Welcome to Security Lifecycle: Prevention – Network Discovery.

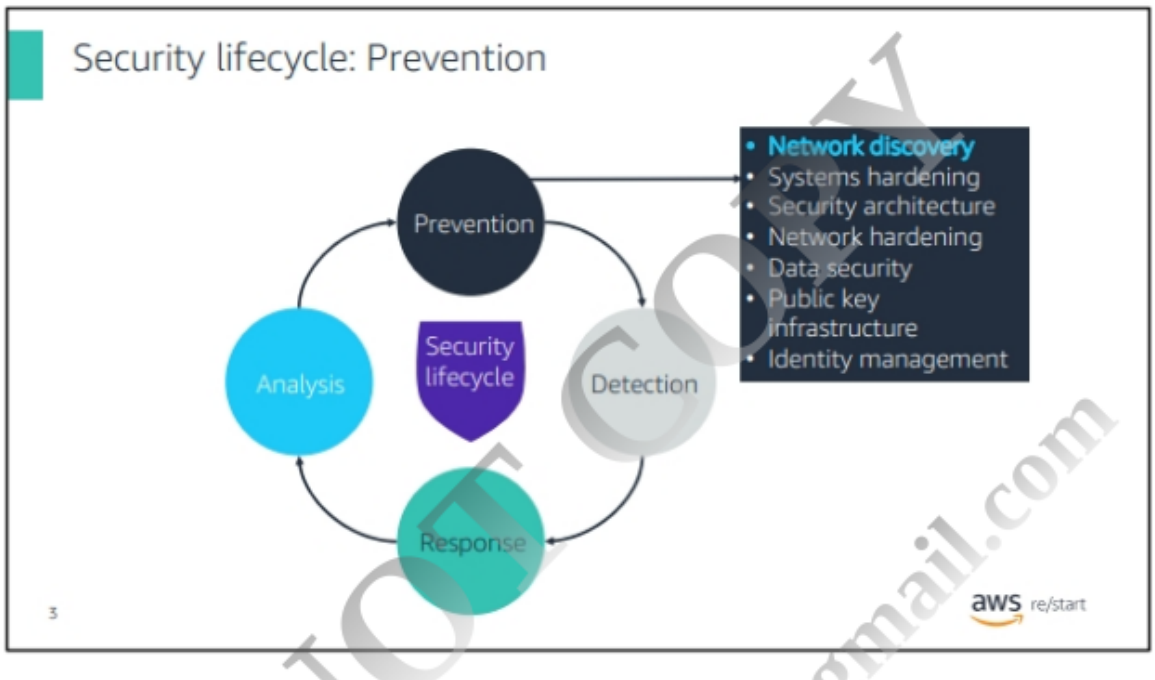
What you will learn

At the core of the lesson

You will learn how to:

- Contrast the security needs of early dedicated networks to those of modern networks
- Explain the value of a layered security model to protect a network environment
- Identify various tools that enable you to discover what is on your network

aws re/start



As a review, the phases of the security lifecycle consist of:

- **Prevention** – The first line of defense.
- **Detection** – Occurs when prevention fails.
- **Response** – Describes what you do upon detection of a security issue.
- **Analysis** – Completes the cycle as you implement new preventative measures to prevent the issue from occurring again in the future.

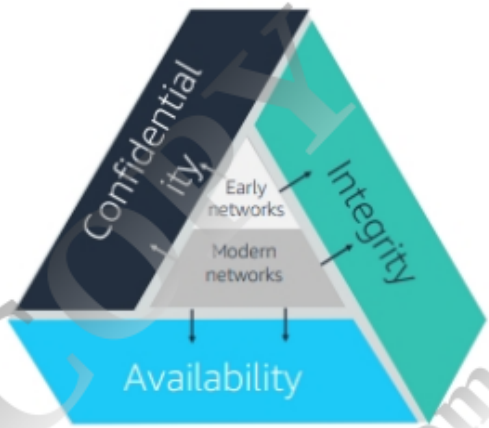
In the Prevention phase, *network discovery* is one of the first areas where you implement security controls. Network discovery is the ability to discover and access your network.

Understanding networks and protocols is essential to understanding network security. Many vulnerabilities are discovered through evaluating the **protocols** in use on a target network. Outside parties can use techniques such as *footprinting*, *scanning*, and *enumeration* to discover basic facts about:

- Your online presence
- Which ports are open
- Which services are active on your systems

Networking review

- Early dedicated networks offered confidentiality and integrity, but not availability.
- Modern networks:
  - Are much more interconnected
  - Offer access 24 hours a day
  - Use more bandwidth than a few years ago
- As availability increases, the need for confidentiality and integrity increases.



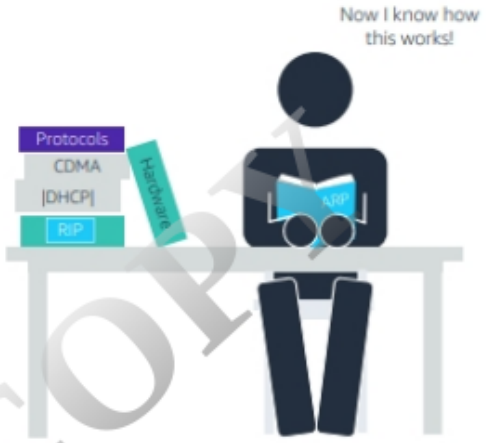
4

aws re/start

Network vulnerabilities

Reasons for vulnerabilities:

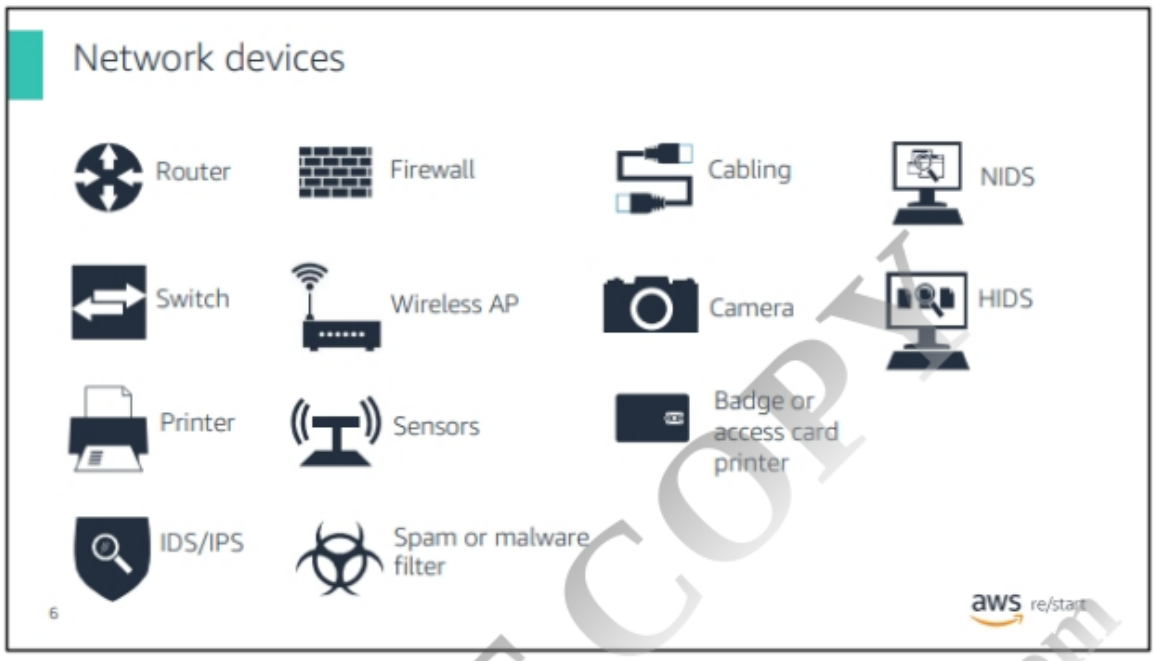
- Earlier protocols considered only dedicated networks and low-risk security events.
- Additional overhead for cryptography is unjustifiable.
- Ubiquitous access increases risk.
- Open standards allow creative exploitation.



5

aws re/start

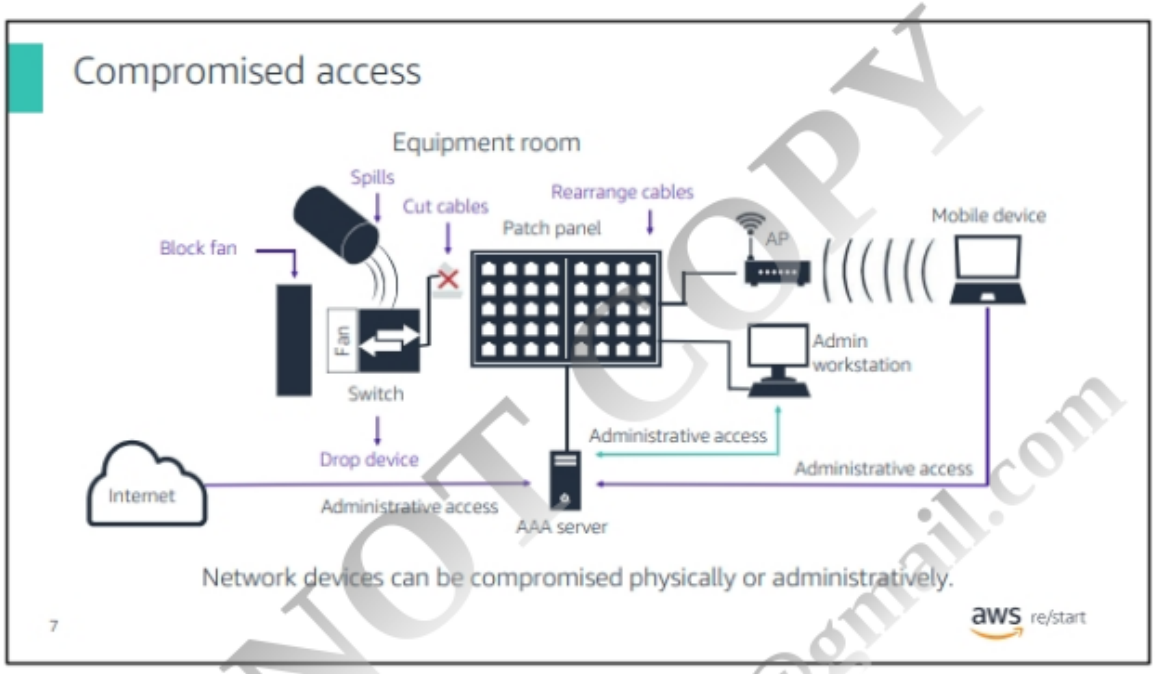
Address Resolution Protocol (ARP)



A network can contain many different types of devices. Evaluate each device to determine whether it is properly secured. Also evaluate *if* and *how* the device contributes to the security of the network.

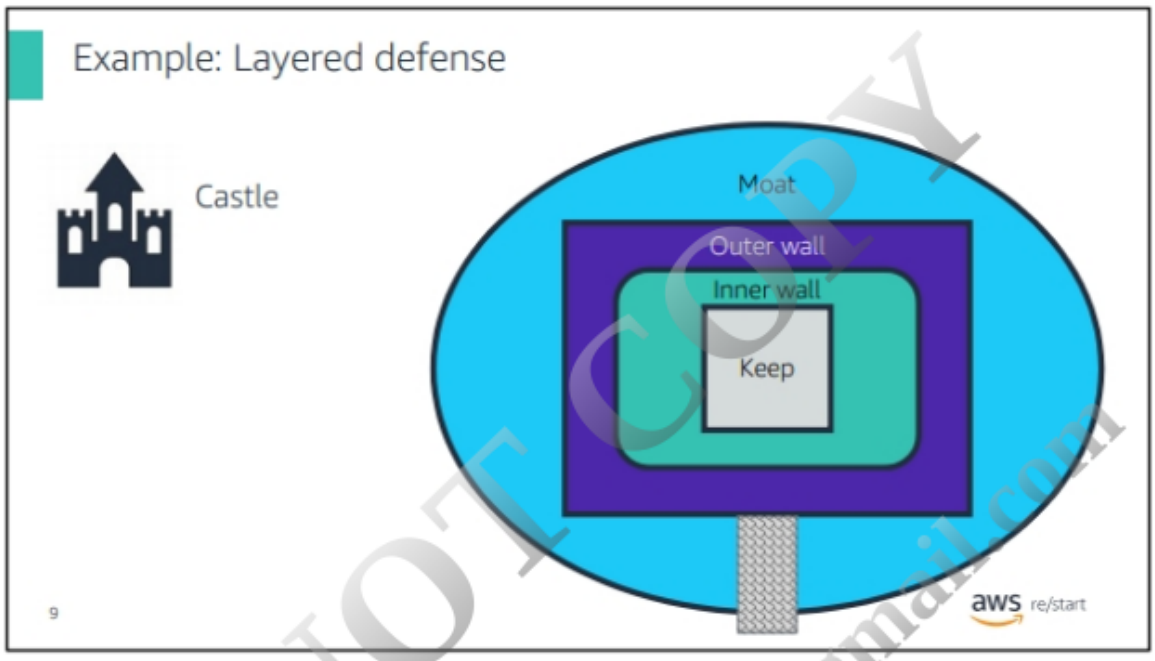
Common acronyms

- Intrusion detection system (IDS)
- Network-based intrusion detection system (NIDS)
- Host intrusion detection system (HIDS)
- Intrusion Prevention System (IPS)



To protect devices on a network, consider that they are vulnerable both physically and administratively.

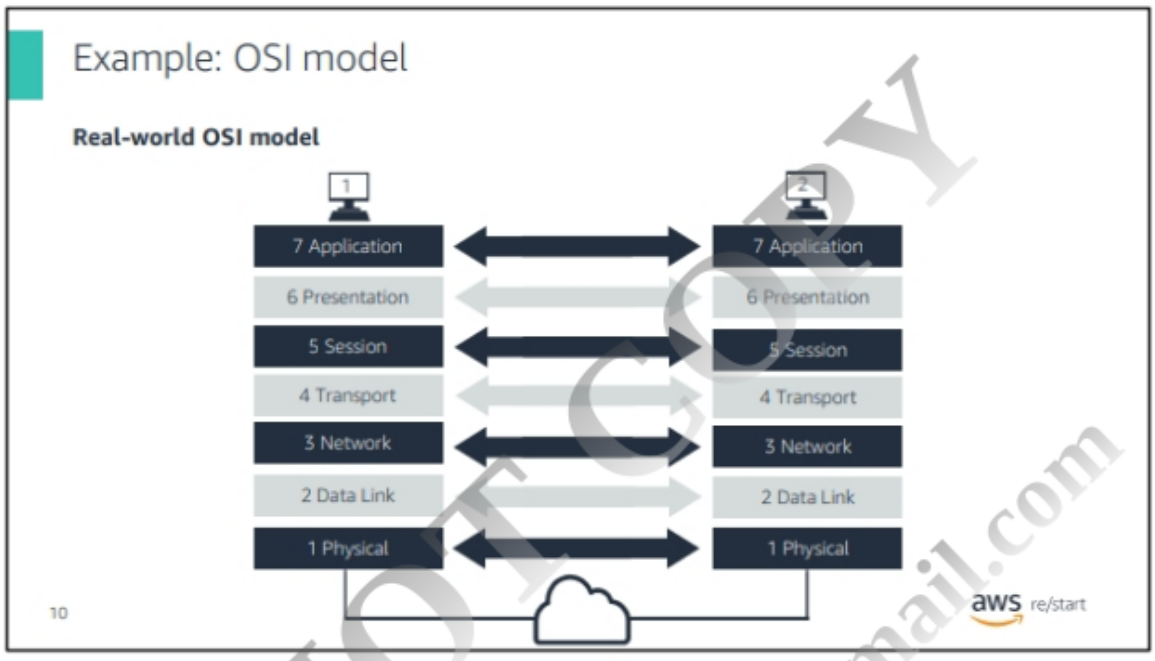
AAA server: Authentication, Authorization, and Accounting server



The best security strategy uses a defense in depth approach. *Defense in depth* means that you implement **several layers** of security that an outside party must penetrate to gain access to information or equipment.

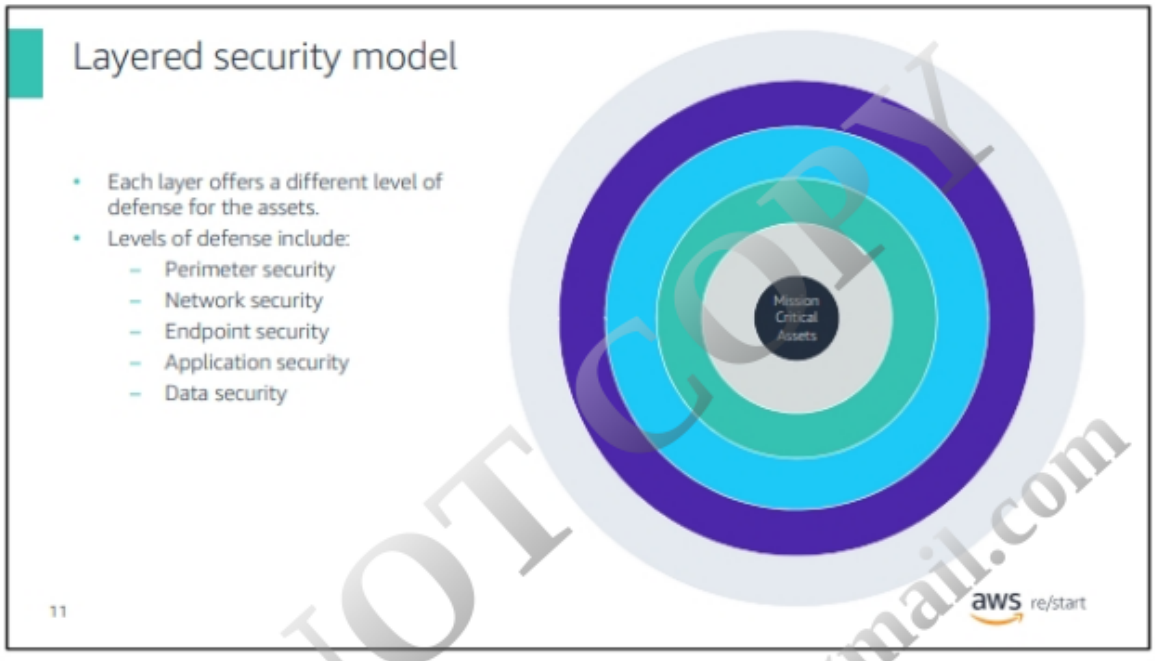
As an example, consider a castle. The castle might have a moat as its first level of defense. The castle also includes the outer wall, an inner wall, and finally, the keep. Each layer must be defeated in order for an attacking army to take the castle.

Similarly, companies implement many layers of defense on their systems to make the systems more difficult to breach. Each layer of the Open Systems Interconnection (OSI) model implements defenses or security controls that make it difficult for an outside party to penetrate that layer. Various forms of cryptography are used at various layers to protect stored data and network communications. Firewalls and IDS/IPS devices are used to detect and prevent penetration at the different layers. Protect each layer separately to make it as difficult as possible for an outside party to breach your defenses and gain access to your resources.



The OSI model provides another example of how security can be implemented in layers. Each of the model's layers provides an opportunity to implement a security solution:

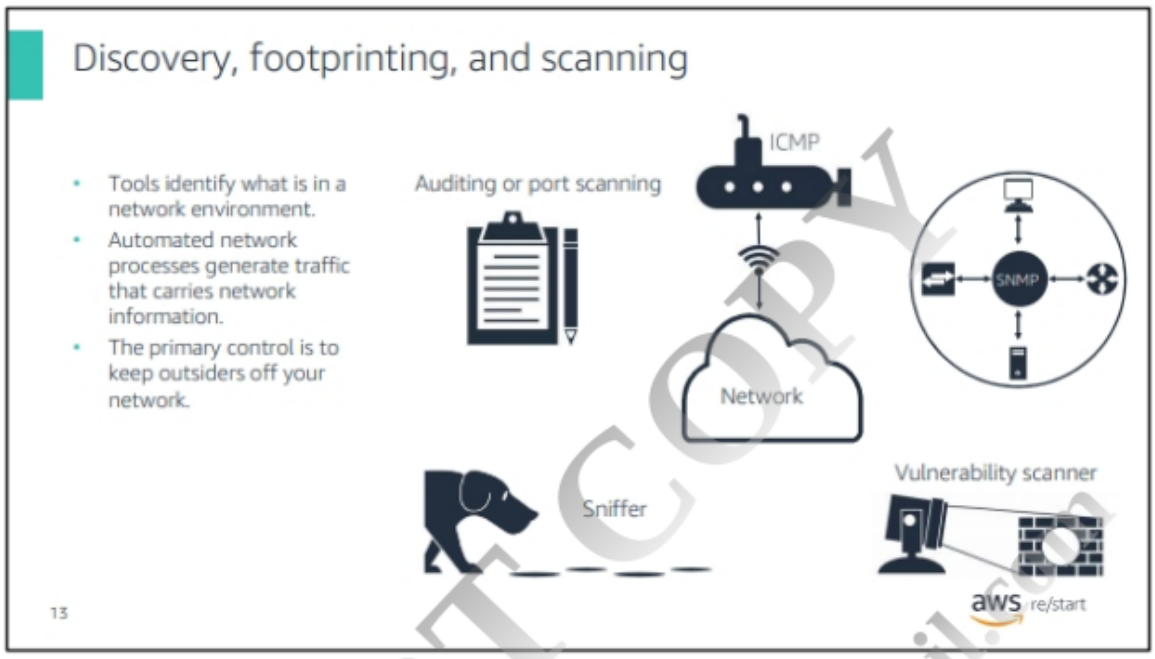
- **Physical** layer – Network devices and equipment are protected from physical access to keep intruders out.
- **Data Link** layer – Filters applied to network switches help prevent attacks based on media access control (MAC) addresses.
- **Network** and **Transport** layers – Implementing firewalls and access control lists (ACLs) help mitigate unauthorized access to internal systems.
- **Session** and **Presentation** layers – By using authentication and encryption methods, you can prevent unauthorized data accesses.
- **Application** layer – Solutions, such as virus scanners and an intrusion detection system (IDS), help protect applications.



Some examples of security layers include:

- Perimeter security
  - Perimeter firewalls
  - IDS or IPS
  - Secure the perimeter networks (also known as *DMZs, demilitarized zones*)
- Network security
  - Network Access Control (NAC)
  - Enterprise IDS or IPS
  - Web proxy content filtering
- Endpoint security
  - Desktop firewall
  - Host IDP or IPS
  - Content security (antivirus)
- Application security
  - Dynamic application testing
  - Web application firewall (WAF)
  - Database monitoring and scanning
- Data security
  - Identity and access management
  - Data wiping cleansing

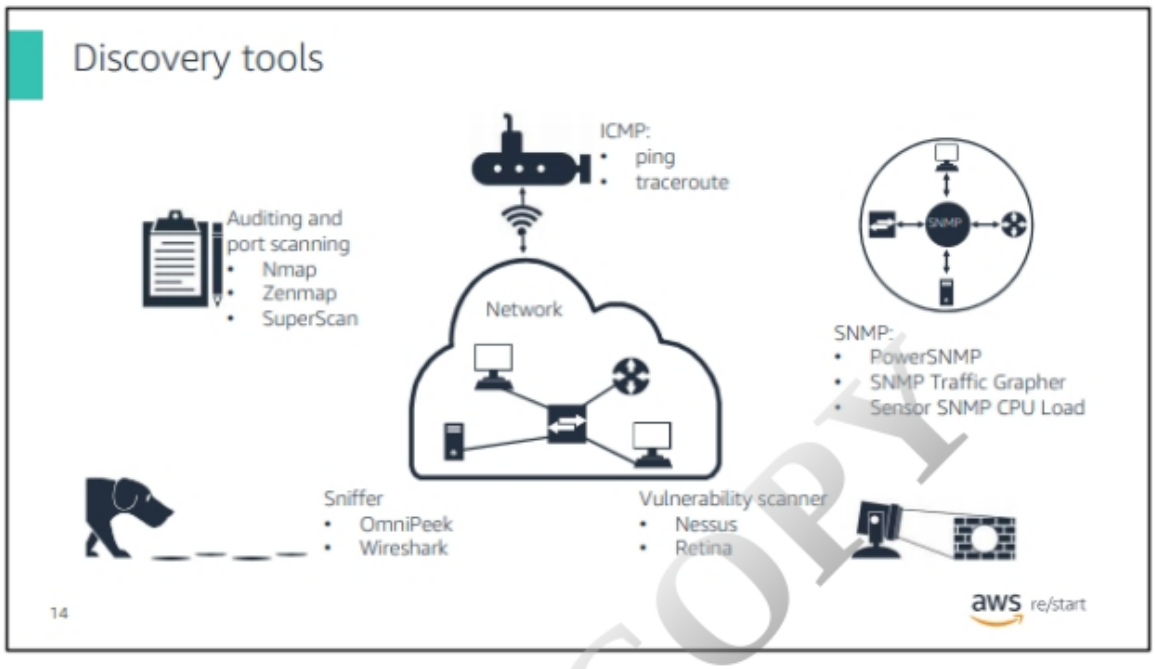
- Data loss prevention (DLP)



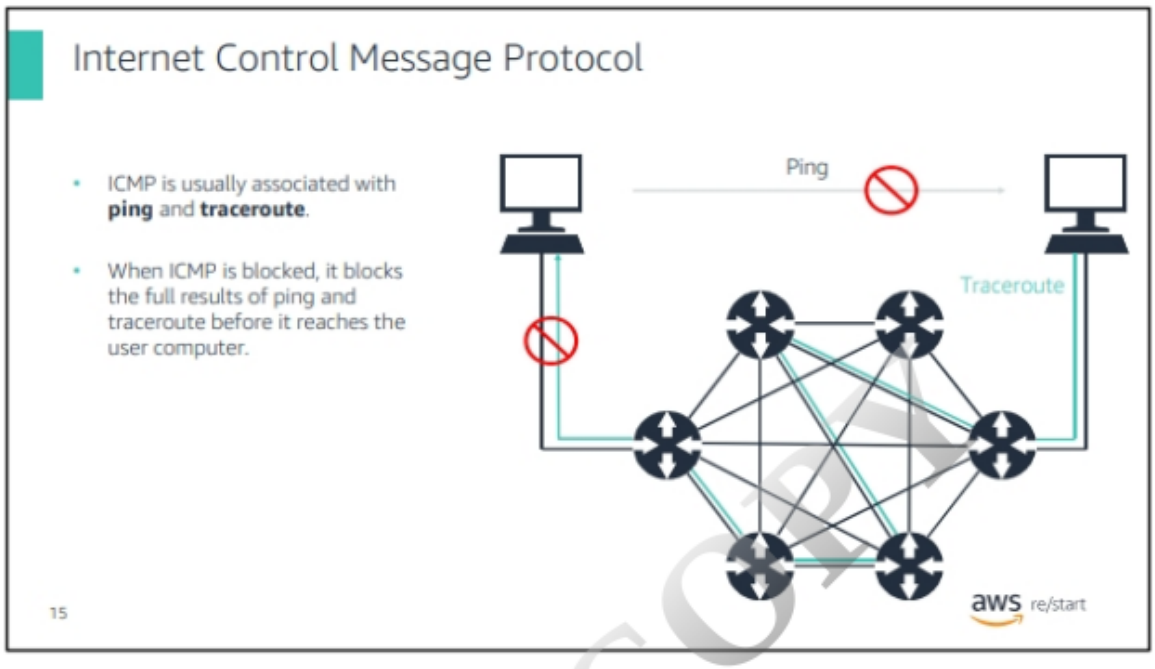
An outside party can discover a network environment using various tools and techniques, including:

- Footprinting – Collecting as much information about a system to penetrate it.
- Scanning – Searching for and detecting security weaknesses in a system.

It is important to understand what these tools are and be aware of the security risks that they present.

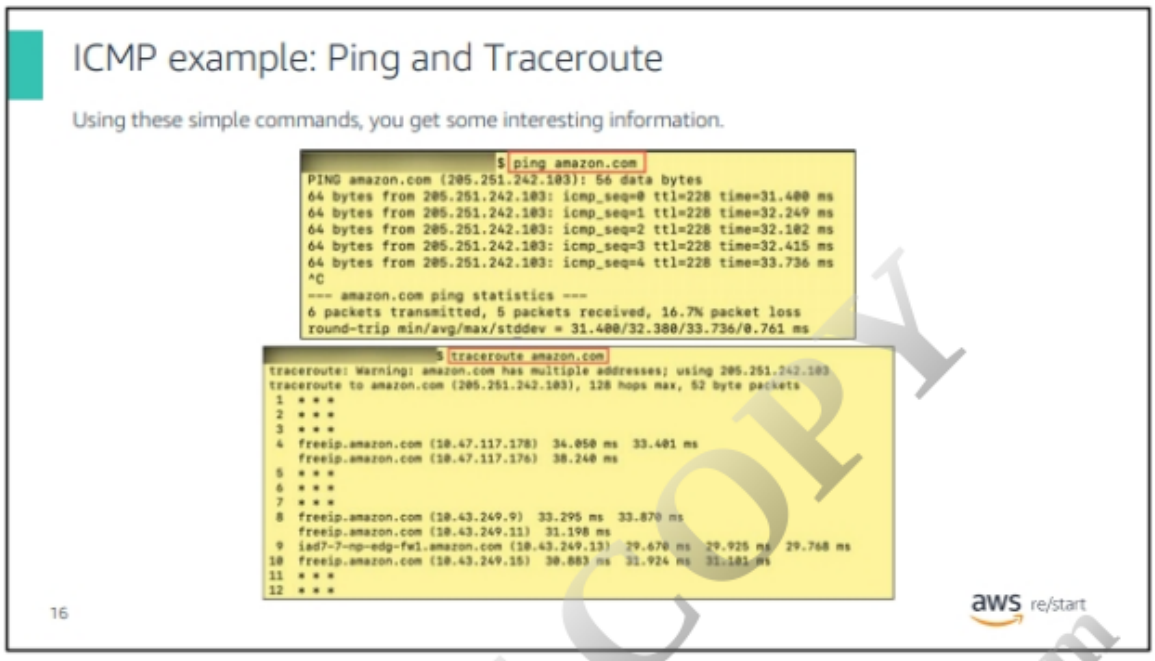


Here are some common tools that can be used to discover information about a network environment.



The most common network discovery tools use the Internet Control Message Protocol (ICMP). For example, the *ping* and *traceroute* commands use ICMP.

At minimum, consider restricting the full use of ICMP to protect against specific types of attacks, such as distributed denial of service (DDoS) attacks.



This example shows the output of a *ping* and *traceroute* of *amazon.com*.

Note how the output of a *traceroute* command enables you to:

- Get an idea of physical location by examining the names of the network devices. For example, **iad7** is an Amazon data center located in the USA. You can get additional information by implementing a WHOIS (Who is) on the IP addresses or names.
- See network path and response times.

With additional *ping* or other ICMP tools, you can build a fairly detailed blueprint of a network.

You can use the website for Internet Assigned Numbers Authority (IANA) to find information about the owner of a public IP address. To do so, follow these steps:

1. In a browser, navigate to **iana.org**.
   IANA is the organization that is responsible for the assignment of IP addresses worldwide.
2. In the **Number Resources** section, select the **IP Addresses & AS Numbers** link.
   This page provides links to the five Regional Internet Registries (RIRs). Each RIR is responsible for managing IP addresses in a particular region of the world.
3. Select the link to visit the **American Region of Internet Numbers (ARIN)** site.
   ARIN is responsible for administering numbers in North America. If you are operating from inside North America, it is probable that the IP address you are researching is in North America. If you are not in North America, and if the organization you are pinging is in the United States or Canada, use the ARIN site as a starting point for your search.
4. In the search box (which is in the upper-right area of the ARIN site), enter the IP address that you want to investigate, and choose **Search**.
   The results of your search are displayed. Results show your IP address as part of a network block of IP addresses. The block is expected for an organization, especially for a large organization.

Information about the owner of the IP address is included in the lower section of the page.

Nmap

Nmap is a network mapper tool that uses ICMP and other protocols to gather and present network data.

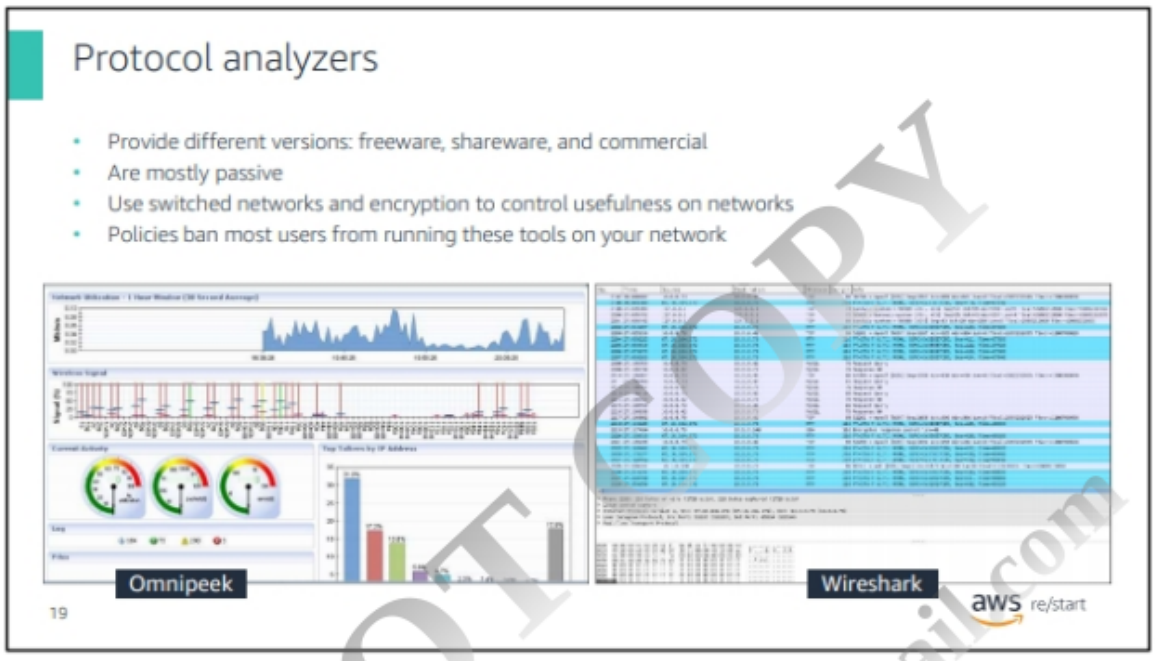
```
C:\nmap-3.81>nmap.exe -O 192.168.1.107 -p 25,80,135,137,139,445

Nmap for Windows v3.81
Original version (WinPCap is required) : http://www.insecure.org/nmap
This version (works without WinPCap)   : http://packetstuff.com
Compiled with Packet Sniffer SDK v2.3  : http://microolap.com/pssdk


Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2006-05-28 13:23 Eastern
Daylight Time
Interesting ports on W2KLAB (192.168.1.107):
PORT    STATE  SERVICE
25/tcp  open   smtp
80/tcp  open   http
135/tcp open   nsrpc
137/tcp closed netbios-ns
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 00:0C:29:D0:16:54 (VMware)
Device type: general purpose
Running: Microsoft Windows 95/98/ME:NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or Advan
ced Server, or Windows XP, Microsoft Windows 2000 SP3

Nmap finished: 1 IP address (1 host up) scanned in 4.500 seconds

C:\nmap-3.81>
```

18

aws re/start

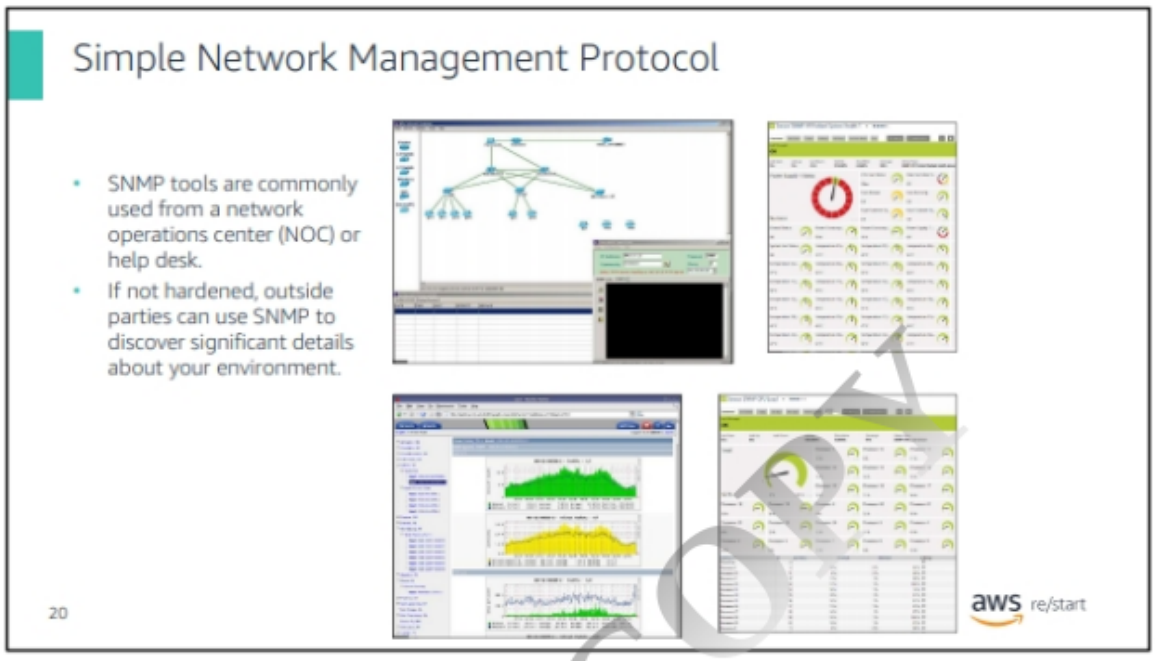
Other tools are available for gathering information about a network, such as:

- **Nmap** – Network mapper that is available for Linux, Microsoft Windows, and macOS
- **Zenmap** – GUI-based version of Nmap
- **SuperScan** – Tool for users of Microsoft Windows

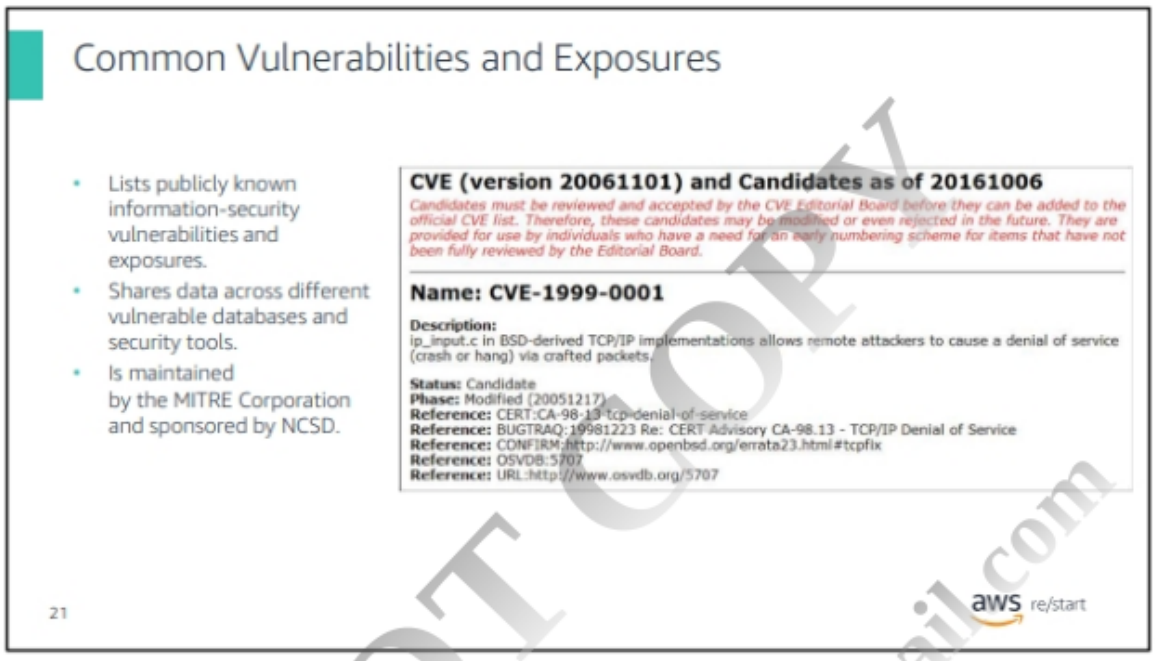


Protocol analyzers, which are also known as *sniffers*, passively watch and store all traffic that goes through a network. The analyzers then format the information that they collect in a human-readable form. Any traffic that is not encrypted can be reassembled into a readable format. You can review the stored packet captures at a later time and share them with others.

The screen captures show Omnipeek and Wireshark protocol analyzers.



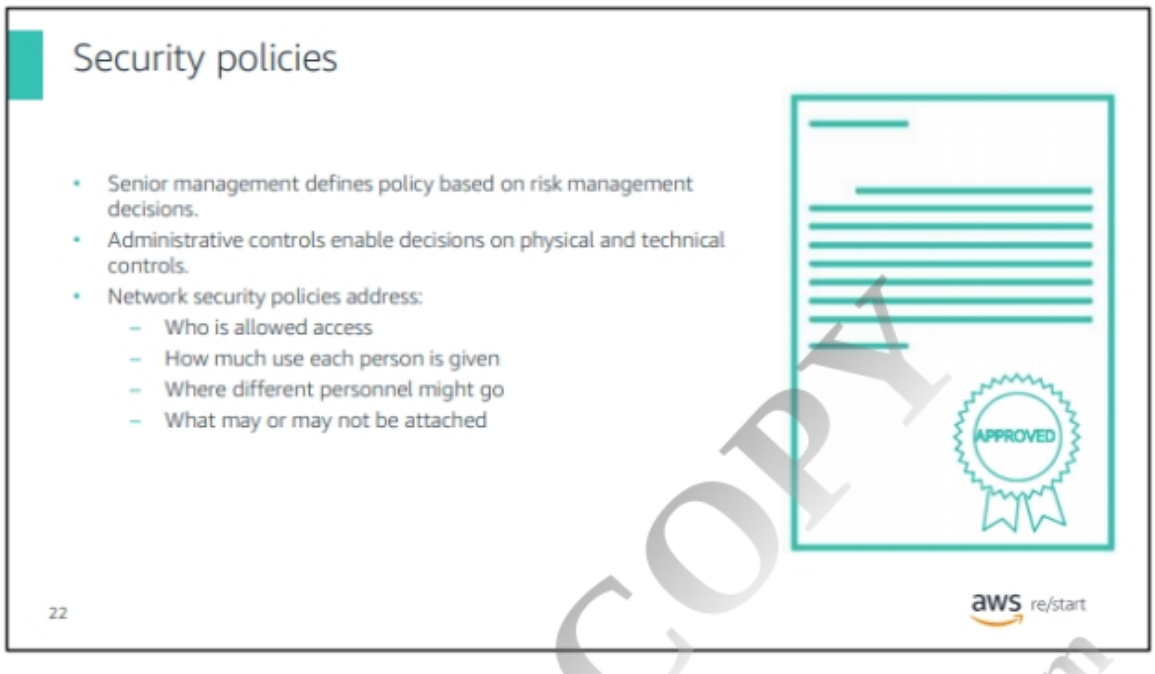
The Simple Network Management Protocol (SNMP) is another mechanism that can be used to discover network traffic. Thus, you must carefully evaluate its availability and use to prevent security attacks.



The Common Vulnerabilities and Exposures (CVE) website is an online resource that lists publicly disclosed cybersecurity vulnerabilities. It is maintained by the MITRE Corporation and is sponsored by the National Cyber Security Division (NCSD). Some scanning tools may point to particular CVEs.

Additional resource

- Cyberthreat maps
  - Have you wondered what the current cyberthreat battleground is like? A number of sites offer a live view of cyberattacks that are happening around the world as they occur in real time.
  - An example is the Cyberthreat Real-time Map.



Use a policy as an administrative control to enforce security measures in your organization. Implementing the proper security policies is vital to an organization's health and existence.

Key takeaways from this lesson include:

- The layered security model provides an effect method of protecting the resources on a network.
- Consider restricting the full use of protocols such as ICMP and SNMP to protect against specific types of attacks that exploit the protocols.
- An organization must implement security policies to protect its assets.