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.
- An IDS detects activity in traffic that may or may not be an intrusion.
- IDSes can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other internal threats.

Why are IDS important?

- The ability to know when an intruder or attacker is engaged in investigation or other malicious activity can mean the difference between being compromised and not being compromised.
- An IDS can alert the administrator of a successful compromise, allowing them the opportunity to implement mitigating actions before further damage is caused
- As Corporations and other Institutions are being legally bound to disclose data breaches and compromises to their affected customers, this can have profound effects upon a compromised company, in the way of bad press, loss of customer trust, and the effects on their stock.

Components of Intrusion Detection System



Host Based Intrusion Detection

- Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.
- It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.
- Host-based IDS are often critical in detecting internal attacks directed towards an organization's servers such as DNS, Mail, and Web Servers.

Network Based Intrusion Detection

- Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
- Instead of analyzing information that originates and resides on a host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
- Most Network-based IDS log their activities and report or alarm on questionable events.
- Network-based IDS work best when located on the DMZ(demilitarized zone) , on any subnets containing mission critical servers and just inside the firewall.

Network Based Intrusion Detection

Host Based

- *Narrow in scope (watches only **specific** host activities)*
- *More complex setup*
- *Better for detecting attacks from the **inside***
- ***More expensive** to implement*
- *Detection is based on what any **single host** can record*
- *Does not see packet headers*
- *Usually only responds **after** a suspicious log entry has been made*
- *OS-specific*
- *Detects local attacks before they hit the network*
- *Verifies success or failure of attacks*

Network Based

- Broad in scope (watches **all** network activities)
- Easier setup
- Better for detecting attacks from the **outside**
- **Less expensive** to implement
- Detection is based on what can be recorded on the **entire network**
- Examines packet headers
- Near **real-time** response
- OS-independent
- Detects network attacks as payload is analyzed
- Detects unsuccessful attack attempts

Hybrid Intrusion Detection

- Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.
- A Hybrid IDS, can monitor system and application events and verify a file system's integrity like a Host-based IDS, but only serves to analyze network traffic destined for the device itself.
- A Hybrid IDS is often deployed on an organization's most critical servers.

Honeypots

- Are trap servers or systems setup to gather information regarding an attacker of intruder into networks or systems.
- Appear to run vulnerable services and capture vital information as intruders attempt unauthorized access.
- Provide you early warning about new attacks and exploitation trends which allow administrators to successfully configure a behavioral based profile and provide correct tuning of network sensors.
- Can capture all keystrokes and any files that might have been used in the intrusion attempt.

Honeypots

- **Honeypot** is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.
- Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

Honeypots

- The **cost of a honeypot** is generally **high** because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system.

Honeypots

- **Types of Honeypot:**

Honeypots are classified based on their deployment and the involvement of the intruder.

Based on their deployment, honeypots are divided into :

Research honeypots- These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.

Production honeypots- Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

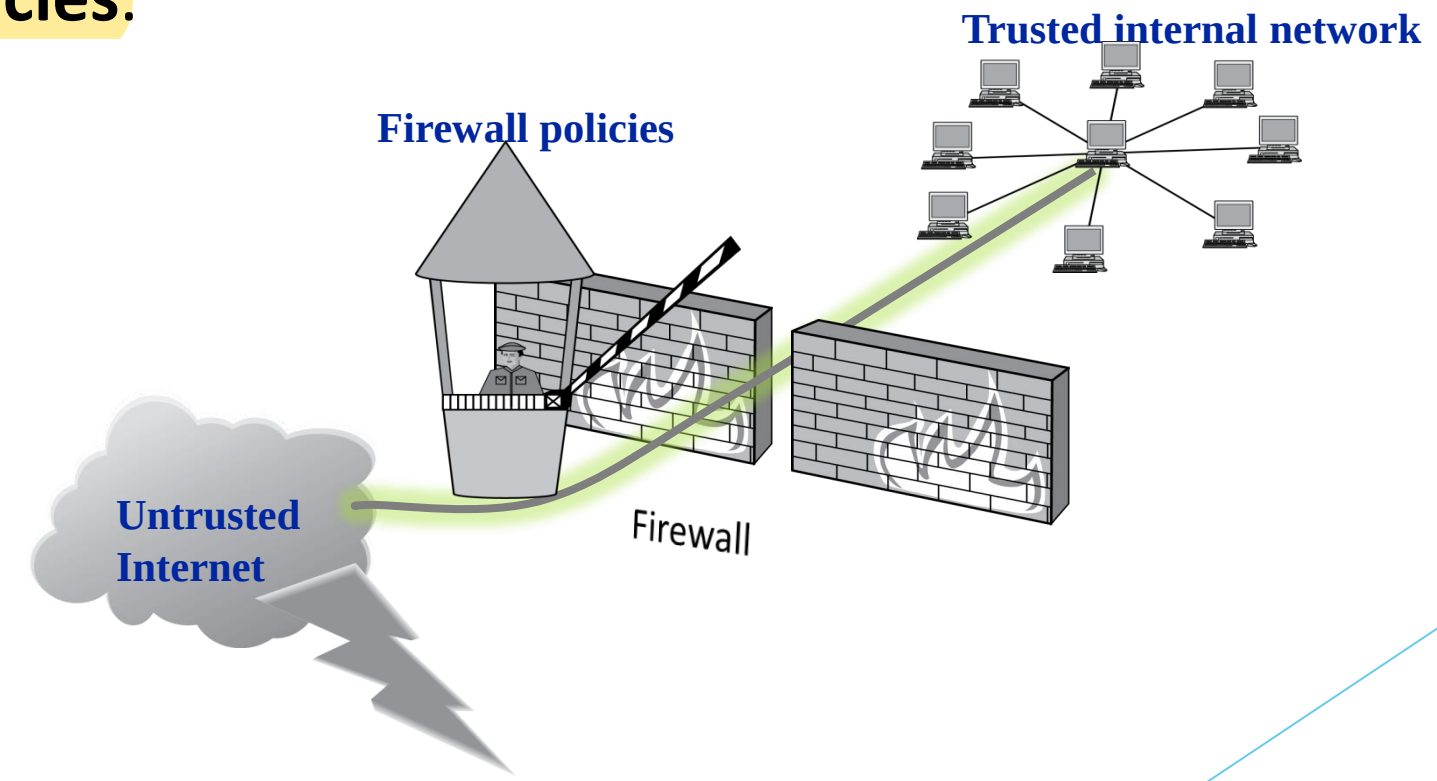
Firewalls

A **firewall** is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.

Firewall Policies

To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
  - **Accepted:** permitted through the firewall
  - **Dropped:** not allowed through with no indication of failure
  - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
  - TCP or UDP
  - **the source and destination IP addresses**
  - **the source and destination ports**
  - the application-level payload of the packet (e.g., whether it contains a virus).

Blacklists and White Lists

Two fundamental approaches to creating firewall policies (or rulesets)

Blacklist approach (default-allow)

- All packets are allowed through except those that fit the rules defined specifically in a blacklist.
- Pros: flexible in ensuring that service to the internal network is not disrupted by the firewall
- Cons: unexpected forms of malicious traffic could go through

Whitelist approach (default-deny)

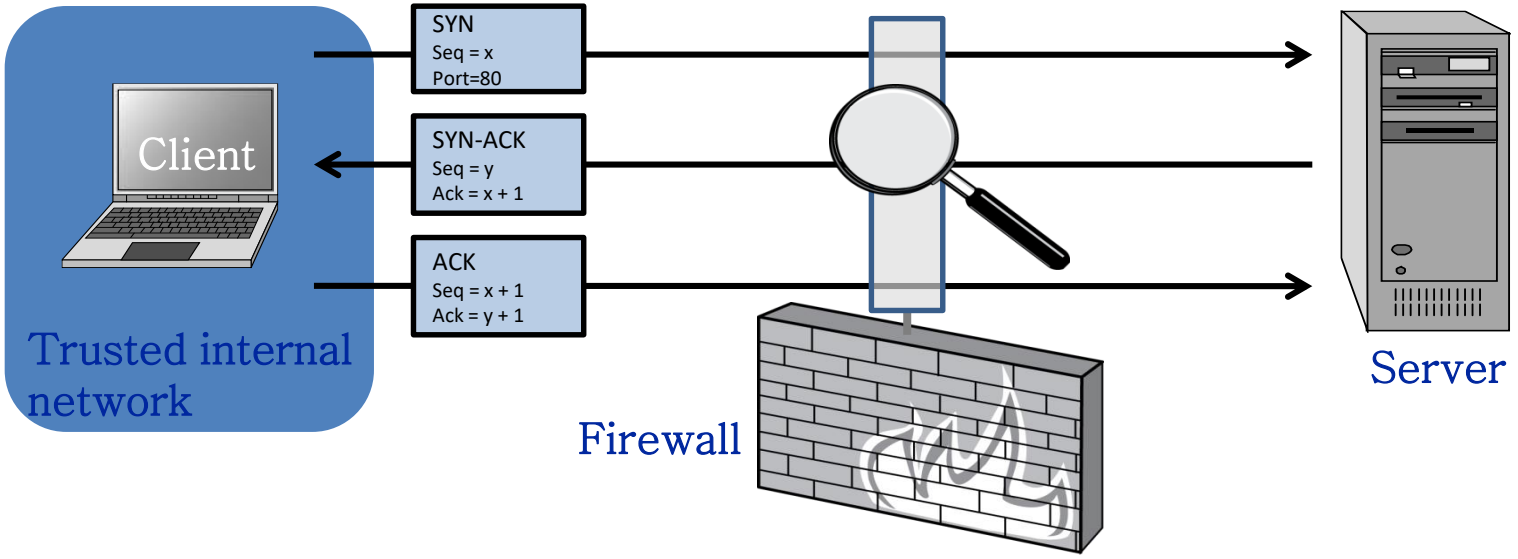
- Packets are dropped or rejected unless they are specifically allowed by the firewall
- Pros: A safer approach to defining a firewall ruleset
- Cons: must consider all possible legitimate traffic in ruleset

Firewall Types

- **packet filters (stateless)**
  - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **"stateful" filters**
  - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
  - It works like a **proxy** it can “understand” certain applications and protocols.
  - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Stateless Firewalls

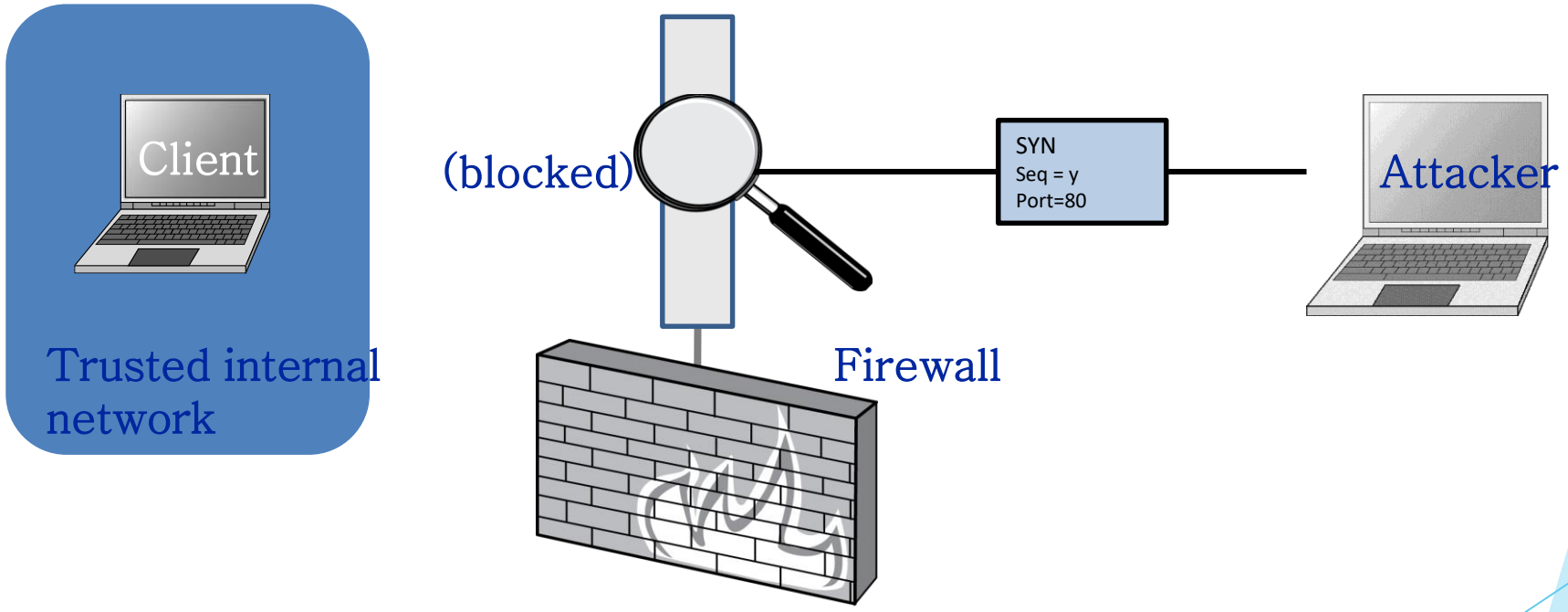
A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN−ACK packets, source port=80

Stateless Restrictions

Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



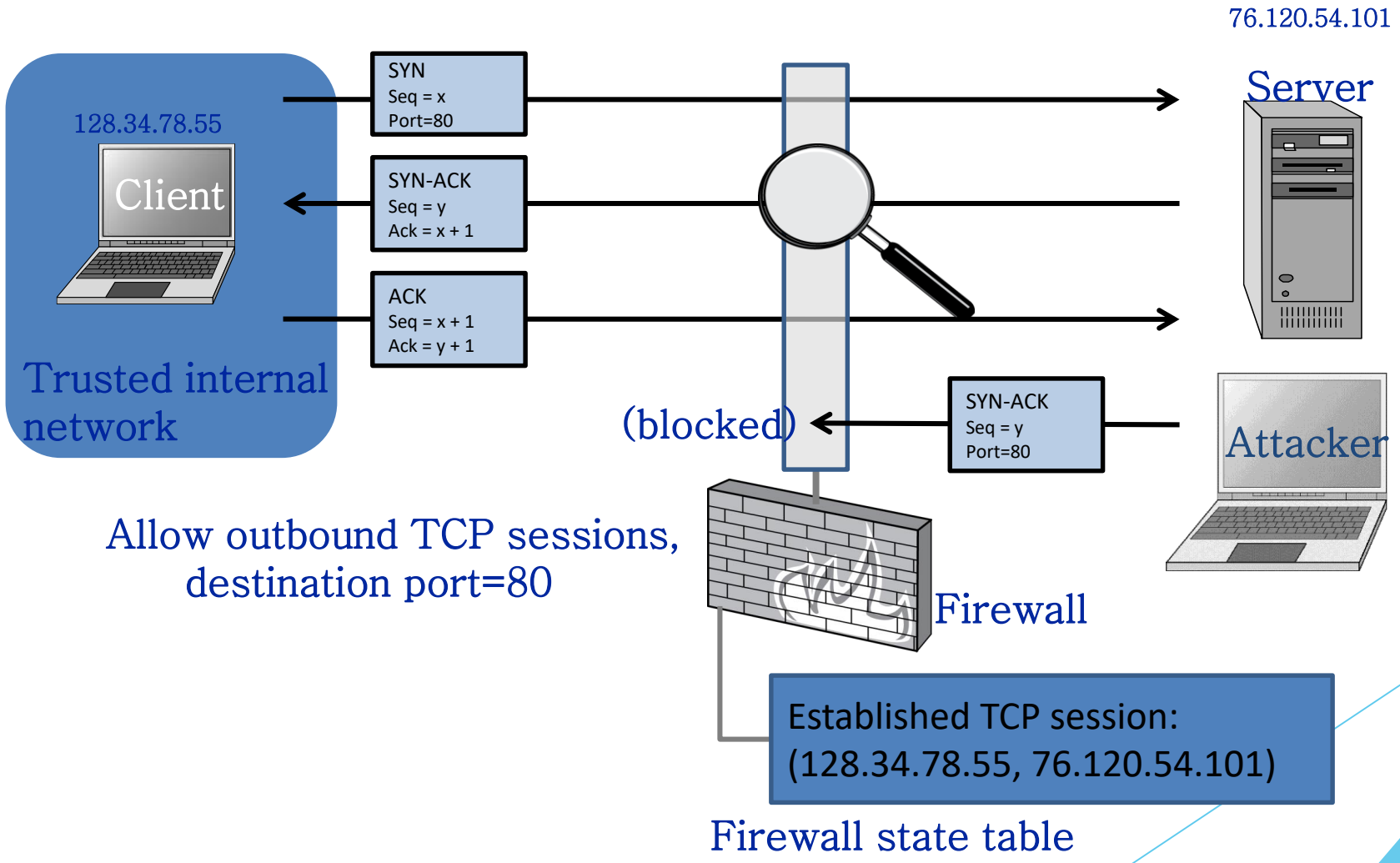
Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Statefull Firewalls

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

Statefull Firewall Example

Allow only requested TCP connections:



Statefull Firewall Example

- TCP-based connections are easy to check
  - TCP SYN packet

- UDP-based traffic is not so clear
  - There is no UDP connection set up
  - Treat a UDP session starts when a legitimate UDP packet is allowed through the firewall (such as from inside to outside)
    - Session is defined by (source IP, source port, dest IP, dest port)

Application-level Firewall

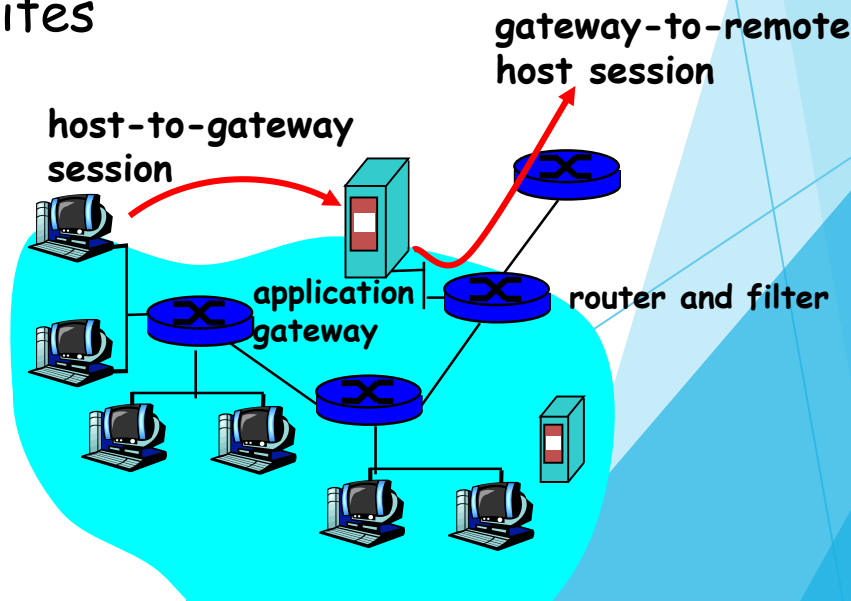
Filters packets on application data as well as on IP/TCP/UDP fields.

Example: allow select internal users to telnet outside.

1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. Router filter blocks all telnet connections not originating from gateway.

Example: block user access to know porn websites

- Check if the Web URL is in a "black-list"



Firewall on Windows and Linux

- On Linux, Iptables is used to provide firewall function
- On Windows, use “control panel”→ “Windows Firewall”

Cryptographic Attacks

- The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

- Hence, They applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised.

Cryptographic Attacks

Ciphertext Only Attacks (COA) – In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.

Known Plaintext Attack (KPA) – In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.

Cryptographic Attacks

Dictionary Attack – This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

Brute Force Attack (BFA) – In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is $2^8 = 256$. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

Cryptographic Attacks

Man in Middle Attack (MIM) – The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

Side Channel Attack (SCA) – This type of attack is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem.

Fault analysis Attacks – In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

Password Cracking

- Password cracking (also called, password hacking) is an attack vector that involves hackers attempting to crack or determine a password. Password hacking uses a variety of programmatic techniques and automation using specialized tools. These password cracking tools may be referred to as 'password crackers'.

- Credentials can also be stolen via other tactics, such as by memory-scraping malware, and tools like Redline password stealer, which has been part of the attack chain in the recent, high-profile Lapsus$ ransomware attacks.

- A password can refer to any string of characters or secret to authenticate an authorized user to a resource. Passwords are typically paired with a username or other mechanism to provide proof of identity.

Password Cracking

Password Guessing Attacks

1. Random Guesses

- The most common variants for passwords susceptible to guessing include these common schemas:

- The word “password” or basic derivations like “passw0rd”
- Derivations of the account owner’s username, including initials. This may include subtle variations, such as numbers and special characters.
- Reformatted or explicit birthdays for the user or their relatives, most commonly, offspring
- Memorable places or events
- Relatives’ names and derivations with numbers or special characters, when presented together
- Pets, colors, foods, or other important items to the individual

Password Cracking

Password Guessing Attacks

2. Dictionary Attacks

- Dictionary attacks are an automated technique utilizing a list of passwords against a valid account to reveal the password. The list itself is a dictionary of words. Basic password crackers use lists of common single words like “baseball” to crack a password, hack an account, and reveal the complete credential.
- The most common method to mitigate the threat of a dictionary attack is account lockout attempts. After “n” times of wrong attempts, a user’s account is automatically locked for a period of time. It must be manually unlocked by an authority, like the help desk or via an automated password reset solution.

Password Cracking

Password Guessing Attacks

3. Brute Force

- Brute force password attacks utilize a programmatic method to try all possible combinations for a password. This method is efficient for passwords that are short in string (character) length and complexity. This can become infeasible, even for the fastest modern systems, with a password of eight characters or more.
- If a password only has alphabetical characters, including capital letters or lowercase, odds are it would take 8,031,810,176 guesses to crack. This assumes the threat attacker knows the password length and complexity requirements. Other factors include numbers, case sensitivity, and special characters in the localized language.

Brute-Force Tools – John the Ripper

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types, including for: user passwords of Unix flavors (Linux, *BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "web apps" (e.g., WordPress), groupware (e.g., Notes/Domino), and database servers (SQL, LDAP, etc.); network traffic captures (Windows network authentication, WiFi WPA-PSK, etc.); encrypted private keys (SSH, GnuPG, cryptocurrency wallets, etc.), filesystems and disks (macOS .dmg files and "sparse bundles", Windows BitLocker, etc.), archives (ZIP, RAR, 7z), and document files (PDF, Microsoft Office's, etc.)

pwdump

pwdump is the name of various Windows programs that outputs the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database and from the Active Directory domain's users cache on the operating system.

It is widely used, to perform both the famous pass-the-hash attack or also can be used to brute-force users' password directly. In order to work, it must be run under an Administrator account, or be able to access an Administrator account on the computer where the hashes are to be dumped. Pwdump could be said to compromise security because it could allow a malicious administrator to access user's passwords.

Packet Filters

- A packet filtering firewall is a network security feature that controls the flow of incoming and outgoing network data. The firewall examines each packet, which comprises user data and control information, and tests them according to a set of pre-established rules.
- If the packet completes the test successfully, the firewall allows it to pass through to its destination. It rejects those that don't pass the test. Firewalls test packets by examining sets of rules, protocols, ports and destination addresses.

Packet Filters

4 types of packet filtering

1. Static packet filtering firewall

- A static packet filtering firewall requires you to establish firewall rules manually. Similarly, internal and external network connections remain either open or closed unless otherwise adjusted by an administrator. These firewall types allow users to define rules and manage ports, access control lists (ACLs) and IP addresses. They're often simple and practical, making them an apt choice for smaller applications or users without a lot of criteria.

Packet Filters

4 types of packet filtering

2. Dynamic packet filtering firewall

- Dynamic firewalls allow users to adjust rules dynamically to reflect certain conditions. You can set ports to remain open for specified periods of time and to close automatically outside those established time frames. Dynamic packet filtering firewalls offer more flexibility than static firewalls because you can set adjustable parameters and automate certain processes.

Packet Filters

4 types of packet filtering

3. Stateless packet filtering firewall

- Stateless packet filtering firewalls are perhaps the oldest and most established firewall option. While they're less common today, they do still provide functionality for residential internet users or service providers who distribute low-power customer-premises equipment (CPE).
- They protect users against malware, non-application-specific traffic and harmful applications. If users host servers for multi-player video games, email or live-streamed videos, for example, they often must manually configure firewalls if they plan to deviate from default security policies. Manual configurations allow different ports and applications through the packet filter.

Packet Filters

4 types of packet filtering

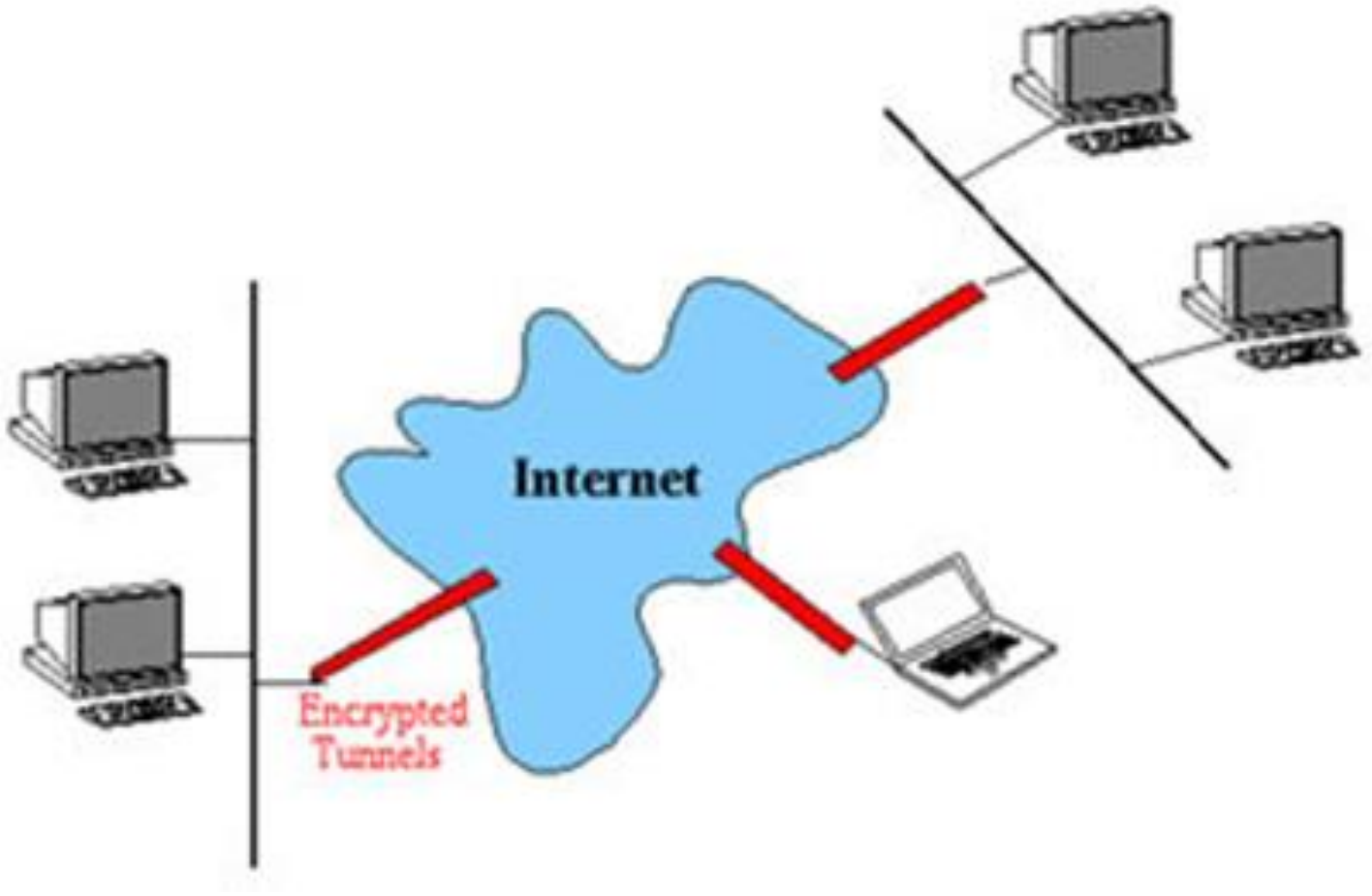
4. Stateful packet filtering firewall

- Unlike stateless packet filtering options, stateful firewalls use modern extensions to track active connections, like transmission control protocol (TCP) and user datagram protocol (UDP) streams. By recognizing incoming traffic and data packets' context, stateful firewalls can better identify the difference between legitimate and malicious traffic or packages. Typically, new connections must introduce themselves to the firewall before they gain access to the approved list of allowed connections.

Virtual Private Network (VPN)

- VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
- A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Virtual Private Network (VPN)



Virtual Private Network (VPN)

- VPN is free to use and it uses site-to-site and remote access methods to work. It uses an arrangement of encryption services to establish a secure connection. It is an ideal tool for encryption; it provides you strong AES256 encryption with an 8192bit key.

How VPN Works?

- VPN works by creating a secure tunnel using powerful VPN protocols. It hides your IP address behind its own IP address that encrypts all your communication. Thus, your communication passes through a secure tunnel that allows you use network resources freely and secretly.

Virtual Private Network (VPN)

VPN protocols

- IP security (IPsec)
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Thank you!