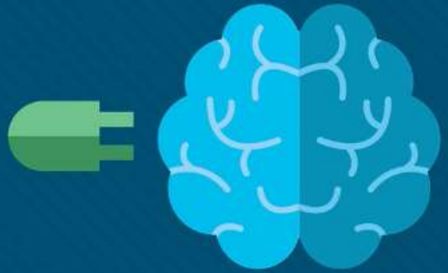
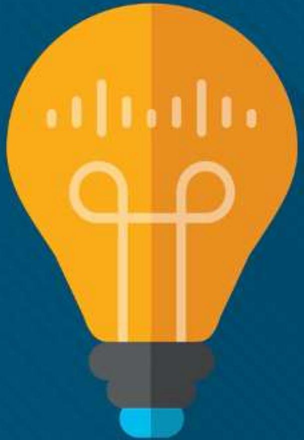
Module 3: Mitigating Threats





Networking Security v1.0
(NETSEC)

Module Objectives

Module Title: Mitigating Threats

Module Objective: Explain tools and procedures to mitigate the effects of malware and common network attacks.

Topic Title	Topic Objective
Defending the Network	Describe methods and resources to protect the network.
Network Security Policies	Explain several types of network security policies.
Security Tools, Platforms, and Services	Explain the purpose of security platforms.
Mitigating Common Network Attacks	Describe the techniques used to mitigate common network attacks.
Cisco Network Foundation Protection Framework	Explain how to secure the three functional areas of Cisco routers and switches.

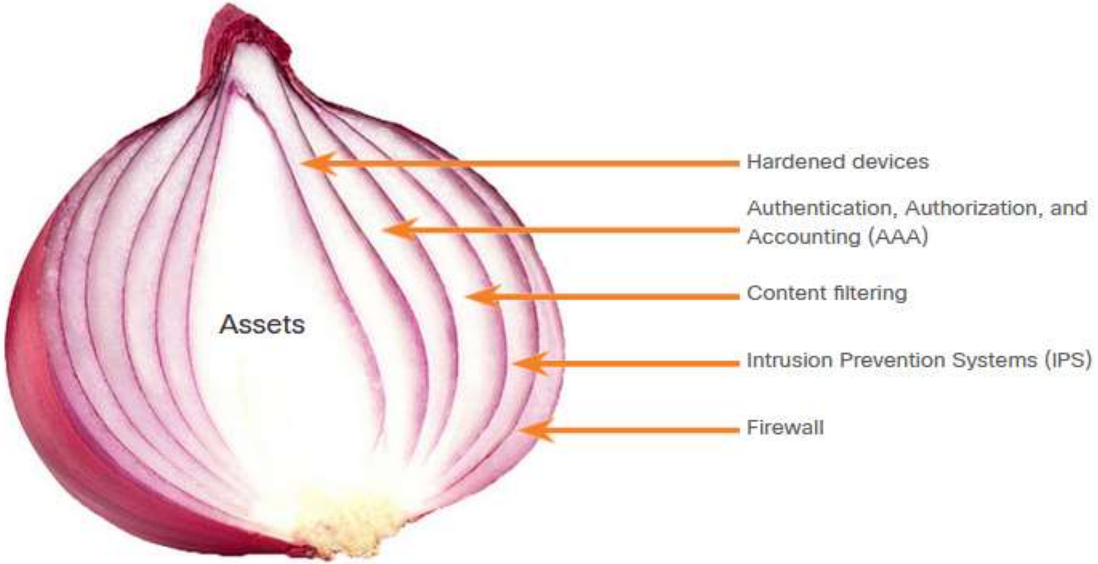
3.3 Security Tools, Platforms, and Services

Security Tools, Platforms, and Services

The Security Onion and The Security Artichoke

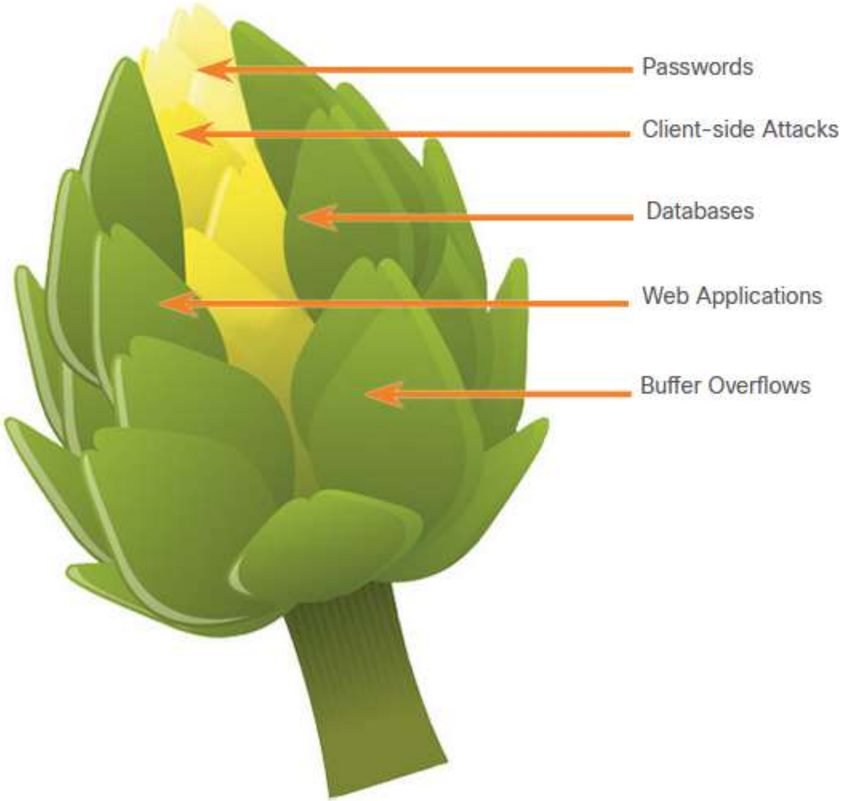
A common analogy used to describe a defense-in-depth approach is called “the security onion.” A threat actor would have to peel away at a network’s defenses layer by layer in a manner similar to peeling an onion. Only after penetrating each layer would the threat actor reach the target data or system.

Note: The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.


Assets
Hardened devices
Authentication, Authorization, and Accounting (AAA)
Content filtering
Intrusion Prevention Systems (IPS)
Firewall

The Security Onion and The Security Artichoke (Cont.)

The changing landscape of networking, such as the evolution of borderless networks, has changed this analogy to the “security artichoke”, which benefits threat actors because they no longer have to peel away each layer. They only need to remove certain “artichoke leaves.” The threat actor peels away the security armor along the perimeter to get to the “heart” of the enterprise.



Security Testing Tools

Ethical hacking involves using different types of tools to test the network and end devices to validate the security of the network. Penetration testing uses hacker techniques and tools to evaluate the strength of network security measures. Cybersecurity personnel must also know how to use these tools when performing network penetration tests.

Categories of Tools	Description
password crackers	Passwords are the most vulnerable security threat. Password cracking tools are often referred to as password recovery tools and can be used to crack or recover the password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password and access the system. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
wireless hacking tools	Wireless networks are more susceptible to network security threats. Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.

Security Testing Tools (Cont.)

Categories of Tools	Description
network scanning and hacking tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
packet crafting tools	Packet crafting tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
packet sniffers	Packet sniffer tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.
rootkit detectors	A rootkit detector is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.
fuzzers to search vulnerabilities	Fuzzers are tools used by threat actors when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
forensic tools	White hat hackers use forensic tools to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.

Security Testing Tools (Cont.)

Categories of Tools	Description
debuggers	Debugger tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.
hacking operating systems	Hacking operating systems are specially designed operating systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, SELinux, Knoppix, Parrot OS, and BackBox Linux.
encryption tools	These tools safeguard the contents of an organization's data when it is stored or transmitted. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Examples of these tools include VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN, and Stunnel.
vulnerability exploitation tools	These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit, and Netsparker.
vulnerability scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of these tools include Nipper, Securia PSI, Core Impact, Nessus, SAINT, and Open VAS.

Data Security Platforms

Data Security Platforms (DSP) are an integrated security solution that combines traditionally independent tools into a suite of tools that are made to work together. Security tools that protect and monitor networks are often made by different vendors. It can be difficult to integrate these tools in such a way that a single view of network security can be achieved.

One such DSP is the Helix platform from FireEye. FireEye Helix is a cloud-based security operations platform that enables organizations to integrate many security functionalities into a single platform. Helix provides event management, network behavior analytics, advanced threat detection, and incident security orchestration, automation, and response (SOAR) for response to threats as they are detected.

FIREEYE™

Data Security Platforms (Cont.)

Another integrated DSP is Cisco SecureX. The Cisco Secure portfolio consists of a broad set of technologies that function as a team - providing interoperability with the security infrastructure, including third-party technologies. This results in unified visibility, automation, and stronger defenses. The Cisco SecureX platform works with diverse products that combine to safeguard your network, users and endpoints, cloud edge, and applications. SecureX functionality is built in to a large and diverse portfolio of Cisco security products including next-generation firewalls, VPN, network analytics, identity service engine, advanced malware protection (AMP), and many other systems that work to secure all aspects of a network. SecureX also integrates a range of third-party security tools.

Security Tools, Platforms, and Services

Security Services

Threat intelligence and security services allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOC), and mitigation techniques. As threats emerge, threat intelligence services create and distribute firewall rules and IOCs to the devices that have subscribed to the service.

One such service is the Cisco Talos Threat Intelligence Group. Talos is one of the largest commercial threat intelligence teams in the world. The goal of Talos is to help protect enterprise users, data, and infrastructure from active adversaries. The Talos team collects information about active, existing, and emerging threats. Talos then provides comprehensive protection against these attacks and malware to its subscribers.

Cisco Security products can use Talos threat intelligence in real time to provide fast and effective security solutions.

Talos
Software
Vulnerability Information
Reputation Center
Library
Support
Careers
Blog
Podcasts
About
Reputation Lookup
Intelligence and response specialists at your side
INTRODUCING
Cisco Talos Incident Response

3.4 Mitigating Common Network Attacks

Defending the Network

Constant vigilance and ongoing education are required to defend your network against attack. The following are best practices for securing a network:

- Develop a written security policy for the company.
- Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- Control physical access to systems.
- Use strong passwords and change them often.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software such as firewalls, IPSs, virtual private network (VPN) devices, antivirus software, and content filtering.
- Perform backups and test the backed-up files on a regular basis.
- Shut down unnecessary services and ports.
- Keep patches up-to-date by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.
- Perform security audits to test the network.

Mitigating Malware

Malware, including viruses, worms, and Trojan horses, can cause serious problems on networks and end devices. Network administrators have several means of mitigating these attacks.

Antivirus software helps prevent hosts from getting infected and spreading malicious code. Several companies that create antivirus software, such as Symantec, McAfee, and Trend Micro. Antivirus products have update automation options so that new virus definitions and new software updates can be downloaded automatically or on demand. This practice is the most critical requirement for keeping a network free of viruses and should be formalized in a network security policy.

These products are installed on computers and servers to detect and eliminate viruses. However, they do not prevent viruses from entering the network. Another way to mitigate malware threats is to prevent malware files from entering the network at all. Security devices at the network perimeter can identify known malware files based on their indictors of compromise. The files can be removed from the incoming data stream before they can cause an incident.

Mitigating Worms

Worms are more network-based than viruses. Worm mitigation requires diligence and coordination on the part of network security professionals. The response to a worm attack can be broken down into four phases: containment, inoculation, quarantine, and treatment.

Phase	Response
1. Containment	The containment phase involves limiting the spread of a worm infection to areas of the network that are already affected. This requires compartmentalization and segmentation of the network to slow down or stop the worm and to prevent currently infected hosts from targeting and infecting other systems. Containment requires using both outgoing and incoming ACLs on routers and firewalls at control points within the network.
2. Inoculation	The inoculation phase runs parallel to or subsequent to the containment phase. During the inoculation phase, all uninfected systems are patched with the appropriate vendor patch. The inoculation process further deprives the worm of available targets.
3. Quarantine	The quarantine phase involves tracking down and identifying infected machines within the contained areas and disconnecting, blocking, or removing them. This isolates these systems appropriately for the treatment phase.
4. Treatment	The treatment phase involves actively disinfecting infected systems. This can involve terminating the worm process, removing modified files or system settings that the worm introduced, and patching the vulnerability the worm used to exploit the system. Alternatively, in more severe cases, the system may need to be reinstalled to ensure that the worm and its by-products are removed.

Mitigating Reconnaissance Attacks

Reconnaissance attacks are typically the precursor to other attacks that are designed to gain unauthorized access to a network or disrupt network functionality. You can detect when a reconnaissance attack is underway by receiving notifications from preconfigured alarms. These alarms are triggered when certain parameters are exceeded, such as the number of ICMP requests per second. Reconnaissance attacks can be mitigated in several ways, including the following:

- Implementing authentication to ensure proper access.
- Using encryption to render packet sniffer attacks useless.
- Using anti-sniffer tools to detect packet sniffer attacks.
- Implementing a switched infrastructure.
- Using a firewall and IPS.

It is impossible to mitigate port scanning. Using an IPS and firewall can limit the information that can be discovered with a port scanner. Ping sweeps can be stopped if ICMP echo and echo-reply are turned off on edge routers; however, when these services are turned off, network diagnostic data is lost.

Mitigating Access Attacks

Several techniques are available for mitigating access attacks, including strong password security, principle of minimum trust, cryptography, and applying operating system and application patches. A surprising number of access attacks are carried out through simple password guessing or brute-force dictionary attacks against passwords. To defend against this, create and enforce a strong authentication policy which includes:

- **Use strong passwords** - Strong passwords are at least eight characters and contain uppercase letters, lowercase letters, numbers, and special characters.
- **Disable accounts after a specified number of unsuccessful logins has occurred** - This practice helps to prevent continuous password attempts.

Use encryption for remote access to a network and routing protocol traffic to reduce the possibility of man-in-the-middle attacks. Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person. Multifactor authentication (MFA) has become increasingly common.

Mitigating DoS Attacks

One of the first signs of a DoS attack is a large number of user complaints about unavailable resources or unusually slow network performance. A network utilization graph showing unusual activity could indicate a DoS attack. To minimize the number of attacks, a network utilization software package should be running at all times.

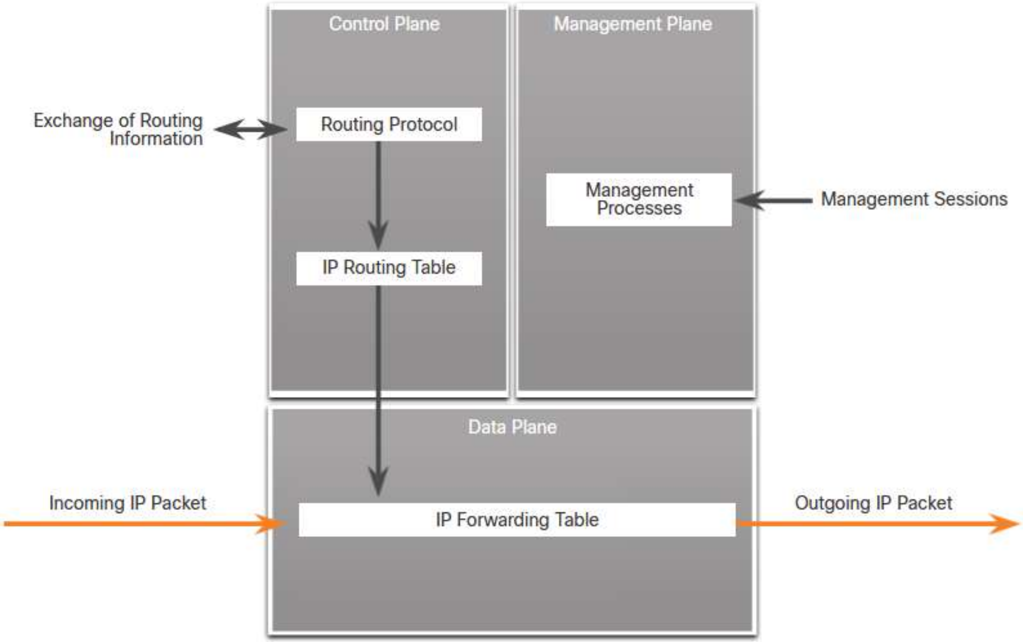
Historically, many DoS attacks were sourced from spoofed addresses. Cisco routers and switches support many antispoofing technologies, such as port security, Dynamic Host Configuration Protocol (DHCP) snooping, IP Source Guard, Dynamic Address Resolution Protocol (ARP) Inspection, and access control lists (ACLs).

3.5 Cisco Network Foundation Protection Framework

NFP Framework

The Cisco Network Foundation Protection (NFP) framework provides comprehensive guidelines for protecting the network infrastructure. These guidelines form the foundation for continuous delivery of service. NFP logically divides routers and switches into three functional areas:

- **Control plane** - Responsible for routing data correctly.
- **Management plane** - Responsible for managing network elements.
- **Data plane** - Responsible for forwarding data.



Securing the Control Plane

Control plane traffic consists of device-generated packets required for the operation of the network itself. Control plane security can be implemented using the following features:

- **Routing protocol authentication** - Routing protocol authentication, or neighbor authentication, prevents a router from accepting fraudulent routing updates.
- **Control Plane Policing (CoPP)** - CoPP is a Cisco IOS feature that lets users control the flow of traffic that is handled by the route processor of a network device.
- **AutoSecure** - This can lock down the management plane functions and the forwarding plane services and functions of a router.

CoPP is designed to prevent unnecessary traffic from overwhelming the route processor. The CoPP feature treats the control plane as a separate entity with its own ingress (input) and egress (output) ports. A set of rules can be established and associated with the ingress and egress ports of the control plane.

Securing the Management Plane

Management plane traffic is generated either by network devices or network management stations using processes and protocols such as Telnet, SSH, and TFTP, etc. The management plane is a very attractive target to hackers.

Management plane security can be implemented using the following features:

- **Login and password policy** - Restricts device accessibility.
- **Present legal notification** - Displays legal notices.
- **Ensure the confidentiality of data** - Protects locally stored sensitive data from being viewed or copied. Uses management protocols with strong authentication to mitigate confidentiality attacks aimed at exposing passwords and device configurations.
- **Role-based access control (RBAC)** - Ensures access is only granted to authenticated users, groups, and services.
- **Authorize actions** - Restricts the actions and views that are permitted by any particular user, group, or service.
- **Enable management access reporting** - Logs and accounts for all access.

Securing the Data Plane

Data plane traffic consists mostly of user packets being forwarded through the router. Data plane security can be implemented using ACLs, antispoofing mechanisms, and Layer 2 security features. ACLs are used to secure the data plane in a variety of ways:

- Blocking unwanted traffic or users
- Reducing the chance of DoS
- Mitigating spoofing attacks.
- Providing bandwidth control
- Classifying traffic to protect the Management and Control planes

Cisco Catalyst switches can use integrated features to help secure the Layer 2 infrastructure. The following Layer 2 security tools are integrated into the Cisco Catalyst switches:

- Port security
- DHCP snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard

3.6 Mitigating Threats Summary

What Did I Learn in this Module?

- Network security professionals are responsible for maintaining data assurance for an organization and ensuring the integrity and confidentiality of information.
- There are several network security organizations to keep you informed, including SANS, Mitre, FIRST, SecurityNewsWire, ISC2, and CIS.
- There are 14 network security domains specified by the ISO/IEC serve as a common basis for developing organizational security standards.
- The Security Onion and Security Artichoke provide analogies for understanding approaches to network security.
- Penetration tools are used by security personnel to validate network security.
- Threat intelligence services, such as Cisco Talos, allow the exchange of the latest threat information.
- Various tools, software, and services help with the mitigation of malware, reconnaissance, DoS and address spoofing attacks.
- The Cisco Network Foundation Protection framework (CoPP) provides comprehensive guidelines for protecting the network infrastructure by addressing security at the control plane, management plane, and data plane (forwarding plane) of network devices.
- The following Layer 2 security tools are integrated into the Cisco Catalyst switches: port security, DHCP snooping, DAI, and IPSG.

New Terms and Commands

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Security Operations (SecOps) Manager
- SysAdmin, Audit, Network, Security (SANS) Institute
- Mitre Corporation
- common vulnerabilities and exposures (CVE)

  Forum of Incident Response and Security Teams (FIRST)
- International Information Systems Security Certification Consortium (ISC^2)
- The Center for Internet Security (CIS)
- Global Information Assurance Certification (GIAC)
- Information Systems Audit and Control Association (ISACA)
- The Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam
- CIA triad
- security onion
- security artichoke
- password crackers
- packet crafting tools
- packet sniffers
- rootkit detectors
- hacking operating systems
- Data Security Platforms (DSP)
- threat intelligence and security services
- Cisco Talos Threat Intelligence Group
- multifactor authentication (MFA)
- Cisco Network Foundation Protection (NFP) framework
- control plane
- management plane
- data plane (forwarding plane)
- Control Plane Policing (CoPP)
- port security
- DHCP snooping
- Dynamic ARP Inspection (DAI)

New Terms and Commands (Cont.)

- IP Source Guard (IPSG)