Module 19: Technologies and Protocols

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Technologies and Protocols

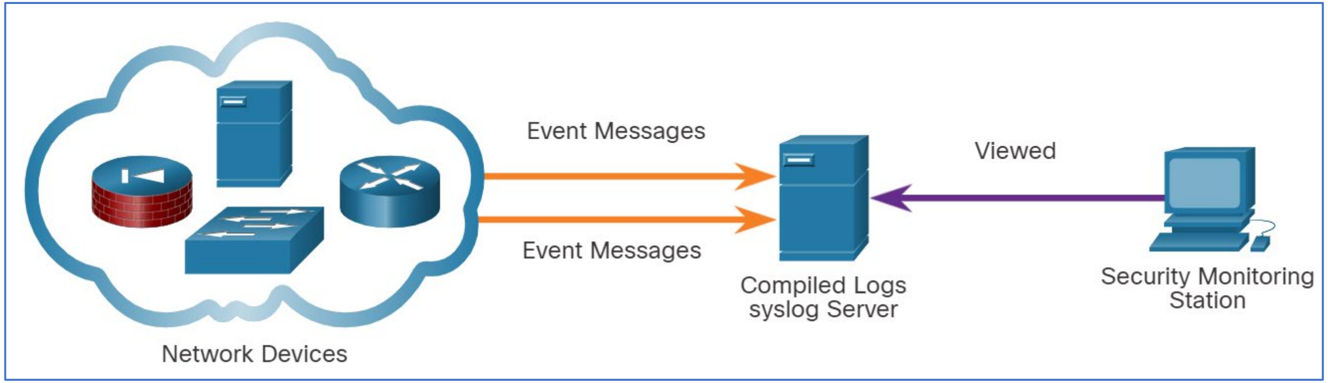
Module Objective: Explain how security technologies affect security monitoring.

Topic Title	Topic Objective
Monitoring Common Protocols	Explain the behavior of common network protocols in the context of security monitoring.
Security Technologies	Explain how security technologies affect the ability to monitor common network protocols.

19.1 Monitoring Common Protocols

Syslog and NTP

- The syslog standard is used for logging event messages from network devices and endpoints.
- The standard allows for a system-neutral means of transmitting, storing, and analyzing messages.
- Many types of devices from many different vendors can use syslog to send log entries to central servers that run a syslog daemon.
- This centralization of log collection helps to make security monitoring practical.
- Servers that run syslog typically listen on UDP port 514.

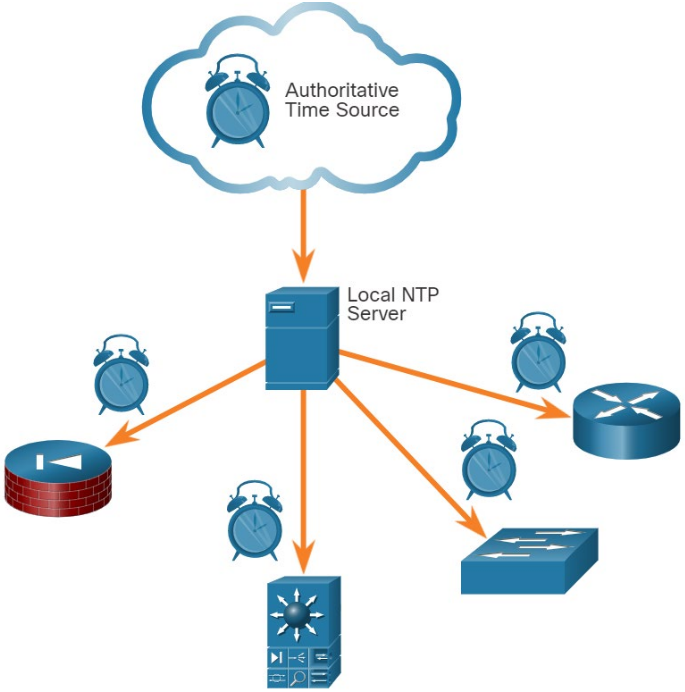


Syslog and NTP (Cont.)

- Because syslog is so important to security monitoring, syslog servers may be a target for threat actors.
- Some exploits, such as those involving data exfiltration, can take a long time to complete because the ways in which data is secretly stolen from the network can be very slow.
- Threat attackers may try to hide the fact that exfiltration is occurring. They attack syslog servers that contain the information that could lead to detection of the exploit.
- Hackers may attempt to block the transfer of data from syslog clients to servers.
- They may tamper with or destroy log data, or the software that creates and transmits log messages.
- The next generation (ng) syslog implementation, (syslog-ng), offers enhancements that can help prevent some of the exploits that target syslog.

NTP

- Syslog messages are usually timestamped.
- This allows messages from different sources to be organized by time to provide a view of network communication processes.
- Because the messages can come from many devices, it is important that the devices share a consistent timeclock.
- One way that this can be achieved is for the devices to use Network Time Protocol (NTP).
- NTP uses a hierarchy of authoritative time sources to share time information between devices on the network.
- NTP operates on UDP port 123.



Monitoring Common Protocols
NTP (Cont.)

- Because events that are connected to an exploit can leave traces across every network device on their path to the target system, timestamps are essential for detection.
- Threat actors may attempt to attack the NTP infrastructure to corrupt time information used to correlate logged network events.
- This can serve to obfuscate traces of ongoing exploits.
- In addition, threat actors have been known to use NTP systems to direct DDoS attacks through vulnerabilities in client or server software.
- While these attacks do not necessarily result in corrupted security monitoring data, they can disrupt network availability.

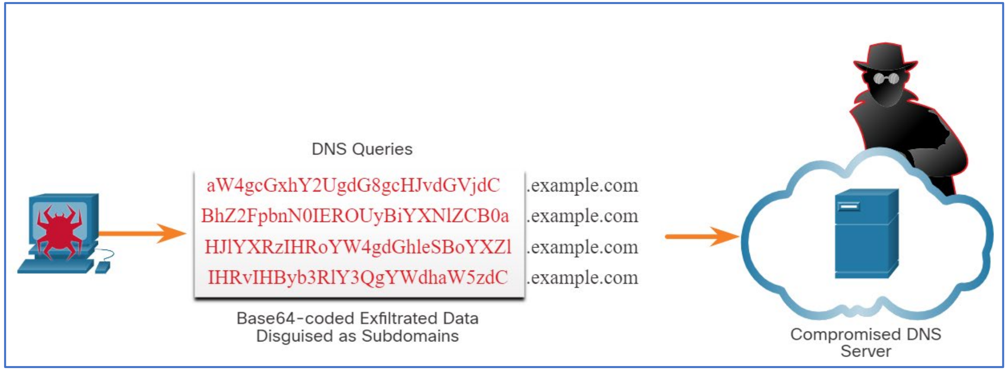
Monitoring Common Protocols
DNS

- Domain Name Service (DNS) is used by millions of people daily.
- Many organizations have less stringent policies in place to protect against DNS-based threats than to protect against other types of exploits.
- Attackers have recognized this and commonly encapsulate different network protocols within DNS to evade security devices.
- DNS is now used by many types of malware.
- Some varieties of malware use DNS to communicate with command-and-control (CnC) servers and to exfiltrate data in traffic disguised as normal DNS queries.
- Various types of encoding, such as Base64, 8-bit binary, and Hex can be used to camouflage the data and evade basic data loss prevention (DLP) measures.

Monitoring Common Protocols

DNS (Cont.)

- For example, malware could encode stolen data as the subdomain portion of a DNS lookup for a domain where the nameserver is under control of an attacker.
- A DNS lookup for ‘long-string-of-exfiltrated-data.example.com’ would be forwarded to the nameserver of example.com, which would record ‘long-string-of-exfiltrated-data’ and reply back to the malware with a coded response.
- The exfiltrated data is the encoded text shown in the box.
- The threat actor collects this encoded data, decodes and combines it, and now has access to an entire data file, such as a username/password database.



DNS Queries

```
aW4gcGxhY2UgdG8gcHJvdGVjdC  .example.com
BhZ2FpbnN0IEROUyBiYXNlZCB0a .example.com
HJlYXRzIHRoYW4gdGhleSBoYXZl .example.com
IHRvIHByb3RlY3QgYWdhaW5zdC  .example.com
```

Base64-coded Exfiltrated Data
Disguised as Subdomains

DNS (Cont.)

- It is likely that the subdomain part of such requests would be much longer than usual requests.
- Cyber analysts can use the distribution of the lengths of subdomains within DNS requests to construct a mathematical model that describes normality.
- They can then use this to compare their observations and identify an abuse of the DNS query process.
- DNS queries for randomly generated domain names, or extremely long random-appearing subdomains, should be considered suspicious, especially if their occurrence spikes dramatically on the network.
- DNS proxy logs can be analyzed to detect these conditions. Alternatively, services such as the Cisco Umbrella passive DNS service can be used to block requests to suspected CnC and exploit domains.

Monitoring Common Protocols

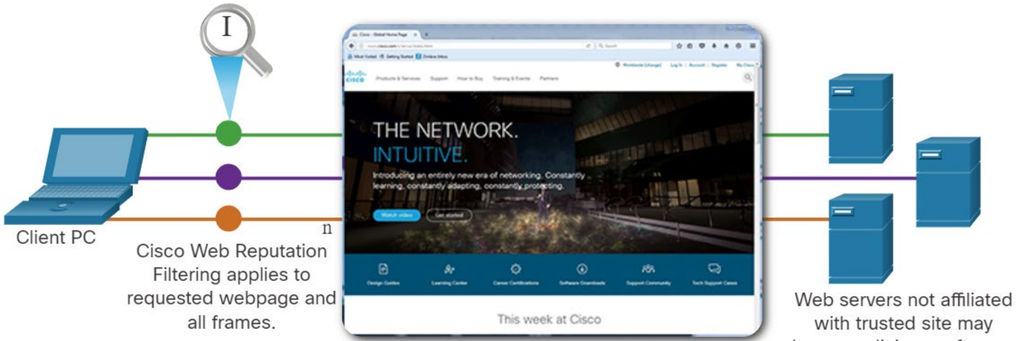
HTTP and HTTPS

- Hypertext Transfer Protocol (HTTP) is the backbone protocol of the World Wide Web.
- However, all information carried in HTTP is transmitted in plaintext from the source computer to the destination on the internet.
- HTTP does not protect data from alteration or interception by malicious parties, which is a serious threat to privacy, identity, and information security.
- All browsing activity should be considered at risk.

Monitoring Common Protocols

HTTP and HTTPS (Cont.)

- A common exploit of HTTP is called iFrame (inline frame) injection.
- In iFrame injection, a threat actor compromises a webserver and plants malicious code which creates an invisible iFrame on a commonly visited webpage.
- When the iFrame loads, malware is downloaded, frequently from a different URL than the webpage that contains the iFrame code.
- Network security services, such as Cisco Web Reputation filtering, can detect when a website attempts to send content from an untrusted website to the host, even when sent from an iFrame.


I
n
THE NETWORK.
INTUITIVE.
Introducing an entirely new era of networking. Constantly learning, constantly adapting, constantly protecting.
This week at Cisco

Client PC

Cisco Web Reputation Filtering applies to requested webpage and all frames.

Trusted Website

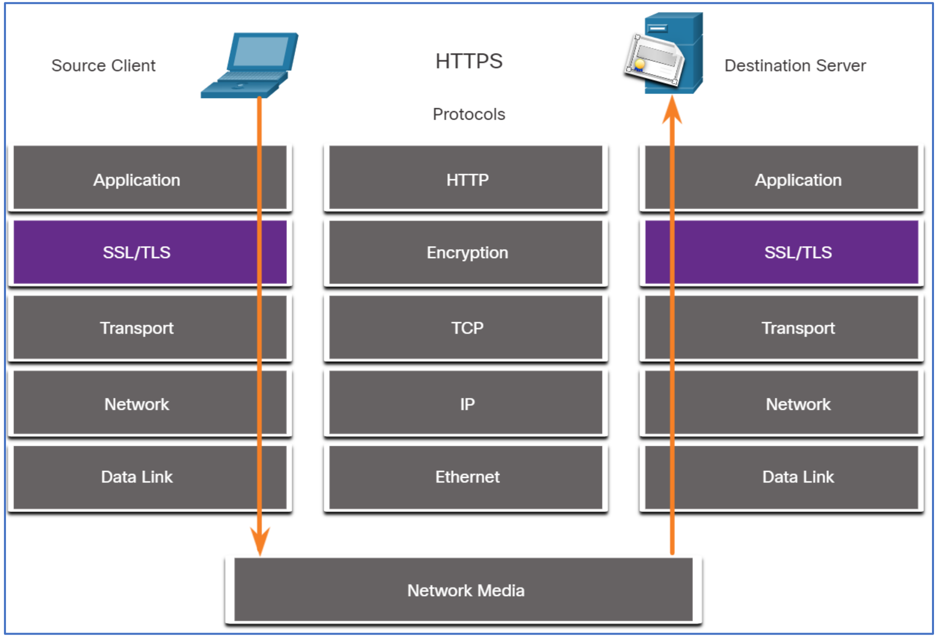
Web servers not affiliated with trusted site may house malicious software.

Accessed webpage calls frames from other sites.

Monitoring Common Protocols

HTTP and HTTPS (Cont.)

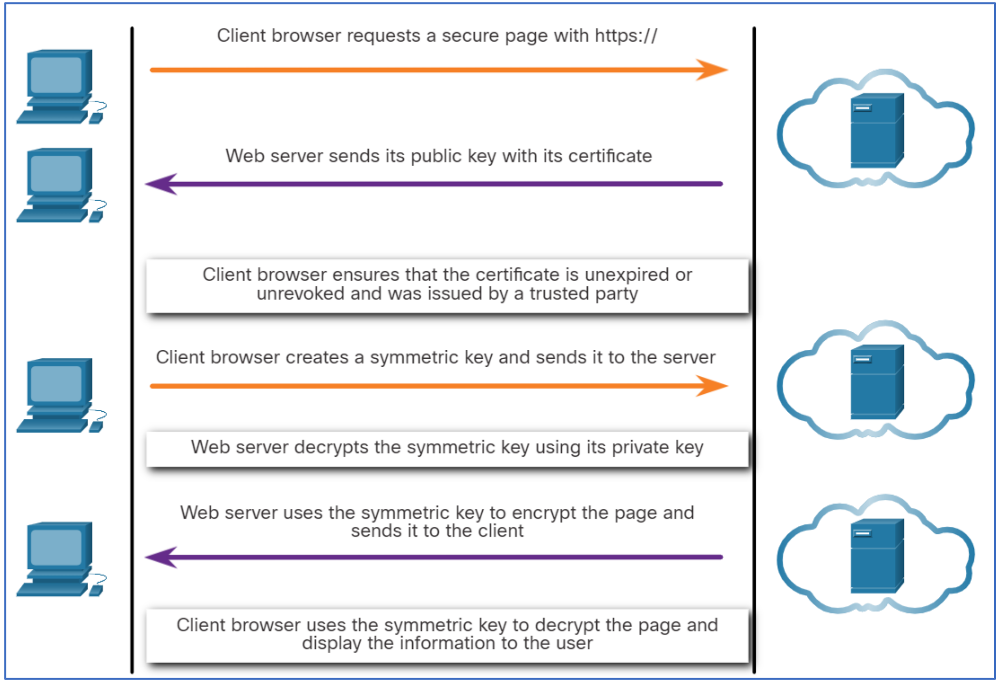
- To address the alteration or interception of confidential data, many commercial organizations have adopted HTTPS or implemented HTTPS-only policies to protect visitors to their websites and services.
- HTTPS adds a layer of encryption to the HTTP protocol by using secure socket layer (SSL).
- This makes the HTTP data unreadable as it leaves the source computer until it reaches the server.
- Note that HTTPS is not a mechanism for web server security. It only secures HTTP protocol traffic while it is in transit.



Monitoring Common Protocols

HTTP and HTTPS (Cont.)

- Unfortunately, the encrypted HTTPS traffic complicates network security monitoring.
- Some security devices include SSL decryption and inspection; however, this can present processing and privacy issues.
- In addition, HTTPS adds complexity to packet captures due to the additional messaging involved in establishing the encrypted connection.
- This process represents additional overhead on top of HTTP.



Client browser requests a secure page with https://

Web server sends its public key with its certificate

Client browser ensures that the certificate is unexpired or unrevoked and was issued by a trusted party

Client browser creates a symmetric key and sends it to the server

Web server decrypts the symmetric key using its private key

Web server uses the symmetric key to encrypt the page and sends it to the client

Client browser uses the symmetric key to decrypt the page and display the information to the user

Email Protocols

- Email protocols such as SMTP, POP3, and IMAP can be used by threat actors to spread malware, exfiltrate data, or provide channels to malware CnC servers.
- SMTP sends data from a host to a mail server and between mail servers. Like DNS and HTTP, it is a common protocol to see leaving the network.
- SMTP has been used in the past by malware to exfiltrate data from the network.
- Security monitoring could reveal this type of data traffic based on features of the email message.
- IMAP and POP3 are used to download email messages from a mail server to the host computer.
- They are the application protocols that are responsible for bringing malware to the host.
- Security monitoring can identify when a malware attachment entered the network, and which host it first infected.
- Retrospective analysis can then track the behavior of the malware from that point forward.
- The malware behavior can better be understood, and the threat identified.
- Security monitoring tools may also allow recovery of infected file attachments for submission to malware sandboxes for analysis.

ICMP

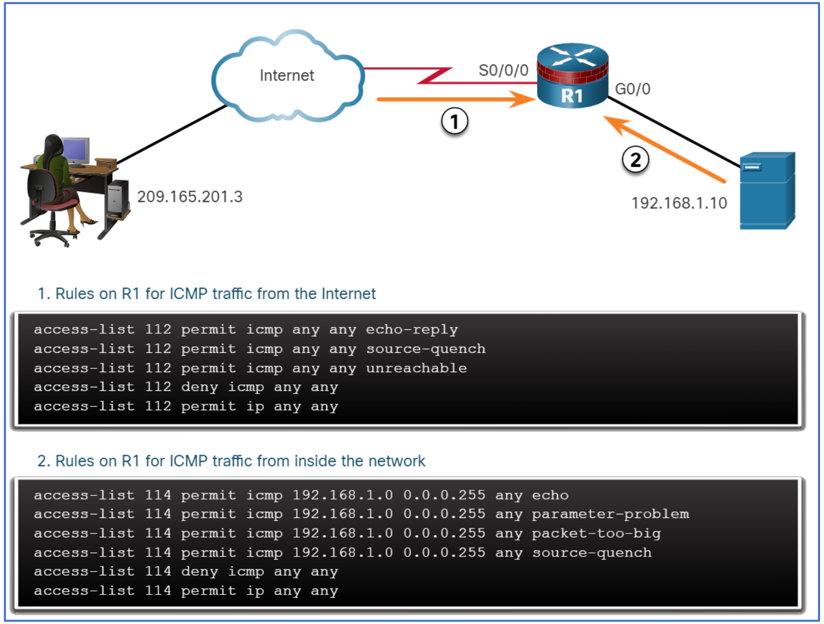
- ICMP has many legitimate uses, however ICMP functionality has also been used to craft several exploits.
- ICMP can be used to identify hosts on a network, the structure of a network, and to determine the operating systems at use on the network. It can also be used as a vehicle for various types of DoS attacks.
- ICMP can also be used for data exfiltration.
- Some varieties of malware use crafted ICMP packets to transfer files from infected hosts to threat actors using the ICMP tunneling method, such as LOKI exploit.
- Several tools exist for crafting tunnels. Search the internet for Ping Tunnel to explore one such tool.

19.2 Security Technologies

ACLs

- Many technologies and protocols can have impacts on security monitoring such as Access Control Lists (ACLs).
- ACLs are technologies that contribute to an evolving set of network security protections but can give a false sense of security if they are overly relied upon.

- The figure illustrates the use of ACLs to permit only specific types of Internet Control (ICMP) traffic.
- The server at 192.168.1.10 is part of the inside network and is allowed to send ping requests to the outside host at 209.165.201.3.
- The outside host's return ICMP traffic is allowed if it is an ICMP reply, source quench (tells the source to reduce the pace of traffic), or any ICMP unreachable message.
- All other ICMP traffic types are denied.



1. Rules on R1 for ICMP traffic from the Internet

```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
access-list 114 permit ip any any
```

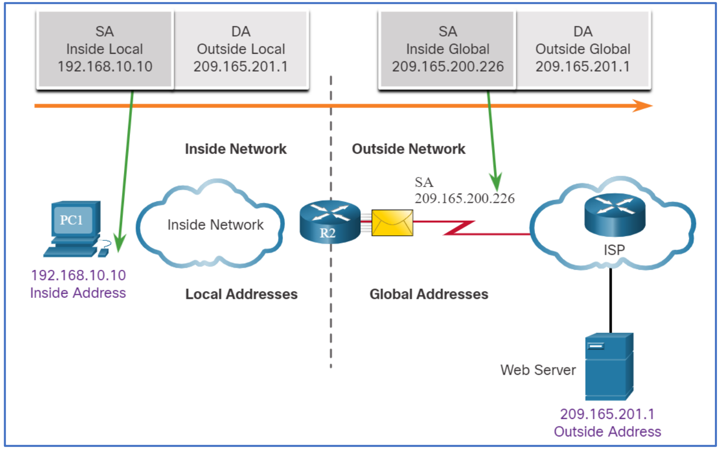
ACLs (Cont.)

- Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs.
- This can be done either by port scanning, penetration testing, or through other forms of reconnaissance.
- Attackers can craft packets that use spoofed source IP addresses.
- Applications can establish connections on arbitrary ports.
- Other features of protocol traffic can also be manipulated, such as the established flag in TCP segments.
- Rules cannot be anticipated and configured for all emerging packet manipulation techniques.
- To detect and react to packet manipulation, more sophisticated behavior and context-based measures need to be taken.
- Cisco Next Generation firewalls, Advanced Malware Protection (AMP), email, and web content appliances can address the shortcomings of rule-based security measures.

Security Technologies

NAT and PAT

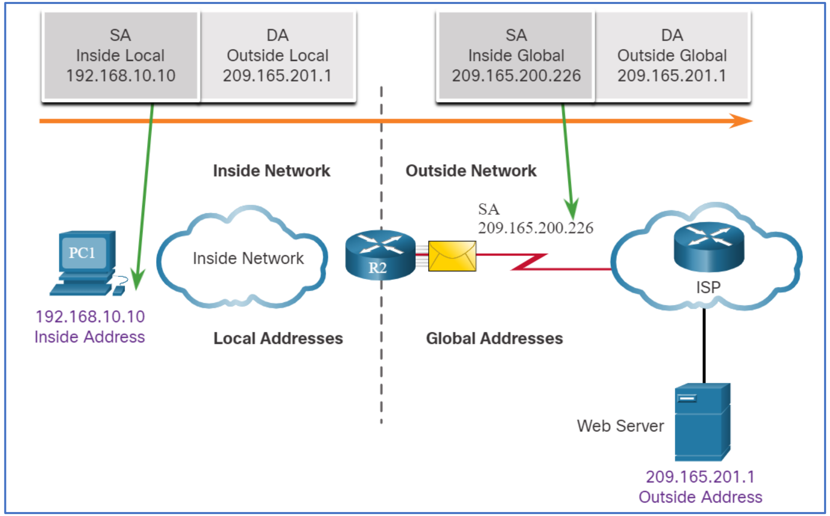
- Network Address Translation (NAT) and Port Address Translation (PAT) can complicate security monitoring.
- Multiple IP addresses are mapped to one or more public addresses that are visible on the internet, hiding the individual IP addresses that are inside the network.
- This problem can be especially relevant with NetFlow data.
- NetFlow flows are unidirectional and are defined by the addresses and ports that they share.
- NAT will essentially break a flow that passes a NAT gateway, making flow information beyond that point unavailable.
- Cisco offers security products that will “stitch” flows together even if the IP addresses have been replaced by NAT.



Security Technologies

NAT and PAT (Cont.)

- The figure illustrates the relationship between internal and external addresses that are used as source addresses (SA) and destination addresses (DA).
- These internal and external addresses are in a network that is using NAT to communicate with a destination on the internet.
- If PAT is in effect, and all IP addresses leaving the network use the 209.165.200.226 inside global address for traffic to the internet, it could be difficult to log the specific inside device that is requesting and receiving the traffic when it enters the network.

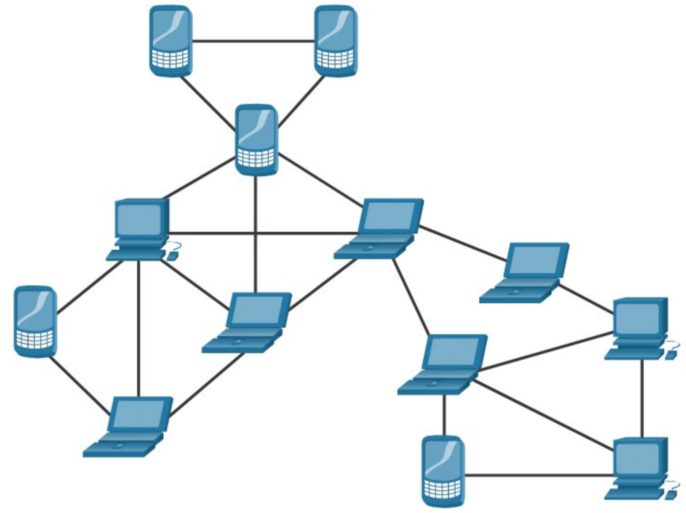


Encryption, Encapsulation, and Tunneling

- As mentioned with HTTPS, encryption can present challenges to security monitoring by making packet details unreadable.
- Encryption is part of VPN technologies. The encrypted traffic essentially establishes a virtual point-to-point connection between networks over public facilities.
- Encryption makes the traffic unreadable to any other devices but the VPN endpoints.
- A similar technology can be used to create a virtual point-to-point connection between an internal host and threat actor devices.
- Malware can establish an encrypted tunnel that rides on a common and trusted protocol and use it to exfiltrate data from the network.
- A similar method of data exfiltration was discussed for DNS.

Peer-to-Peer Networking and Tor

- In peer-to-peer (P2P) networking, hosts can operate in both client and server roles.
- Three types of P2P applications exist: file sharing, processor sharing, and instant messaging.
- In P2P file sharing, files on a participating machine are shared with members of the P2P network.
- Bitcoin is a P2P operation that involves the sharing of a distributed database, or ledger, that records Bitcoin balances and transactions.
- BitTorrent is a P2P file sharing network.



Unstructured P2P Logical Connections through which file sharing and other services may occur.

Peer-to-Peer Networking and Tor (Cont.)

- Any time unknown users are provided access to network resources, security is a concern.
- P2P file-sharing applications should not be allowed on corporate networks.
- P2P network activity can circumvent firewall protections and is a common vector for the spread of malware.
- P2P is inherently dynamic. It can operate by connecting to numerous destination IP addresses, and it can also use dynamic port numbering.
- Shared files are often infected with malware, and threat actors can position their malware on P2P clients for distribution to other users.
- P2P processor sharing networks donate processor cycles to distributed computational tasks.
- Cancer research, searching for extraterrestrials, and scientific research use donated processor cycles to distribute computational tasks.
- Instant messaging (IM) is also considered to be a P2P application.
- IM has legitimate value within organizations that have geographically distributed project teams. In this case, specialized IM applications are available, such as the Webex Teams platform, which are more secure than IM that uses public servers.

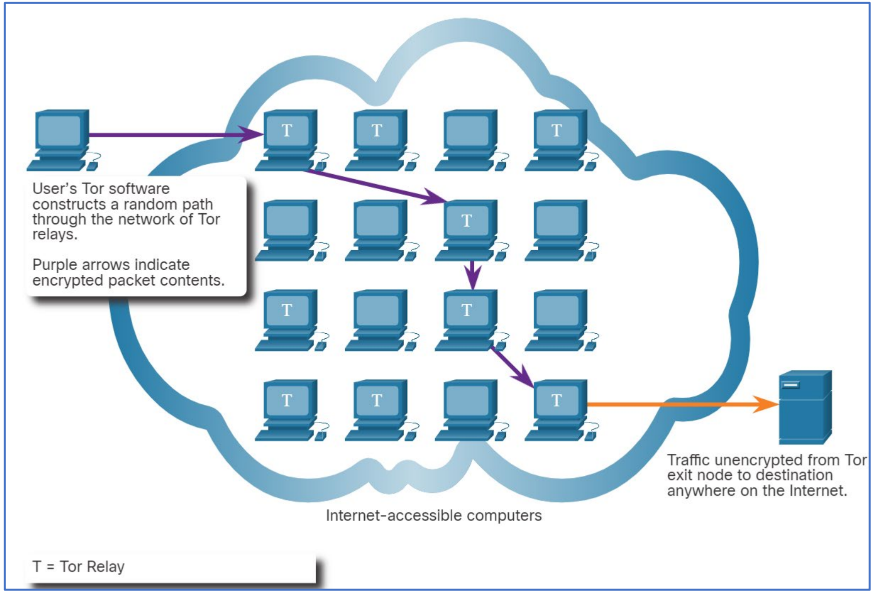
Security Technologies

Peer-to-Peer Networking and Tor (Cont.)

- Tor is a software platform and network of P2P hosts that function as internet routers on the Tor network.
- The Tor network allows users to browse the internet anonymously by using a special browser.
- When a browsing session is begun, the browser constructs a layered end-to-end path across the Tor server network that is encrypted.
- Each encrypted layer is “peeled away” like the layers of an onion (hence “onion routing”) as the traffic traverses a Tor relay.
- The layers contain encrypted next-hop information that can only be read by the router that needs to read the information.
- In this way, no single device knows the entire path to the destination, and routing information is readable only by the device that requires it.
- Finally, at the end of the Tor path, the traffic reaches its internet destination. When traffic is returned to the source, an encrypted layered path is again constructed.

Peer-to-Peer Networking and Tor (Cont.)

- Tor presents several challenges to cybersecurity analysts.
- First, Tor is widely used by criminal organizations on the “dark net.”
- In addition, Tor has been used as a communications channel for malware CnC.
- Because the destination IP address of Tor traffic is obfuscated by encryption, with only the next-hop Tor node known, Tor traffic avoids block lists that have been configured on security devices.



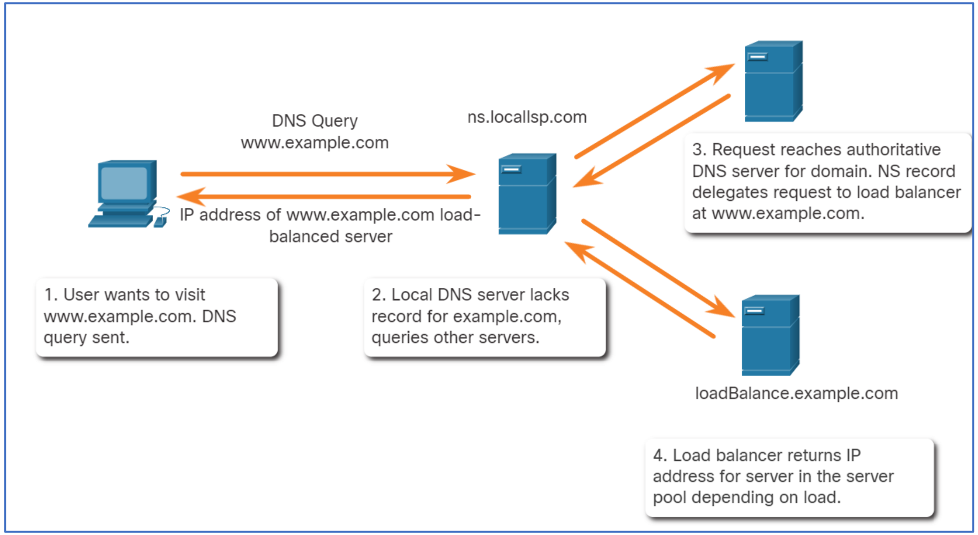
User’s Tor software constructs a random path through the network of Tor relays.

Purple arrows indicate encrypted packet contents.

Traffic unencrypted from Tor exit node to destination anywhere on the Internet.

Load Balancing

- Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic.
- If redundant resources exist, a load balancing algorithm or device will work to distribute traffic between those resources, as shown in the figure.
- One way this is done on the internet is through various techniques that use DNS to send traffic to resources that have the same domain name but multiple IP addresses.



1. User wants to visit www.example.com. DNS query sent.

2. Local DNS server lacks record for example.com, queries other servers.

3. Request reaches authoritative DNS server for domain. NS record delegates request to load balancer at www.example.com.

4. Load balancer returns IP address for server in the server pool depending on load.

Load Balancing (Cont.)

- In some cases, the service distribution may be to servers that are distributed geographically.
- This can result in a single internet transaction being represented by multiple IP addresses on the incoming packets.
- This may cause suspicious features to appear in packet captures.
- In addition, some load balancing manager (LBM) devices use probes to test for the performance of different paths and the health of different devices.
- For example, an LBM may send probes to the different servers that it is load balancing traffic to detect that the servers are operating.
- This is done to avoid sending traffic to a resource that is not available.
- However, these probes can appear to be suspicious traffic if the cybersecurity analyst is not aware that this traffic is part of the operation of the LBM.

19.3 Technologies and Protocols Summary

Technologies and Protocols Summary

What Did I Learn in this Module?

- Many types of devices from different vendors can use syslog to send log entries to central servers making security monitoring more practical.
- Hackers may attempt to block the transfer of data from syslog clients to servers, tamper with or destroy log data, or tamper with software that creates and transmits log messages.
- Devices can use NTP to share a consistent timeclock which can aid in the detection of exploits.
- Threat actors may attempt to attack the NTP infrastructure to corrupt time information or use NTP systems to direct DDoS attacks through client or server software vulnerabilities.
- Some varieties of malware use DNS to communicate with CnC servers and to exfiltrate data in traffic disguised as normal DNS queries.
- Various types of encoding can be used to camouflage the data and evade basic DPL measures.
- HTTP does not protect data from alteration or interception by malicious parties.
- A common exploit of HTTP is iFrame injection.
- HTTPS adds a layer of encryption to the HTTP protocol by using SSL.
- Email protocols such as SMTP, POP3, and IMAP can be used by threat actors to spread malware, exfiltrate date, or provide channels to malware CnC servers.

What Did I Learn in this Module? (Cont.)

- ICMP can be used as a vehicle for various types of DoS attacks and data exfiltration.
- ICMP tunneling uses crafted ICMP packets by some varieties of malware to transfer files from infected hosts to threat actors.
- ACLs can give a false sense of security if they are overly relied upon since attackers can determine which IP addresses, protocols, and ports are allowed by ACLs.
- Rules cannot be anticipated and configured for all emerging packet manipulation techniques.
- NAT and PAT can complicate security monitoring by hiding the individual IP addresses that are inside the network.
- Malware can establish an encrypted tunnel that rides on a common and trusted protocol and use it to exfiltrate data from the network.
- In P2P networking, hosts can operate in both client and server roles.
- Three types of P2P applications exist: file sharing, processor sharing, and instant messaging.
- Tor is widely used by criminal organizations on the “dark net" and has been used as a communications channel for malware CnC.
- Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic.
- LBM devices can use probes to test for the performance of paths and the health of devices.