

Protecting the Organization

- There is **no single security appliance** that can solve all network security needs. It is thus important that they all **work together as part of a system**.
- Security appliances can be **stand-alone devices**, like a router or firewall, a card that can be installed into a network device, or a **module** with its own processor and cached memory. Security appliances can also be **software tools** that are run on a network device.
- **Routers** - Cisco Integrated Services Router (ISR) routers, have firewall capabilities besides just routing, including traffic filtering, ability to run an Intrusion Prevention System (IPS), encryption, and VPN capabilities.
- **Firewalls** - Cisco Next Generation Firewalls have all the capabilities of an ISR router, as well as, advanced network management and analytics.
- **IPS** - Cisco Next Generation IPS devices are dedicated to intrusion prevention.
- **VPN** - Cisco security appliances are equipped with a Virtual Private Network (VPN) server and client for secure encrypted tunneling.
- **Malware/Antivirus** - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.
- **Other Security Devices** – This includes web and email security appliances, decryption devices, client access control servers, and security management systems.



Firewall

- A Firewall is designed to control, or **filter**, which **communications** are allowed **in** and which are allowed **out** of a device or network.
- It can be installed on a single computer with the purpose of protecting that one computer (**host-based firewall**), or it can be a stand-alone network device that protects an entire network of computers (**network-based firewall**).
- **Network Layer Firewall** – filtering based on source and destination IP addresses
- **Transport Layer Firewall** – filtering based on source and destination data ports, and filtering based on connection states
- **Application Layer Firewall** – filtering based on application, program or service
- **Context Aware Application Firewall** – filtering based on the user, device, role, application type, and threat profile
- **Proxy Server** – filtering of web content requests like URL, domain, media, etc.
- **Reverse Proxy Server** – placed in front of web servers, reverse proxy servers protect, hide, offload, and distribute access to web servers
- **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
- **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system



Intrusion Detection/Prevention System

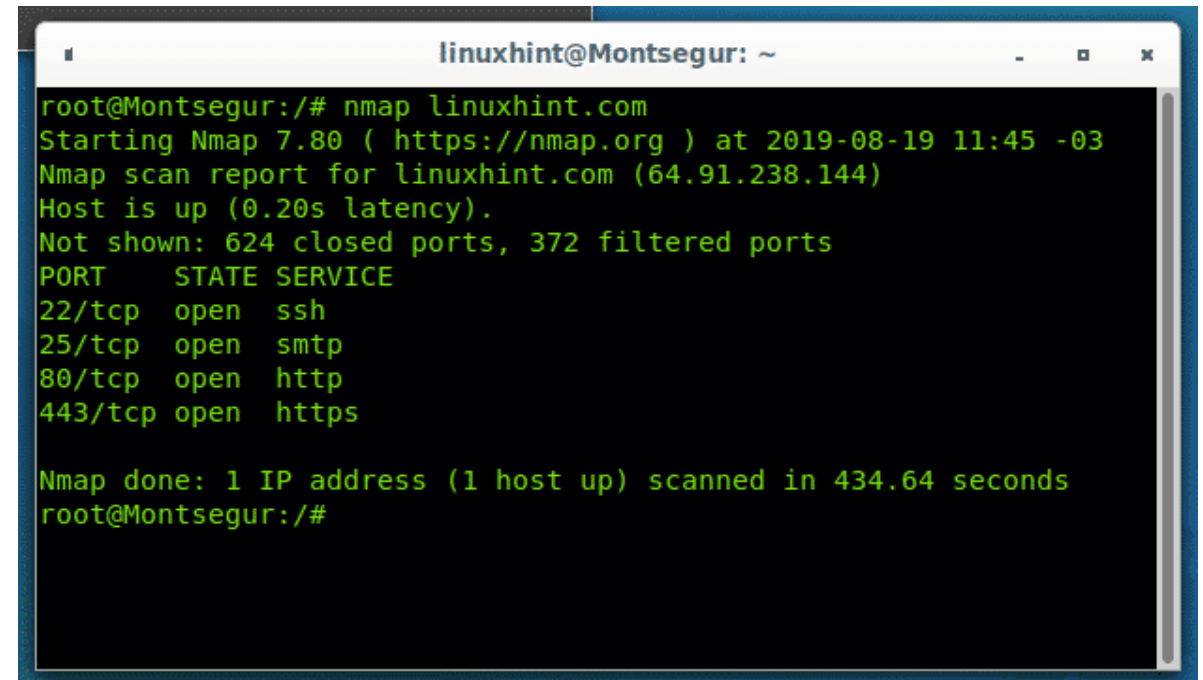
- An **Intrusion Detection System (IDS)** is either a dedicated **network device**, or one of several **tools** in a server or firewall that scans data against a database of rules or attack signatures, looking for malicious traffic.
- If a match is detected, the IDS will **log the detection**, and **create an alert** for a network administrator.
- The scanning performed by the IDS slows down the network (known as latency). To prevent against network delay, an IDS is **usually placed offline**, separate from regular network traffic. **Data** is copied or **mirrored** by a switch and then forwarded to the IDS for offline detection.
- There are also **IDS tools** that can be installed on top of a host computer operating system, like Linux or Windows.
- An **Intrusion Prevention System (IPS)** has the ability to **block or deny traffic** based on a positive rule or signature match.
- One of the most well-known IPS/IDS systems is [Snort](#). The commercial version of Snort is Cisco's Sourcefire.
- Sourcefire has the ability to perform real-time traffic and port analysis, logging, content searching and matching, and can detect probes, attacks, and port scans. It also integrates with other third party tools for reporting, performance and log analysis.



Port Scanning

- Port-scanning is a process of **probing** a computer, server or other device **for open ports**. Each application running on a device is assigned an identifier called a port number. It is used on both ends of the transmission so that data is passed to the correct application.
- Port-scanning can be used maliciously as a **reconnaissance tool** to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to **verify network security policies** on the network.
- You can use a port-scanning tool like **Nmap** to find all the open ports on your network. Port-scanning **can be seen as a precursor to a network attack** and therefore **should not be done on public servers on the Internet**, or on a company network without permission.
- To execute a **port-scan** of your network **from outside** of the network against your firewall or router, you will need to initiate the scan with **public IP address**.

- Go to an [Nmap Online Port Scanner](#) and enter your public IP address. If the response is open for any of the ports: 21, 22, 25, 80, 443, or 3389 then most likely, port forwarding has been enabled on your router or firewall, and you are running servers on your private network.

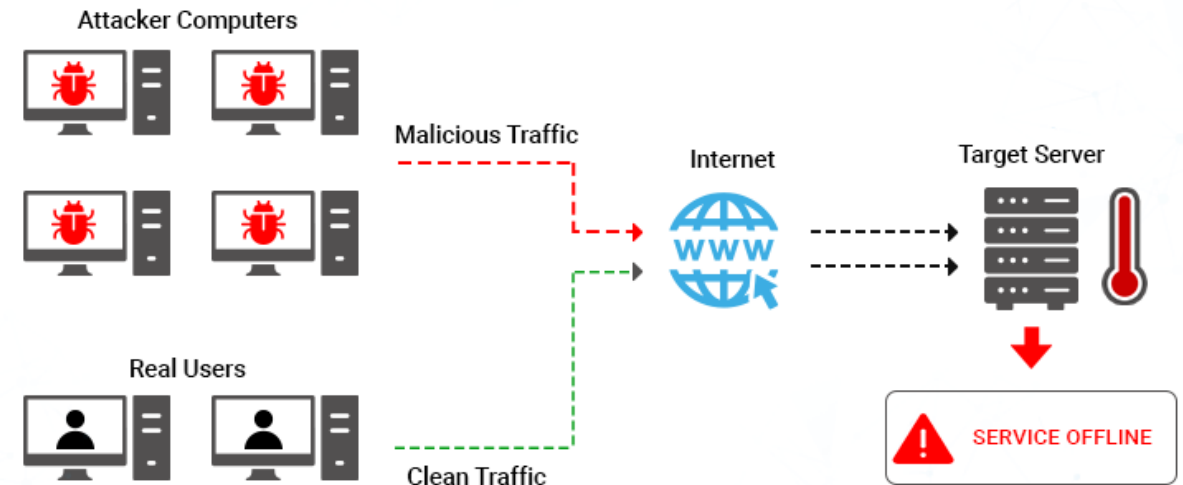
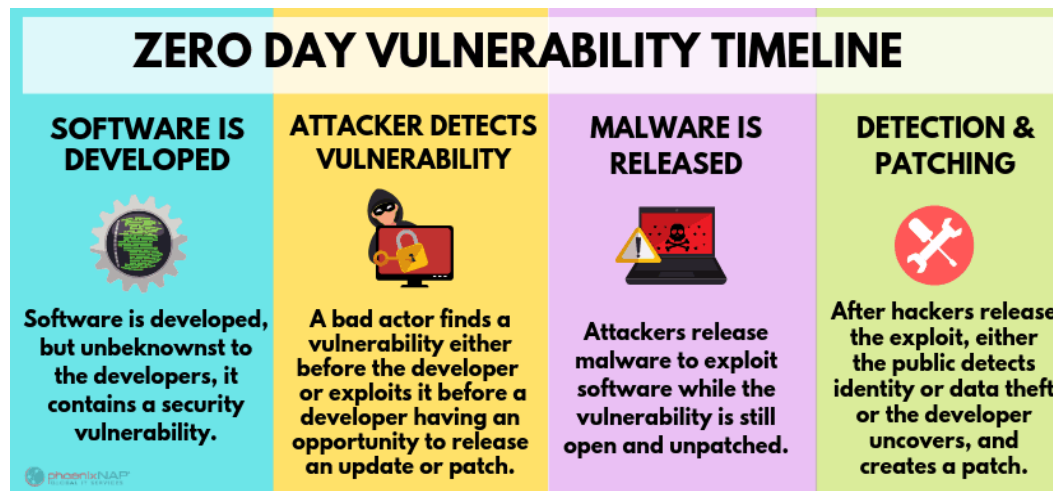
A terminal window titled 'linuxhint@Montsegur: ~' showing the output of an Nmap scan. The user has entered 'nmap linuxhint.com'. The output shows the scan starting at 2019-08-19 11:45 -03, reporting the host as up with 0.20s latency. It lists 624 closed ports and 372 filtered ports. A table shows four open ports: 22/tcp (ssh), 25/tcp (smtp), 80/tcp (http), and 443/tcp (https). The scan completed in 434.64 seconds.

```
linuxhint@Montsegur: ~
root@Montsegur:/# nmap linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-19 11:45 -03
Nmap scan report for linuxhint.com (64.91.238.144)
Host is up (0.20s latency).
Not shown: 624 closed ports, 372 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 434.64 seconds
root@Montsegur:/#
```

Detecting Attacks in Real Time

- Software is not perfect. When a hacker exploits a flaw in a piece of software before the creator can fix it, it is known as a **zero-day attack**.
- Due to the sophistication of zero-day attacks found today, it is becoming common that attacks will succeed, and success is now measured as how quickly a network can respond to it.
- The ability to **detect attacks** as they happen in real-time, as well as **stopping the attacks immediately**, or within minutes of occurring, is the ideal goal.
- **Real Time Scanning from Edge to Endpoint** - Actively scan for attacks using firewall and IDS/IPS devices. Connections to online global threat centers must also be used. Devices and software should support context-based analysis and behavior detection.
- **DDoS Attacks and Real Time Response** - DDoS attacks are extremely difficult to defend against because the attacks originate from hundreds, or thousands of zombie hosts, and appear as legitimate traffic. Regularly occurring DDoS attacks cripple Internet servers and reduce availability.



Cyber Kill Chain

- Kill Chain is the **stages of an information systems attack**. It was developed by Lockheed Martin as a security framework for incident detection and response.
- **1. Reconnaissance** - The attacker gathers information about the target.
- **2. Weaponization** - The attacker creates an exploit and malicious payload to send to the target.
- **3. Delivery** - The attacker sends the exploit and malicious payload to the target by email or other method.
- **4. Exploitation** - The exploit is executed.
- **5. Installation** - Malware and backdoors are installed on the target.
- **6. Command and Control** - Remote control of the target is gained through a command and control server.
- **7. Action** - The attacker performs malicious actions like information theft, or executes additional attacks within the network by working through the Kill Chain again.

CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED

Targeted, Coordinated, Purposeful

P : PERSISTENT

Month after Month, Year after Year

T : THREAT

Person(s) with intent, opportunity, and capability

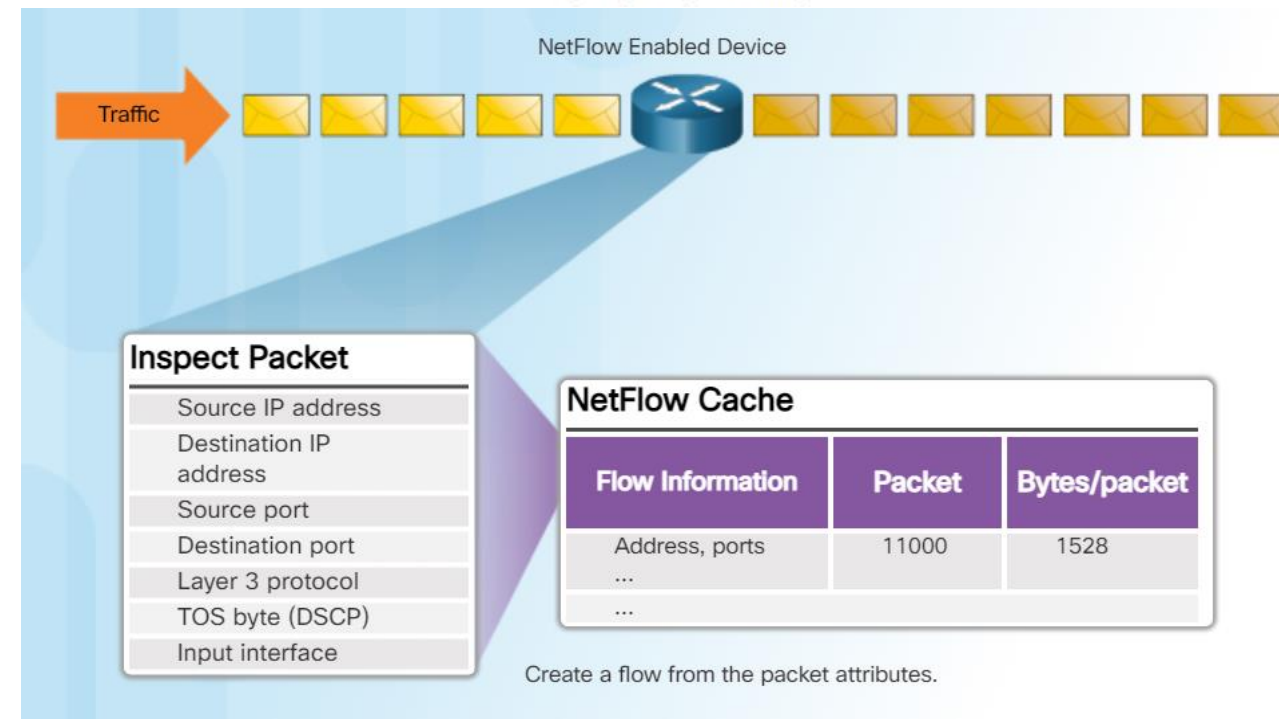
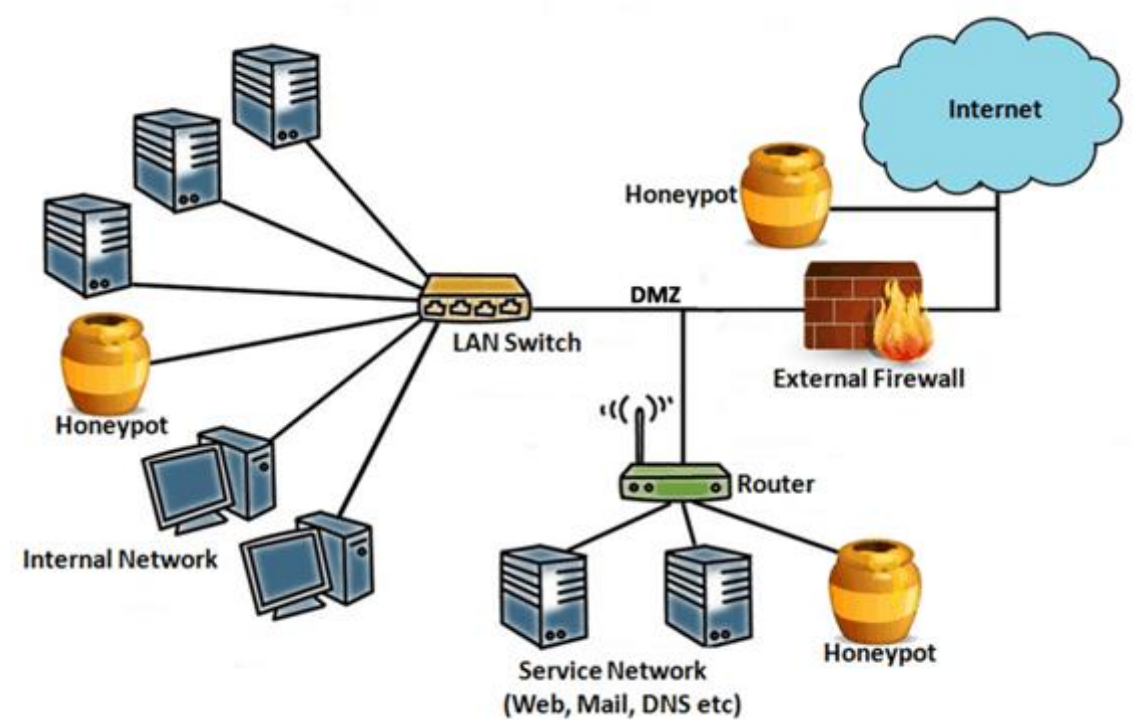


Learn how defenders have the advantage at:
lockheedmartin.com/cyber



Behaviour-Based Security

- Behavior-based security is a form of threat detection that does not rely on known malicious signatures, but instead involves **capturing and analyzing communication** between a local user and a remote destination. These reveal **behavior patterns** which can help **detect anomalies**.
- **Honeypots** - A Honeypot tool first lures the attacker in by appealing to the predicted pattern of malicious behavior, and then, when inside the honeypot, the network administrator can capture, log, and analyze the attacker's behavior. This allows the administrator to gain more knowledge and build a better defense.
- **NetFlow** - NetFlow technology shows you who and what devices are in your network, as well as when and how users and devices accessed. Switches, routers, and firewalls equipped with NetFlow can report information about data travelling through the network. This is sent to Collectors that collect, store, and analyze the records.



CSIRT

- Many large organizations have a **Computer Security Incident Response Team (CSIRT)** to receive, review, and respond to computer security incident reports.
- The primary mission of CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents.
- There are **national and public CSIRT organizations** like the **CERT Division of the Software Engineering Institute at Carnegie Mellon University**, that are available to help organizations, and national CSIRTs, develop, operate, and improve their incident management capabilities.
- One of the best way to prepare for a security breach is to prevent one. When a security breach is detected, appropriate actions should be taken to minimize its impact and damage. The **response plan should be flexible** with multiple action options during the breach.

