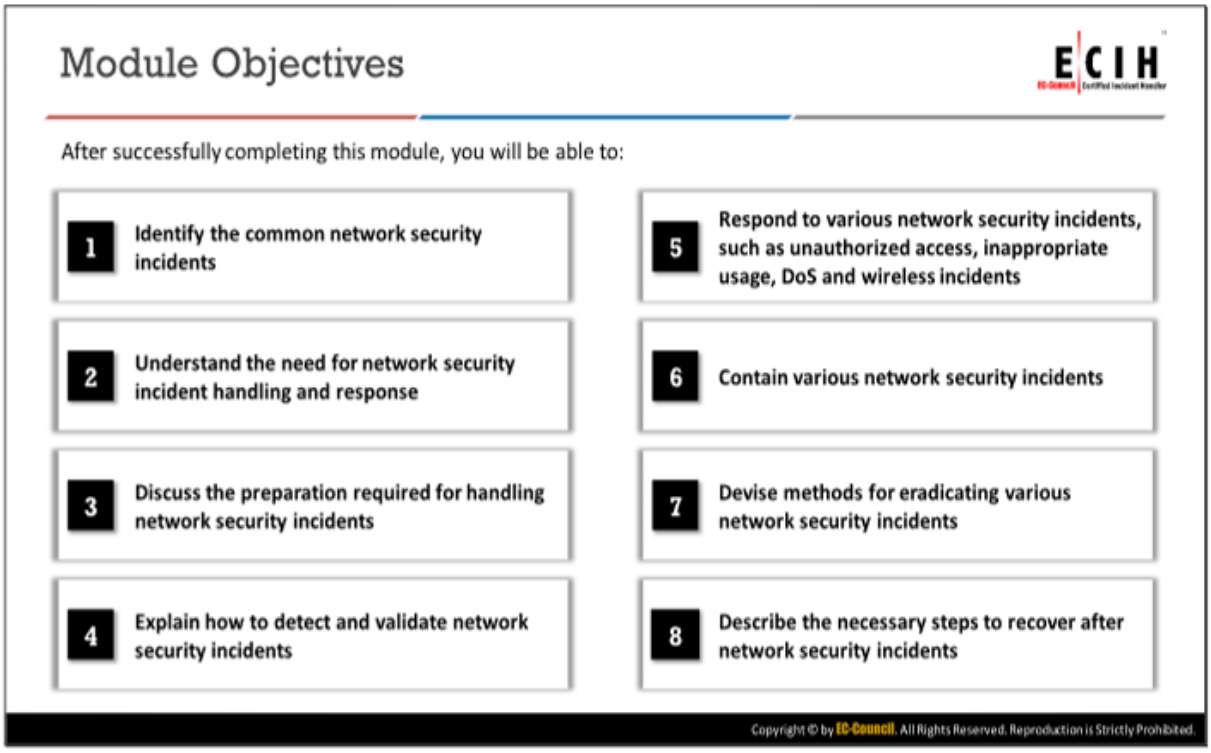
Module 06

Handling and Responding to Network Security Incidents

This page is intentionally left blank.

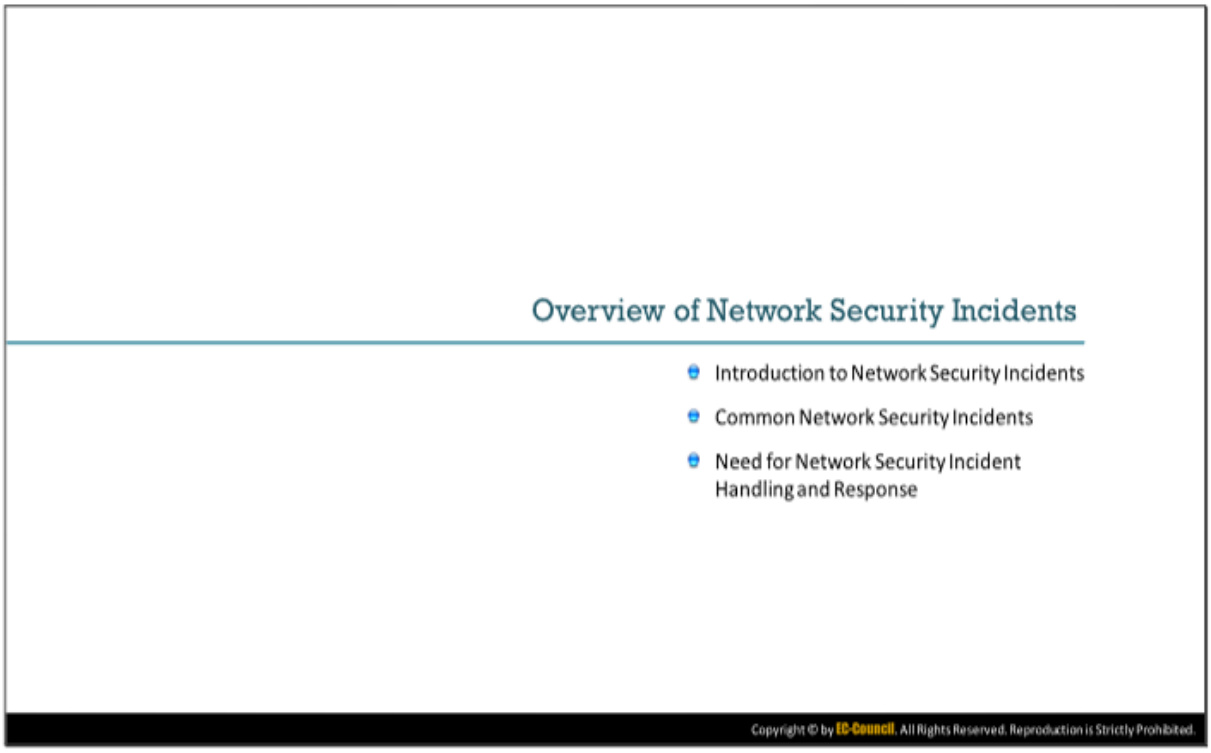


Module Objectives

In the previous modules, we discussed the handling of email and web application incidents. In this module, we will discuss in detail the handling of network security incidents. Most organizations have several computer networks to handle multiple tasks. Despite deploying various network security measures, most networks become compromised at some point, which can result in severe damage to the organization. As a member of an incident handling and response team, you must be able to quickly detect, contain, and eradicate any network security incidents and recover the machines affected by the incident to maintain business continuity.

At the end of this module, you will be able to:

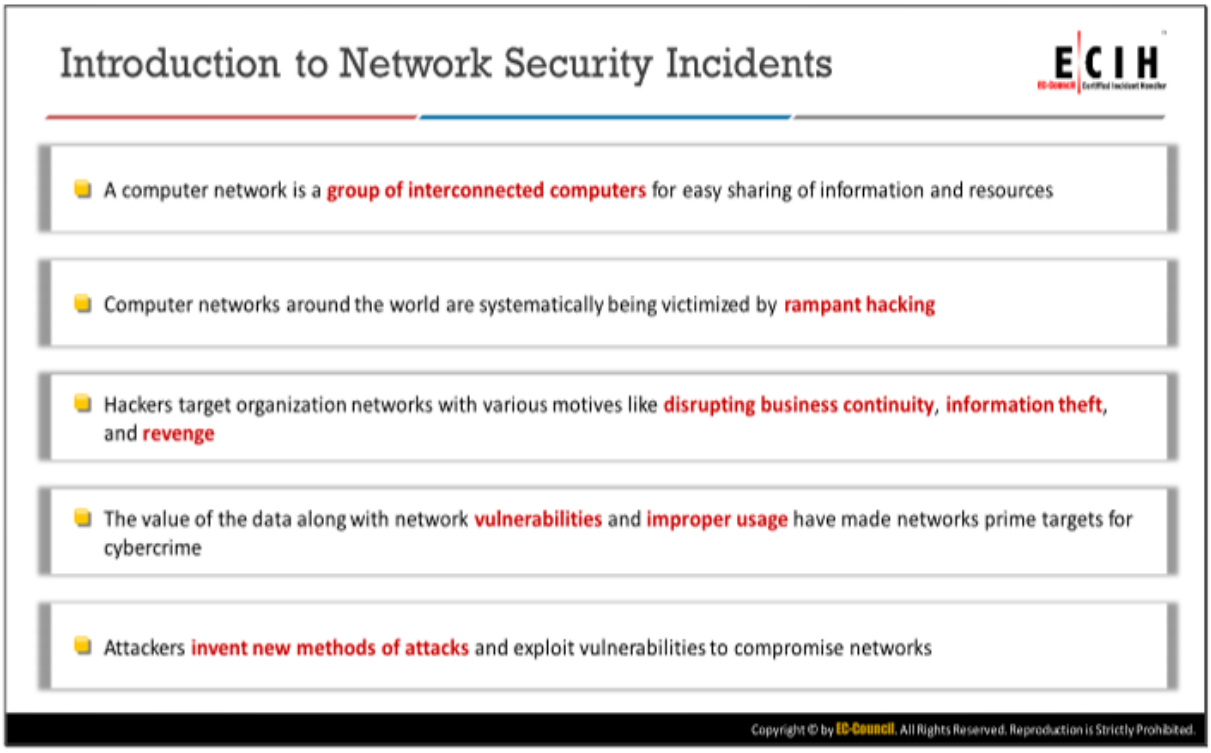
- Identify the common network security incidents
- Understand the need for network security incident handling and response
- Discuss the preparation required for handling network security incidents
- Explain how to detect and validate network security incidents
- Respond to various network security incidents, such as those related to unauthorized access, inappropriate use, DoS, and wireless network security
- Contain various network security incidents
- Devise methods for eradicating various network security incidents
- Explain steps to follow to recover after network security incidents



Overview of Network Security Incidents

A network is a communication medium that allows devices to exchange data, through either wired or wireless connections. Therefore, any attack targeted against a device needs to pass through the network. This has made networks one of the prime targets for attackers.

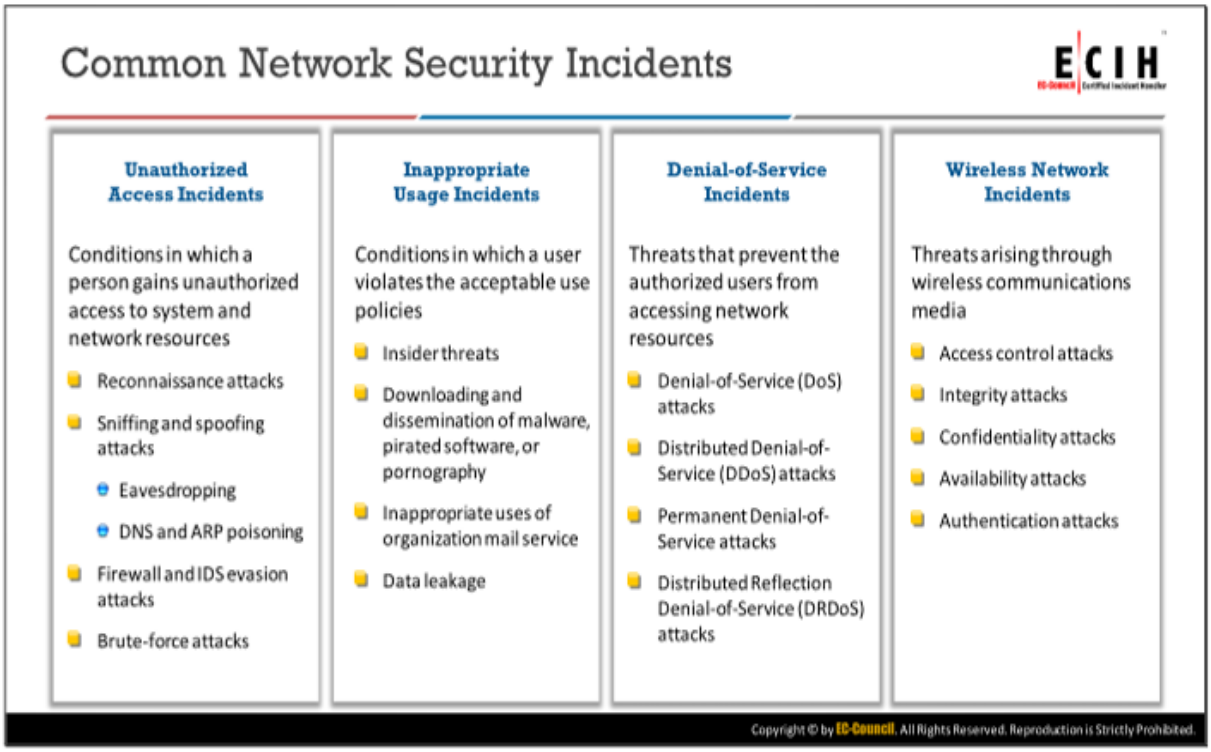
This section introduces network security incidents, common network security incidents, and the need for network security incident handling and response.



Introduction to Network Security Incidents

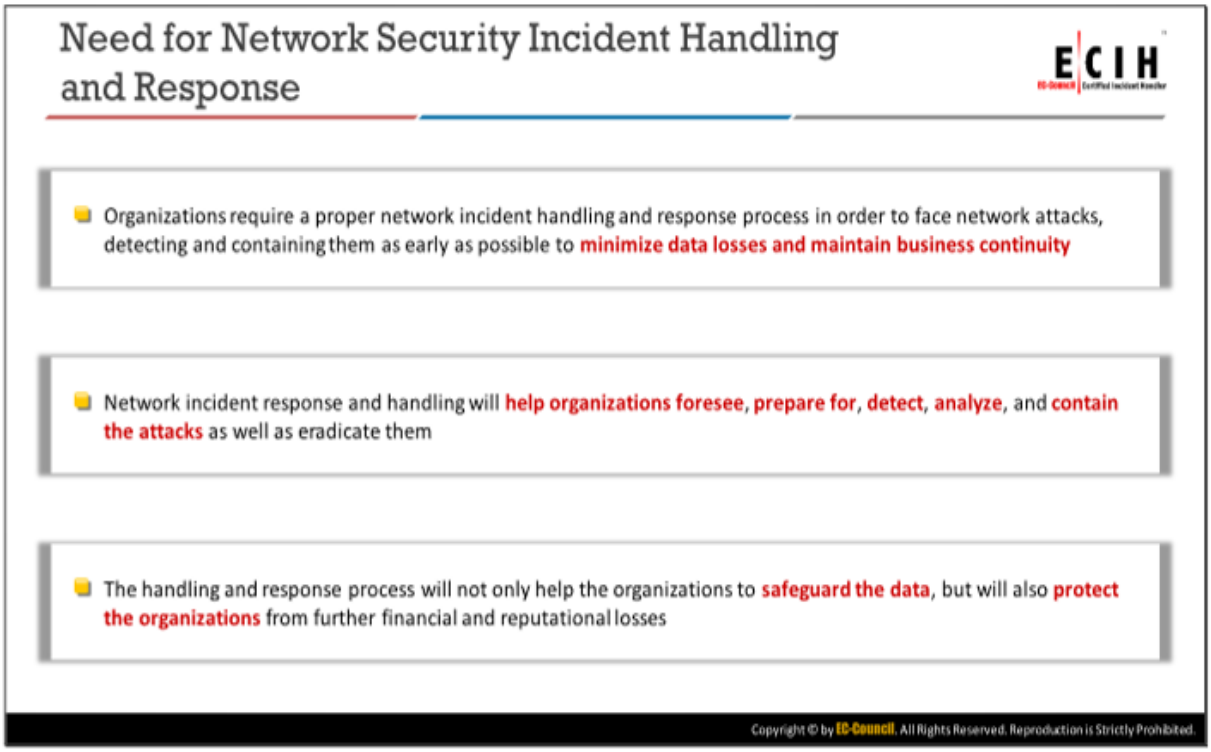
A computer network is a group of computers connected to each other to allow easy sharing of information and resources. The computers share information using a data path. Rapid technological developments have increased the number of devices used that have boosted adoption of the networks. Different devices use different types of networks and connectivity protocols that include various technologies and security mechanisms.

Computer networks around the world are systematically being attacked by rampant hacking. Such network hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value, and completely erase their tracks. Hackers have various motives for targeting organizational networks, such as disrupting business continuity, information theft, and revenge. The unknown vulnerabilities and improper usage have further increased the rate of crime against networks. The attackers are constantly developing new techniques to breach the networks and exploit vulnerabilities to compromise networks and access sensitive data stored on various devices connected to it.



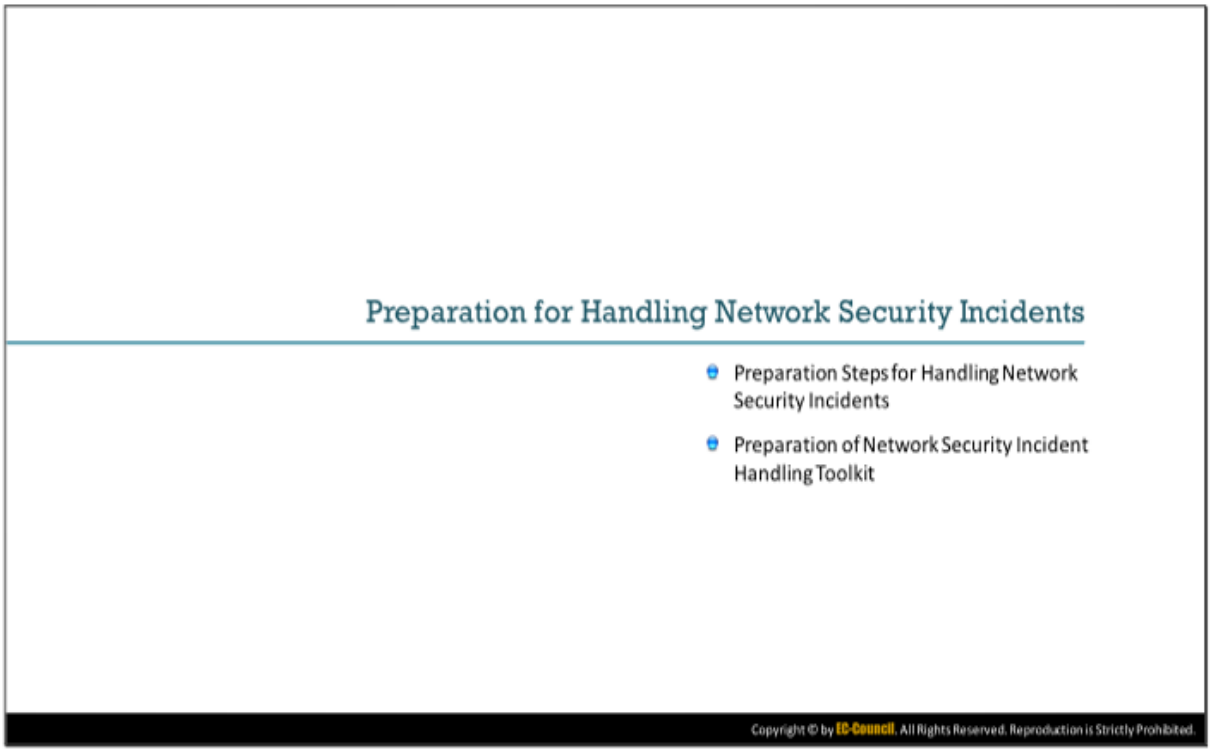
Common Network Security Incidents

Some of the most common network security incidents are mentioned in the above slide.



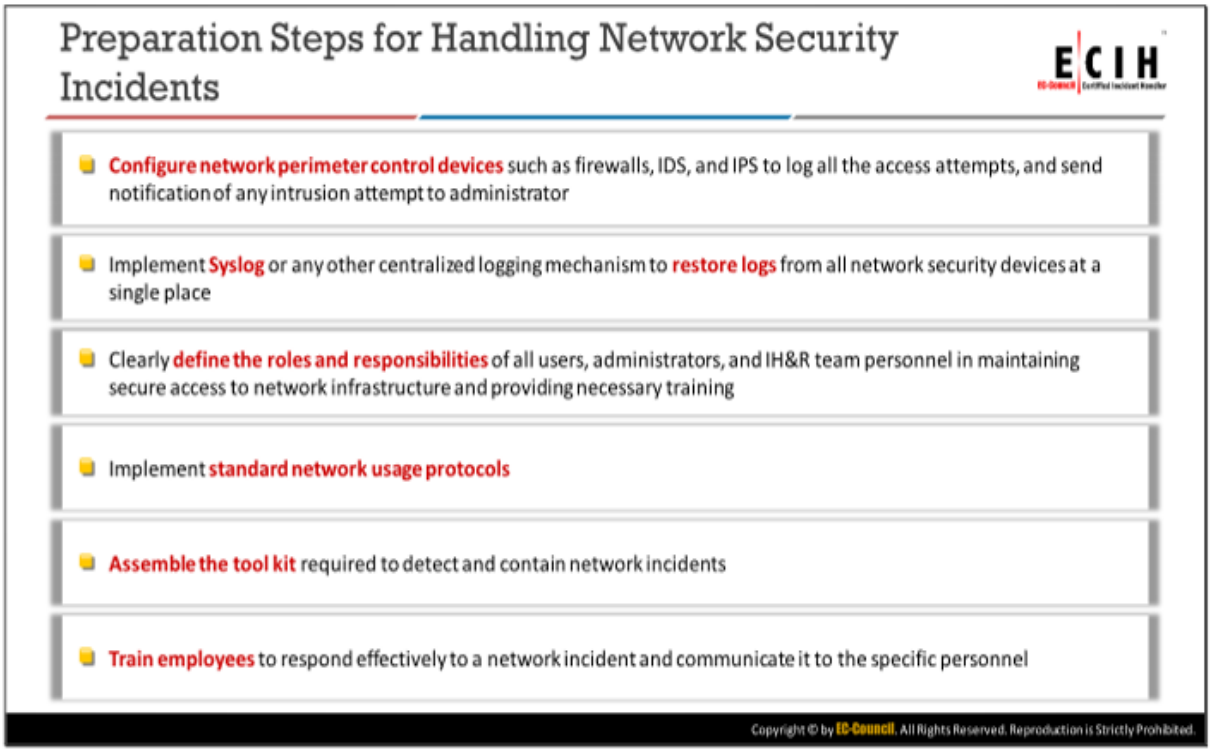
Need for Network Security Incident Handling and Response

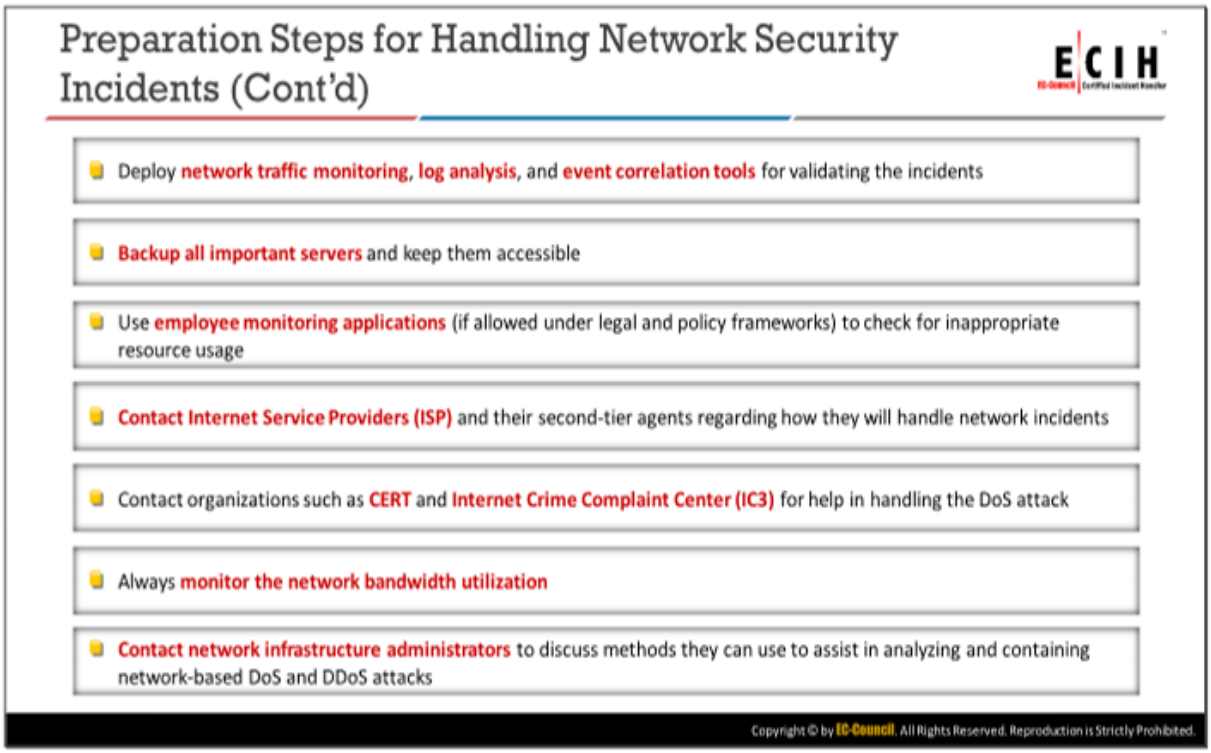
Organizations require a proper network incident handling and response (IH&R) process to detect and contain network attacks as early as possible to minimize data losses and maintain business continuity. Network incident response and handling helps organizations predict, prepare, detect, analyze, contain, and eradicate such network attacks, while developing measures to prevent them in the future. This process helps organizations safeguard their data, and also protect themselves from further financial and reputational losses. In addition, the network IH&R process helps organization develop threat intelligence, build an incident response team, gather proper tools, and prepare to face existing, as well as new, threats.



Preparation for Handling Network Security Incidents

The IH&R team is responsible for handling all types of network security incidents. Hence, this team must be properly trained to handle network security incidents prior to an incident taking place. This section discusses the various steps that should be followed by the incident responder, and discusses the preparation of a network incident handling toolkit.





Preparation Steps for Handling Network Security Incidents

The incident handler should ensure that the organization is ready to respond to any type of network attack or incident. As part of this preparation, the organization should develop and implement usage policies, build network incident response teams, prepare the necessary response tools, and enable configurations across the network and connected devices that can assist the incident response process.

In preparation for network incidents, the IH&R team should consider the following preparation steps and guidelines.

- Configure network perimeter control devices, such as firewalls, IDS, and IPS systems to log all access attempts and send notifications regarding intrusion attempts to the administrator or IH&R team.
- Implement Syslog or another centralized logging mechanism to backup logs from all network security devices to a single location. This helps in analysis and correlation of logs.
- Clearly define the roles and responsibility of all users, administrators, and IH&R team members during the incident response process to maintain secure access to the network infrastructure.
- Implement standard network usage protocols.
- Provide all IH&R team members with necessary training and conduct practice sessions to verify their efficiency.
- Prepare tools for assisting detection and containment of the threat. Enlist tools required for various tasks, such as monitoring, capturing and analyzing network traffic and logs, correlating the logs, and preparing the attack timeline.
- Train the employees to effectively respond to a network incident and communicate it to the necessary personnel.
- Install network sniffing tools, security solutions, and other logging tools across all network servers to record all incoming and outgoing traffic, in addition to alerting administrators about the current incidents.
- Backup all important servers and keep them accessible.
- Make an agreement with network infrastructure administrators regarding the assistance they can provide in analyzing and containing network-based DoS and DDoS attacks.
- Use employee monitoring applications (if allowed under legal and policy frameworks) to check for inappropriate resource usage.
- Contact internet service providers (ISPs) and their second-tier agents to gather information about the incident handling and response processes for the network incidents on their end.
- Communicate the goals of the IH&R process and always have a backup network ready for emergencies.
- Keep the contact details of national and government security organizations, such as CERT and the Internet Crime Complaint Center (IC3) to seek help in case of attacks that can affect national security.
- Create a procedure for the employees to enable them change login credentials and update their devices immediately after containment of an incident. Include such procedures in the organizational password policy.

- Collaborate with human resources and legal departments to frame fair usage policies for all employees.
- Communicate with the physical security team regarding the behavior of internal users and train them to report all discrepancies.
- Design a process for interviewing a perpetrator with the help of legal authorities, as the perpetrators may be mentally unstable or become violent on confrontation. Interviewing such users or acquiring a user's workstation can place the incident handler at risk.
- Form a legal department from IH&R team that would handle liability issues and incidents targeting customers, clients, and third-party service providers.
- The members of the legal department should always obtain proper permission before informing the victims about the incident and have clear understanding of the knowledge they need to reveal.
- The organizations should log user activities, such as FTP commands, web requests, and email headers with the help of proxies, application logs, and network-based IDPS sensors.
- Seek help from ISPs for handling network-based DoS attacks.
- Obtain and use the traffic logs that ISPs maintain to detect the source of attacks and contain them.
- Configure IDS and IPS software to detect DoS traffic.
- Discuss the method of intrusion detection with the ISPs to restrict the attacker's access to organizational resources.
- Define proper data collection and accumulation strategies and define the types of data to be collected while performing network forensic analysis.
- Define live analysis laboratory configurations and determine host hardening and sandbox environments.
- Estimate capture requirements and identify the type of capture required (e.g., limited capture, full packet capture) while performing network data capturing.
- Determine appropriate capture device deployment locations and ensure the integrity and security of the network after introduction of a capture device.
- Avoid overwhelming capture devices by collecting sufficient data and ensure that all arguments and evidence supporting integrity of captured data is obtained.

Preparation of Network Security Incident Handling Toolkit

Windows-based Tools to Analyze Incidents

Registry Analysis Tools

- jv16 Power Tools 2017 (*https://www.macecraft.com*)
- regshot (*https://sourceforge.net*)
- Reg Organizer (*https://www.chemtable.com*)

Network Analysis Tools

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- TCPView (*https://docs.microsoft.com*)

File System Analysis Tools

- PE Explorer (*http://www.heaventools.com*)
- Pescan (*https://tzworks.net*)
- PEView (*https://www.aldeid.com*)

Malware Analysis Tools

- VirusTotal (*https://www.virustotal.com*)
- IDA Pro (*https://www.hex-rays.com*)
- Ollydbg (*http://www.ollydbg.de*)

Preparation of Network Security Incident Handling Toolkit (Cont'd)

Windows-based Tools to Analyze Incidents

Process Analysis Tools

- Process Monitor (*https://docs.microsoft.com*)
- Process Explorer (*https://docs.microsoft.com*)
- Tasklist (*https://docs.microsoft.com*)

Service Analysis Tools

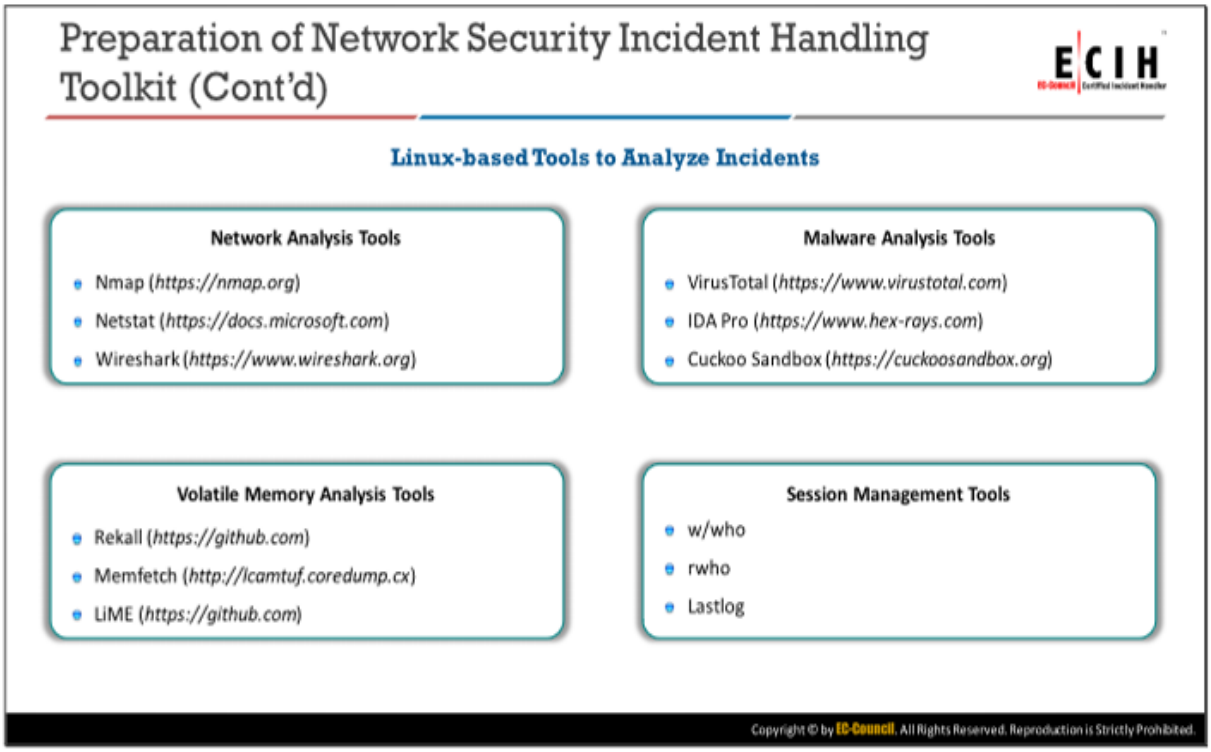
- Services.msc (*https://docs.microsoft.com*)
- MSConfig (*https://docs.microsoft.com*)
- SrvMan (*http://tools.sysprogs.org*)

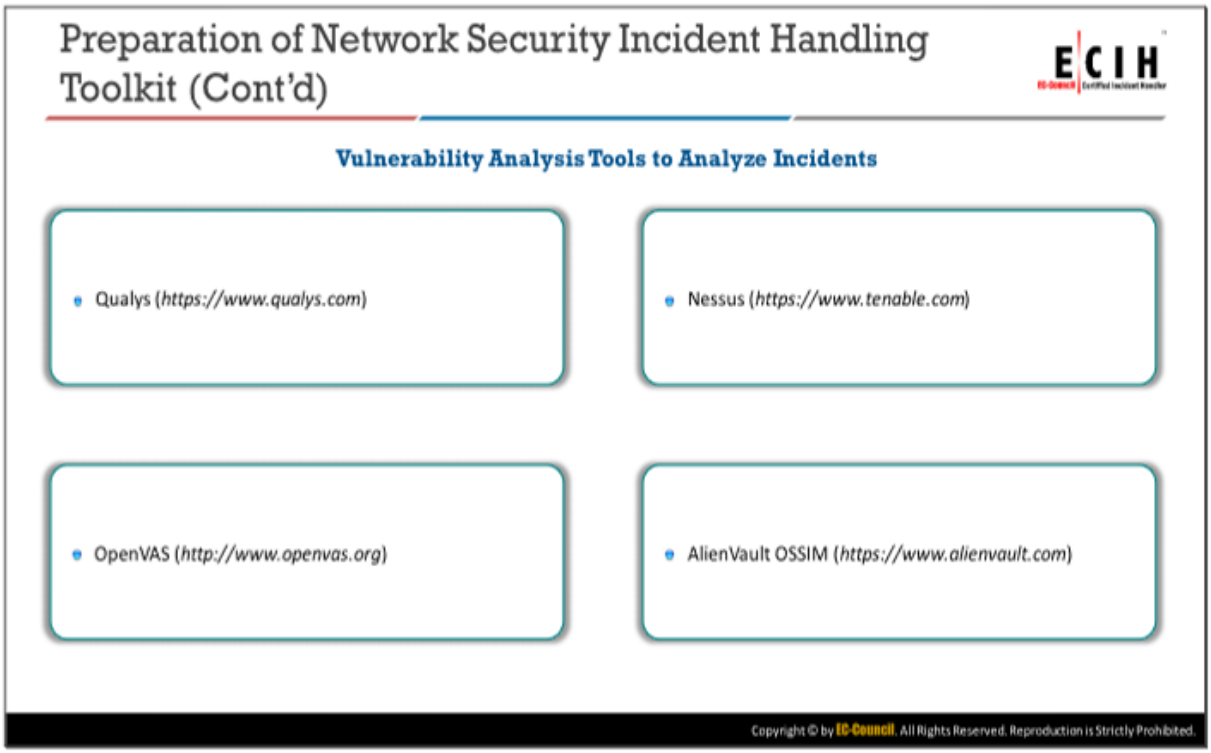
Volatile Memory Analysis Tools

- Rekall (*https://github.com*)
- Memdump (*https://support.microsoft.com*)
- MemGator (*http://e5hforensics.com*)

Active Directory Tools

- SolarWinds Server & Application Monitor (*https://www.solarwinds.com*)
- Adaxes (*https://www.adaxes.com*)
- ADManager Plus (*https://www.manageengine.com*)





Preparation of Network Security Incident Handling Toolkit

It is the responsibility of the IH&R team to build an appropriate network security incident handling toolkit that is suitable for various purposes. In this section, we list some of the tools that can be included in a security toolkit for analyzing network security incidents.

Windows-based tools

Type of Tool	Tool name and link
Registry Analysis Tools	▪ jv16 Power Tools 2017 (*https://www.macecraft.com*) ▪ regshot (*https://sourceforge.net*) ▪ Reg Organizer (*https://www.chemtable.com*) ▪ Registry Viewer (*http://accessdata.com*) ▪ RegScanner (*http://www.nirsoft.net*)
Network Analysis Tools	▪ Nmap (*https://nmap.org*) ▪ Wireshark (*https://www.wireshark.org*) ▪ TCPView (*https://docs.microsoft.com*) ▪ Netstat (*https://docs.microsoft.com*) ▪ Nbtstat (*https://docs.microsoft.com*) ▪ Tracert (*https://support.microsoft.com*) ▪ Packet Capture (*https://www.netscantools.com*) ▪ Real-Time NetFlow Analyzer (*https://www.solarwinds.com*) ▪ ManageEngine NetFlow Analyzer (*https://www.manageengine.com*)
File System Analysis Tools	▪ PE Explorer (*http://www.heaventools.com*) ▪ Pescan (*https://tzworks.net*) ▪ PEView (*https://www.aldeid.com*) ▪ Resource Hacker (*http://www.angusj.com*) ▪ WinDirStat (*https://windirstat.net*) ▪ DiskSavvy (*https://www.disksavvy.com*) ▪ MD5sums (*http://www.pc-tools.net*) ▪ md5deep (*https://github.com*) ▪ Hashtab (*http://implbits.com*)
Malware Analysis Tools	▪ VirusTotal (*https://www.virustotal.com*) ▪ IDA Pro (*https://www.hex-rays.com*) ▪ Ollydbg (*http://www.ollydbg.de*)

	▪ Windbg (*https://docs.microsoft.com*) ▪ Cuckoo Sandbox (*https://cuckoosandbox.org*) ▪ Blueliv Sandbox (*https://www.blueliv.com*)
Process Analysis Tools	▪ Process Monitor (*https://docs.microsoft.com*) ▪ Process Explorer (*https://docs.microsoft.com*) ▪ Tasklist (*https://docs.microsoft.com*) ▪ Monit (*https://mmonit.com*) ▪ ESET SysInspector (*https://www.eset.com*) ▪ System Explorer (*http://systemexplorer.net*)
Service Analysis Tools	▪ Services.msc (*https://docs.microsoft.com*) ▪ MSConfig (https://docs.microsoft.com) ▪ SrvMan (*http://tools.sysprogs.org*) ▪ Net start (*https://docs.microsoft.com*) ▪ Task Scheduler (*https://docs.microsoft.com*)
Volatile Memory Analysis Tools	▪ Rekall (*https://github.com*) ▪ Memdump (*https://support.microsoft.com*) ▪ MemGator (*http://e5hforensics.com*) ▪ Memoryze (*https://www.fireeye.com*) ▪ KnTTools (*http://www.gmgsystemsinc.com*)
Active Directory Tools	▪ SolarWinds Server & Application Monitor (*https://www.solarwinds.com*) ▪ Adaxes (*https://www.adaxes.com*) ▪ ADManager Plus (*https://www.manageengine.com*) ▪ ADAudit Plus (*https://www.manageengine.com*) ▪ Anturis Active Directory Monitor (*https://anturis.com*)

Table 6.1: Windows-based tools for analyzing incidents

Linux-based tools

Type of Tool	Tool name and link
Network Analysis Tools	▪ Nmap (*https://nmap.org*) ▪ Netstat (*https://docs.microsoft.com*) ▪ Wireshark (*https://www.wireshark.org*) ▪ Tcpdump (*http://www.tcpdump.org*) ▪ MD5sums (*http://www.pc-tools.net*) ▪ md5deep (*https://github.com*) **Command Line Tools** ▪ traceroute ▪ ARP ▪ ifconfig ▪ File system ▪ lsof ▪ dd ▪ df ▪ fdisk ▪ strings ▪ grep
Malware Analysis Tools	▪ VirusTotal (*https://www.virustotal.com*) ▪ IDA Pro (*https://www.hex-rays.com*) ▪ Cuckoo Sandbox (https://cuckoosandbox.org) **Command Line Tools** ▪ Processes ▪ htop ▪ top ▪ ps
Volatile Memory Analysis Tools	▪ Rekall (https://github.com) ▪ Memfetch (*http://lcamtuf.coredump.cx*)

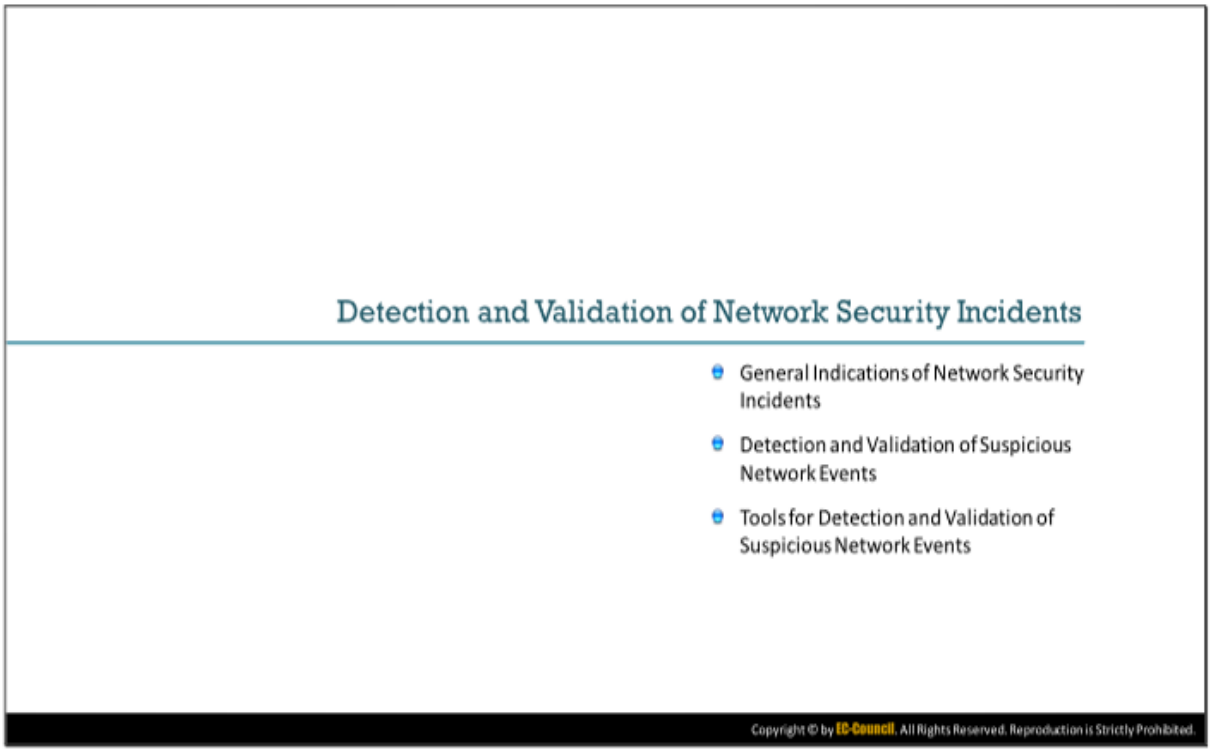
	▪ LiME (*https://github.com*) ▪ Volatilitux (*https://code.google.com*)
Session Management Tools	**Command Line Tools** ▪ w/who ▪ rwho ▪ Lastlog

Table 6.2: Linux-based tools for analyzing incidents

Vulnerability analysis tools

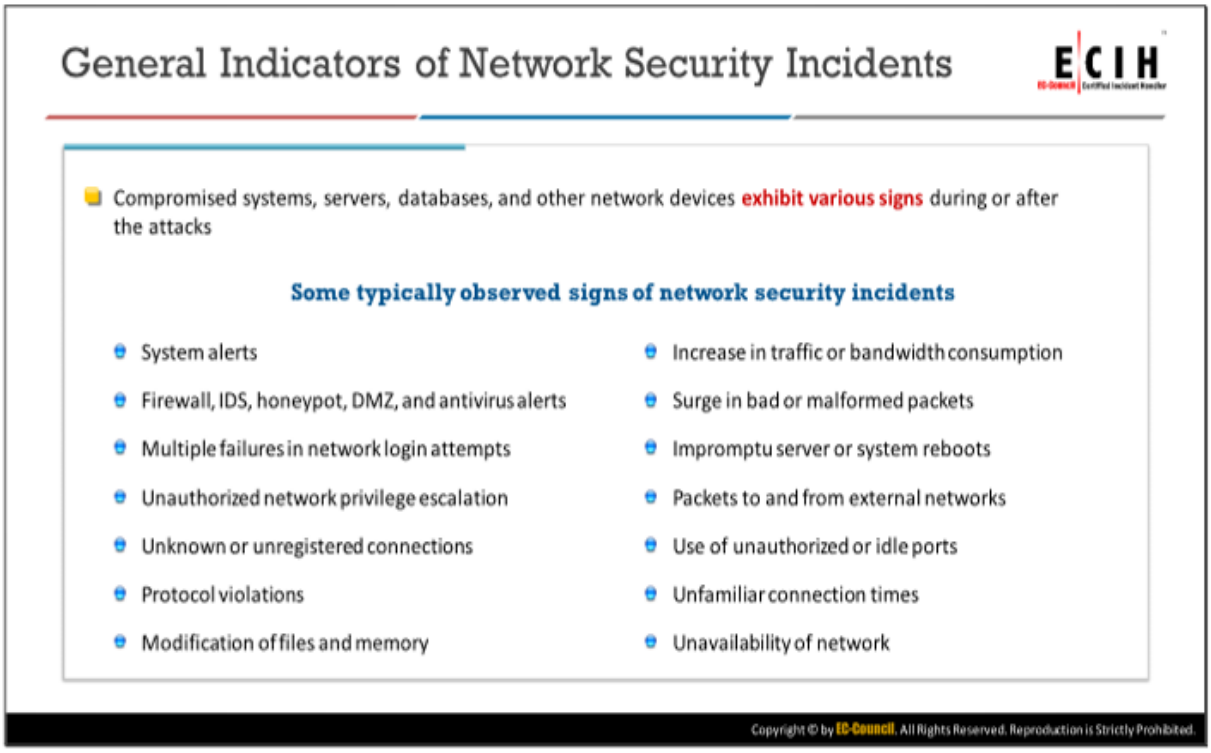
Type of Tool	Tool name and link
Vulnerability Analysis Tools	▪ Qualys (*https://www.qualys.com*) ▪ Nessus (*https://www.tenable.com*) ▪ OpenVAS (*http://www.openvas.org*) ▪ AlienVault OSSIM (*https://www.alienvault.com*) ▪ Nikto (https://cirt.net) ▪ Burp Suite (*https://portswigger.net*)

Table 6.3: Vulnerability analysis tools



Detection and Validation of Network Security Incidents

Detection and validation of the network security incident is one of the crucial tasks performed by IH&R personnel, as it allows them to effectively respond to the incident, and contain and eradicate the threat. This section presents the general indications of network security incidents and discusses the detection and validation of suspicious network events.



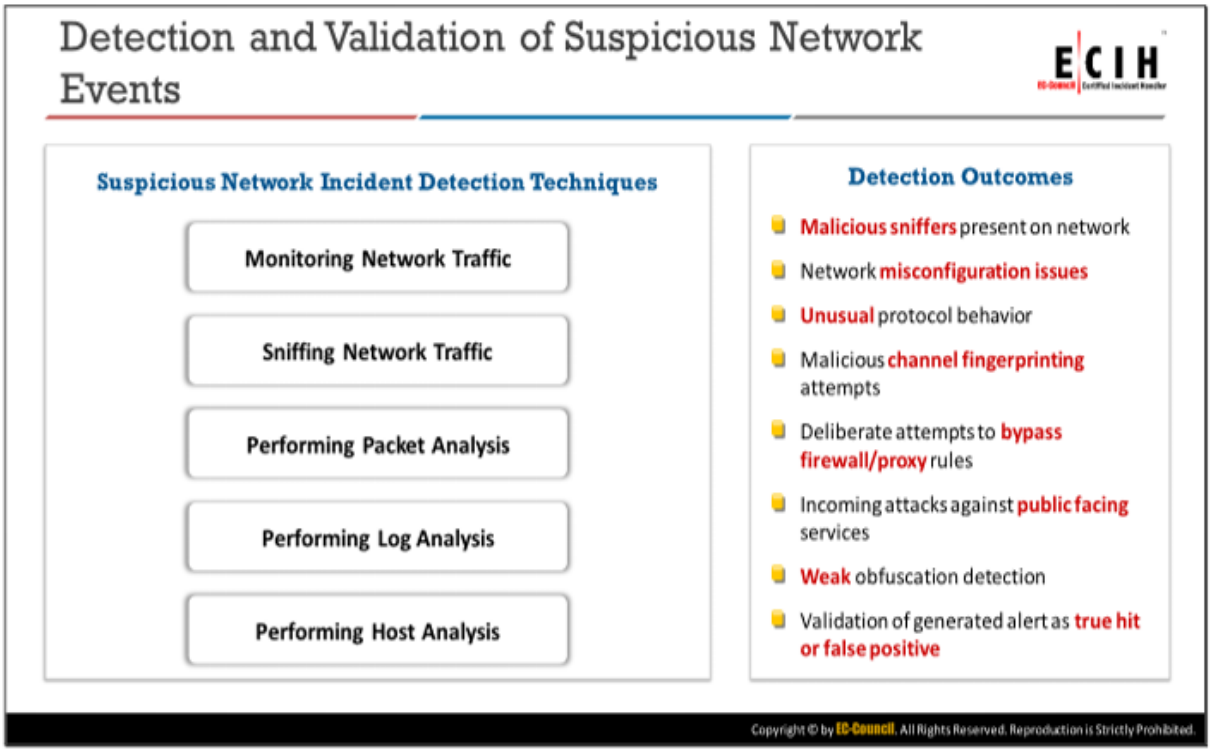
General Indicators of Network Security Incidents

Compromised systems, servers, databases, and other network devices exhibit various signs during or after the attacks. Users or administrators of the devices will be the first to observe these signs and report them to the security personnel.

Some commonly observed signs of network security incidents include the following.

- System alerts from system-based security solutions.
- Firewall, IDS, honeypot, DMZ, and antivirus alerts.
- Multiple failures in network login attempts can represent theft of login credentials or DoS attack on the network.
- Unauthorized network privilege escalation occurs when the attacker obtains access to an administrator account and tries to escalate privileges of other compromised accounts.
- Unknown or unregistered connections in an organizational network appear when the attacker gains access to the network.
- Protocol violations, such as SSL and TSL, occur when the attacker tries to access an IP-based network from networks based on other protocols.
- Modification of files and memory indicates that the attacker has successfully obtained access to the data after bypassing the security mechanisms.
- Increase in traffic or bandwidth consumption occurs when attackers try to upload the stored content or download malicious content from external servers.

- Surges in bad or malformed packets occur when attackers try to hide data theft by breaking it into small chunks.
- Impromptu server or system reboots are a sign of malware or installation of new or unauthorized software.
- Packets to and from unknown external networks indicate theft of data to an external server. Attackers can also try to temporarily store stolen data on internal networks that they can easily access later.
- Use of unauthorized, idle, or open ports is a technique used by attackers to access systems and other network devices.
- Unfamiliar connection times indicate malware stored on the device or an attacker trying to transmit data without alerting the security personnel or mechanisms.
- Unavailability of the network is a sign of DoS or DDoS attack, which usually becomes obvious when many users complain about the lack of service.



Detection and Validation of Suspicious Network Events

Incident responders need to verify that suspicious events represent an attack or other significant incident by performing analysis of the indicators reported by victims, users, or employees. The process also includes monitoring of logs for suspicious network connections, correlation of logs, and event timeline analysis.

Incident responders can detect and validate network incidents using the following techniques.

- **Monitoring Network Traffic**

  Incident responders should monitor the incoming and outgoing traffic as all types of network activity create traffic. Network monitoring tools record all types of activity over the network, which can include: user details such as the IP address and MAC address, time, date, protocols, ports, type of connection, systems/URLs accessed, and size of files shared. Incident responders can use these details to locate suspicious events.

  Network incidents result in changes in network utilization, bandwidth allocations, and performance. Sudden changes in speed and quality can be a sign of ongoing attack or reconnaissance of the network as part of a pre-attack process. Incident responders need to observe the network utility pattern and create a baseline of maximum and minimum thresholds. They should closely monitor any sudden spike or plunge in network performance. Unexpected, unusual, or suspicious network traffic may also be a sign of intrusion. The incident responder needs to monitor the traffic, verify its source and destination IP addresses, and scan the network connections for proxies.

  In general, attackers scan the networks to find vulnerabilities, such as open connections, non-updated systems, and weak authentications, to enable access to the network. The incident responder should monitor the use of probes, scans, and mapping tools on the

network. They should also monitor volume, directions, QoS, timing, and custom or standard encryption of the network traffic.

Finally, the incident responder should use the firewall and IDS to look for suspicious IP addresses, and tools to collect the details of the intruder. They need to identify the network devices used by the intruder via network monitoring tools, device logs, and user login attempts. Unusual connection or connections to or from unknown IP addresses and URLs should be identified by monitoring network traffic using tools such as Wireshark, Colasoft Network Analyzer, and Observer Analyzer.

- **Sniffing Network Traffic**

  During a network incident, the incident responder needs to identify compromised devices, the source of the incident, propagation path through the network, and gather other evidence. The best way to gather such information is by sniffing the data packets passing through the network using a software application called a packet analyzer or packet sniffer. This is a tool that can intercept and log traffic passing through a network.

  The sniffer helps network management by enabling responders to monitor and analyze the data packets to detect intrusions, supervise network content, troubleshoot the network, and control traffic. Sniffers also help analyze the behavior of an application or device causing network issues. The sniffers can extract the complete data packets and store them on a system for analysis. The first step in monitoring the data is to establish a baseline of network operations. This baseline defines the common usage practices of the network by capturing network performance and bandwidth consumption during regular traffic hours.

  Packet sniffer applications, such as Wireshark, Tcpdump, Cain & Abel, or Kismet are installed on a device that connects an external network to the internal network. This ensures that the application captures all data passing through the network, including wireless connections.

- **Performing Packet Analysis**

  Packet analysis is the process of capturing a data packet transmitted through a network and analyzing it to gather information about the packet, such as the network, ports, protocols, devices, issues in network transmission, and other network specifications. The process includes use of a network sniffer to capture the data and a packet analyzer application to read the specifications. Network sniffing and packet capture tools include Wireshark and NetworkMiner. Tools such as ngrep can be used to search for particular strings, binary structures, or patterns throughout the captured packets. Incident responders can also deploy a hex editor to view the raw bits of the packet, which include data such as the metadata of a file. A record of the following should be maintained:

  - Source and destination IP addresses
  - Links and website addresses requested or redirected
  - Data accessed or files downloaded

- Time of sending and receiving the packet, and downloading the file
- Ports and protocols used to establish the connection
- DNS, TTL, or SSL certificates
- Location and type of any network issue

Some of the tools that can used to perform packet analysis include Cain & Abel, dSniff, ettercap, Network Grep, OmniPeek, Snoop, and Tcpdump. By performing packet analysis, incident responders can look for unusual protocol behavior or protocol violations, such as invalid option bits or invalid sequence numbers in a TCP packet, invalid flags, and invalid fragments. These protocol violations are a result of an intruder's attempt to bypass a firewall. Locating data packets with external source and destination addresses indicate compromised firewall hosts or an IP-spoofing attack. The responder should look for connections performed at unusual times or suspicious use of internet relay chat (IRC).

- **Performing Log Analysis**

Incident handling requires minute details of the network activities, such as their type, location, and time, to determine the incident process. Log files are the records of devices that include the processes performed using them over the duration of the log. Hence, such files provide a valuable source of evidence of malicious behavior on the network. Out of all the collected logs, one must identify, collect, and save the suspicious logs along with the firewall protocols for investigation purposes. Log analysis can take place either manually or with the help of log analysis tools. After analyzing the logs, filters are applied to avoid unnecessary data analysis.

The reliability of the log files directly depends on their accuracy, as modification of the logs can affect the validity of the entire log and subject it to suspicion.

- **Router logs**: These logs store network connectivity details, such as the date, time, and source and destination IPs and ports used. Routers follow different standards for storing logs in a network and contain details like date, time, source IP address, source-port, URL accessed, URL's IP address, and port used. These details can help incident responders during their investigations when they collect router logs to extract information such as the IP addresses and protocols.
- **Firewall logs**: These logs contain the date and time, mnemonic message, firewall action, source IP address and port, destination IP address and port, and type of request. These details are also useful to the investigators.
- **Intrusion detection system (IDS) logs**: In addition to monitoring and analyzing events to identify undesirable activity, all types of IDS technologies record information related to observed events. IDS devices store information locally and send it to other systems, such as centralized logging servers, security information and event management (SIEM) systems, and enterprise management systems. The IDS logs include the data and time, device IP address, attack type and severity,

source address and port, and destination address. These details also help the incident responders in detection of incidents.

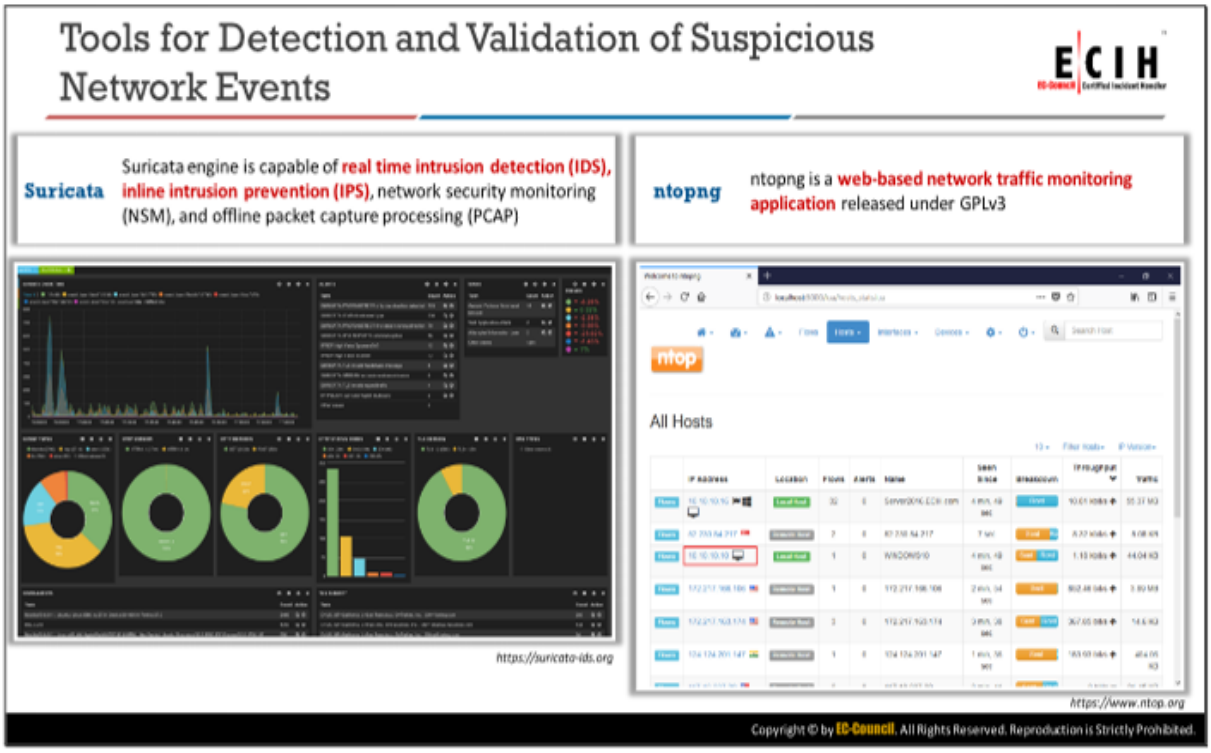
- **Performing Host Analysis**

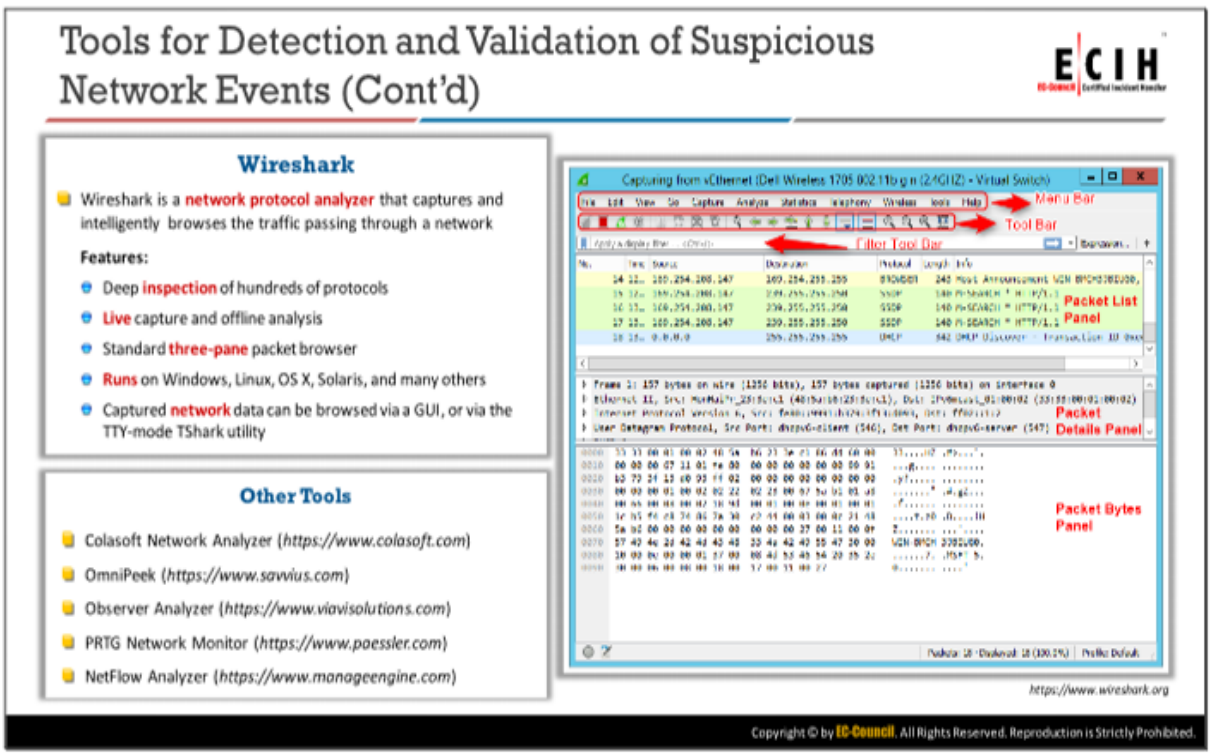
  To detect any malicious network security incident, incident responders should also perform host machine analysis to identify the presence of any malicious application, process, or service. This allows the incident responder to detect malicious process and its associated network sockets. First, suspicious files are located on the windows host and then static and dynamic analysis of the files is performed to extract information from the files and their associated functionalities. When incident responders perform host analysis, they use static malware analysis techniques such as file fingerprinting, local and online malware scanning, string searches, methods for identifying packing/obfuscation, location of portable executables (PE), and identification of file dependencies. In addition, malware disassembly and dynamic malware analysis techniques are used, including monitoring and analysis of ports, processes, registries, Windows services, startup programs, event logs, installations, files and folders, device drivers, network traffic, DNS, and API calls.

Detection Outcomes

By following the above techniques, incident responder can detect the following:

- Malicious sniffers present on the network
- Network misconfiguration issues such as IP routing issues, DNS information leakage, email routing issues, and non-functional firewall rules
- Unusual protocol behavior, such as invalid option bits or invalid sequence numbers in a TCP packet, invalid flags, and invalid fragments
- Malicious channel fingerprinting attempts
- Deliberate attempts to bypass firewall/proxy rules
- Incoming attacks against public-facing services
- Weak obfuscation, including XOR and ROR, to identify approaches to de-obfuscation
- Whether a generated alert is a true hit or false positive





Tools for Detection and Validation of Suspicious Network Events

Following are some of the tools that can be used to detect and validate network security incidents.

- **Suricata**

  Source: *https://suricata-ids.org*

  The Suricata engine has a real-time IDS, inline intrusion prevention system (IPS), network security monitoring (NSM), and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats. Standard input and output formats (e.g., YAML and JSON) allow easy integration with tools such as existing SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases. Suricata implements a complete signature language to match known threats, policy violations, and malicious behavior. Suricata can also detect many anomalies in the traffic it inspects, and uses the specialized Emerging Threats Suricata and VRT rulesets.

- **ntopng**

  Source: *https://www.ntop.org*

  ntopng is a web-based network traffic monitoring application released under GPLv3. ntopng is the next generation version of the original ntop, a network traffic probe that monitors network usage. It is based on libpcap and has been written in a portable way to virtually run on every Unix platform, MacOSX, and Windows.

  Features:

  - Sorts network traffic according to many criteria, including IP address, port, L7 protocol, throughput, and autonomous systems (ASs)
  - Shows real-time network traffic and active hosts
  - Produces long-term reports for several network metrics, including throughput and application protocols
  - Identifies top talkers (senders/receivers), ASs, and L7 applications
  - Monitors and reports live throughput, network and application latencies, round trip time (RTT), TCP statistics (retransmissions, out of order packets, packet lost), and bytes and packets transmitted
  - Stores persistent traffic statistics on disk to allow future investigation and post-mortem analyses
  - Geolocates and overlays hosts on a map
  - Identifies application protocols (Facebook, YouTube, BitTorrent, etc.) by leveraging nDPI, ntop Deep Packet Inspection (DPI) technology
  - Characterizes HTTP traffic by leveraging characterization services provided by Google and HTTP Blacklist.
  - Analyzes IP traffic and sorts it according to the source/destination.
  - Reports IP protocol usage sorted by protocol type

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark is a widely used network protocol analyzer. It captures and intelligently browses the traffic passing through a network. The components of Wireshark include:

  - **Menu Bar**: Hosts the features of Wireshark
  - **Tool Bar**: Hosts the more frequently used tools and icons
  - **Filter Tool Bar**: Filters the traffic based on filter options
  - **Packet List Panel**: Displays the captured packets
  - **Packet Details Panel**: Displays the detailed information regarding the captured packets at a granular level
  - **Packet Byte Panel**: Displays the captured packet's bytes in a hex dump format

  Features

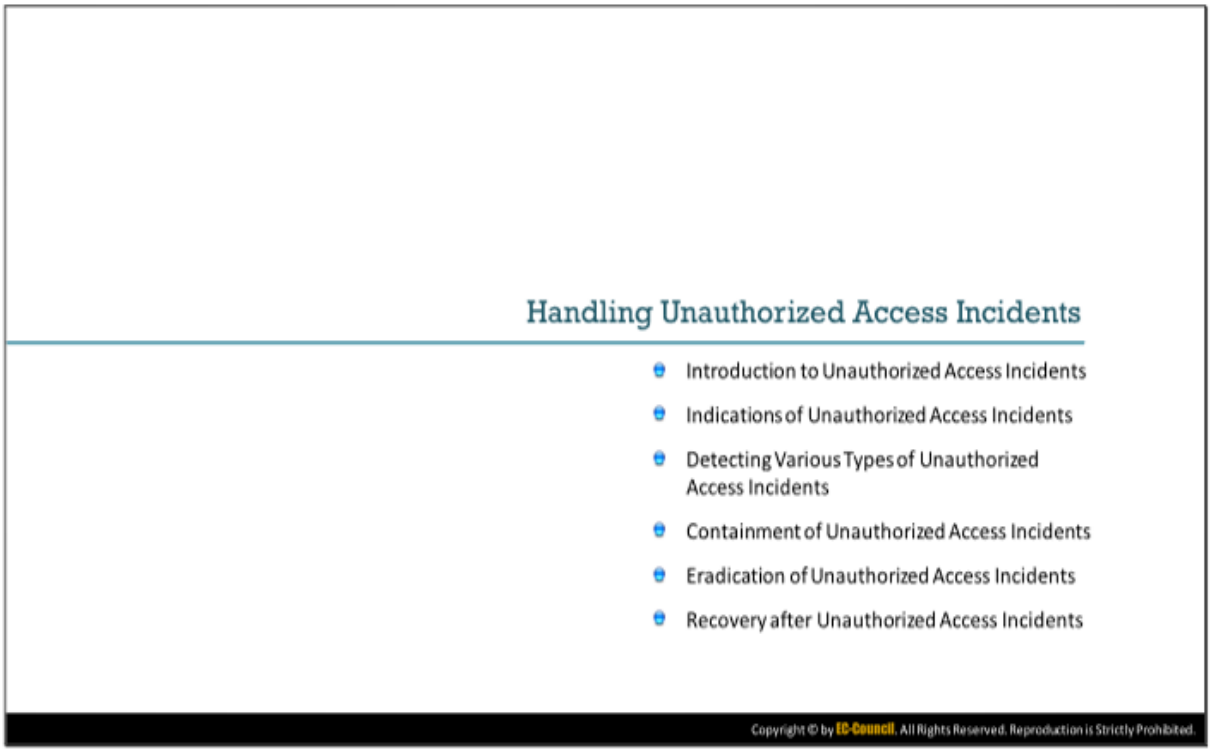
  - Deep inspection of hundreds of protocols
  - Live capture and offline analysis
  - Standard three-pane packet browser
  - Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
  - Captured network data can be browsed via a GUI, or the TTY-mode TShark utility

  Wireshark Capture and Display Filters

  - Application Layer
    - The filters are applied before starting the capture on the selected network interface
    - Filters are used to capture specific traffic on the network
    - Within the **Capture** menu, **Capture Filters…** is used to view all available capture filters
  - Transport Layer
    - Display filters are used to filter captured packets
    - Within the **Analyze** menu, **Display Filters…** is used to view all available display filters

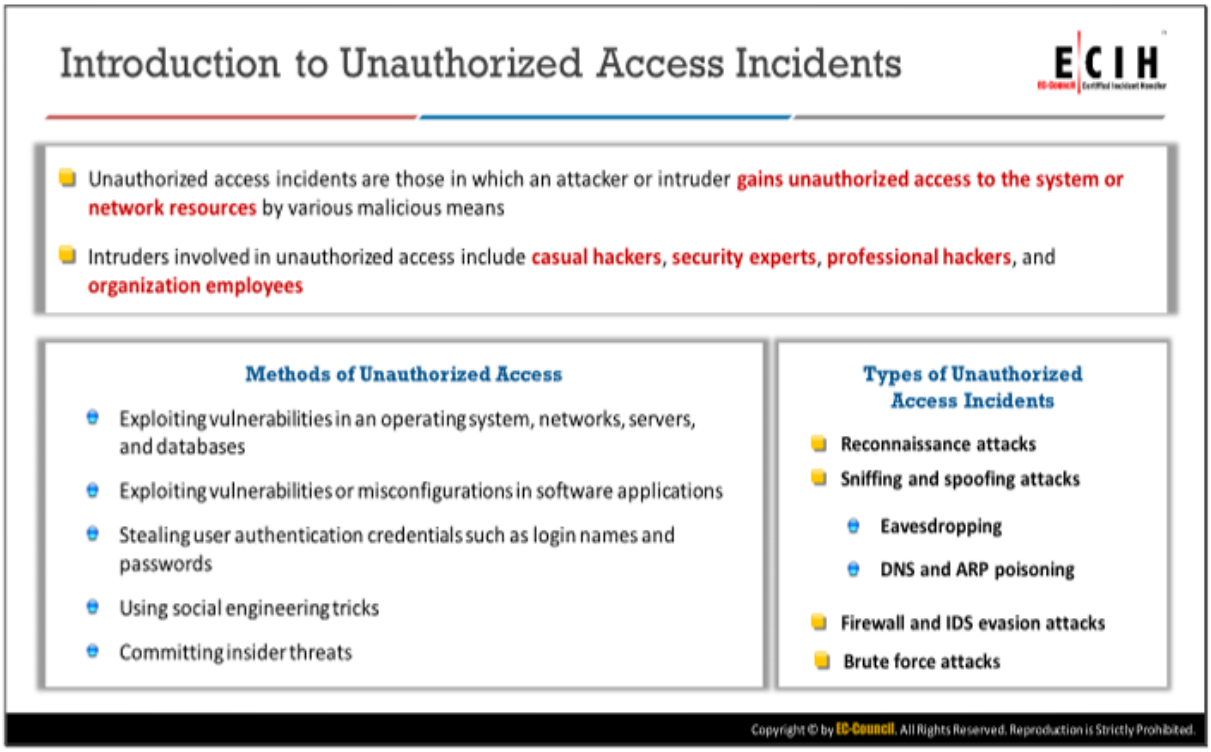
Some additional tools that can be used to monitor network traffic include:

- Colasoft Network Analyzer (*https://www.colasoft.com*)
- OmniPeek (*https://www.savvius.com*)
- Observer Analyzer (*https://www.viavisolutions.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- NetFlow Analyzer (*https://www.manageengine.com*)



Handling Unauthorized Access Incidents

Unauthorized access incidents are one of the most common network security incidents, where an attacker or intruder gains unauthorized access to the system or network resources by various malicious means. This section discusses the fundamental concepts of unauthorized access incidents and their indicators, along with techniques for the detection, containment, eradication, and recovery after these incidents.



Introduction to Unauthorized Access Incidents

An unauthorized access incident involves gaining illegal access to resources without authorization. Intruders involved in unauthorized access include casual hackers, security experts, professional hackers, and organizational employees.

An attacker can obtain unauthorized access in following ways:

- Access important data without permission
- Use accounts assigned to others
- Use the assigned account to obtain unauthorized access to particular services

Methods of unauthorized access include:

- Exploiting vulnerabilities in an operating system, networks, servers, and databases
- Exploiting vulnerabilities or misconfigurations in software applications
- Stealing user authentication credentials, such as login names and passwords
- Using social engineering tricks
- Insider threats

Generally, the attackers gain limited access to systems through an OS or application vulnerability and later escalate their privileges to higher levels.

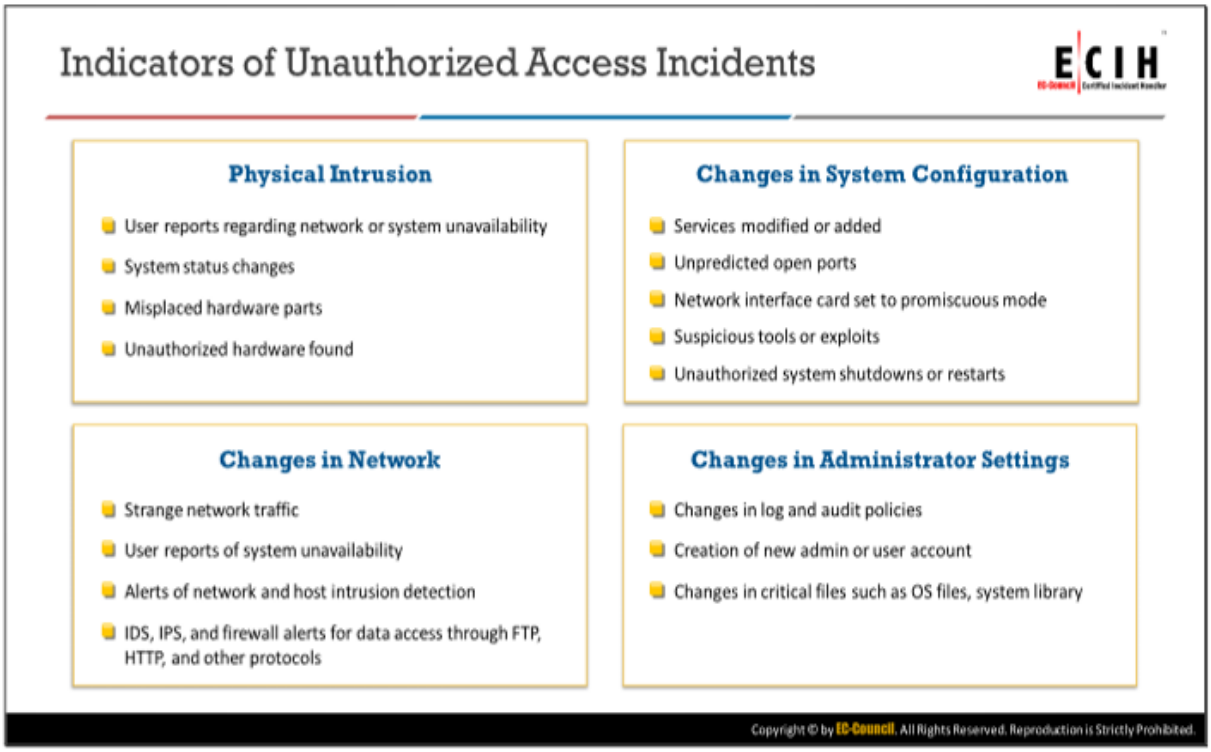
Unauthorized access incidents include:

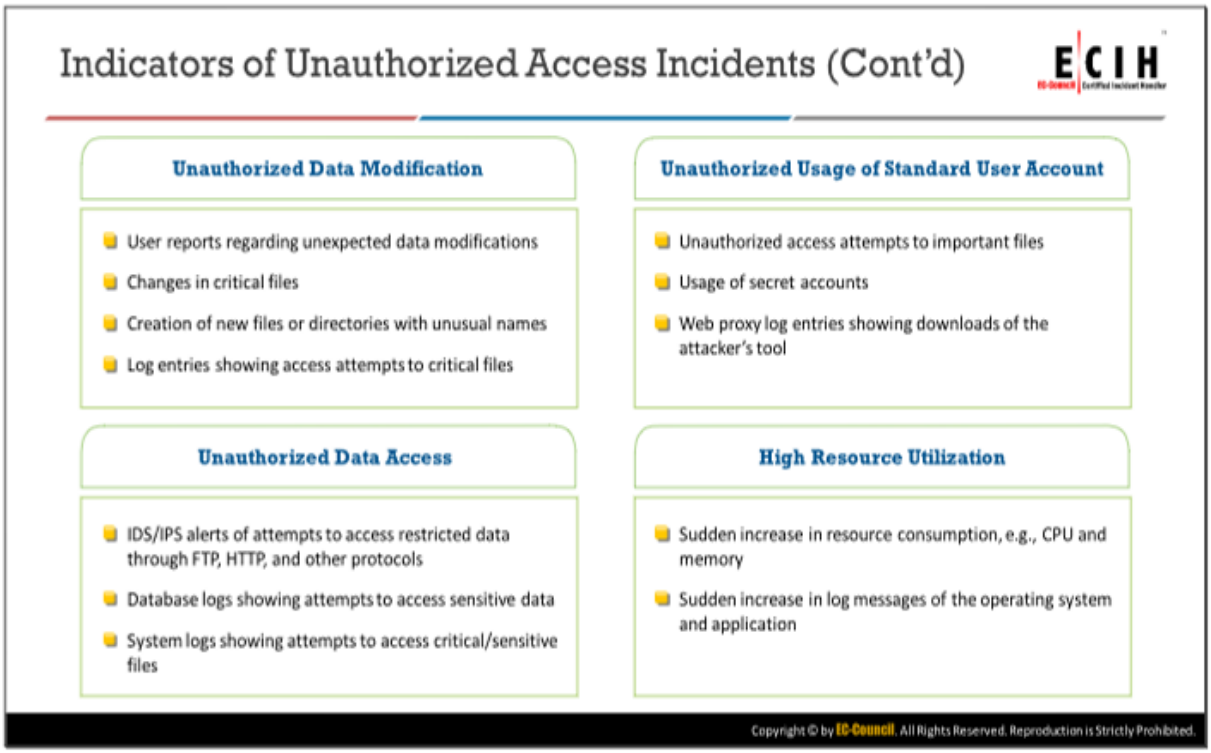
- Compromising the root of remote servers

- Changing web server contents that may result in webpage defacement or unavailability of web pages
- Guessing or cracking system and applications passwords
- Copying sensitive data without authorization
- Installing and running a packet sniffer on the workstation
- Using the FTP server to distribute data
- Internal network access by unsecured modem dialing
- Using social engineering to get the password from the help desk
- Accessing a workstation using a false ID

Following are some of the types of network attacks that help attackers gain unauthorized access:

- Reconnaissance attacks
- Sniffing and spoofing attacks
  - Eavesdropping
  - DNS and ARP poisoning
- Firewall and IDS evasion attacks
- Brute-force attacks





Indicators of Unauthorized Access Incidents

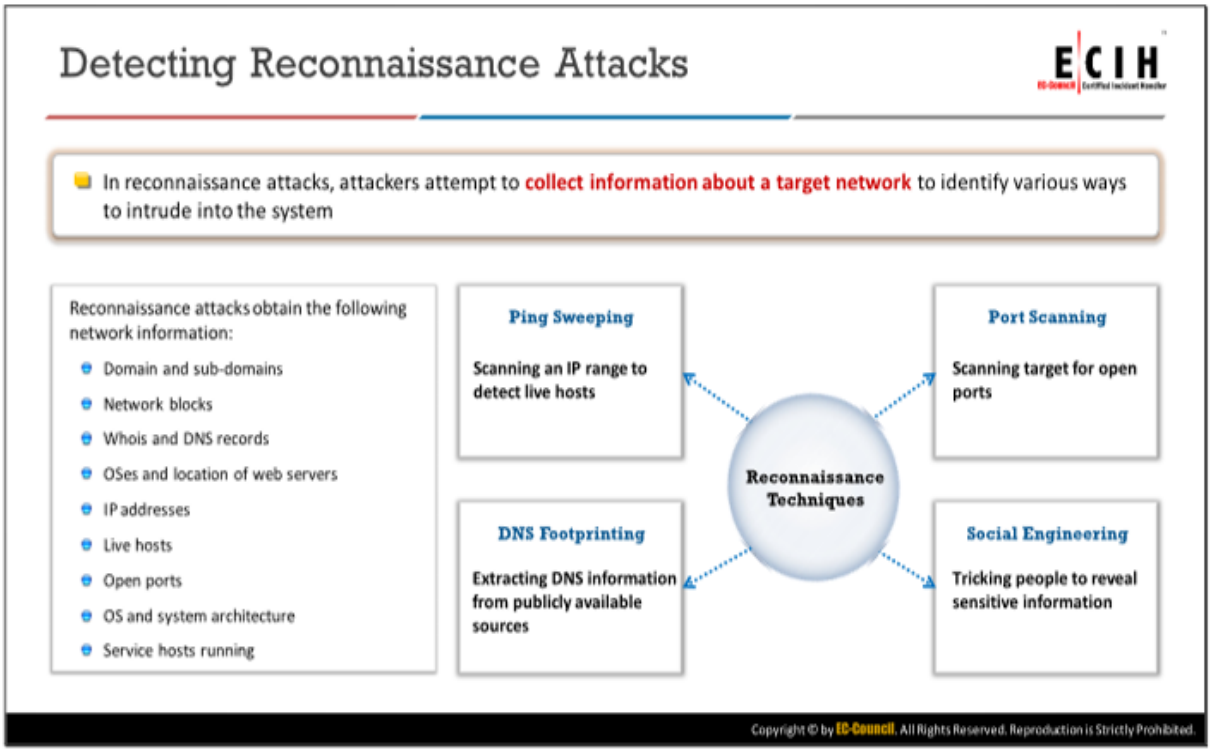
Unauthorized access incidents show some indicators that can help incident handlers classify the incidents. The system, network devices, administrator settings, security solutions, etc. can be subjected to this type of attack and exhibit indicators of compromise.

The following are possible indications of unauthorized access incidents:

- **Physical Intrusion**
  - User reports regarding network or system unavailability
  - System status changes
  - Misplaced hardware parts
  - Unauthorized hardware found
- **Changes in System Configuration**: The attackers modify the systems settings and configurations to perform attacks over the network, resulting in the following signs.
  - Modifications or addition of services
  - Unpredicted open ports
  - Network interface cards set to promiscuous mode
  - Suspicious tools or exploits
  - Unauthorized system shut down or restart
- **Changes in Network**: This type of intrusion occurs when attackers compromise networks and use it to gain access to sensitive data, resulting in the following indicators:
  - Unusual network traffic
  - User reports of system unavailability
  - Network intrusion detection system (NIDS) and host intrusion detection system (HIDS) alerts
  - IDS, IPS, and firewall alerts for data access through FTP, HTTP, and other protocols
- **Changes in Administrator Settings**: Attackers try to access administrator accounts and modify their settings to create backdoors and enable remote access, resulting in the following indicators:
  - Changes in log and audit policies
  - Creation of new administrative-level user accounts or groups
  - Changes in significant files such as OS files or a system library
  - Creation of new files or directories with unusual names
  - Increase in resource usage
  - Instances of log messages from the operating system and application
  - Instances of log entries showing access attempts to critical files
- **Unauthorized Data Modification**: Attacks including malware installation, data theft, and data deletion can result in data modification, with the following indicators:
  - User reports regarding unexpected data modifications

- Changes in critical files
- Creation of new files or directories with unusual names
- Logs entries showing access attempts to the critical files

- **Unauthorized Usage of a Standard User Account**: Attackers access accounts of employees to compromise organizational networks, with the following indicators:
  - Unauthorized attempts to access important files
  - Usage of secret account
  - Web proxy log entries showing downloads of the attacker's tool
- **Unauthorized Data Access:** Hackers exploit the networks and gain access to sensitive data, with the following indicators:
  - IDS/IPS system alerts of attempts to gain access to the restricted data through FTP, HTTP, and other protocols
  - Database logs showing attempts to access sensitive data
  - System logs showing attempts to access critical/sensitive files
- **High Resource Utilization**: Attackers perform malicious attempts like DoS and DDoS attacks on the networks to overwhelm network resources, which results in the following indicators:
  - Sudden increase in resource consumption e.g. CPU and memory
  - Sudden increase in log messages of the operating system and application



Detecting Reconnaissance Attacks

Reconnaissance refers to gathering of information. In reconnaissance attacks, attackers try to gather crucial information about the target network that is required to perform an attack. Network reconnaissance is one of the major forms of network attack. Attackers use network mapping tools such as Nmap and Network Topology Mapper to identify network vulnerabilities and exploit them.

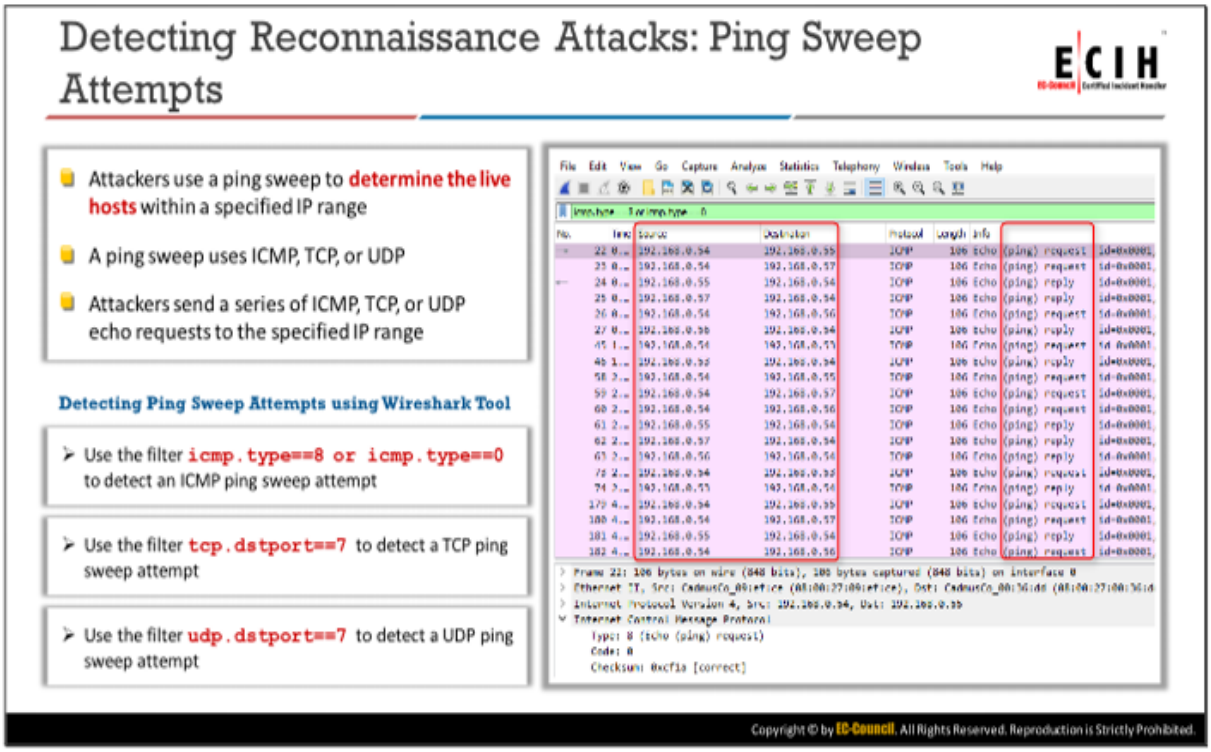
The following network information is obtained using reconnaissance attacks:

- Domain and sub-domains
- Network blocks
- Whois and DNS records
- OSes and location of web servers
- IP addresses
- TCP and UDP services running
- Live hosts
- Open ports
- OS and system architecture
- Running services on hosts
- Access control mechanisms and ACLs
- Networking protocols

- VPN points
- Deployed IDS and firewalls
- Employee details
- Web technologies used in the organization
- Analog/digital telephone numbers
- Employed authentication mechanisms

Following are some of the most common types of reconnaissance attacks used by attackers to exploit networks:

- **Ping Sweeping**: Scanning an IP range to detect live hosts
- **Port Scanning**: Scanning target for open ports
- **DNS Footprinting**: Extracting DNS information from publically available sources
- **Social Engineering**: Tricking people to reveal sensitive information



Detecting Reconnaissance Attacks: Ping Sweep Attempts

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique that is used to determine which range of IP addresses map to live hosts (computers). Although a single ping will tell the user whether one specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts. If a specified host is active, it will return an ICMP ECHO reply. Ping sweeps are among the oldest and slowest methods used to scan a network. This utility distributed across almost all the platforms acts as a roll call for systems; a system that is active on the network answers the ping query that another system sends out.

The TCP/IP packet needs to be understood to better understand pings. When a system pings, it sends a single packet across the network to a specific IP address. This packet contains 64 bytes (56 data bytes and 8 bytes of protocol header information). The sender then waits or listens for a return packet from the target system. If the connections are good and the target computer is "alive," a good return packet is expected. However, this will not be the case if there is a disruption in the communication. The ping also records the amount of time it takes for a packet to make the complete trip (round-trip time). In addition, the ping also helps resolve hostnames. In this case, if the packet bounces back when sent to an IP address, but not when sent to the name, then the system is unable to resolve the name of the specific IP address.

Attackers calculate subnet masks using subnet mask calculators to identify the number of hosts present in the subnet. Attackers subsequently use ping sweeps to create an inventory of live systems in the subnet, and determine the live hosts within a specified IP range by sending a series of ICMP, TCP, or UDP echo requests to the specified IP range.

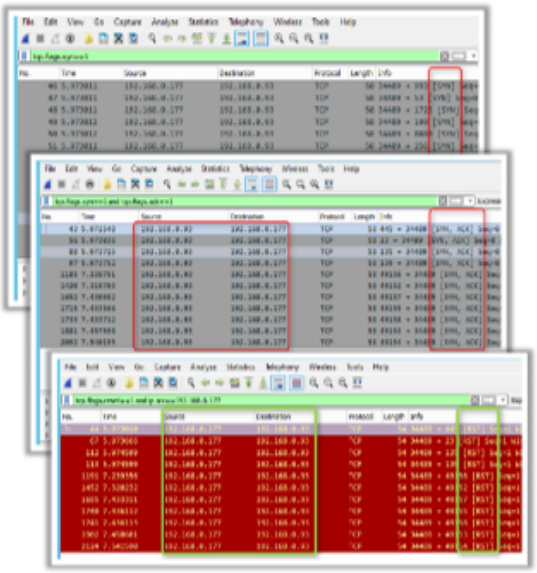
Incident handlers use the Wireshark tool to detect such ping sweep attempts on an organizational network. For example:

- Use the filter **`icmp.type==8 or icmp.type==0`** to detect an ICMP ping sweep attempt
- Use the filter **`tcp.dstport==7`** to detect a TCP ping sweep attempt
- Use the filter **`udp.dstport==7`** to detect an UDP ping sweep attempt

Detecting Reconnaissance Attacks: Port Scanning Attempts

Half Open/Stealth Scan Attempts

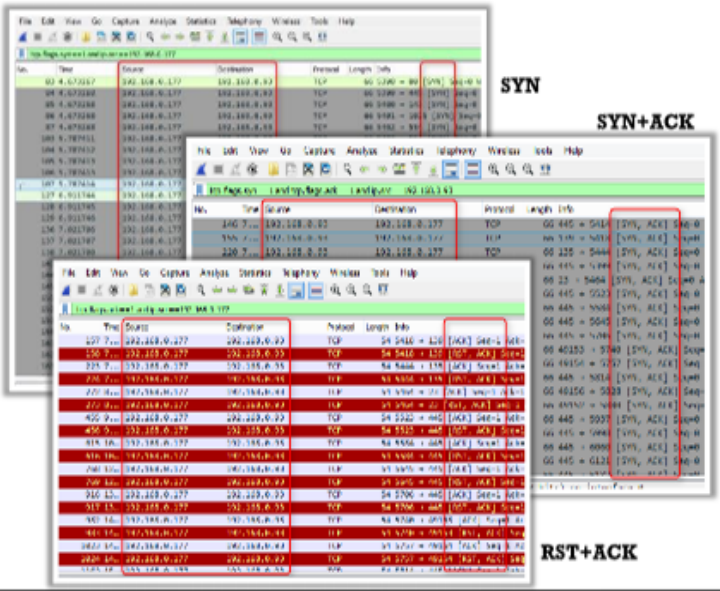
- Attackers use the TCP Half Open/Stealth port scan technique to find open TCP ports on the target system
- An attacker sends a SYN packet and receives a **SYN+ACK** response if the port is open and an **RST** response if the port is closed
- A stealth scan attempt is recognized if there is a large amount of **RST** or **ICMP type 3** packets.
- To detect stealth scans using Wireshark tool,
  - Go to **Statistics → Conversations** and click on the **TCP** tab to view and analyze multiple TCP sessions
  - If the TCP session is less than 4 packets of communications, then it is a sign of a TCP port scan on the network

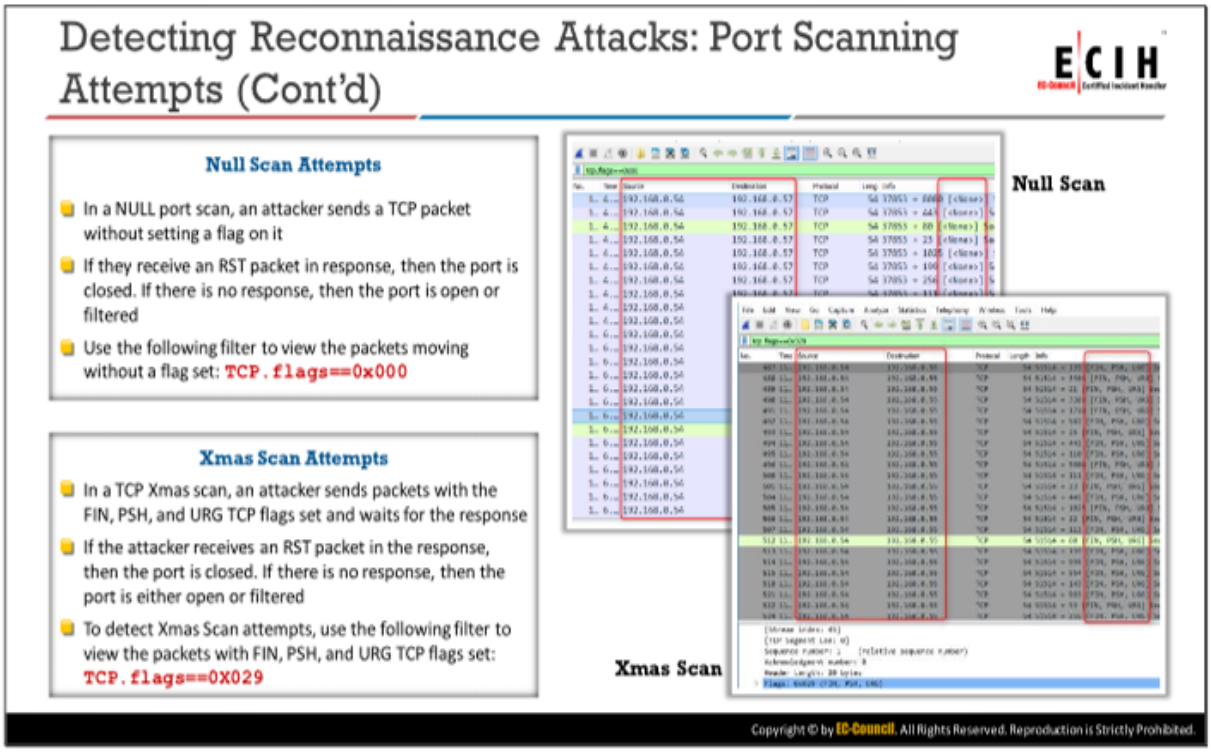


Detecting Reconnaissance Attacks: Port Scanning Attempts (Cont'd)

Full Connect Scan Attempts

- In a TCP full connect scan, the attacker performs a complete three-way handshake to find open ports on the target system
- A TCP full connect scan is recognized using the same methods used for detecting a stealth scan attempt
- To detect a full connect scan using the Wireshark tool, check for **SYN**, **SYN+ACK** and **RST+ACK**, packets or **ICMP type 3** packets





Detecting Reconnaissance Attacks: Port Scanning Attempts

It lists the open ports and services. Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a listening state. The listening state provides information about the operating system and the application currently in use. Sometimes, active services that are listening may allow unauthorized user access to misconfigure systems or to run software with vulnerabilities. Attackers perform port scanning to learn and gather information about open ports and services on the target network devices.

Detecting Half-open/Stealth-scan Attempts

The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, which leaves the connection half open. A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers. This type of scan sends a single frame with the expectation of a single response. The half-open scan partially opens a connection but stops halfway through. The stealth scan is also called a "SYN scan," because it only sends the SYN packet. This prevents the service from notifying the incoming connection. TCP SYN or half-open scanning is a stealth method of port scanning. The stealth scan also implements the three-way handshake methodology. In the last stage, it examines the packets entering the interface and terminates the connection before triggering a new initialization to identify remote ports. The stealth scan process is shown below.

- The client sends a single SYN packet to the server on the appropriate port.
- If the port is open, the server subsequently responds with an SYN/ACK packet.

- If the server responds with an RST packet, then the remote port is in the "closed" state.
- The client sends the RST packet to close the initiation before a connection can be established.

Attackers use the TCP half-open/stealth port scan technique to find open TCP ports on the target system. An attacker sends a SYN packet and receives a SYN+ACK response if the port is open and an RST response if the port is closed. A stealth scan attempt is recognized if there are a large amount of RST or ICMP type-3 packets.

Incident handler can use the Wireshark tool to detect half-open/stealth scan attempts via the steps below:

- Under **Statistics → Conversations,** the **TCP** tab is used to view and analyze multiple TCP sessions.
- If the TCP session is less than four communication packets, then it is a sign of a TCP port scan on the network.

In the Wireshark screenshots shown on the above slide, a three-way hand shake process is shown, as a result of half-open/stealth scan attempts. The source machine with the IP address 192.168.0.177 initiated scanning by sending a SYN packet to the destination machine with IP address 192.168.0.93. Then, the destination machine responds to the source with SYN+ACK packets. Later, the handshaking process ends when the source machine sends RST packets to the destination machine.

Detecting Full Connect Scan Attempts

In TCP connect scanning, the TCP connect() call system of the OS tries to open a connection to every interesting port on the target machine. If the port is listening, the connect() call will result in a successful connection with the host on that particular port; otherwise, it will return an error message stating that the port is not reachable. The TCP connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with a SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is complete, the scanner sends an RST packet to end the connection.

Making a separate connect() call for every targeted port in a linear fashion would take a long time over a slow connection. The attacker can accelerate the scan using many sockets in parallel. Using a non-blocking process, the I/O allows the attacker to set a low time-out period and watch all sockets simultaneously. The drawback of this type of scan is that it is easily detectable and filterable, and logs in the target system will disclose the connection. This type of scanning does not require super-user privileges.

In a TCP full connect scan, the attacker performs a complete three-way handshake to find open ports on the target system. The incident handler can use Wireshark to detect half-open/stealth scans using the same methods used for detecting a stealth scan attempt, i.e., checking for SYN, SYN+ACK, and RST+ACK packets or ICMP type-3 packets. In the Wireshark screenshots shown on the above slide, the source machine with IP address 192.168.0.177 initiates the scan by sending SYN packets to the destination machine with IP address 192.168.0.93. Later, the

destination machine responds with SYN+ACK packets. Finally, the source responds with RST+ACK packets, completing the initiation of the full connect scan.

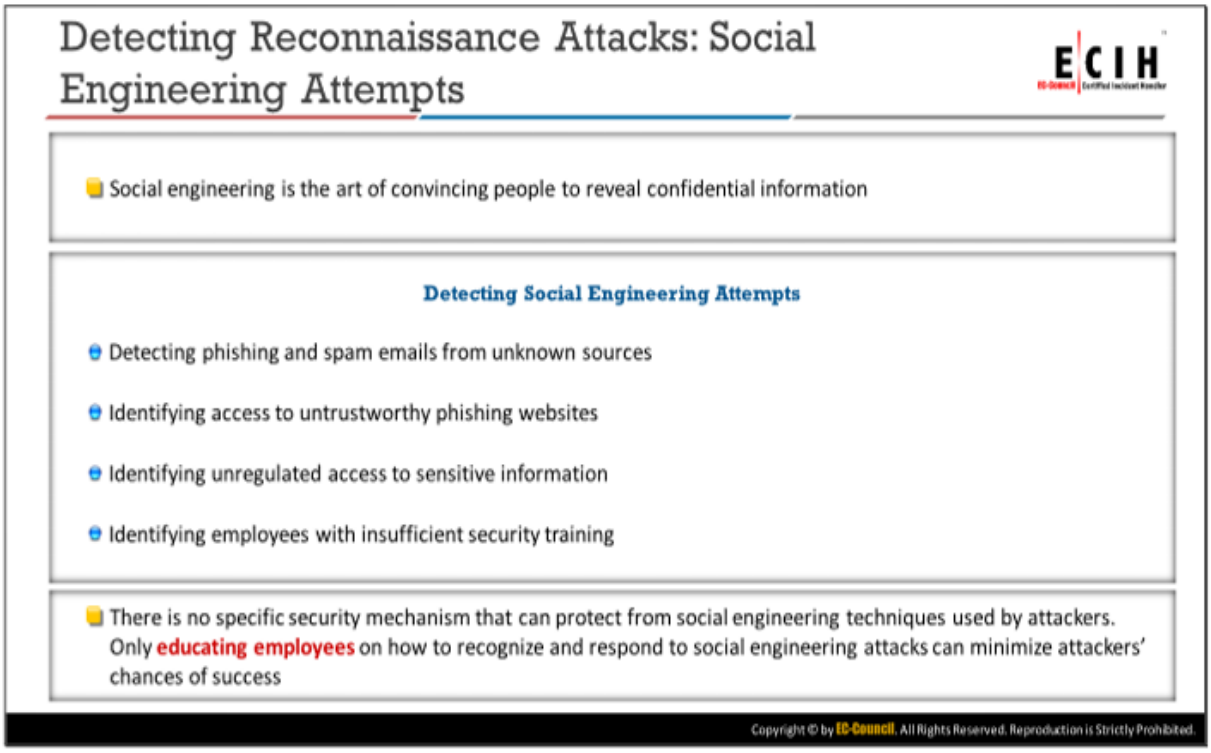
Detecting Null Scan Attempts

In a null port scan, an attacker sends a TCP packet without setting a flag on it. If they receive an RST packet in response, then the port is closed. If there is no response, then the port is open or filtered. The **TCP.flags==0x000** filter in Wireshark is used to view the packets moving without a flag set. In the Wireshark screenshot shown on the above slide, the source IP address is 192.168.0.54 which is null scanning the destination machine 192.168.0.57.

Detecting Xmas Scan Attempts

A Xmas scan is a port scan technique with FIN, URG, and PUSH flags set to send a TCP frame to a remote device. If the target has opened the port, then no response will be received from the remote system. If the target has closed the port, then a remote system reply is received with an RST. This port-scanning technique is used to scan large networks and identify which host is active and what services it is offering. This is a technique for describing all TCP flags that are set. When all flags are set, some systems hang; so, the flags most often set are the URG-PSH-FIN.

Attackers use the TCP XMAS scan to determine if ports are closed on the target machine via an RST packet. This scan only works when systems are compliant with RFC 793-based TCP/IP implementation. It will not work with any current version of Microsoft Windows. In a TCP Xmas scan, an attacker sends packets with the FIN, PSH, and URG TCP flags set and waits for the response. If an RST packet is received in response, then the port is closed. If there is no response, then the port is either open or filtered. The **tcp.flags==0X029** filter in Wireshark is used to view the packets with FIN, PSH, and URG TCP flags set.

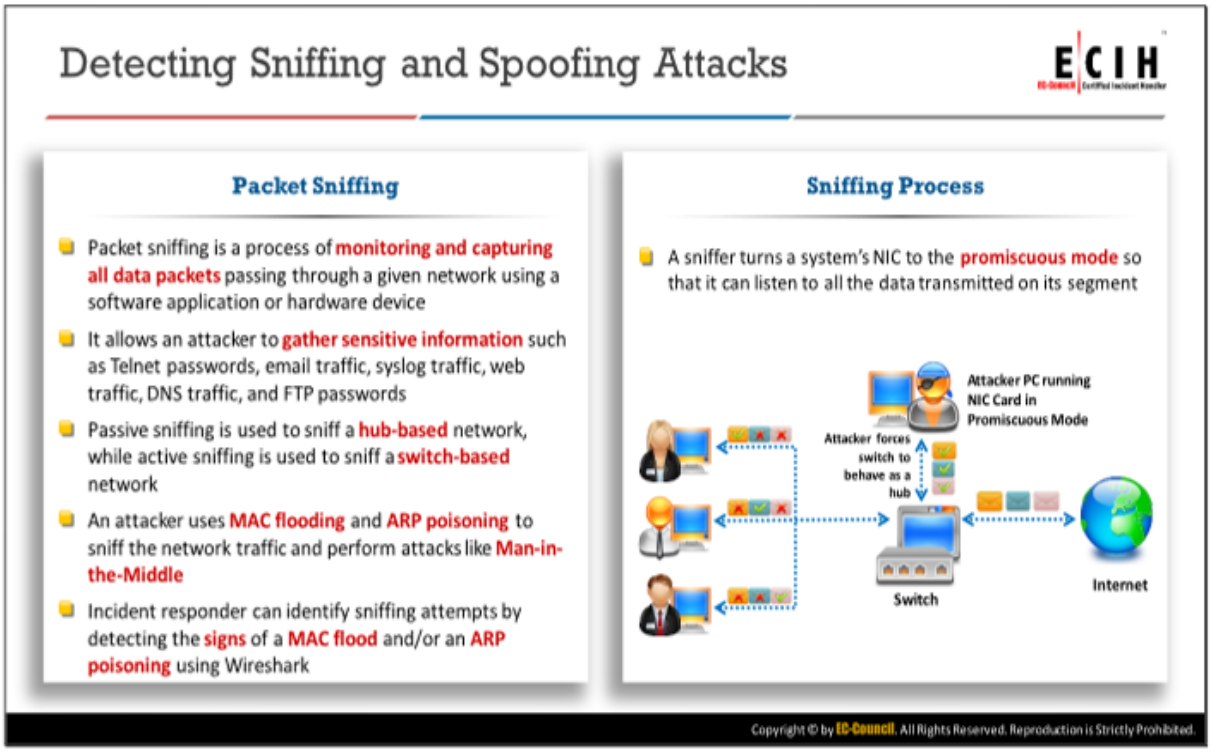


Detecting Reconnaissance Attacks: Social Engineering Attempts

Social engineering is the art of convincing people to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, and system administrators. Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it. Some techniques that can be used by an incident responder to detect social engineering attacks include:

- Detecting phishing and spam emails from unknown sources
- Identifying access to untrusted phishing websites
- Identifying unregulated access to the sensitive information
- Identifying employees with insufficient security training

There is no single specific security mechanism that can protect an organization from the social engineering techniques used by attackers. Only educating employees on how to recognize and respond to social engineering attacks can minimize the attackers' chance of success.



Detecting Sniffing and Spoofing Attacks

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all hosts associated with that segment. However, most current networks work using switches, which are advanced computer networking devices. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the media access control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network. Passive sniffing is used to sniff a hub-based network, while active sniffing is used to sniff a switch-based network.

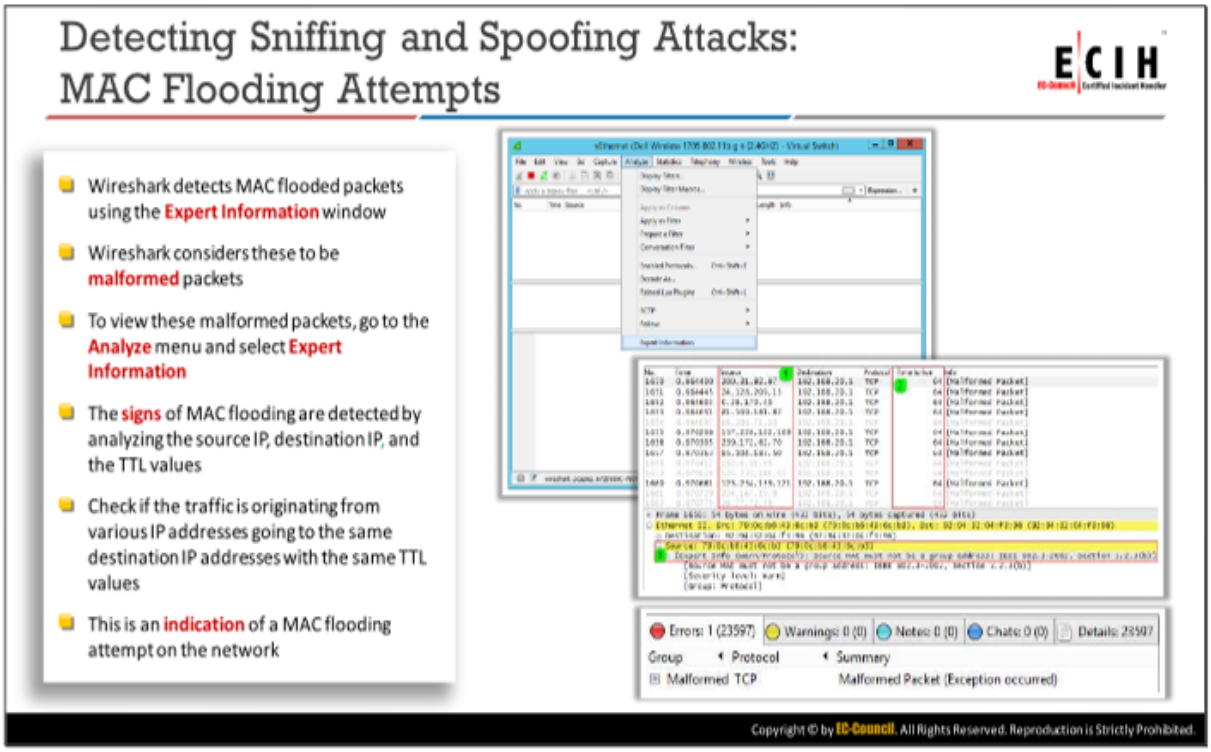
Though most networks today employ switch technology, packet sniffing is still useful. This is because installing remote sniffing programs on network components with heavy traffic flows, such as servers and routers, is relatively easy. This allows an attacker to observe and access the entire network traffic from one point. Packet sniffers can capture data packets containing sensitive information, such as passwords, account information, syslog traffic, router configuration, DNS traffic, email traffic, web traffic, chat sessions, and FTP passwords. In addition, attackers can read passwords in clear text, along with emails, credit card numbers, financial transactions, and other sensitive information. This method also allows an attacker to sniff SMTP, POP, IMAP traffic, POP, IMAP, HTTP Basic, Telnet authentication, SQL database, SMB, NFS, and FTP traffic. An attacker can access much information by reading captured data packets and then using that data to break into the network. An attacker carries out attacks that are more effective by combining these techniques with active transmission. The following schematic shows an attacker sniffing the data packets between two legitimate network users.

Figure 6.1: Packet sniffing through a switch

Sniffing Process

The most common way of networking computers is through an Ethernet. A computer connected to a local area network (LAN) has two addresses: a MAC address and an internet protocol (IP) address. A MAC address uniquely identifies each node in a network and is stored on the NIC itself. The Ethernet protocol uses the MAC address to transfer data to and from a system while building data frames. The data link layer (DLL) of the OSI model uses an Ethernet header with the MAC address of the destination machine instead of the IP address. The network layer is responsible for mapping IP network addresses to the MAC address as required by the data link protocol. It initially looks for the MAC address of the destination machine in a table, usually called the address resolution protocol (ARP) cache. If there is no entry for the IP address, an ARP broadcast of a request packet gets sent to all machines on the local sub-network. The machine with that particular address responds to the source machine with its MAC address. The ARP cache of the source machine adds this MAC address to the table, which then uses this MAC address in all communication with the destination machine.

An attacker spoofs his identity and uses Mac flooding or ARP poisoning to sniff the network traffic and perform attacks such as a man-in-the-middle attack. Indicators of a Mac flood and/or an ARP poisoning can be detected by an incident responder using Wireshark to identify spoofing and sniffing attempts.

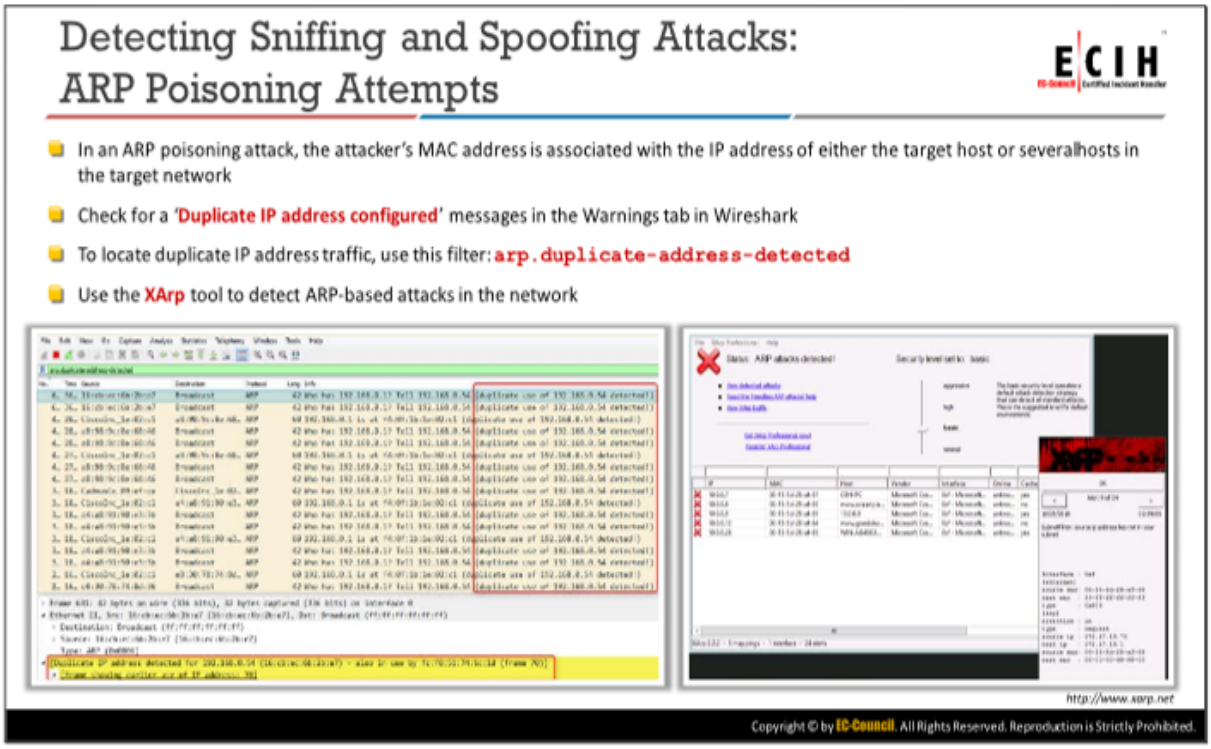


Detecting Sniffing and Spoofing Attacks: MAC Flooding Attempts

Switches keep a translation table that maps various MAC addresses to the physical ports on the switch. Hence, they can intelligently route packets from one host to another. However, switches have limited memory. MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches become overloaded and enter fail-open mode. In this condition, the switch starts acting as a hub by broadcasting packets to all ports on the switch, which makes it easy to perform sniffing.

Wireshark detects MAC-flooded packets using the **Expert Information** window and considers these malformed packets. To view these malformed packets:

- Under the **Analyze** menu, **Expert Information** is used.
- The signs of a MAC flooding are detected by analyzing the source IP, destination IP, and the TTL values.
- It is then confirmed if the traffic is originating from various IP addresses and being sent to the same destination IP addresses with the same TTL values. This is an indication of a MAC flooding attempt on the network.



Detecting Sniffing and Spoofing Attacks: ARP Poisoning Attempts

ARP is stateless. The machine can send an ARP reply even without receiving a request, and accepts such a reply. When a machine wants to sniff the traffic originating from another system, it can ARP spoof or poison the gateway of the network. The ARP cache of the target machine will then have a wrong entry for the gateway. In this way, all traffic destined to pass through the gateway will now pass through the machine that spoofed the gateway MAC address. ARP packets can be forged to send data to the attacker's machine. ARP spoofing involves constructing a large number of forged ARP requests and reply packets to overload a switch. The switch enters "forwarding mode" after the ARP table is flooded with spoofed ARP replies, allowing attackers to sniff all network packets. Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning. In an ARP poisoning attack, the attacker's MAC address is associated with the IP address of the target host or several hosts in the target network.

An incident handler can use Wireshark to detect ARP poisoning attempts:

- Checking for "**duplicate IP address configured**" messages in the **Warnings** tab.
- To locate duplicate IP address traffic, the following filter is used:

  `arp.duplicate-address-detected`
- **XArp**

  Source: *http://www.xarp.net*

  Incident handlers can also use XArp as a tool to detect ARP-based attacks in the network. This tool detects critical network attacks that firewalls cannot block and uses advanced techniques to detect ARP attacks like ARP spoofing. The detection mechanism

relies on two techniques: inspection modules and discoverers. Inspection modules look at ARP packets and check their correctness and validity with respect to the established databases. Discoverers actively validate IPMAC mappings and actively detect attackers. The mechanism detects ARP attacks and keeps data private. This application even monitors whole subnets for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

Some other ARP spoofing detection tools are listed below:

- Capsa Network Analyzer (*http://www.colasoft.com*)
- ArpON (*http://arpon.sourceforge.net*)
- ARP AntiSpoofer (*https://sourceforge.net*)
- ARPStraw (*https://github.com*)
- shARP (*https://github.com*)

Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques

Promiscuous Mode

- Users will need to **check which machines are running** in the promiscuous mode
- Promiscuous mode allows a network device to **intercept and read in its entirety each network packet** that arrives

IDS

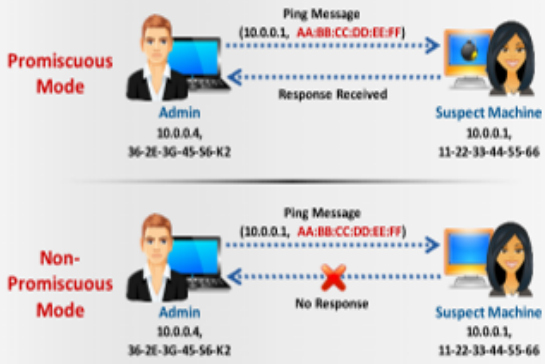
- **Run IDS** and notice if the **MAC address** of certain machines has changed (Example: check router's MAC address)
- IDS can alert the administrator about **suspicious activities**

Network Tools

- Run network tools such as **Capsa Network Analyzer** to monitor the network and detect strange packets
- Enables users to **collect**, **consolidate**, **centralize**, and **analyze traffic data** across different network resources and technologies

Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques (Cont'd)

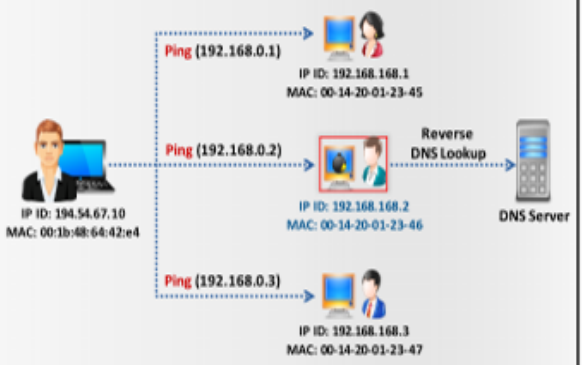
Ping Method



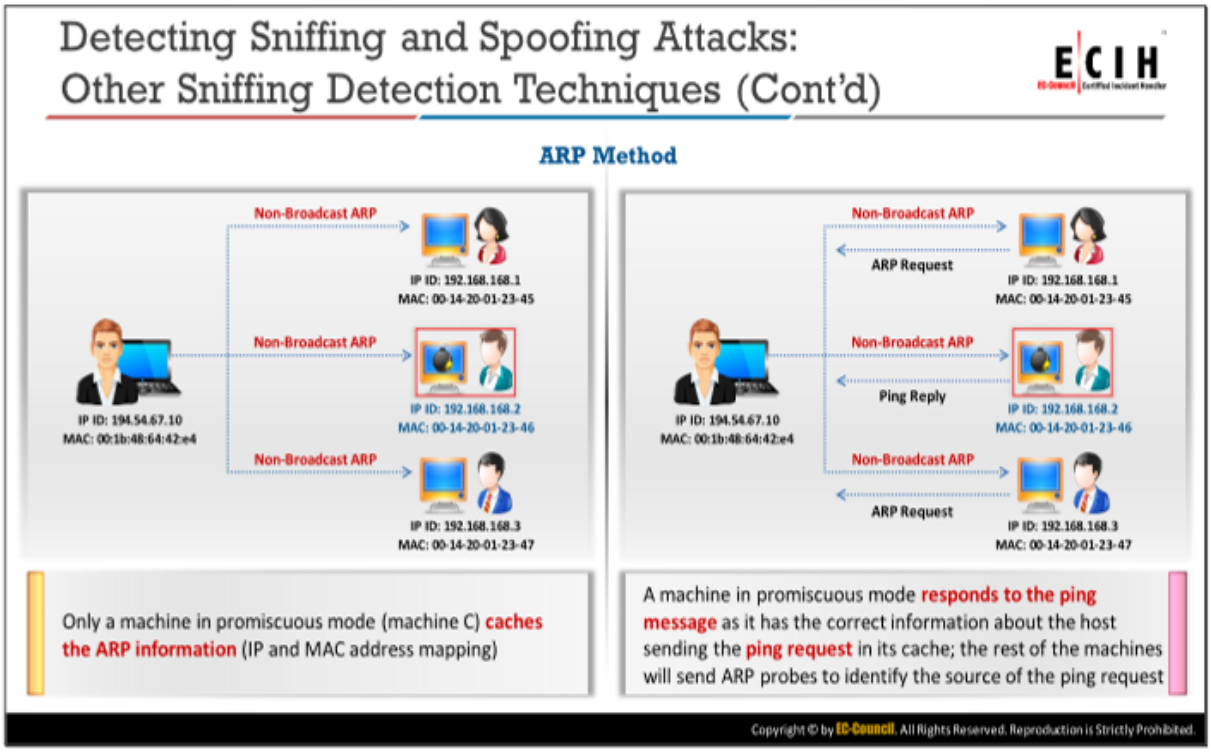
- A ping method sends a ping request to the suspect machine with its IP address and **incorrect MAC address**. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the **sniffer responds** to it as it does not reject packets with different MAC addresses

DNS Method

- Most of the sniffers perform **reverse DNS lookup** to identify the machine from the IP address



- A machine generating **reverse DNS lookup traffic** will be most likely running a sniffer



Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques

Some other sniffing detection techniques are discussed below.

- **Promiscuous Mode**

  It is not easy to detect a sniffer on a network as it only captures data and runs in promiscuous mode, which is a NIC mode that allows all packets (traffic) to pass, without validating its destination address. This allows a network device to intercept and read

each network packet that arrives in its entirety. Standalone sniffers leave no trace as they do not transmit data. To find sniffers, the tool needs to check for systems that are running in promiscuous mode. The reverse DNS lookup method helps detect non-standalone sniffers. There are many tools, such as the Nmap, which are used to detect use of promiscuous mode.

- **IDS**

  IDS is run to check if the MAC address of certain machines (e.g., a router) has changed. The IDS can detect sniffing activities on a network and send a notification or alert to the administrator when a suspicious activity such as sniffing or MAC spoofing occurs.

- **Network Tools**

  Network tools, such as Capsa Network Analyzer, monitor the network for strange packets, such as those with spoofed addresses. This tool can collect, consolidate, centralize, and analyze traffic data across different network resources and technologies.

- **Ping Method**

  To detect a sniffer on a network, the system on the network running in promiscuous mode can be identified using the ping method. In this method, a ping request is sent to the suspected machine with its IP address and incorrect MAC address. The adapter will reject it since the MAC address does not match, whereas the suspect machine running the sniffer responds to it, as it does not reject packets with different MAC addresses. Hence, this response identifies the sniffer in the network.

- **DNS Method**

  The reverse DNS lookup is the opposite of the DNS lookup method. Sniffers using reverse DNS lookup increase network traffic, which can be used as an indicator of the presence of a sniffer on the network. Users can perform a reverse DNS lookup remotely or locally. Monitor the organization's DNS server to identify incoming reverse DNS lookups. The method of sending ICMP requests to a non-existing IP address can also monitor reverse DNS lookups. The computer performing the reverse DNS lookup would respond to the ping, thus identifying it as hosting a sniffer. For local reverse DNS lookups, the detector is configured in promiscuous mode. An ICMP request is sent to a non-existing IP address, and the response is observed. If the system receives a response, the user can identify the responding machine as performing reverse DNS lookups on the local machine, which is most likely running a sniffer.

- **ARP Method**

  This technique sends a non-broadcast ARP to all nodes in the network. The node running in promiscuous mode on the network will cache the local ARP address. Then, it will broadcast a ping message on the network with the local IP address, but a different MAC address. In this case, only the node with the MAC address cached earlier can respond to the broadcast ping request. A machine in promiscuous mode replies to the ping message as it has correct information in its cache about the host that is sending the

ping request, while the other machines send ARP probes to identify the source of the ping request. This identifies the node on which the sniffer is running.

- **Using Promiscuous Detection Tools**
  - **PromqryUI**

    Source: *https://www.microsoft.com*

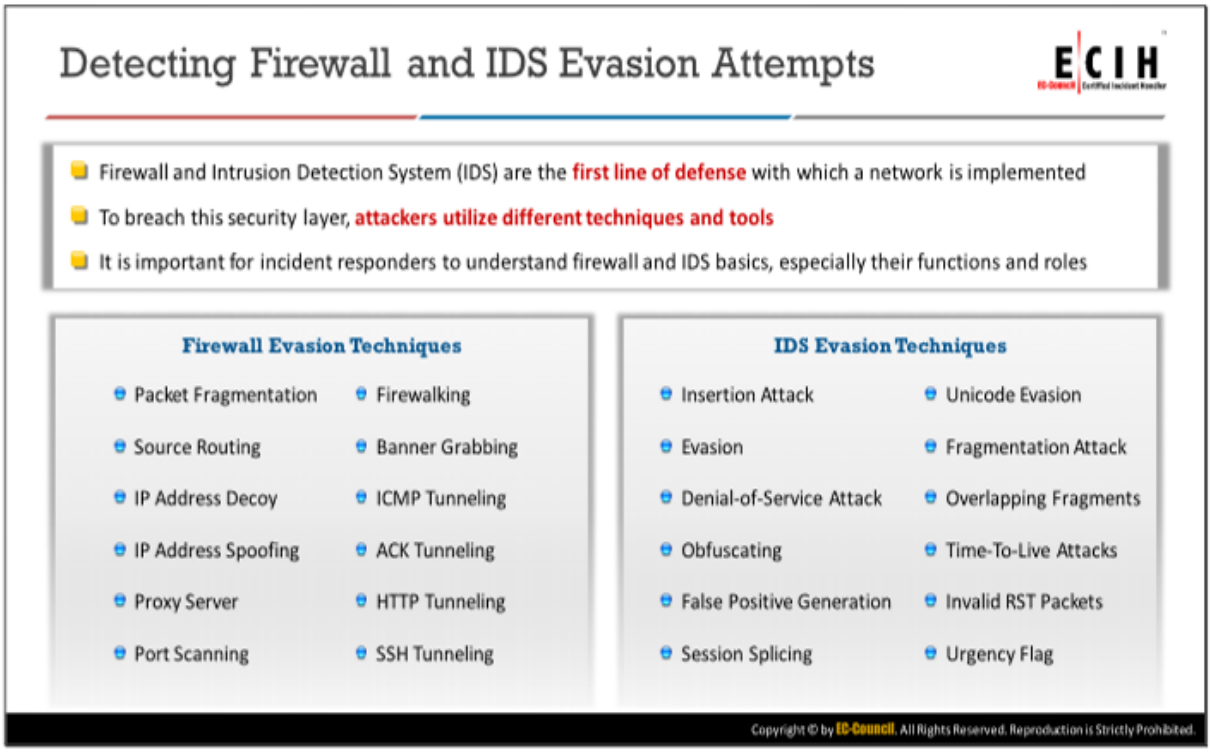
    The PromqryUI tool can accurately determine which network interface card on a Windows system is running in promiscuous mode, which can indicate the presence of a network sniffer. A version of PromqryUI is available as a command line tool. PromqryUI can query the interfaces of a local computer, a single remote computer, and various remote computers.

  - **Nmap**

    Source: *https://nmap.org*

    Nmap's NSE script can check if a target on a local Ethernet has its network card in promiscuous mode using the following command:

    ```
    nmap --script=sniffer-detect [Target IP Address/Range of IP addresses
    ```



Detecting Firewall and IDS Evasion Attempts

The firewall and IDS are the first line of defense for a network. To breach this security layer, the attackers use different techniques and tools. Hence, it is important for an incident responder to understand the basic concepts of firewalls and IDS, especially their functioning, roles, placement, and design in their implementation to protect an organization's network. This enables the incident responder to understand how an attacker evades the security of firewalls and IDS.

Techniques used to Evade Firewalls

Bypassing firewalls is a technique where an attacker manipulates the attack sequence to avoid being detected by an underlying security firewall. The firewall operates on a predefined set of rules, which can be bypassed by an attacker with appropriate knowledge and skills using various techniques that trick the firewall into letting the malicious traffic through its filter.

Following are some of the firewall bypassing techniques:

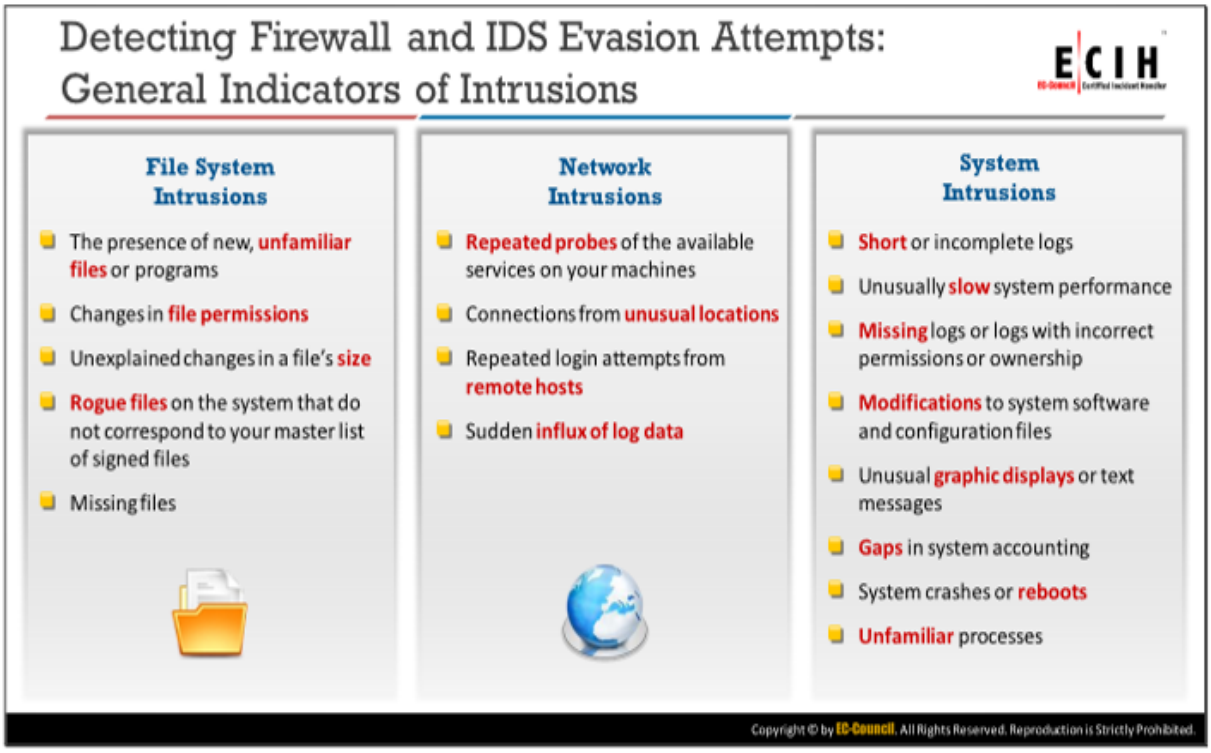
- Port scanning
- Firewalking
- Banner grabbing
- IP address spoofing
- Source routing
- Tiny fragments
- Using IP address in place of URL

- Using anonymous website surfing sites
- Using a proxy server
- ICMP tunneling
- ACK tunneling
- HTTP tunneling
- SSH tunneling
- Via external systems
- Via MITM attack
- Via content
- Via XSS attack

Techniques used to Evade IDS

An IDS provides an extra layer of security in the organization's infrastructure and hence is a target for attackers. Attackers implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. IDS evasion is the process of modifying the attacks to fool the IDS/IPS systems into labeling the malicious traffic as legitimate, and preventing the IDS from triggering an alert. There are many different IDS evasion techniques, including:

- Insertion attack
- Evasion
- Denial-of-service attack
- Obfuscating
- False positive generation
- Session splicing
- Unicode evasion
- Fragmentation attack
- Overlapping fragments
- Time-to-live attacks
- Invalid RST packets
- Urgency flag
- Polymorphic shellcode
- ASCII shellcode
- Application-layer attacks
- Desynchronization
- Encryption
- Flooding

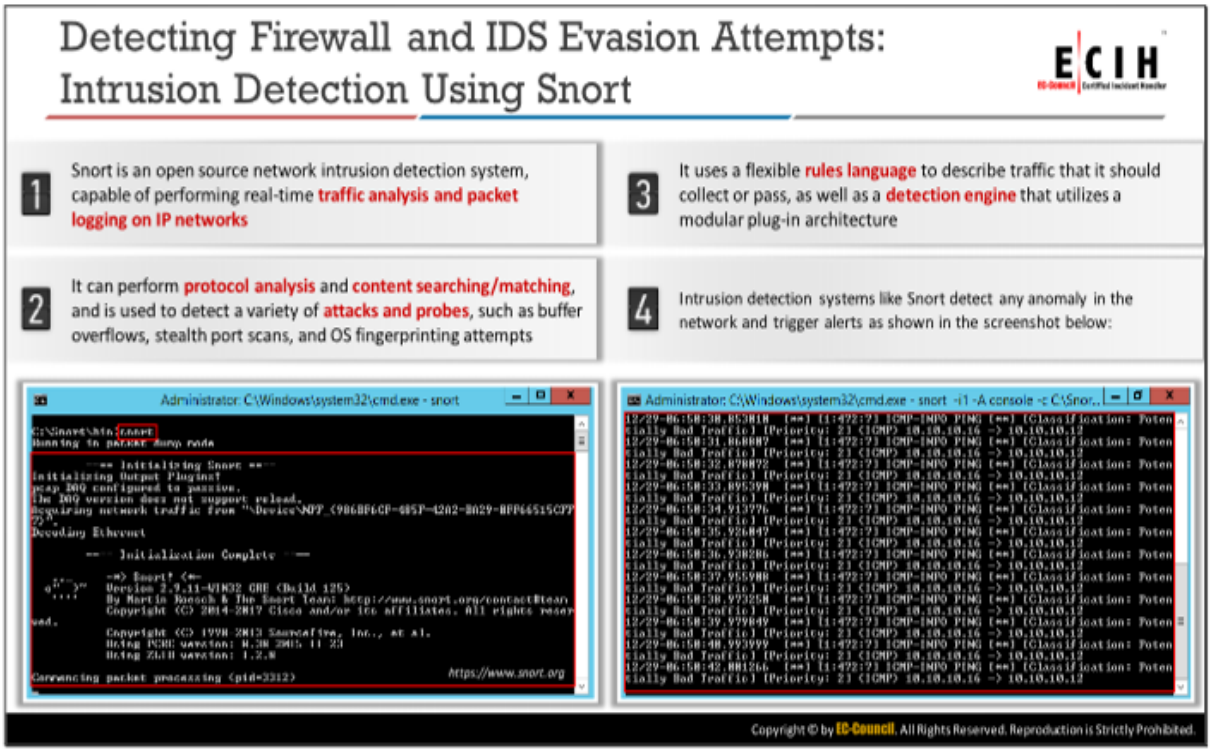


Detecting Firewall and IDS Evasion Attempts: General Indicators of Intrusions

Following are some of the general indicators of intrusions:

- **File System Intrusions**
  - The presence of new, unfamiliar files, or programs
  - Changes in file permissions
  - Unexplained changes in a file size
  - Rogue files on the system that do not correspond to your master list of signed files
  - Missing files
- **Network Intrusions**
  - Repeated probes of the available services on your machines
  - Connections from unusual locations
  - Repeated login attempts from remote hosts
  - Sudden influx of log data
- **System Intrusions**
  - Short or incomplete logs
  - Unusually slow system performance
  - Missing logs or logs with incorrect permissions or ownership
  - Modifications to system software and configuration files

- Unusual graphic displays or text messages
- Gaps in system accounting
- System crashes or reboots
- Unfamiliar processes



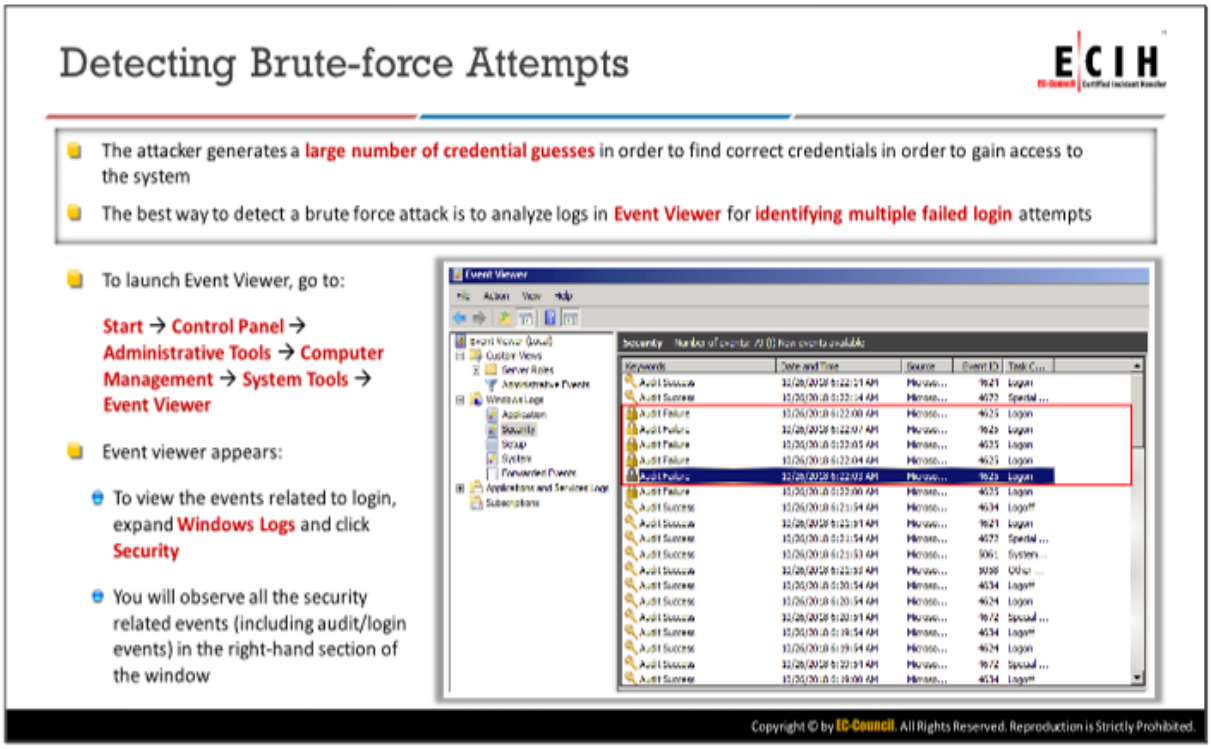
Detecting Firewall and IDS Evasion Attempts: Intrusion Detection Using Snort

Source: *https://www.snort.org*

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, and OS fingerprinting attempts. It uses a language with flexible rules to decide whether traffic should be collected or allowed to pass, as well as a detection engine that uses a modular plug-in architecture. Intrusion detection systems like Snort detect any anomaly in the network and trigger alerts, as shown in the screenshots on the above slide.

Detecting Firewall and IDS Evasion Attempts: Reviewing Firewalls/IDS Logs

Firewall and IDS devices are generally configured to maintain secure operations and identify any intrusions. If the deployed firewall or IDS does not detect any evasion attempt, an incident responder can manually examine Windows Firewall logs to check if any malicious traffic entered the server, as shown in the screenshot on the above slide.



Detecting Brute-force Attempts

Attackers perform trial-and-error methods that try to guess the valid input for a particular field. Applications that allow any number of input attempts are generally prone to brute-force attacks. In a brute-force attack, attackers try every combination of characters until the password is broken. The attacker generates a large number of credential guesses to find correct credentials to gain access to the system. Brute-force attacks lead to loss of privacy and data confidentiality. These attacks are performed to obtain sensitive information, such as passwords for the administrator or common-user accounts. For example, after hacking any Microsoft Windows OS based machine, attackers try to enumerate the Microsoft Active Directory to acquire valid user names. An attacker who succeeds in extracting valid user names can conduct a brute-force attack using tools like L0phtCrack and Hydra to crack the respective passwords.

Brute-force attacks require a lot of resource and time; however, it is considered an effective method for achieving results. For any non-flawed protocol, the average time needed to find the key in a brute-force attack is proportional to the length of the key. A brute-force attack will be successful only if the attacker has sufficient time to discover the key.

The best way to detect such brute-force attacks over an enterprise network or application is to analyze logs in the **Event Viewer** for identifying multiple failed login attempts from the same IP address. When someone tries to gain unauthorized access to an account by entering wrong credentials, those events are recorded in the Event Viewer.

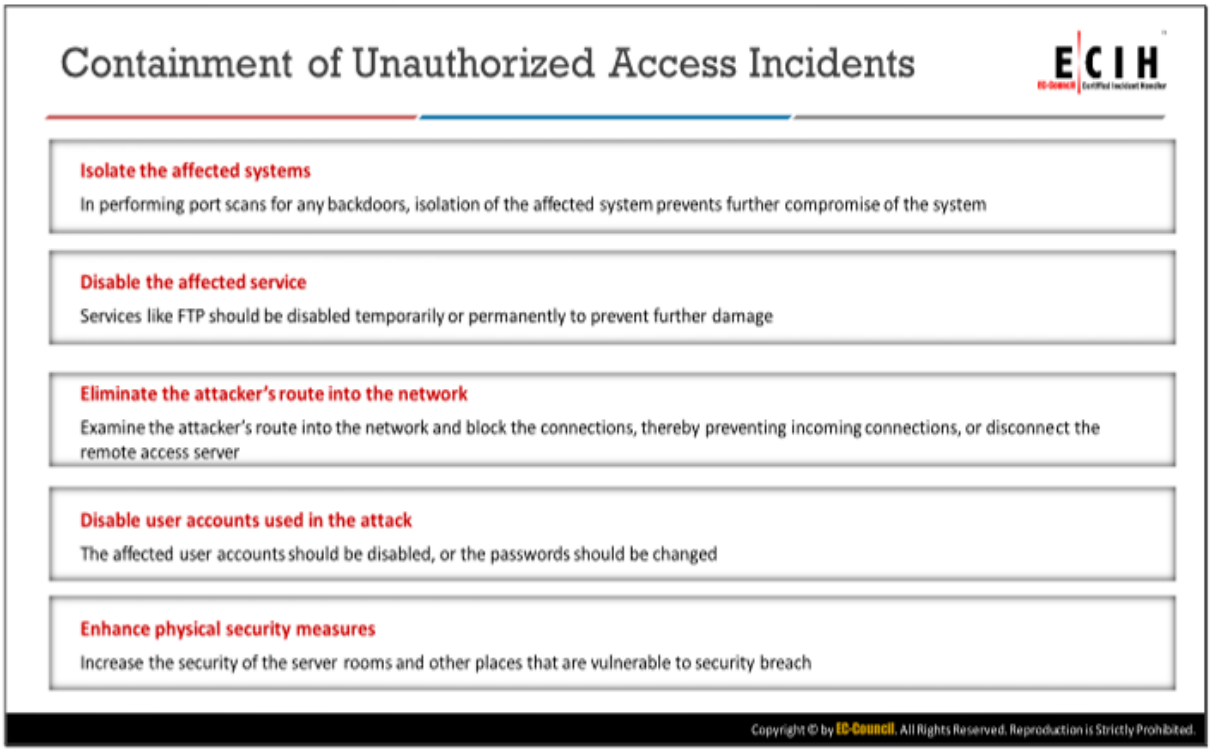
- To launch Event Viewer:

  Start → Control Panel → Administrative Tools → Computer Management → System Tools → Event Viewer

- To view the events related to login, expand **Windows Logs** and click on **Security** to see all security-related events (including audit/login events) in the right-hand section of the window.

Some of the other techniques to detect brute-force attempts include:

- Excessive traffic flow and network bandwidth usage in a single session
- Sometimes, the networks can be compromised through web applications. Incident handlers can also monitor the web server logs for brute-force attacks on user accounts, which record an HTTP 401 status code for each unsuccessful login attempt.



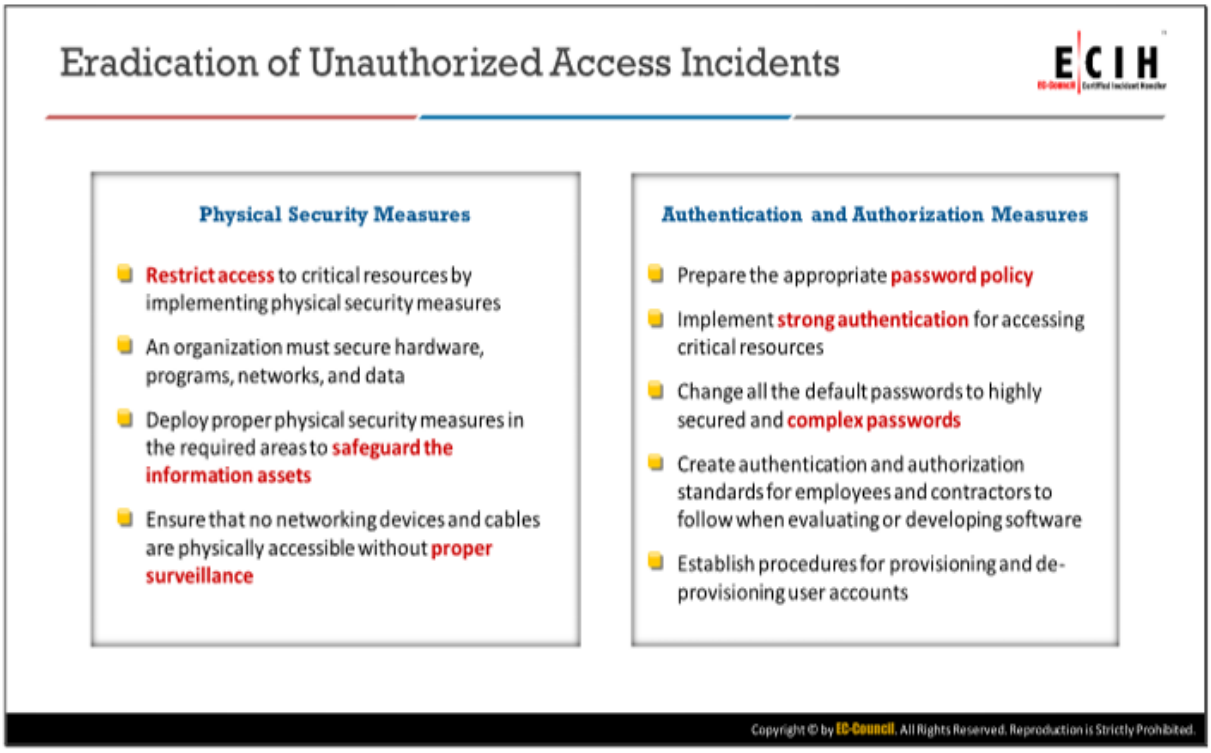
Containment of Unauthorized Access Incidents

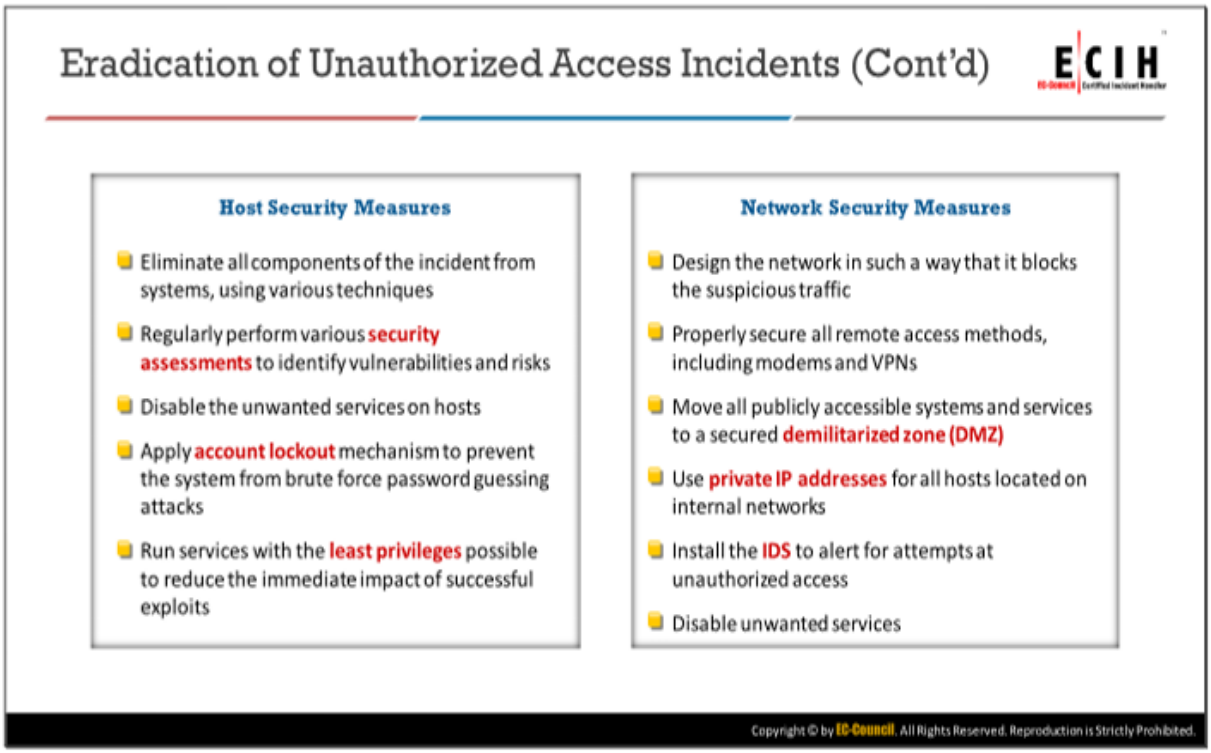
Incident responders can use combinations of the following steps as a containment strategy against the unauthorized access incidents.

- **Isolate the affected systems**: Incident responders should disconnect each affected system from the network to contain an unauthorized access incident and prevent it from further compromise. The most challenging part of the incident handling process is identifying all affected systems. Attackers can compromise one system and use it as a source of attack against another internal system. Handlers must verify other systems for any signs of successful attacks and contain them. If they need to check multiple systems, they can deploy automated tools and methods, such as port scans for backdoors and remote access.
- **Disable the affected service**: If the attacker compromises services to gain unauthorized access to the system, then the incident responders should temporarily disable and replace it, if the issue is repairable, or permanently disable the service. Services such as FTP should be disabled temporarily or permanently to prevent further damage.
- **Eliminate the attacker's route into the network**: Network access to all critical resources in the organization should be secured. In addition, access should be limited to a few key authorized users, along with use of two-factor authentication, limiting the number of network access attempts, and blocking access to these resources during incidents. For example, this includes blocking the incoming connection temporarily for some network segment or disconnecting the remote access server.
- **Disable the user accounts used in an attack**: The accounts and passwords acquired from an infected system can be used by the attacker for malicious activities, so these

accounts need to be disabled. The incident handler must check for new accounts that may have been created by the attacker during the incident and disable them. Then, all employees should be alerted and asked to change the passwords of their accounts immediately.

- **Enhance physical security measures**: Incident responders should implement additional containment strategies in the event of an attack that included a physical security breach of the network. For example, securing the server room to prevent access by an intruder.
- **Other containment methods**:
  - Review and update IDS/IPS rules configuration to stop the ongoing attack.
  - Deploy a network segmentation mechanism to separate the infected section of the network from others. This can restrict the spreading and impact of the incident.
  - Block the identified port immediately after identifying the suspicious attempts.
  - Deploy various network security measures/tools such as firewalls, IDS/IPS, antimalware software, endpoint security solutions, and DLPs to contain the unauthorized access incidents.





Eradication of Unauthorized Access Incidents

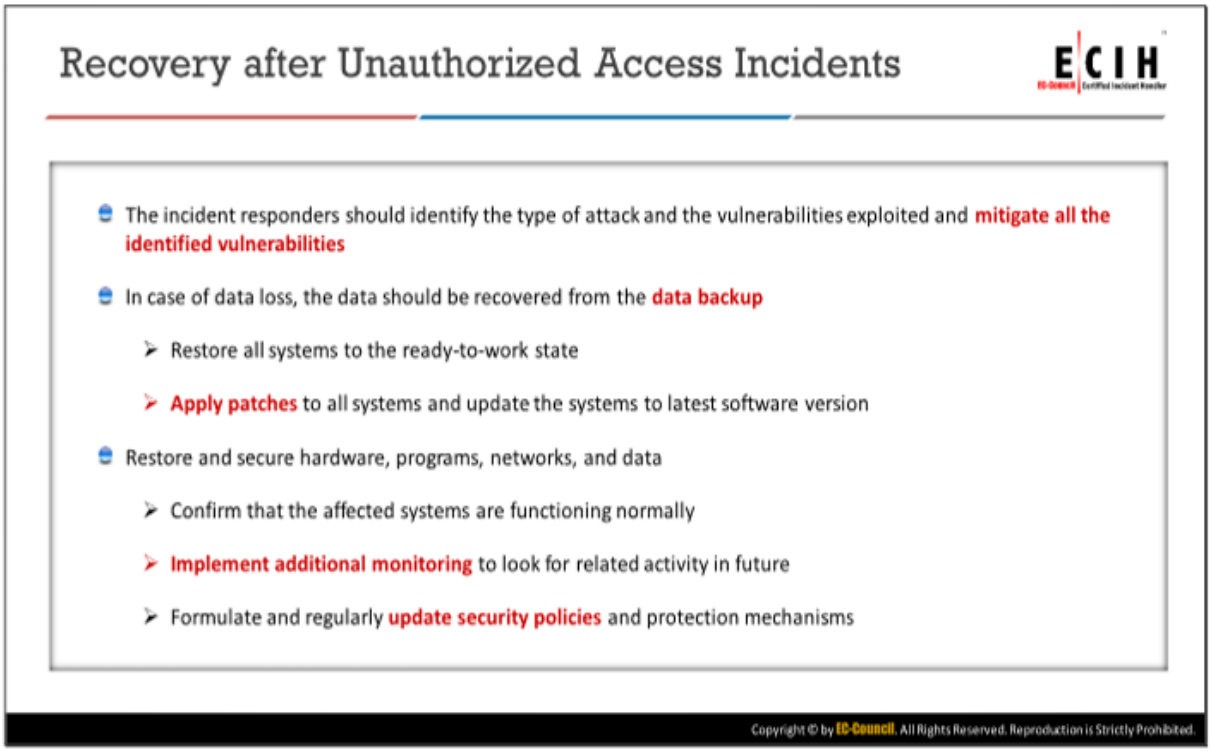
Following are some guidelines that should be followed by an IH&R team to eradicate the unauthorized access incidents:

- **Physical Security Measures**
  - Restrict access to critical resources by implementing physical security measures

- Secure hardware, programs, networks, and data at an organizational level
- Deploy proper physical security measures in the required areas to safeguard the information assets
- Ensure that no networking devices and cables are physically accessible without proper surveillance

- **Authentication and Authorization Measures**
  - Prepare an appropriate password policy
  - Implement strong authentication for accessing critical resources
  - Change all default passwords to highly secure and complex ones
  - Create authentication and authorization standards for employees and contractors to follow when evaluating or developing software
  - Establish procedures for provisioning and de-provisioning user accounts
- **Host Security Measures**
  - Eliminate all components of the incident from systems using various techniques
  - Regularly perform various security assessments to identify vulnerabilities and risks
  - Disable unwanted services on hosts
  - Apply account lockout mechanisms to prevent the system from brute-force attacks on passwords
  - Run services with the least privileges possible to reduce the immediate impact of successful exploits
  - Use host-based/personal firewall software to limit exposure of the individual host to attacks
  - Limit unauthorized physical access to logged-in systems by requiring hosts to lock idle screens automatically and asking users to log off before leaving the office
  - Regularly verify the permission settings for critical resources, including password files, sensitive databases, and public web pages
  - Create and implement a password policy
  - Restore or reinstall systems that appear to have suffered a root compromise
- **Network Security Measures**
  - Design the network to block suspicious traffic
  - Properly secure all remote access methods, including modems and VPNs
  - Move all publicly accessible systems and services to a secured demilitarized zone (DMZ)
  - Use private IP addresses for all hosts located on internal networks

- Install an IDS to create alerts for unauthorized access attempts
- Disable unwanted services
- Limit the number of accepted connections from a source in a network to prevent brute-force attacks
- Select mitigation strategies considering both short- and long-term business objectives
- Configure centralized logging for all users
- Provide the details of the management change to the IH&R team



Recovery after Unauthorized Access Incidents

The recovery process depends on the type of attack. If the attack has resulted in compromise of administrator access, then it allows the attackers to install rootkits and gain root access to the system. In this situation, it is better to restore the system from scratch and change all system passwords. However, if the attacker only obtained a low level of access, it is easy to recover to that point before the attack. If the attacker gains only user-level access by guessing or brute forcing a user password, then eradication involves simply changing the password.

Scenario to recover from the incident:

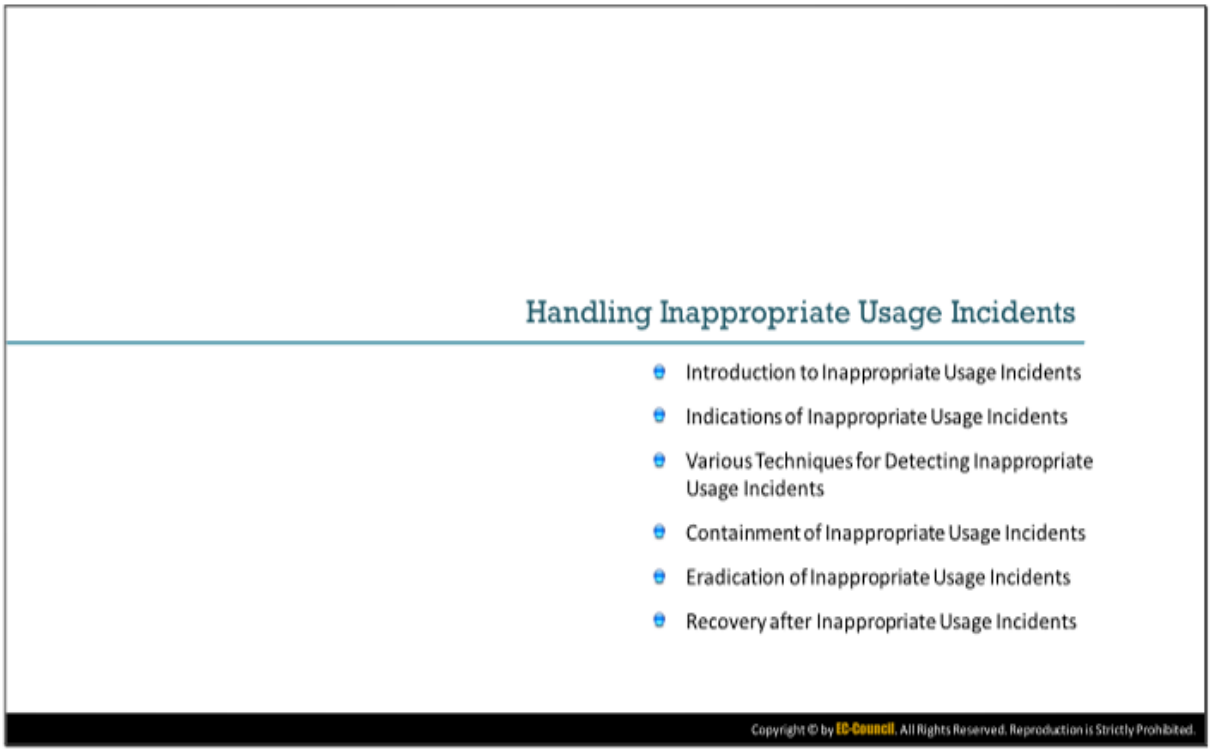
- The incident responders should identify the type of attack and the vulnerabilities exploited and mitigate all identified vulnerabilities

In case of data loss, the data is recovered from backup files

- Restore all the systems to the ready-to-work state
- Apply patches to all systems and update them with the latest software version

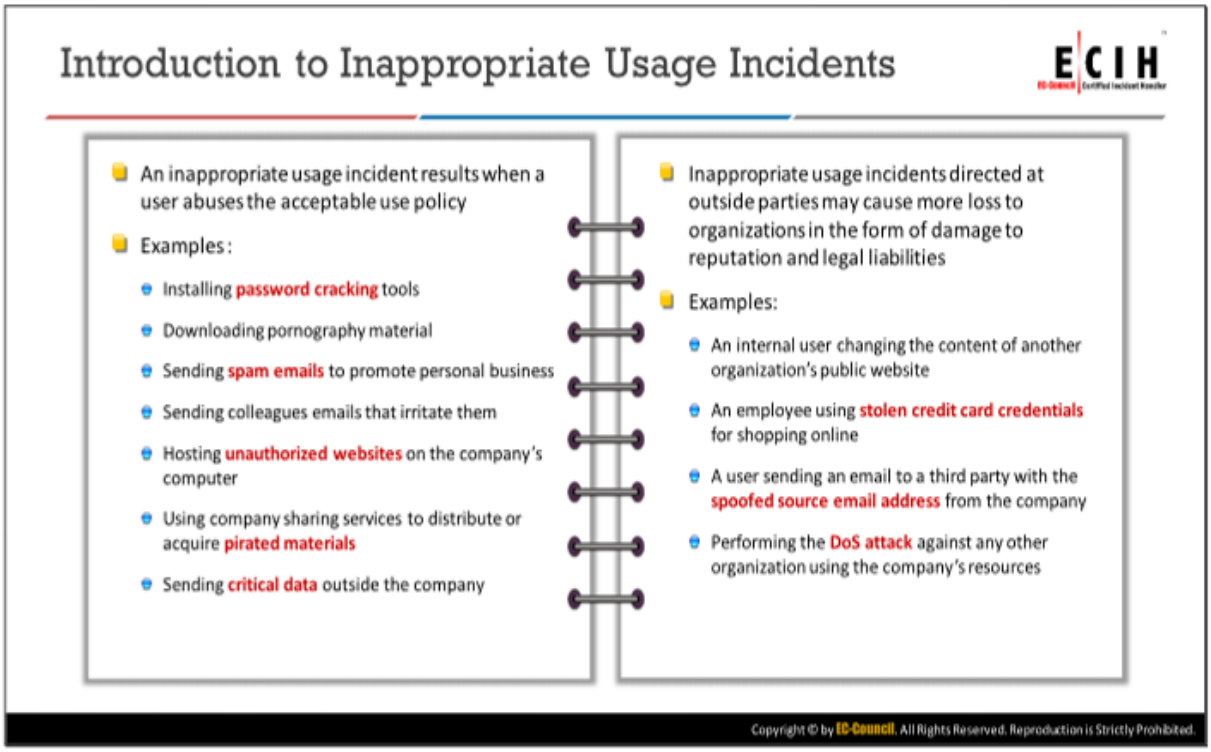
Restore and secure hardware, programs, networks, and data

- Confirm that the affected systems are functioning normally
- Implement additional monitoring to look for related activity in the future
- Formulate and regularly update security policies and protection mechanisms



Handling Inappropriate Usage Incidents

In the previous section, we discussed in detail the process of handling unauthorized access incidents. This section discusses the concepts of inappropriate usage incidents and the steps that should be followed for their detection, containment, eradication, and recovery.



Introduction to Inappropriate Usage Incidents

Inappropriate usage refers to incidents in which a user violates the acceptable computing use policies. Even though these types of incidents are not security related, they have IH&R processes similar to that of security-related incidents. These might include intentional or unintentional actions of the users and result in various network attacks.

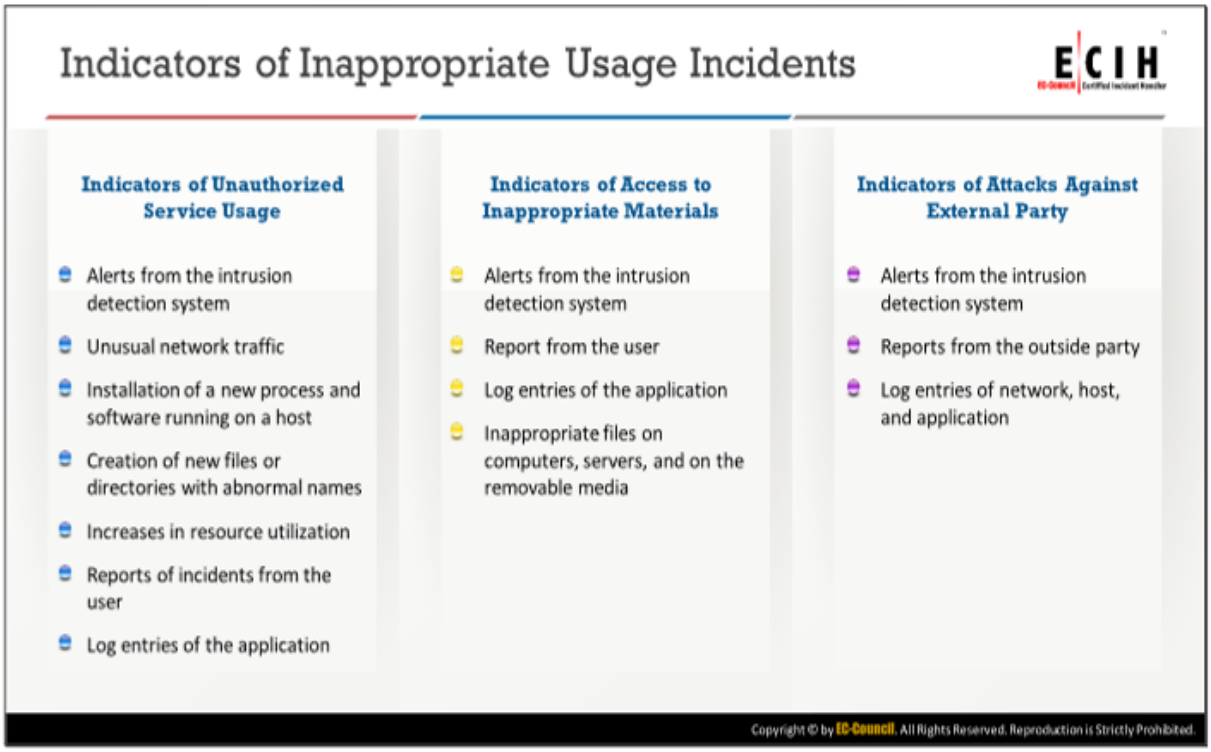
The inappropriate usage incidents that a team might handle include:

- Installing password cracking or key logger tools
- Downloading software, pornography, pirated files, and malicious files
- Sending spam emails which promote a personal business
- Sending malicious emails or abusive content to colleagues
- Hosting unauthorized or malicious websites on the company's computer
- Using the company's shared networks or sharing services to distribute or acquire pirated materials
- Sending critical data outside the company
- Providing login credentials on a spoofed website

Inappropriate usage incidents aimed at external agencies/organizations are difficult to handle and may cause more loss to organizations in the form of damage to reputation and legal liabilities. These types of incidents can become a liability for the organization. Examples of these types of incidents include:

- An internal user changing the content of another organization's public website

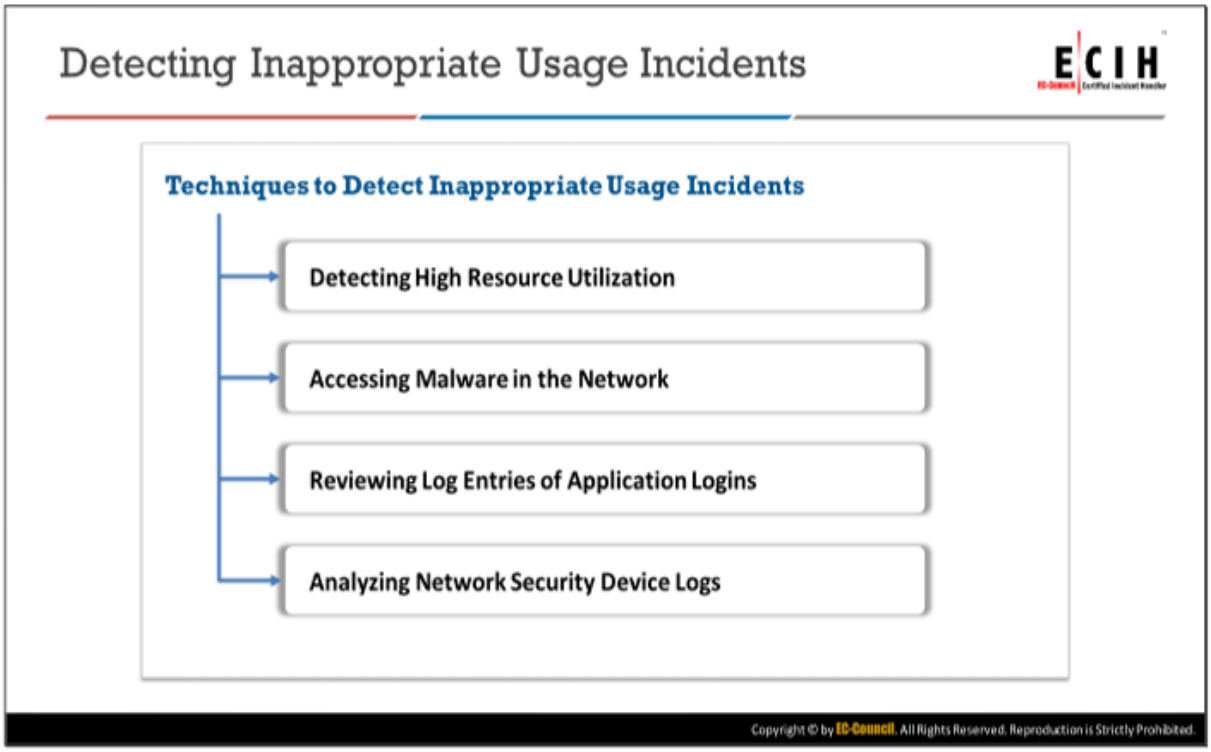
- An internal user purchasing items by shopping online using a stolen credit card number
- Sending email(s) to a third party with a spoofed source email address from the company
- Performing a DoS attack against any other organization using company resources



Indicators of Inappropriate Usage Incidents

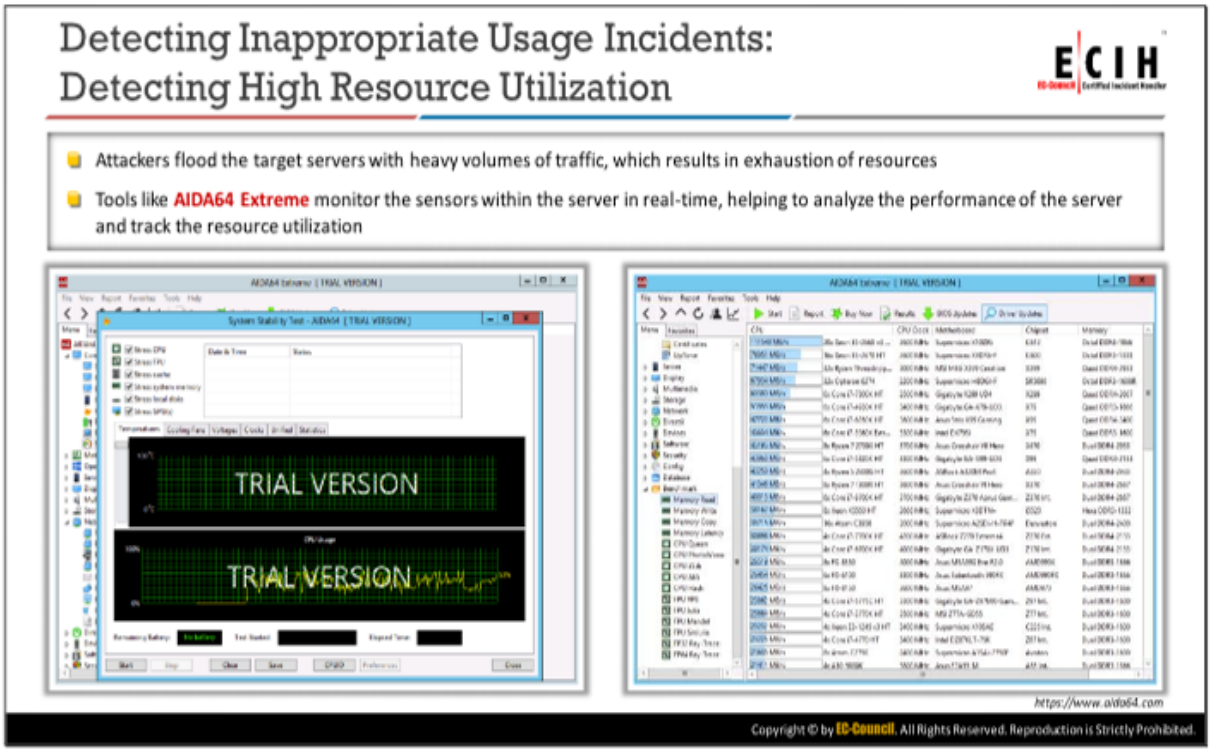
User reports generally help detect inappropriate usage incidents. The following are possible ways of locating inappropriate usage incidents.

- **Indicators of unauthorized service usage**
  - Alert from an intrusion detection system
  - Unusual network traffic
  - Installation of new processes and software running on a host
  - Creation of new files or directories with abnormal names
  - Increase in resource utilization
  - Reports of incidents from a user
  - Log entries of the application
- **Indicators of access to inappropriate materials**
  - IDS alert
  - Reports from a user
  - Application log entries
  - Inappropriate files on computers, servers, or removable media
- **Indicators of an attack against an external party**
  - IDS alert
  - Reports from an outside party
  - Log entries from the network, host, and applications



Detecting Inappropriate Usage Incidents

Inappropriate usage incidents occur often in an enterprise network. The IH&R team is responsible for quickly detecting incidents and performing recovery steps to minimize the impact of such attacks. Incident responders can apply various techniques, including detecting high resource utilization, accessing malware in the network, reviewing log entries of application logins, and analyzing network security device logs, to detect inappropriate usage incidents.



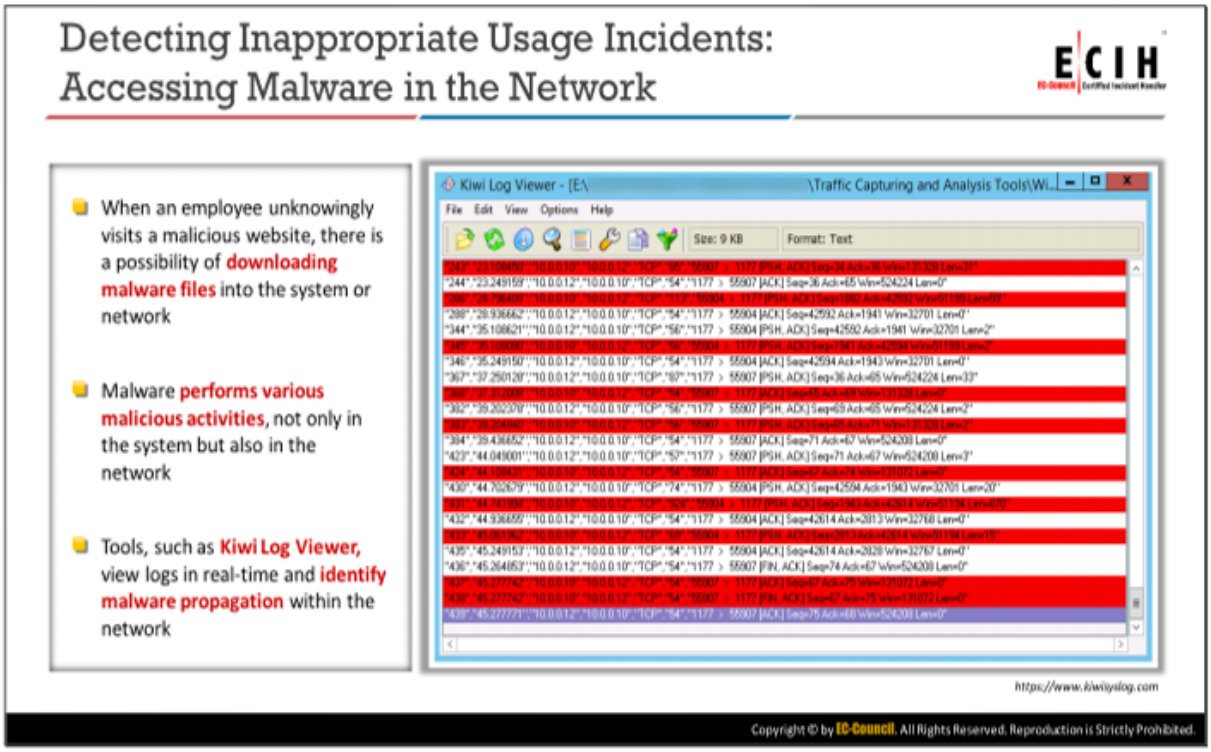
Detecting Inappropriate Usage Incidents: Detecting High Resource Utilization

When an employee unknowingly visits a malicious site and compromises the network, the attackers behind the site attempt to flood the target systems and servers with heavy volumes of traffic. This results in exhaustion of resources, which prevents legitimate users from accessing the resources. The incident responder can detect any such high resource utilization happening over a network using various tools, such as AIDA64 Extreme.

- **AIDA64 Extreme**

  Source: *https://www.aida64.com*

  AIDA64 Extreme monitors the sensors within the server in real-time and helps analyze the performance of the server. It is effective for tracking network resource utilization.



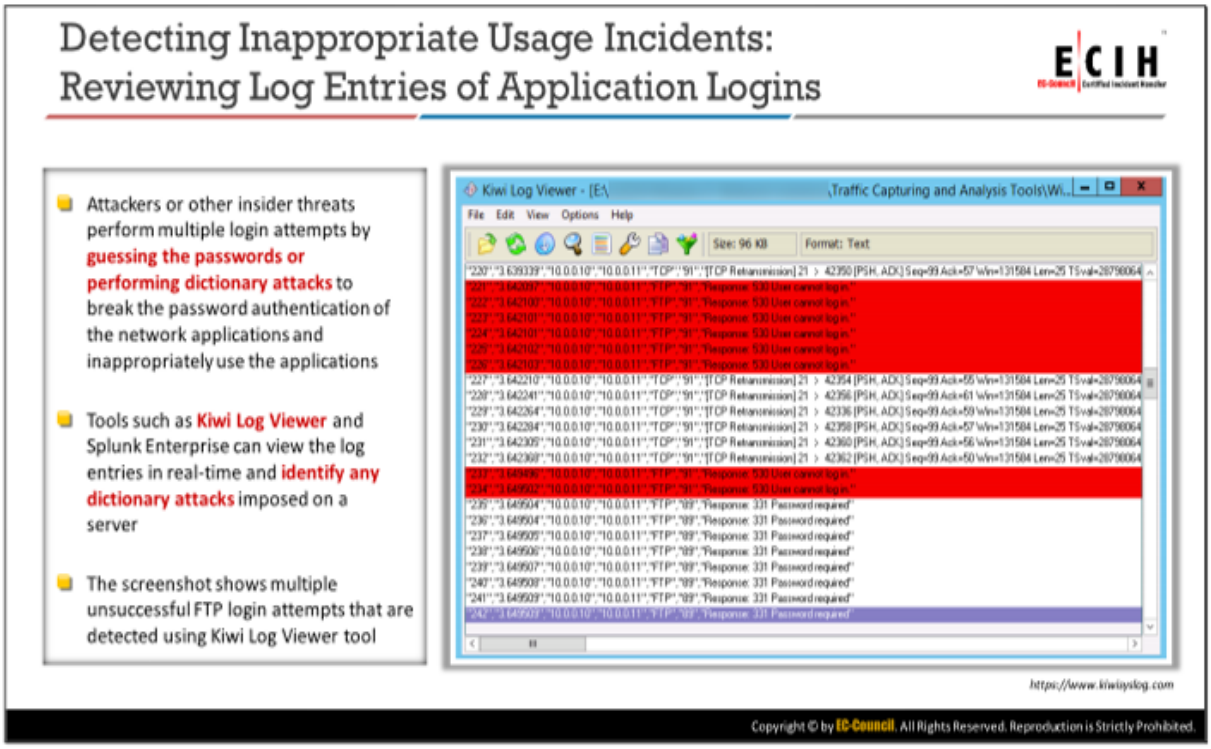
Detecting Inappropriate Usage Incidents: Accessing Malware in the Network

When an employee unknowingly visits a malicious website, there is a possibility of downloading malware files that are designed to perform various malicious activities in both the system and network. Incident responders detect and access the malware present in the network and eliminate it using tools such as Kiwi Log Viewer and Splunk Enterprise to view logs in real-time and identify malware propagation within the network.

- **Kiwi Log Viewer**

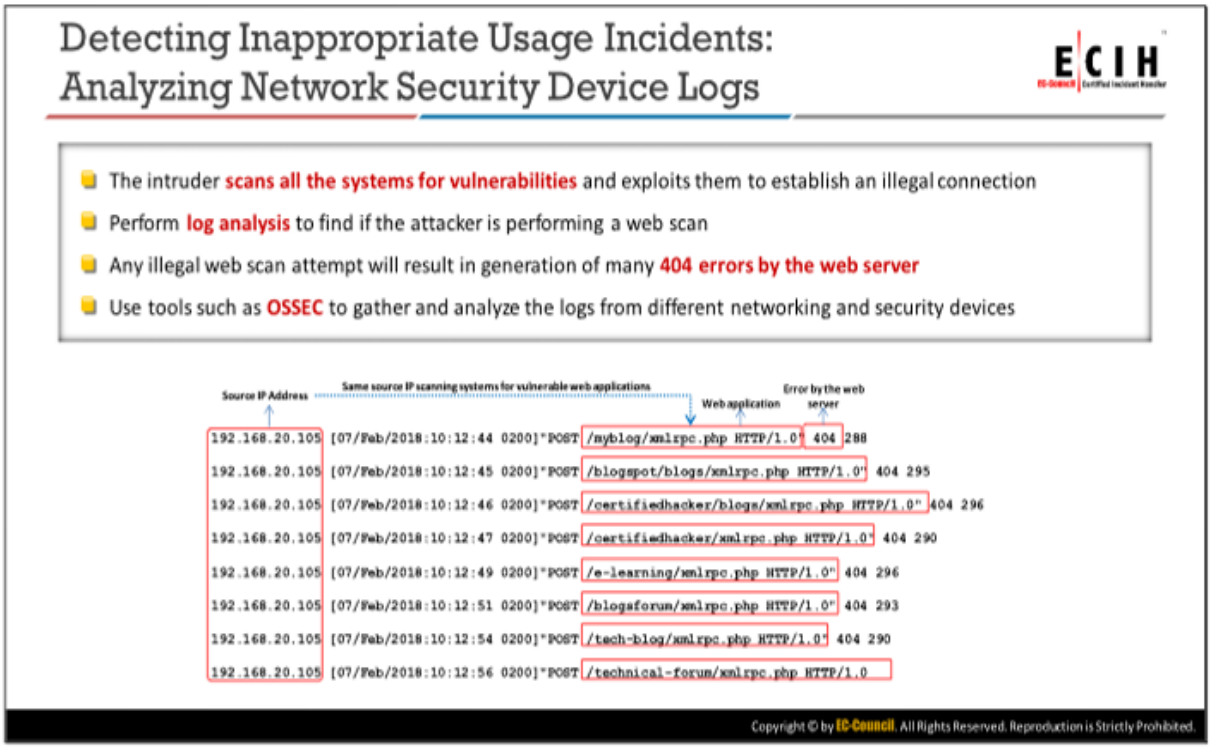
  Source: *https://www.kiwisyslog.com*

  This software allows an incident responder to monitor log files for changes. It displays changes in real-time and can be set up to automatically monitor for specific keywords, phrases, or patterns. Kiwi Log Viewer only runs on Windows and provides similar functionality to the Unix/Linux Tail command.



Detecting Inappropriate Usage Incidents: Reviewing Log Entries of Application Logins

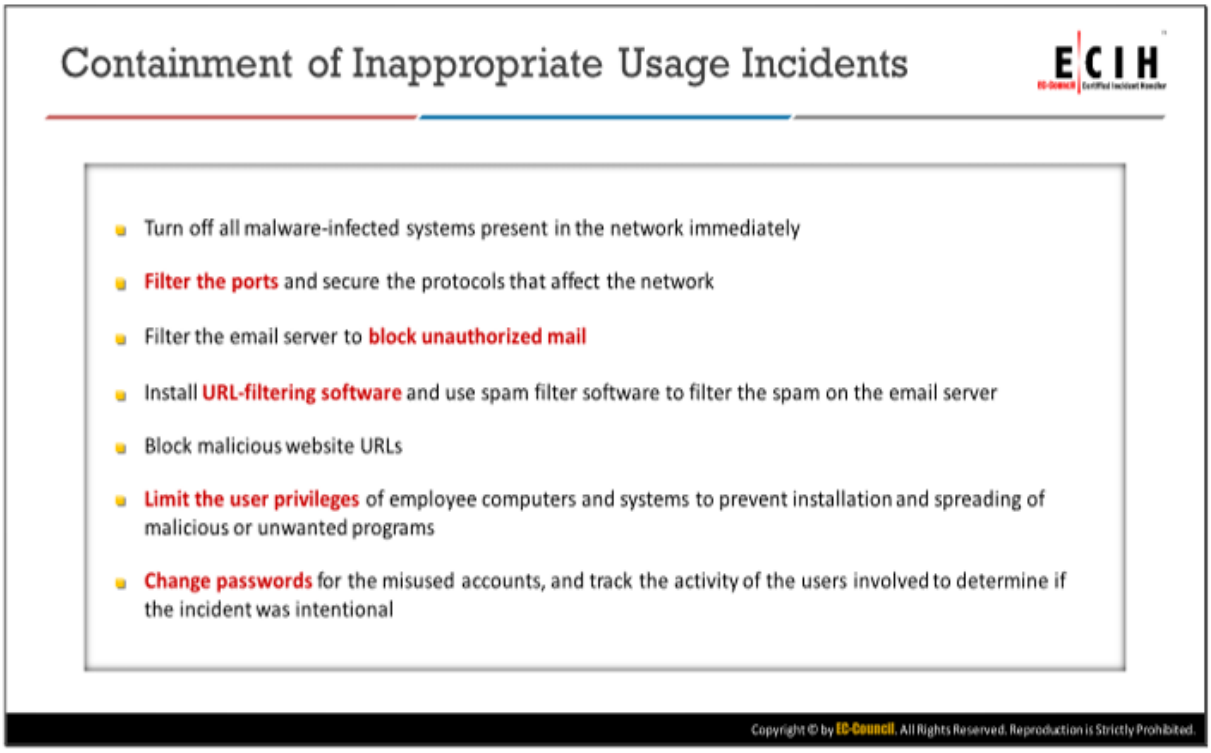
Attackers or other insider threats perform multiple login attempts by guessing the passwords or performing dictionary attacks to break the password authentication of network applications and use them inappropriately. Incident handlers review the log entries of application logins to detect any inappropriate user login attempts. Kiwi Log Viewer and Splunk Enterprise can be used to view log entries in real-time and identify any dictionary attacks imposed on a server. The screenshot on the above slide shows multiple unsuccessful FTP login attempts detected using the Kiwi Log Viewer tool.



Detecting Inappropriate Usage Incidents: Analyzing Network Security Device Logs

Attackers try to gain access to the networks by finding the vulnerabilities present in the connected devices, services, and applications. The intruder scans all systems for vulnerabilities and exploits them to establish an illegal connection. Incident responders can perform log analyses to locate such scans. In addition, they can detect inappropriate activities by analyzing the network logs of devices, such as network servers, firewalls, IDS, routers, and centralized servers. Analyzing logs from different sources and correlating the events using an SIEM tool can verify an inappropriate usage incident. Incident responders should identify the individual responsible for the incident and verify if they had criminal intentions. If a crime is involved, these incidents can cause reputational losses to the organization and call for high-priority containment.

Incident responders use tools such as OSSEC to gather and analyze logs from different networking and security devices. In the following network logs, the attacker with source IP address 192.168.20.105 tries to scan the web application to find any existing vulnerabilities and misuse them to attack the network. This resulted in generation of many 404 errors by the web server. When these errors are detected, immediate action should be taken to quickly block the intruder with the identified IP address. If the site has broken links, it will generate false positives where .gif, .jpg and .png extensions can be ignored.

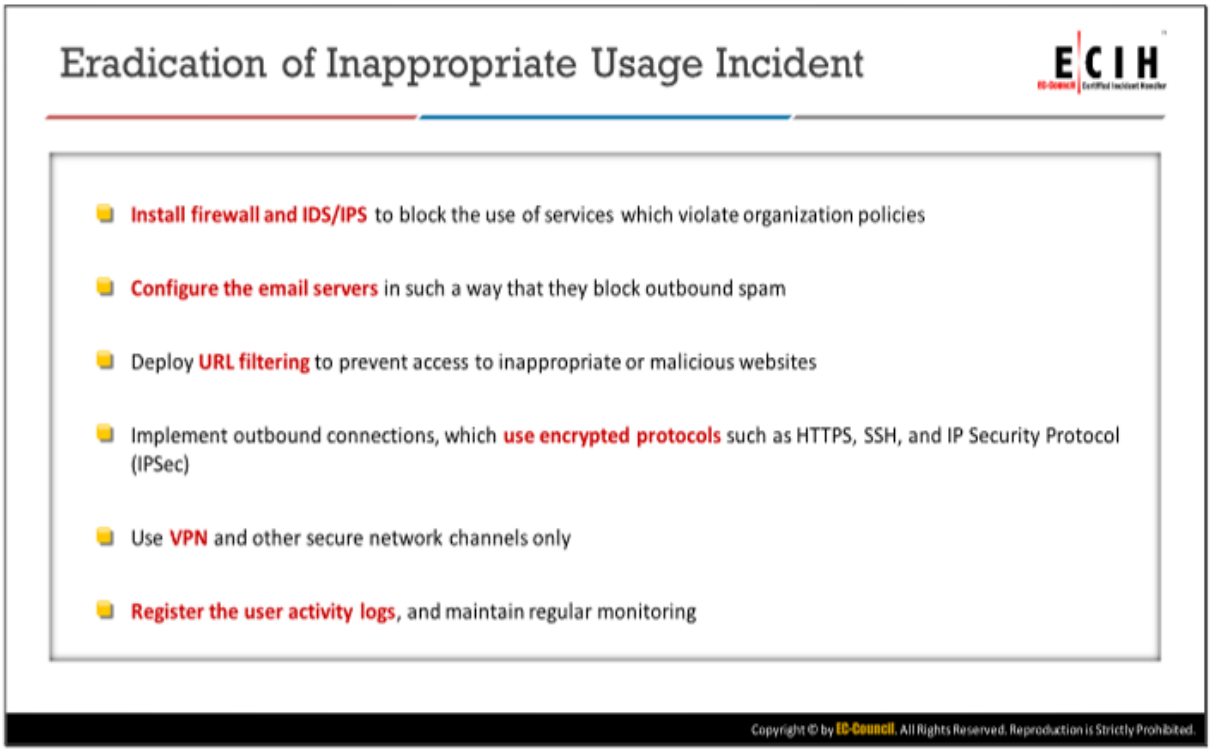


Containment of Inappropriate Usage Incidents

Inappropriate usage incidents can result in huge losses if not contained quickly, as they can result in installation of malware; compromise of accounts, applications, services, and systems; theft of sensitive data; and criminal offenses against other organizations that can appear intentional. All such actions can result in financial and reputational losses for the companies, and invite legal action in some cases.

The main recommendations for containing inappropriate usage incidents are:

- Immediately disconnect all malware-infected systems in the network.
- Filter the ports and secure the protocols that are affecting the network.
- Filter the email server to block unauthorized mails.
- Install URL filtering software and use spam filter software on the email server.
- Block malicious website URLs.
- Limit the user privileges of employee computers and systems to prevent installation and spreading of malicious or unwanted programs.
- Change passwords for the misused accounts and track the activity of the users involved to determine whether the incident was intentional.

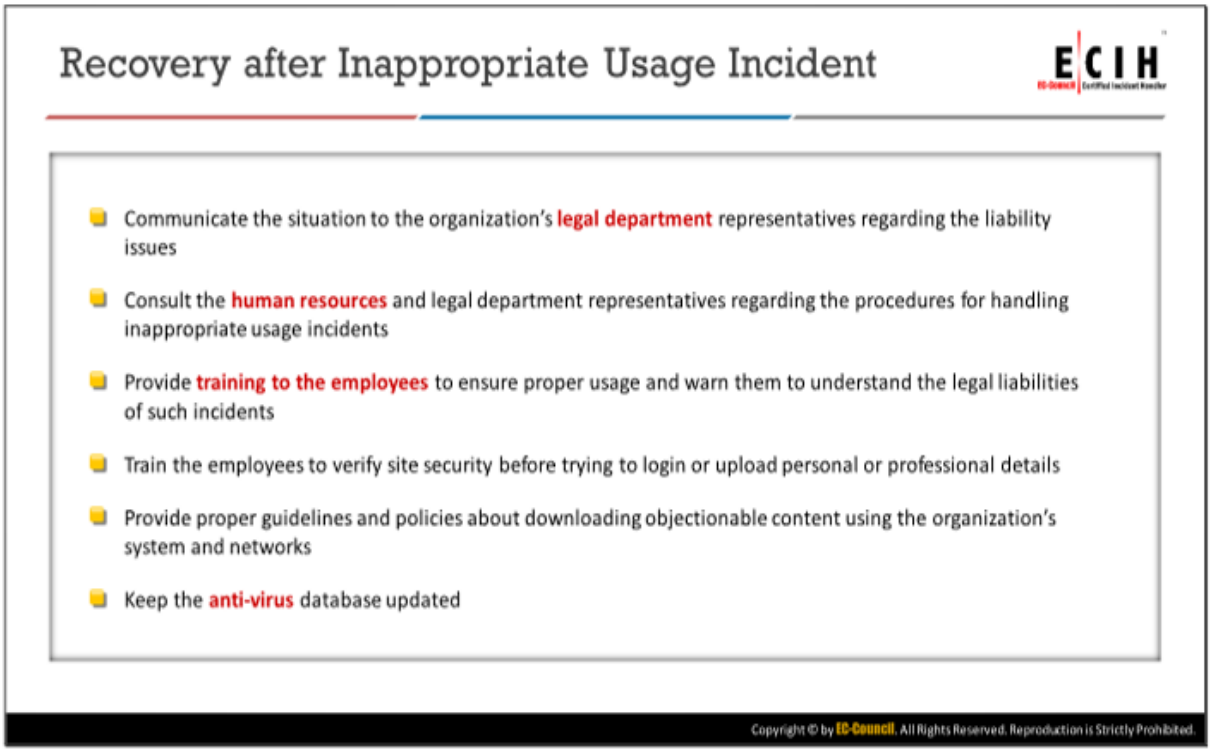


Eradication of Inappropriate Usage Incident

Increasing awareness of appropriate behavior among users is the best action to prevent inappropriate usage incidents. By reading and signing appropriate usage policies, users should know the rules about the organization's monitoring activity. The actions taken to reduce certain types of inappropriate usage incidents include:

- Installing firewall and IDS/IPS to block services that violate organizational policy. Note that it is practically impossible to block all services.
- Configuring the email servers to block outbound spam. Installing spam filter software blocks spam messages to and from the internal users.
- Filtering the URL to prevent access to inappropriate or malicious websites by creating a web proxy server that runs URL filtering software. Configuring the network firewall to send outgoing requests through proxy servers. To access any website, users must pass through one of the proxy servers.
- Limiting outbound connections that use encrypted protocols, such as Secure Shell (SSH), HTTP Secure (HTTPS), and IP Security Protocol (IPsec). Encrypted connections may tempt the user to perform malicious actions as the organization cannot monitor them directly. For example, the user can use the proxy server to download illegal material from websites through the encrypted connection. In this case, network security controls cannot determine the nature of the activity. To limit such incidents, the HTTPS proxy server is blocked.
- Using VPN and other secure network channels only.
- Registering the user activity logs and keep monitoring them regularly.

- Always storing sensitive data in remote servers and restricting its access.
- Enabling authentication for sharing files across the network.



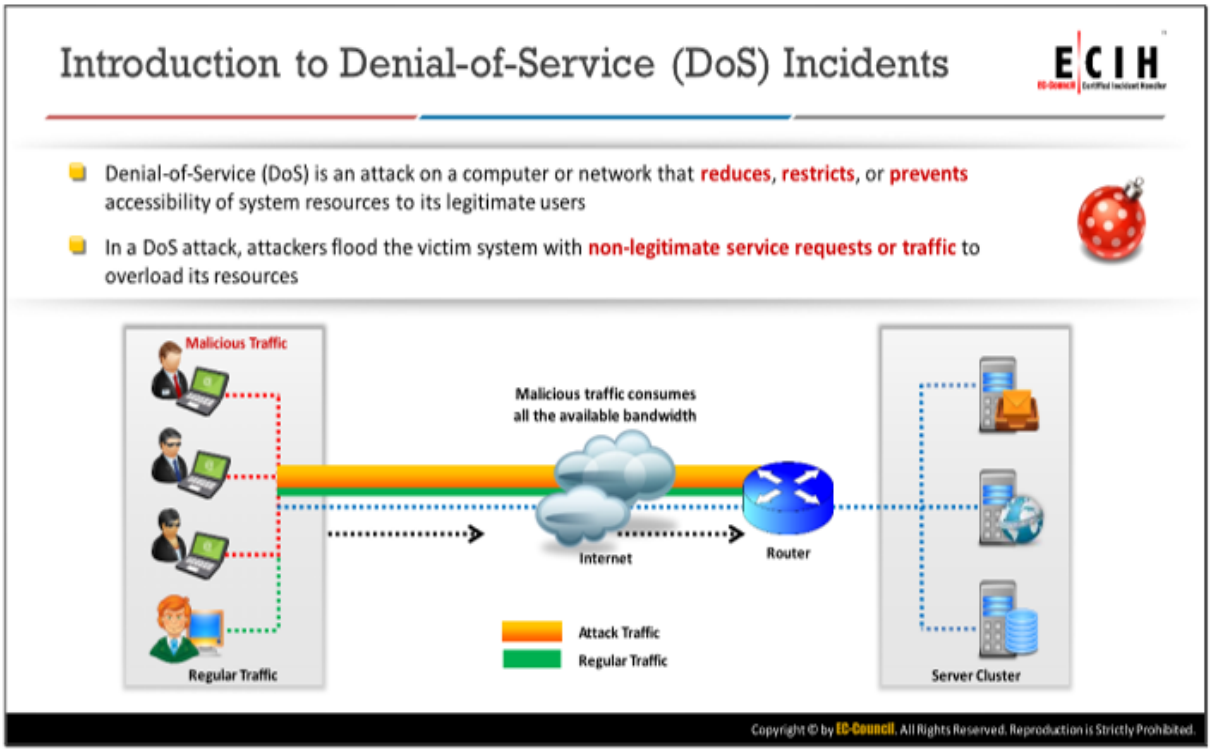
Recovery after Inappropriate Usage Incident

After any inappropriate usage incident, IH&R personnel are responsible for recovering the affected systems and restoring the operational state. The Incident responder can follow the steps below while recovering the systems and network:

- Communicate the situation to the organization's legal department representatives regarding the liability issues.
- Consult the human resource and legal department representatives regarding the procedures for handling inappropriate usage incidents.
- Provide training to the employees to ensure proper usage and ensure that they understand the legal liabilities of such incidents.
- Train the employees to verify site security before trying to login or upload personal or professional details onto it.
- Provide proper guidelines and policies regarding downloading objectionable content using the organization system and networks.
- Keep the antivirus database updated.

Handling Denial-of-Service Incidents

DoS and DDoS attacks prevent authorized users from accessing a computer or network, and are most common attacks affecting large organizations. The attackers attempt to flood the networks with many requests to make the network resources unavailable for legitimate users. It is the responsibility of IH&R personnel to handle these incidents effectively. This section gives an introduction to DoS and DDoS attacks, the indicators of these attacks, detection techniques, and the strategies for containment, eradication, and recovery.



Introduction to Denial-of-Service (DoS) Incidents

DoS is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users. In a DoS attack, attackers flood a victim's system with non-legitimate service requests or traffic to overload its resources, bringing the system down, making the target website unavailable or at least significantly slowing down the system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or to corrupt data, but to prevent legitimate users from accessing the system.

Following are the examples of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (e.g., IRC) with more events than it can handle
- Crashing a TCP/IP stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

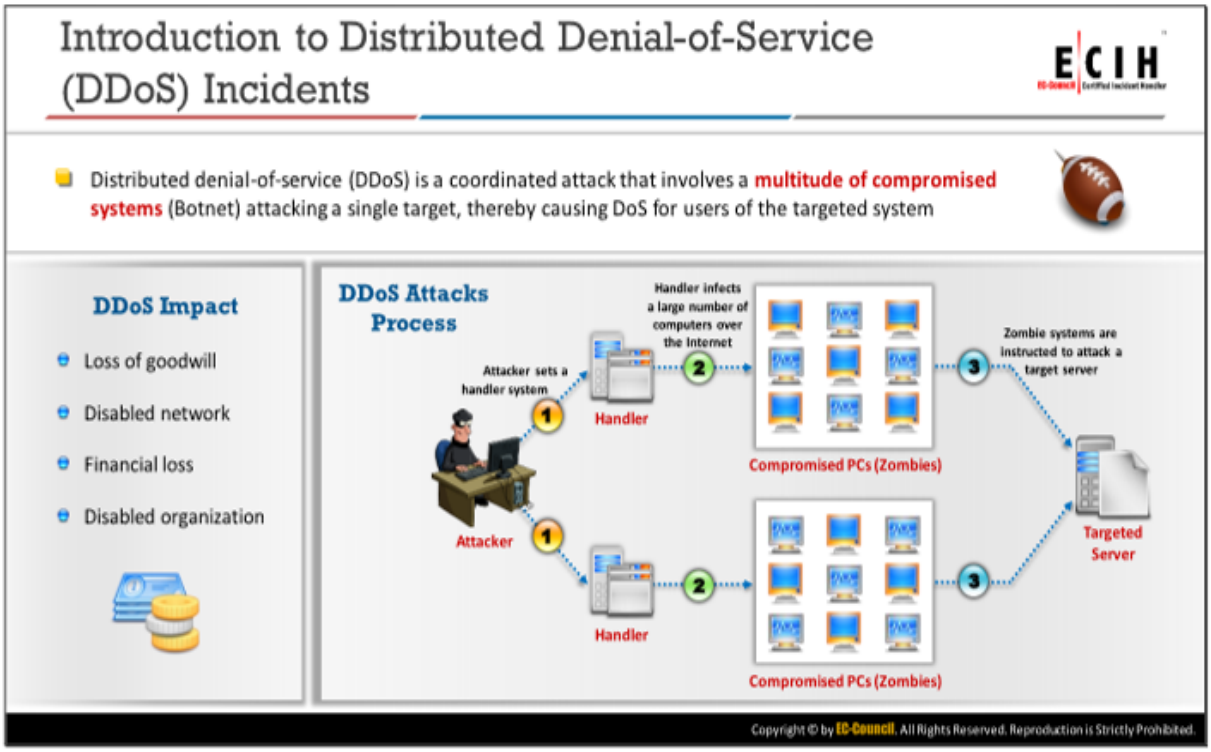
DoS attacks come in a variety of forms and target a variety of services. The attacks may cause the following:

- Consumption of scarce and nonrenewable resources
- Consumption of bandwidth, disk space, CPU time, or data structures
- Actual physical destruction or alteration of network components
- Destruction of programming and files in a computer system

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available resources of the OS so that the computer cannot process the requests of legitimate users.

Imagine a pizza delivery company, which does much of its business over the phone. An attacker who wanted to disrupt this business could tie up the company's phone lines, making it impossible for the company to do business. This is how a DoS attack works; the attacker uses all available ways to connect to the system, making legitimate business impossible.

DoS attacks are a kind of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. However, failure to address the issue could result in the loss of a service, such as email. In a worst-case scenario, a DoS attack can result in the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of an attack.



Introduction to Distributed Denial-of-Service (DDoS) Incidents

Source: *http://searchsecurity.techtarget.com*

A DDoS attack is a large-scale coordinated attack on the availability of services on a victim's system or network resources, launched indirectly through many compromised computers (botnets) on the internet. As defined by the World Wide Web Security FAQ: "A distributed denial-of-service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator can multiply the effectiveness of the denial of service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms." The flood of incoming messages to the target system forces it to shut down, thereby denying service to the legitimate users.

The services under attack are those of the "primary victim," whereas the compromised systems used to launch the attack are the "secondary victims." The use of secondary victims in performing a DDoS attack provides the attacker with the ability to perform a larger and more disruptive attack while making it more difficult to locate the original attacker. The primary objective of any DDoS attacker is to first gain administrative access on as many systems as possible. In general, attackers use customized attack scripts to identify potentially vulnerable systems. Once an attacker gains access to the target systems, they upload DDoS software and run it on these systems at the chosen time of attack.

DDoS attacks have become popular because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous because they can quickly consume the capacity of the largest hosts on the internet, rendering them useless. The impact of DDoS includes loss of goodwill, disabled networks and organizations, and financial loss.

DDoS Attack Process

In a DDoS attack, many applications flood the target browser or network with fake exterior requests that make the system, network, browser, or site slow or unavailable. The attacker initiates the DDoS attack by sending a command to zombie agents, which then send a connection request to many reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of the zombie agents due to false IP address. Hence, they send the requested information (response to the connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This either reduces the performance or completely shuts down the victim's machine.

Types of DoS/DDoS Incidents

Volumetric Attacks

- The attack consumes the bandwidth of the target network or service
- The magnitude of the attack is measured in **bits-per-second (bps)**
- Types of bandwidth depletion attacks:
  - Flood attacks
  - Amplification attacks

Attack Techniques

- UDP flood attack
- ICMP flood attack
- Ping of Death attack
- Smurf attack

Protocol Attacks

- The attack consumes other types of resources like **connection state tables** present in the network infrastructure components such as **load-balancers**, **firewalls**, and **application servers**
- The magnitude of the attack is measured in **packets-per-second (pps)**

Attack Techniques

- SYN flood attack
- Fragmentation attack
- ACK flood attack
- TCP state exhaustion attack

Application Layer Attacks

- The attack consumes the **application resources** or service, thereby making it unavailable to legitimate users
- The magnitude of attack is measured in **requests-per-second (rps)**

Attack Techniques

- HTTP GET/POST attack
- Slowloris attack

Types of DoS/DDoS Incidents (Cont'd)

Permanent DoS Attack

Phlashing

Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware

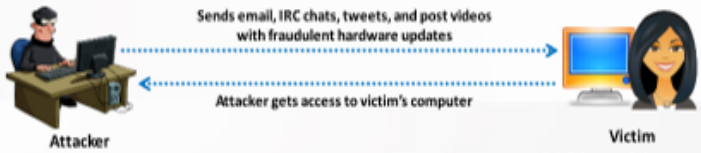
Sabotage

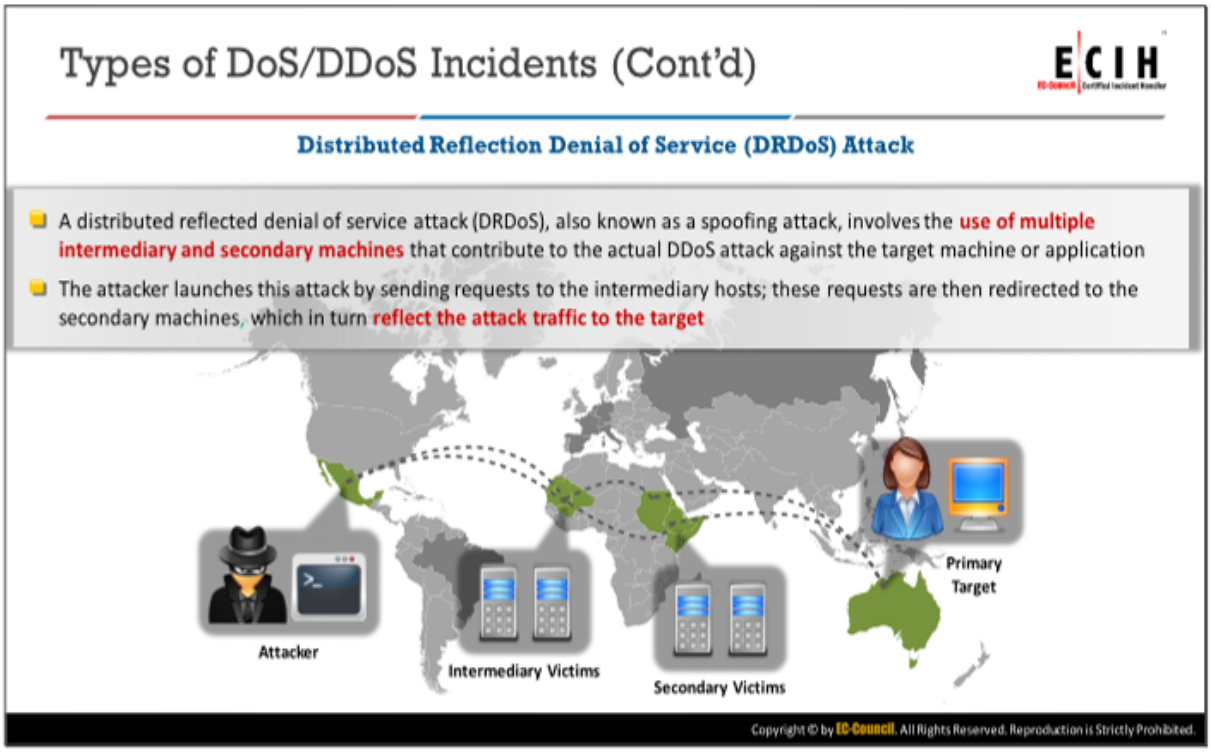
Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

Bricking a system

- This attack is carried out using a method known as "**bricking a system**"
- Using this method, attackers send **fraudulent hardware updates** to the victims

Process





Types of DoS/DDoS Incidents

Attackers implement various techniques to launch DoS/DDoS attacks on target computers or networks. DDoS attacks usually try to limit the network bandwidth, or exhaust the network, application, or service resources, thereby restricting the legitimate users from accessing their system or network resources. The following are common types of DoS/DDoS incidents:

- **Volumetric Attacks**

  These attacks exhaust the bandwidth either within the target network/service, or between the target network/service and the rest of the internet to block legitimate traffic. The magnitude of an attack is measured in bits per second (bps). Volumetric DDoS attacks generally target protocols that are stateless and do not have built-in congestion avoidance. Generation of a large number of packets can cause the consumption of the entire bandwidth of the network. A single machine cannot make enough requests to overwhelm network equipment. Hence, in DDoS attacks, the attacker uses several computers to flood a victim. In this case, the attacker can control all of the machines and instruct them to direct traffic to the target system. DDoS attacks flood a network, which overwhelms network equipment such as switches and routers with the significant statistical change in network traffic. Attackers use the processing power of a large number of geographically distributed machines to generate huge traffic directed to the victim.

  There are two types of bandwidth depletion attacks:

  - A **flood attack** involves zombies sending large volumes of traffic to a victim's systems to occupy the system bandwidth.

- An **amplification attack** engages the attacker or zombies to transfer messages to a broadcast IP address. This method amplifies malicious traffic that consumes the bandwidth.

Following are some of the volumetric attack techniques:

- User datagram protocol (UDP) flood attack
- Internet control message protocol (ICMP) flood attack
- Ping of death attack
- Smurf attack
- Malformed IP packet flood attack
- Spoofed IP packet flood attack

- **Protocol Attacks**

  In addition to volumetric attacks that consume bandwidth, attackers can also prevent access to a target by consuming other types of resources, such as connection state tables. Protocol DDoS attacks exhaust resources available on the target system, or on a specific device between the target and the internet. These attacks consume the connection state tables present in the network infrastructure devices, such as load-balancers, firewalls, and application servers. In this case, no new connections will be allowed since the device will be waiting for existing connections to close or expire. The magnitude of attack is measured in packets per second (pps) or connections per second (cps). These attacks can even take over millions of connections maintained by high-capacity devices. Following are some of the protocol attack techniques:

  - SYN flood attack
  - ACK flood attack
  - TCP connection flood attack
  - TCP state exhaustion attack
  - Fragmentation attack
  - RST attack

- **Application-layer Attacks**

  Attackers try to exploit the vulnerabilities in an application-layer protocol or in the application itself to prevent user access. Attacks on unpatched, vulnerable systems require less bandwidth than protocol or volumetric DDoS attacks. In application DDoS attacks, the application layer or resources will be consumed by opening connections and then leaving them open until no new connections can be made. These attacks destroy a specific aspect of an application or service and are effective with one or few attacking machines producing a low traffic rate (very hard to detect and mitigate). The magnitude of the attack is measured in requests-per-second (rps).

Application-level flood attacks result in the loss of services of a particular network, such as emails, network resources, and temporary loss of applications and services. In this way, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests. Several types of DoS attacks rely on software-related exploits, such as buffer overflows. A buffer overflow attack sends excessive data to an application that either brings down the application or forces the data sent to the application to run on the host system. The attack crashes a vulnerable system remotely by sending excessive traffic to an application. Sometimes, attackers can also execute arbitrary code on the remote system via buffer overflow vulnerability. Sending too much data to the application overwrites the data that controls the program, and runs the hacker's code instead.

Using application-level flood attacks, attackers attempt to:

- Flood web applications to prevent legitimate user traffic
- Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- Jam the application database connection by crafting malicious SQL queries

Application-level flood attacks can result in substantial loss of money, service, and reputation for organizations. It is difficult to detect such attacks as they occur after a connection is established, where the traffic entering the target appears to be legitimate. However, if the user identifies the attack, it can be stopped and traced back to a specific source more easily than other types of DDoS attacks. Application-layer attack techniques include HTTP flood attack and Slowloris attack.

- **Permanent DoS Attack**

  Permanent DoS (PDoS) attacks, also known as phlashing, purely target hardware and cause irreversible damage. Unlike other DoS attacks, it sabotages the system's hardware, requiring the victim to replace or reinstall the hardware. The PDoS attack exploits security flaws in a device, thereby allowing remote administration of the management interfaces of the victim's hardware, such as printers, routers, or other networking devices.

  This type of attack is quicker and is more destructive than traditional DoS attacks. It works with a limited number of resources, unlike a DDoS attack, in which attackers use a set of zombies to attack a target. Attackers perform PDoS attacks using a method known as "bricking a system." In this method, the attacker sends email, IRC chats, tweets, and post videos to the victim with a request to install hardware updates. The attacker places fraudulent content within the updates by modifying and corrupting them via vulnerabilities or defective firmware. When the victim clicks on the links or pop-up windows related to the fraudulent hardware updates, the malware is installed on their system, and gives the attacker complete control over the system.

- **Distributed Reflection Denial of Service (DRDoS) Attack**

  A distributed reflection denial-of-service attack (DRDoS), also known as a "spoofed" attack, uses multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application. The DRDoS attack exploits the TCP three-way handshake vulnerability. This attack involves the attacker's machine, intermediary victims (zombies), secondary victims (reflectors), and the target machine. The attack is launched by sending requests to the intermediary hosts, which in turn reflect the attack traffic to the target.

  DRDoS attack process

  First, the attacker commands the zombies to send a stream of packets (TCP SYN) with the primary target's IP address as the source IP address to other noncompromised machines (secondary victims or reflectors) to exhort them to establish connection with the primary target. Therefore, the reflectors send a huge volume of traffic (SYN/ACK) to the primary target to establish a new connection with it, as they believe it was the host that requested it. The primary target discards the SYN/ACK packets received from the reflectors, as they did not send the actual SYN packet.

  The reflectors keep waiting for the acknowledgment (ACK) response from the primary target. Assuming that the packet lost its path, these bunches of reflector machines resend SYN/ACK packets to the primary target in an attempt to establish the connection, until time-out occurs. This way, a heavy volume of traffic is flooded onto the target machine with the available reflector machines. The combined bandwidth of these reflector machines overwhelms the target machine.

  DRDoS attacks are a form of intelligent attack, and it is very difficult or even impossible to trace the attacker as the secondary victim (reflector) seems to directly attack the primary target rather than the actual attacker. This attack is more effective than a typical DDoS attack as multiple intermediary and secondary victims generate huge attack bandwidth.

DoS/DDoS Attack Tools

Attackers use the following tools to perform DoS/DDoS attacks over organizational networks:

- **High Orbit Ion Cannon (HOIC)**

  Source: *https://sourceforge.net*

  HOIC is a network stress and DoS/DDoS attack application. This tool is written in BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP POST and GET requests to a computer that uses lulz-inspired GUIs.

  Features:

  - High-speed multi-threaded HTTP flood
  - Simultaneously flood up to 256 websites at once
  - Built-in scripting system to allow the deployment of "boosters," which are scripts designed to thwart DDoS counter measures and increase DoS output
  - Can be ported over to Linux/Mac with a few bug fixes
  - Ability to select the number of threads in an ongoing attack
  - Ability to throttle attacks individually with three settings: LOW, MEDIUM, and HIGH

- **Low Orbit Ion Cannon (LOIC)**

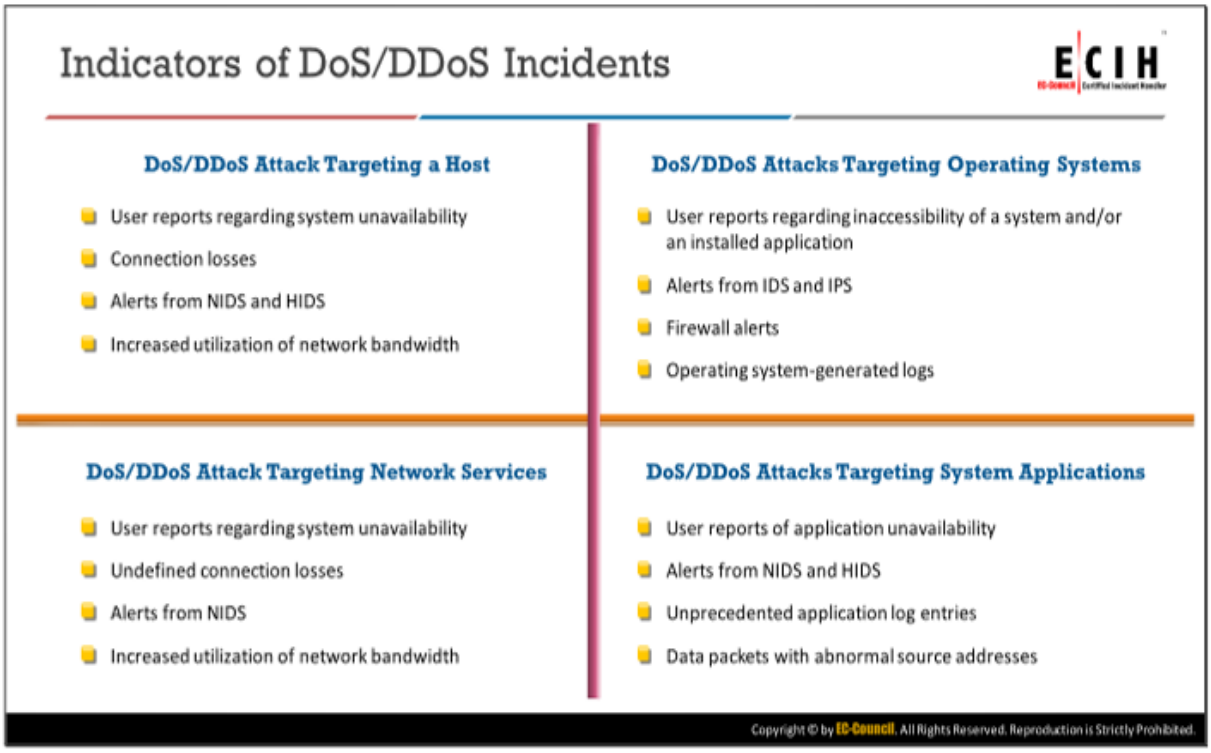
  Source: *https://sourceforge.net*

  LOIC is a network stress testing and DoS attack application. It is also called an application-based DOS attack as it mostly targets web applications. We can use LOIC on

a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

Following are some other DoS/DDoS attack tools:

- HULK (*https://github.com*)
- Metasploit (*https://www.metasploit.com*)
- Nmap (*https://nmap.org*)
- Blackhat Hacking Tools (*https://sourceforge.net*)
- DAVOSET (*https://packetstormsecurity.com*)
- Tsunami (*https://sourceforge.net*)
- R-U-Dead-Yet (*https://sourceforge.net*)
- UDP Flooder (*https://sourceforge.net*)
- DLR_DoS (*https://sourceforge.net*)
- Moihack Port-Flooder (*https://sourceforge.net*)
- DDOSIM (*https://sourceforge.net*)

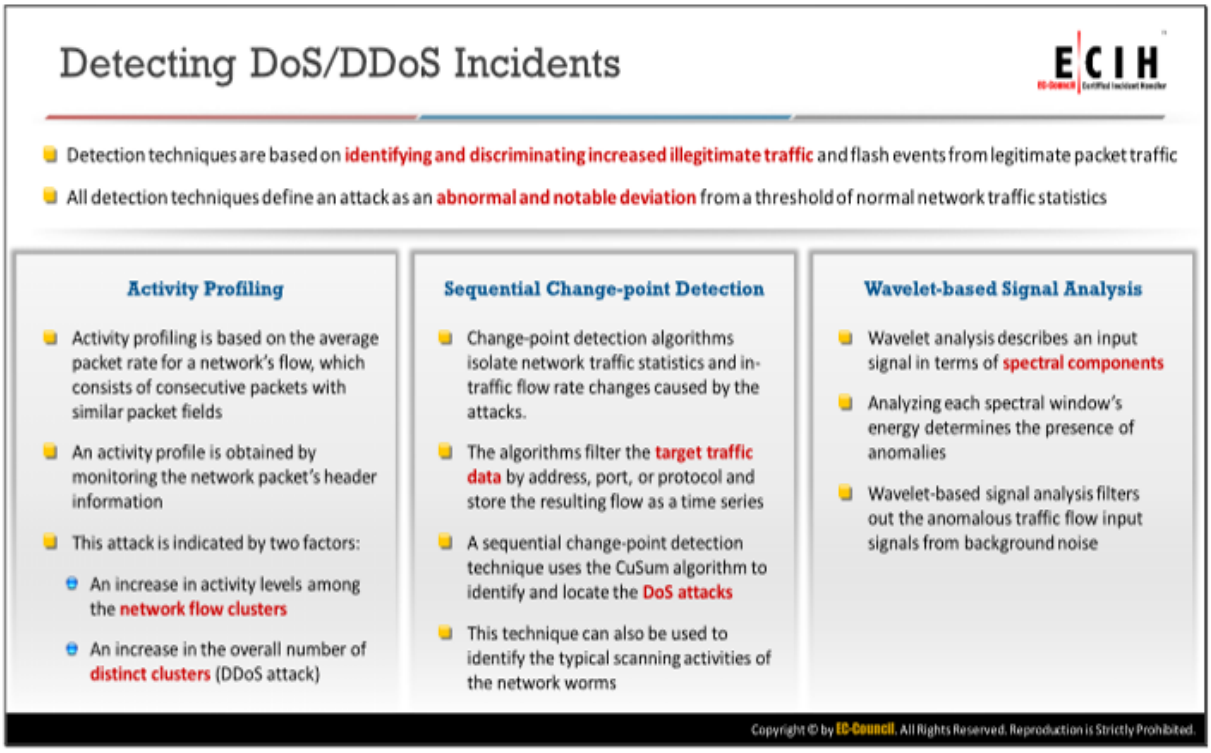


Indicators of DoS/DDoS Incidents

The following are indicators of different types of DoS/DDoS attacks.

- Indicators of a network-based DoS/DDoS attack targeting a host
  - User reports of system unavailability
  - Connection losses
  - Alerts from NIDS and HIDS
  - Increase in network bandwidth utilization
  - A host has several connections
  - An asymmetric network traffic pattern
  - Unprecedented log entries at the firewall and router
  - Data packets have abnormal source addresses
- Indicators of DoS/DDoS attacks on the host targeting an operating system
  - User reports of inaccessibility of a system and/or installed application
  - IDS and IPS alerts
  - Firewall alerts
  - OS-generated logs
  - Data packets with abnormal source addresses

- Indicators of network-based DoS/DDoS attacks targeting network services
  - User reports of system unavailability
  - Undefined connection losses
  - NIDS alerts
  - Increased utilization of network bandwidth
  - Asymmetric network traffic pattern
  - Unprecedented log entries at the firewall and router
  - Data packets with abnormal source addresses
  - Packets with abnormal destination addresses
- Indicators of DoS/DDoS attacks on a host targeting system applications
  - User reports of application unavailability
  - NIDS and HIDS alerts
  - Unprecedented application log entries
  - Data packets with abnormal source addresses



Detecting DoS/DDoS Incidents

Early detection techniques help to prevent DoS/DDoS attacks. Detecting a DoS/DDoS attack is a tricky job. A DoS/DDoS attack traffic detector needs to distinguish between a genuine and a bogus data packet, which is not always possible as the available techniques have limitations. There is always a chance of confusion between traffic generated by a legitimate network user and that generated by a DoS/DDoS attack. Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic. One problem in filtering bogus traffic from legitimate traffic is simply the volume of traffic; it is impossible to scan each data packet to entirely prevent a DoS/DDoS attack. All detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. Three types of detection techniques are described below.

- **Activity Profiling**

  Activity profiling is based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information (e.g., destination and sender IP addresses, ports, and transport protocols used). Indicators of an attack include:

  - An increase in activity levels among the network flow clusters
  - An increase in the overall number of distinct clusters (DDoS attack)

  High average packet rates or activity levels of a data flow correspond to less time between consecutive matching packets. Randomness in average packet rates or activity levels can indicate suspicious activity. The entropy calculation method measures randomness in activity levels, which increases when a network is under attack. One of the major challenges of activity profiling methods is the large volume of traffic, which

can be overcome by clustering packet flows with similar characteristics. DoS attacks generate a large number of data packets that are very similar, so an increase in the average packet rate or diversity of packets could indicate a DoS attack.

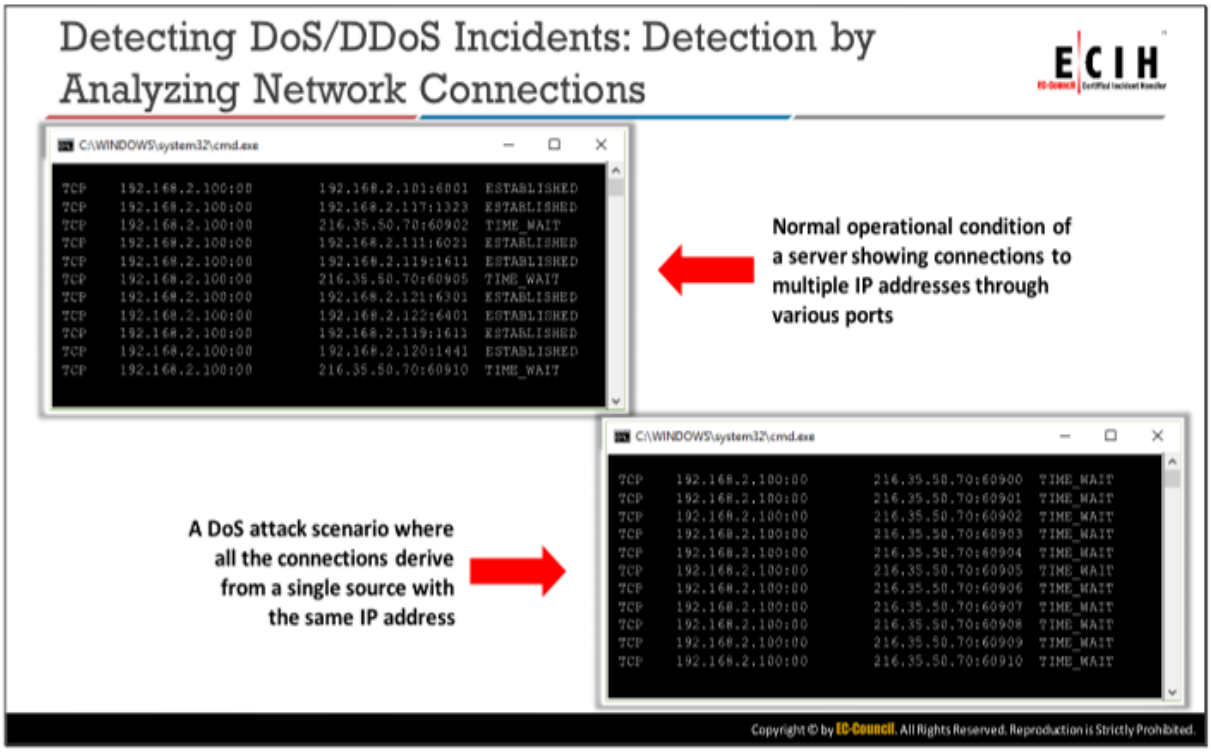
- **Sequential Change-point Detection**

  The sequential change-point detection technique filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate versus time. Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks. Drastic changes in the traffic flow rate can indicate a DoS attack.

  This technique uses **Cumulative Sum** (Cusum) algorithms to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series. The sequential change-point detection technique identifies the typical scanning activities of the network worms.

- **Wavelet-based Signal Analysis**

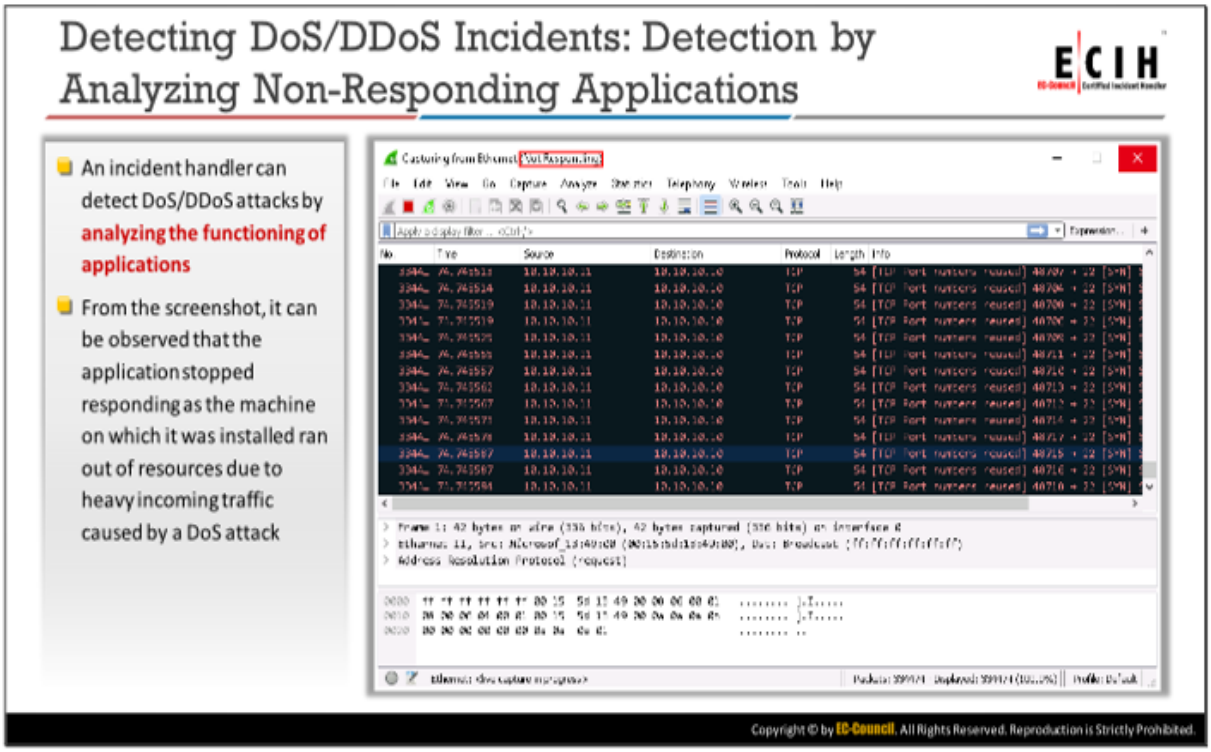
  The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. Analyzing the energy of each spectral window determines the presence of anomalies. These techniques check frequency components present at a specific time and provide a description of those components. The presence of an unfamiliar frequency indicates suspicious network activity. A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.



Detecting DoS/DDoS Incidents: Detection by Analyzing Network Connections

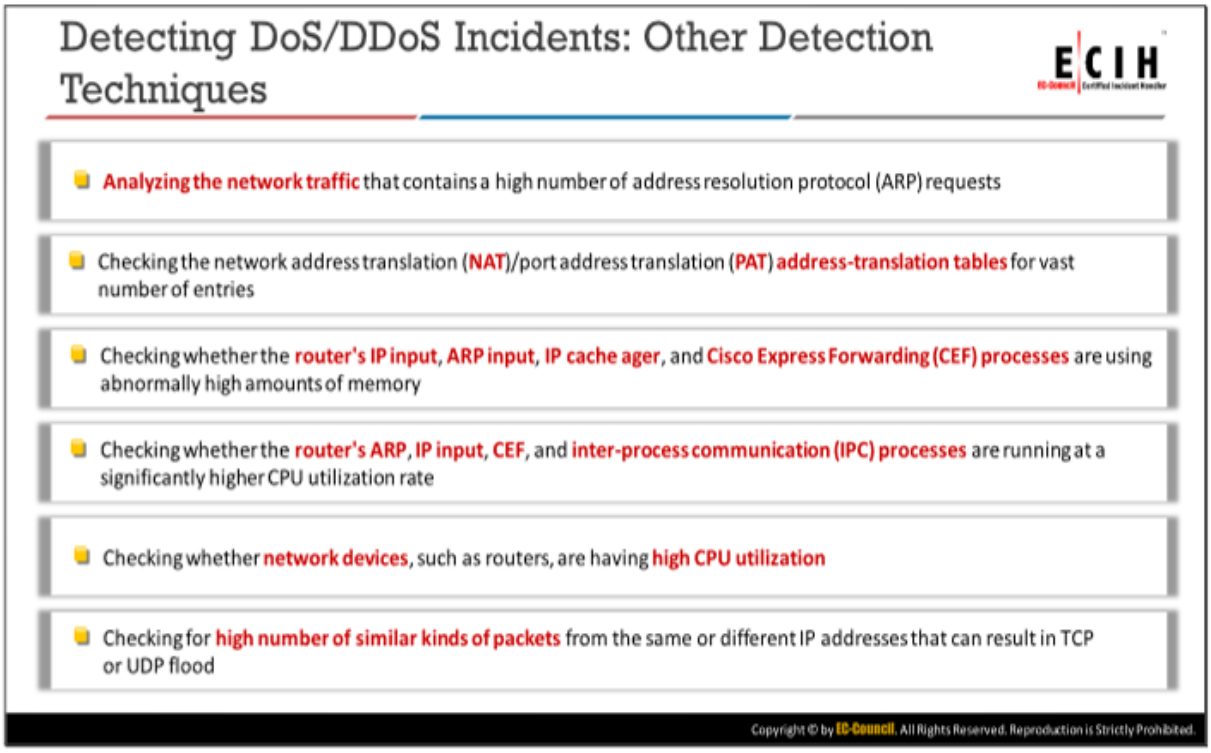
In addition to the above-mentioned techniques, there are several ways to detect a DoS attack, although all of them involve first examining the router. Incident responders can look for evidence of DOS attacks on the network at various network points, including the monitored network traffic, captured data packets, and logs from the IDS, firewall, ISP side, and others systems. In general, it is difficult to locate the DoS attack if the target was a service, application, system, or server because these devices may also stop running when they encounter internal hardware or software problems. Incident responders need to check the networks connecting the compromised devices, services, application, and servers to validate a DoS attack. Under normal operation conditions, a server shows multiple connections to multiple IP addresses through various ports, as shown in the screenshot on the above slide.

However, in a DoS attack scenario, all the connections are from a single source with the same IP address, as shown in the screenshot on the above slide.



Detecting DoS/DDoS Incidents: Detection by Analyzing Non-Responding Applications

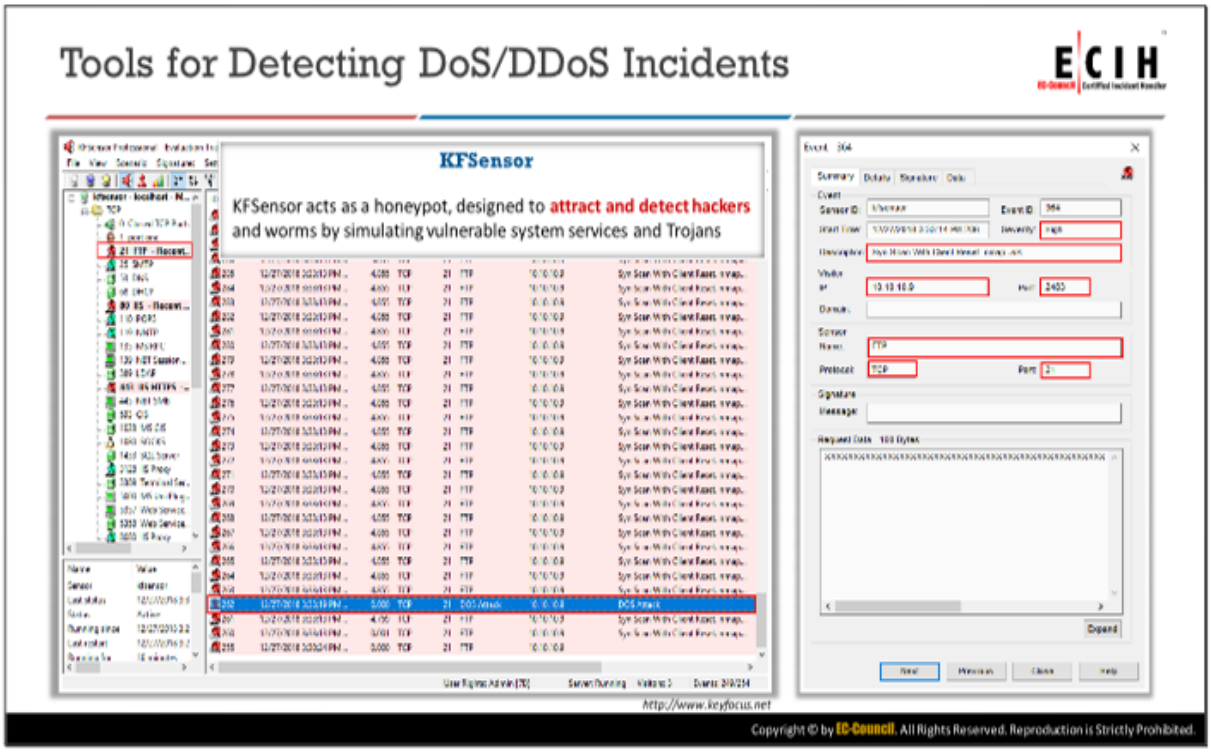
An incident handler can also detect DoS/DDoS attacks by analyzing how an application functions. The screenshot given on the slide shows an example of a typical DoS attack, where the application stopped responding as the machine (Windows 10) on which it is installed ran out of resources due to heavy incoming traffic caused by a DoS attack.



Detecting DoS/DDoS Incidents: Other Detection Techniques

Some other techniques for detecting DoS attack include:

- Analyzing the network traffic that contains high numbers of ARP requests
- Checking the network address translation (NAT)/port address translation (PAT) address-translation tables for large numbers of entries
- Checking whether the router's IP input, ARP input, IP cache ager, and Cisco Express Forwarding (CEF) processes are using abnormally high amounts of memory
- Checking whether the router's ARP, IP input, CEF, and inter-process communication (IPC) processes are running at a much higher CPU utilization rate than normal
- Checking whether the network devices, such as routers, have high CPU utilization
- Checking for a large number of similar kinds of packets from the same or different IP addresses that can result in TCP or UDP flood



Tools for Detecting DoS/DDoS Incidents

Discussed below are some of the important tools used for detecting DoS/DDoS incidents.

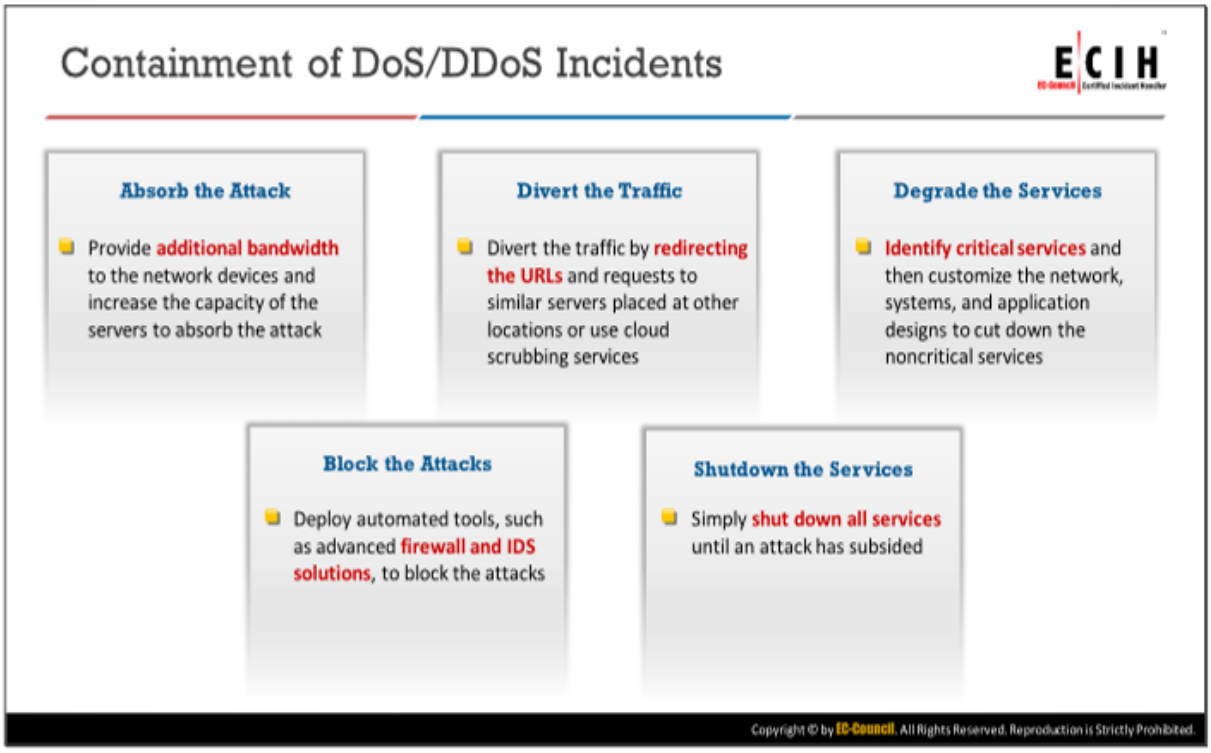
- **KFSensor**

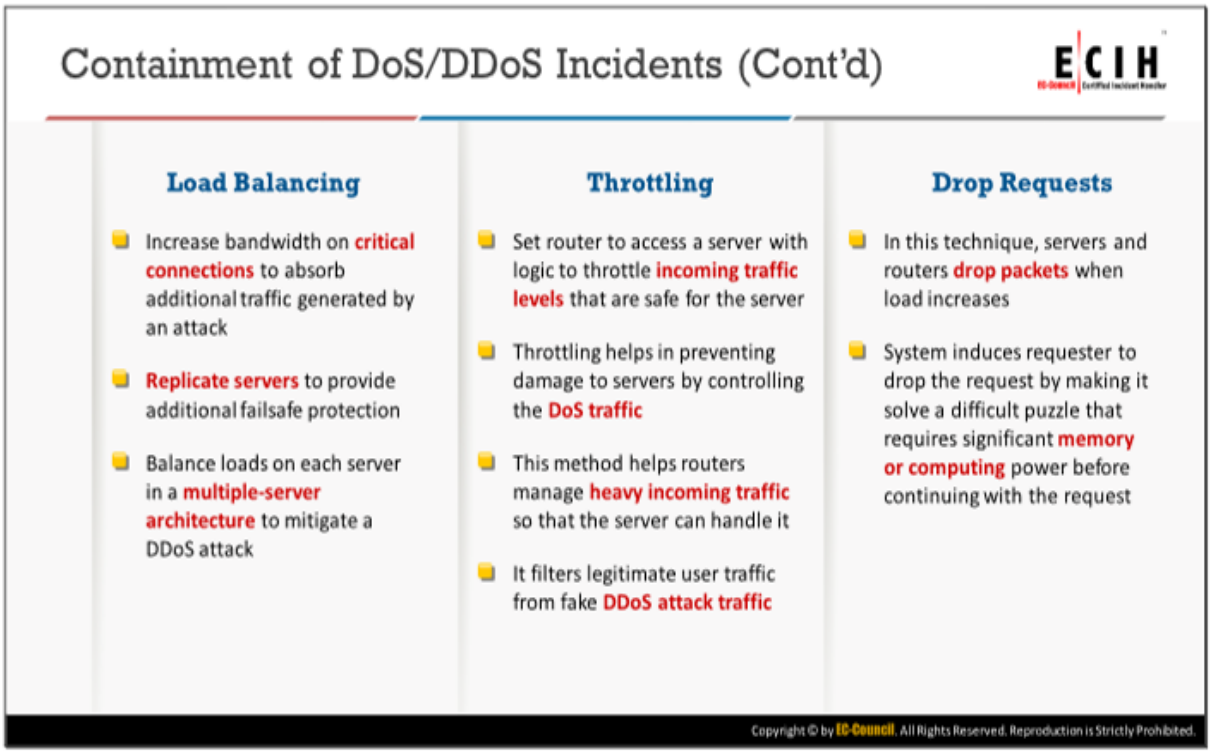
  Source: *http://www.keyfocus.net*

  KFSensor is a Windows-based honeypot IDS. It acts as a honeypot, which is designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By responding with an emulation of a real service, KFSensor can reveal the nature of an attack while maintaining total control and avoiding the risk of compromise. By acting as a decoy server, it can divert attacks from critical systems and provide more information than can be achieved using firewalls and NIDS alone.

Some additional tools for detecting DoS/DDoS incidents include:

- SSHHiPot (*https://github.com*)
- Artillery (*https://github.com*)





Containment of DoS/DDoS Incidents

There is no foolproof solution for containing DoS attacks. Organizations should select their DoS response strategy according to quality of service (QoS) requirements, bandwidth availability, and importance of the operations.

The major DoS response strategies are as follows:

- **Absorb the Attack**

  In this strategy, the organization contains the DoS attack by providing additional bandwidth to the network devices and increasing the capacity of the servers to absorb the attack. This process is possible only when the organizations have enough available bandwidth and are sure that the attack cannot consume the entire bandwidth (to avoid service disruption). In this case, they prefer not to react to the DoS attack, but instead absorb the attack traffic. This strategy requires advanced planning to assign the additional resources and capacity. This method has the disadvantage of the cost of the additional resources, which need to be in place even when no attacks are under way.

- **Divert the Traffic**

  Organizations can also divert the traffic by redirecting the URLs and requests to similar servers placed at other locations, or by using cloud scrubbing services with backup resources to divert the traffic.

- **Degrade the Services**

  This strategy works when quality of service (QoS) is not the most critical factor for business operations. In this strategy, organizations identify critical services and stop noncritical ones while identifying indicators of DoS attack. Stopping noncritical services makes extra resources available to absorb a DoS attack. First, the critical services are identified, followed by modification of the network, systems, and application designs to limit noncritical services and help critical services stay functional during an attack.

- **Block the Attacks**

  In this strategy, automated tools are deployed, such as advanced firewall and IDS solutions, which can detect DoS attacks using traffic distance and timing techniques and block them before they affect services.

- **Shutdown the Services**

  This strategy is the last possible solution to overcome a DoS attack. If the organization does not have resources to absorb the DoS attack and cannot sustain even critical services, then it is preferable to stop all services until the attack subsides.

- **Load Balancing**

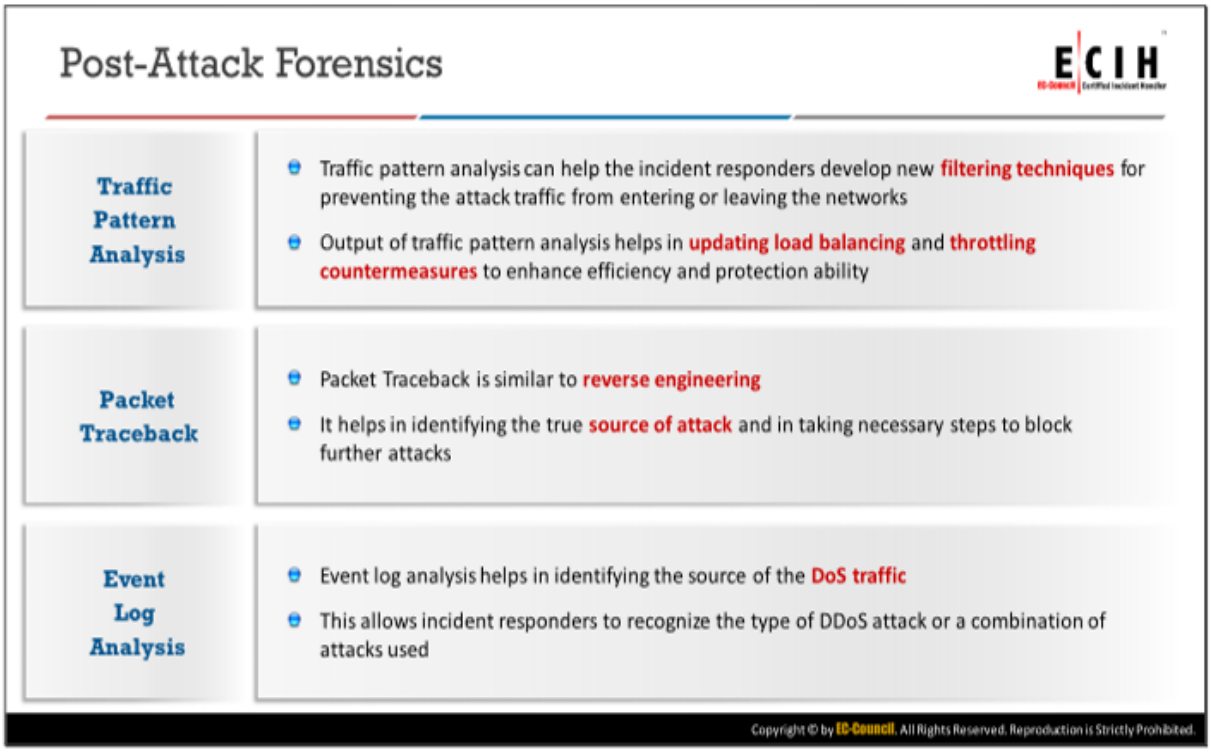
  Bandwidth providers can increase their bandwidth on the critical connections during a DDoS attack to prevent their servers from going down. Using a replicated server model provides additional failsafe protection. Replicated servers provide better load management by balancing loads on each server in a multiple-server architecture, enhancing normal network performance while mitigating the effect of a DDoS attack.

- **Throttling**

  In this case, routers are set to access a server and throttle incoming traffic to a safe level. "Min-max fair server-centric router" throttles (minimum and maximum throughput controls) help users prevent their servers from crashing. Throttling helps manage heavy incoming DoS traffic and prevent damage to servers. This method filters legitimate user traffic from fake DDoS attack traffic. The major limitation of this method is that it may trigger false alarms. Sometimes, it allows malicious traffic to pass while rejecting legitimate traffic.

- **Drop Requests**

  Another method is to drop packets when a load increases, usually performed by the router or server. The system presents a difficult puzzle that requires a lot of memory or computing power to solve in an attempt to induce the requester to drop the request. This can result in performance degradation of zombie systems, which could be noticed by the user and possibly stop them from taking part in transferring DDoS attack traffic.



Post-attack Forensics

After detecting and containing a potential DoS/DDoS attack, incident responders perform forensic investigation to extract more information regarding the incident and the attacker. Following are some of the forensic techniques used to extract such crucial information.

- **Traffic Pattern Analysis**

  During a DDoS attack, the traffic pattern tool stores post-attack data, which users analyze to determine the special characteristics of the attacking traffic. These data are helpful in updating load balancing and throttling countermeasures to enhance their efficiency and protection ability. Moreover, DDoS attack traffic patterns can help incident responders develop new filtering techniques to prevent DDoS attack traffic from entering or leaving their networks. Analyzing DDoS traffic patterns can also help incident responders ensure that an attacker cannot use their servers as a DDoS platform and access other sites.

- **Run Zombie Zapper Tool**

  One important method is use of the Zombie Zapper tool. When a company is unable to ensure the security of its servers and a DDoS attack starts, the network IDS will notice the high volume of traffic that indicates a potential problem. The targeted victim can run Zombie Zapper to stop the packets from flooding the system. There are two versions of Zombie Zapper: one for UNIX and one for Windows systems. Currently, this tool acts as a defense mechanism against Trinoo, TFN, Shaft, and Stacheldraht.

- **Packet Traceback**

  Packet Traceback refers to tracing back attack traffic, analogous to reverse engineering. The targeted victim works backward by tracing the packet to its original source. Once the victim identifies the true source, they can take necessary steps to block further attacks from that source by developing necessary preventive techniques. In addition, Packet Traceback can give information regarding the various tools and techniques that the attacker used, which can help in the development and implementation of various filtering techniques to block future attacks.

- **Event Log Analysis**

  DDoS event logs assist in forensic investigation and law enforcement, especially when the attacker caused destruction resulting in major financial damage. The providers can use honeypots and other network security mechanisms, such as firewalls, packet sniffers, and server logs, to store all information regarding the events that have taken place during the setup and execution of the attack. This allows incident responders to recognize the types of DDoS attacks used. In addition, the response team will analyze the router, firewall, and IDS logs to identify the source of the DoS traffic and try to trace back the attacker's IP address with the help of intermediary ISPs and law enforcement agencies.

- **Countermeasures**
  - Turn off the character generator protocol (CHARGEN) service to stop the attack
  - Download the latest updates and patches for servers

Eradicating DoS/DDoS Incidents: Blocking Potential Attacks

Egress Filtering

- Egress filtering **scans the headers of IP packets** leaving a network
- Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network
- The packets will not reach the targeted address if they do not meet the necessary specifications

Ingress Filtering

- Ingress filtering **prevents source address spoofing** of Internet traffic
- It **protects from flooding attacks** which originate from valid prefixes (IP addresses)
- It enables tracing of the originator to its true source

TCP Intercept

- TCP intercept feature in router protects TCP servers from a TCP SYN-flooding attack
- Configuring TCP Intercept **prevents DoS attacks** by intercepting and validating the TCP connection requests

Rate Limiting

- Rate limiting **controls the rate of outbound or inbound traffic** of a network interface controller
- It **reduces the high volume, inbound traffic** that can cause a DDoS attack

Eradicating DoS/DDoS Incidents: Disabling Botnets

RFC 3704 Filtering

RFC 3704 filtering limits the impact of DDoS attacks by denying traffic with **spoofed addresses**

Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link

Cisco IPS Source IP Reputation Filtering

Reputation services help in determining if an **IP or service** is a threat or not

Cisco IPS regularly **updates its database** with known threats such as botnets, botnet harvesters, and malware and helps in filtering DoS traffic

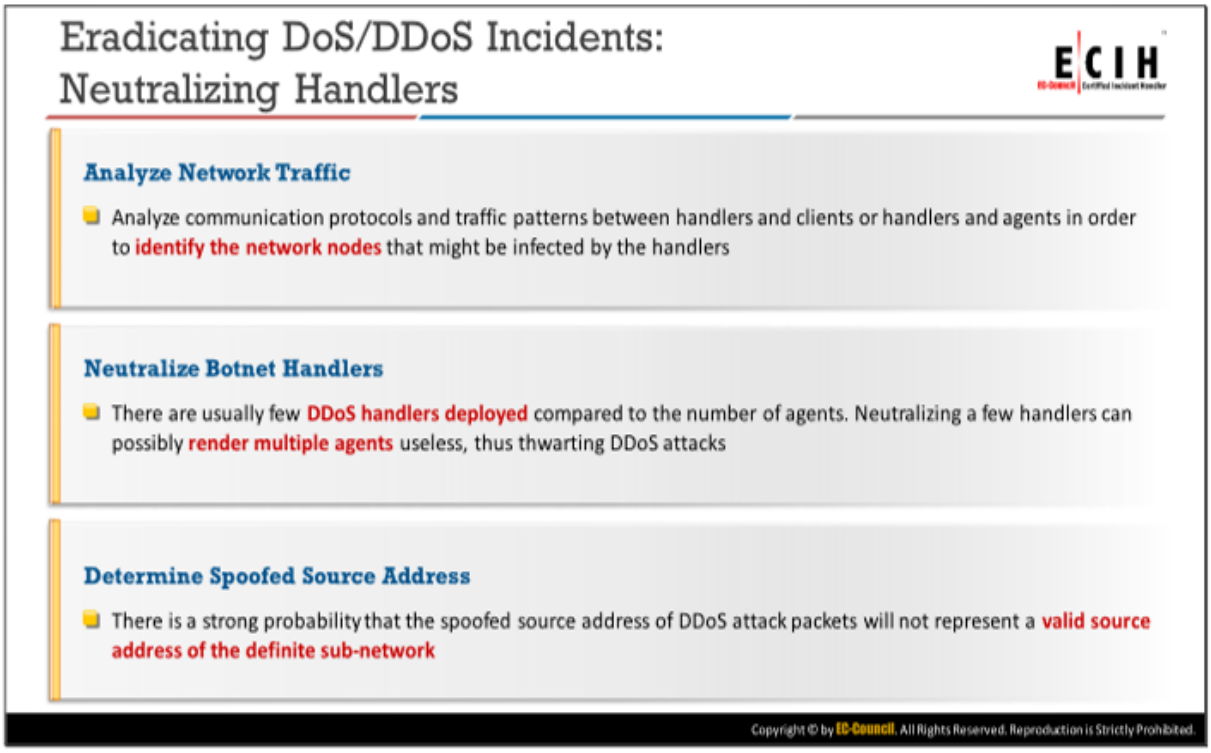
Black Hole Filtering

Black hole filtering refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient

Black hole filtering refers to **discarding packets** at the routing level

DDoS Prevention Offerings from ISP or DDoS Service

Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the **DHCP snooping binding database** or IP source bindings, prevents a bot from sending spoofed packets



Eradicating DoS/DDoS Incidents

To completely eradicate potential DoS/DDoS attacks, an incident handler can perform various precautionary measures, such as blocking potential attacks, disabling botnets, and neutralizing botnet handlers.

Blocking Potential Attacks

To block the various potential DoS/DDoS attacks, organizations can deploy ingress filtering, egress filtering, TCP intercepting, and rate limiting methods, among others.

- **Egress Filtering**

  Egress filtering scans the headers of IP packets leaving a network. If the packets pass the specifications, they can route out of the sub-network from which they originated. The packets will not reach the targeted address if they do not meet the necessary specifications. Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network. As DDoS attacks generate spoofed IP addresses, establishing protocols that require all legitimate packets leaving a company network to have a source address where the network portion matches the internal network can help mitigate attacks. A properly developed firewall for the sub-network can filter many DDoS packets with spoofed IP source addresses.

  If a web server is vulnerable to a zero-day attack known only to the underground hacker community, applying all available patches to the server could be insufficient. However, if the user enables egress filtering, they can protect the integrity of a system by keeping the server from establishing a connection back to the attacker. This also limits the effectiveness of many payloads used in common attacks. Outbound exposure can be

restricted to the required traffic, which limits the attacker's ability to connect to other systems and gain access to tools that can enable deeper access into the network.

- **Ingress Filtering**

  Ingress filtering is a packet-filtering technique used by many ISPs to prevent source address spoofing of internet traffic, and thus indirectly combat several types of net abuse by making internet traffic traceable to its true source. It protects against flooding attacks that originate from valid prefixes (IP addresses).

- **TCP Intercept**

  TCP intercept is a traffic-filtering feature in routers to protect TCP servers from a TCP SYN-flooding DoS attack. In a SYN-flooding attack, the attacker sends a huge volume of requests to connect to unreachable return addresses. As the addresses are not reachable, the connections cannot be established and remain unresolved. This huge volume of unresolved open connections overwhelms the server and can result in rejection of valid requests, i.e. legitimate users may not be able to access services.

  In TCP intercept mode, the router intercepts the SYN packets sent by the clients to the server and matches with an extended access list. If there is a match, the intercept software establishes a connection with the client on behalf of the destination server. Similarly, the intercept software establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the intercept software combines them transparently. Thus, the TCP intercept software prevents fake connection attempts from reaching the server and acts as a mediator between the server and client throughout the connection.

- **Rate limiting**

  Rate limiting is a technique used to control the rate of outbound or inbound traffic of a network interface controller. This technique effectively reduces the high volume of inbound traffic during DDoS attacks. This technique is often used in hardware configured to limit the rate of requests on layers 4 and 5 of an OSI model.

Disabling Botnets

Four ways to defend against botnets are discussed below.

- **RFC 3704 Filtering**

  RFC 3704 is a basic ACL filter, which limits the impact of DDoS attacks by denying traffic with spoofed addresses. This filter requires packets sourced from valid, allocated address space, consistent with the topology and space allocation. A "**bogon list**" consists of all unused or reserved IP addresses that should not come in from the internet. If any of the IP addresses from the bogon list appears, it is classified as a spoofed source IP and the filter removes it. Users can check with their ISP that they apply RFC 3704 filtering in the cloud to prevent bogus traffic entering their internet connection. The bogon list changes regularly, so, in case that the ISP does not apply this filter, then the user has to manage their own bogon ACL rules or switch to another ISP.

- **Cisco IPS Source IP Reputation Filtering**

  Reputation services help to determine if an IP or service is a threat or not. Cisco Global Correlation, a new security capability of Cisco IPS 7.0, uses immense security intelligence. The Cisco SensorBase Network contains all information about known threats on the internet, including botnets, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS uses this network to filter DoS traffic before it damages critical assets. To detect and prevent malicious activity even earlier, it incorporates the global threat data into its system.

- **Black-hole Filtering**

  Black-hole filtering is a common technique to defend against botnets and prevent DoS attacks. Black holes refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach the intended recipient. Undesirable traffic can be dropped before it enters a protected network using a technique called remotely triggered black-hole (RTBH) filtering. As this is a remotely triggered process, this filtering needs to be conducted in collaboration with the ISP. This method uses border gateway protocol (BGP) host routes to route traffic heading to victim servers to a "null0" next hop.

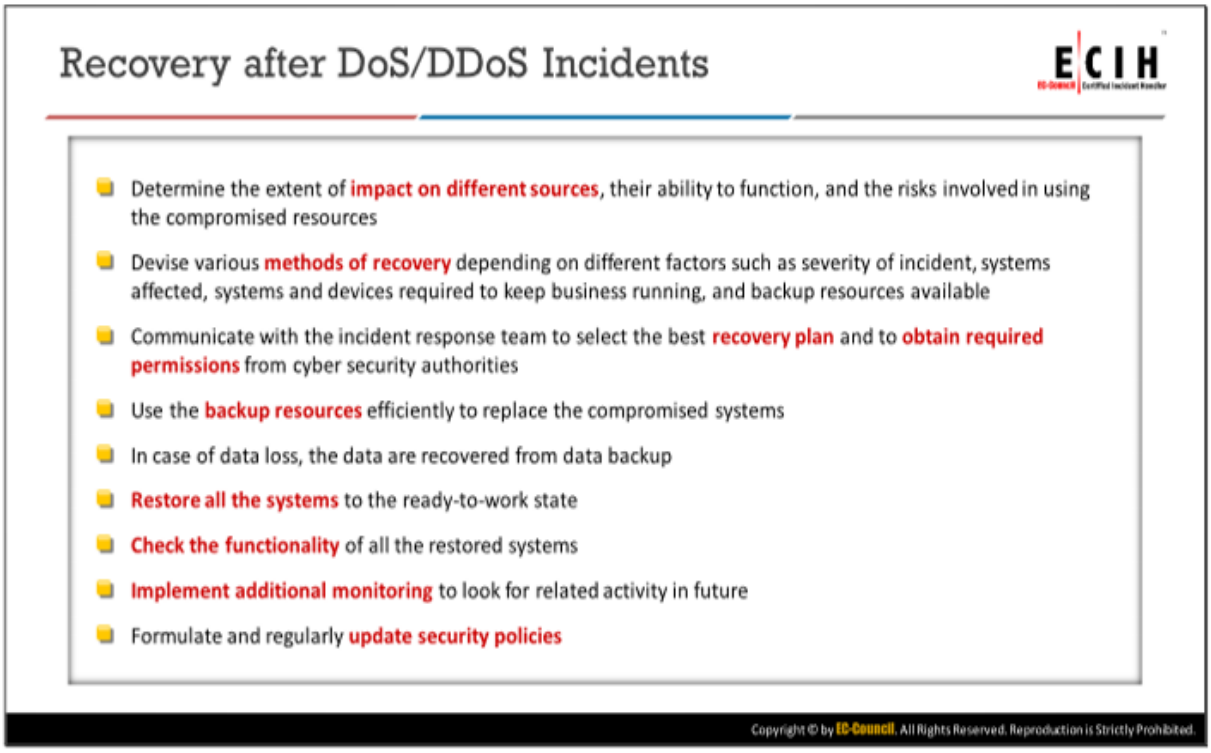
- **DDoS Prevention Offerings from ISP or DDoS Service**

  This method is effective in preventing IP-spoofing at the ISP level. Here, the ISP scrubs the traffic prior to allowing it to enter the internet link. Since this service runs in the cloud, the DDoS attack cannot saturate the internet links. In addition, some third parties offer cloud DDoS prevention services. IP Source Guard (in CISCO) or similar features in other routers can be used to filter traffic based on the DHCP snooping binding database or IP source bindings, which prevent a bot from sending spoofed packets.

Neutralizing Handlers

An important method used to stop DDoS attacks is to detect and neutralize handlers. This can be achieved by network traffic analysis, neutralizing botnet handlers, and identifying spoofed source address. In the agent-handler DDoS attack-tool arsenal, the handler works as an intermediary for the attacker. Analyzing communication protocols and traffic patterns between handlers and clients (or agents) can identify the network nodes that are infected by handlers. Identifying the handlers in the network and disabling them can be a quick method of disrupting the DDoS attack. As there are usually few DDoS handlers deployed in the network, compared to the number of agents, neutralizing a few handlers can potentially neutralize multiple agents, thus preventing DDoS attacks.

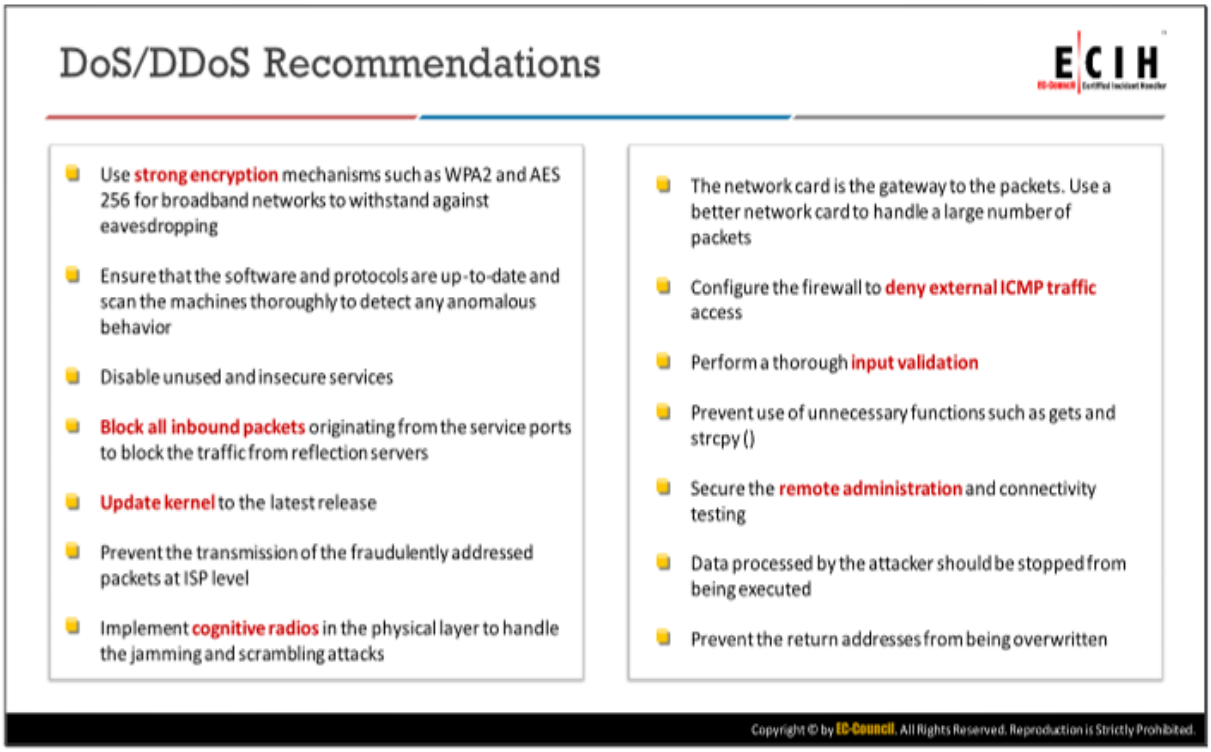
Furthermore, there is a significant probability that the spoofed source address of DDoS attack packets will not have a valid source address for the specific sub-network. Hence, identifying a spoofed source address will prevent a DDoS attack. The prevention of DDoS attacks is possible by applying a thorough understanding of communication protocols and traffic among handlers, clients, and agents.



Recovery after DoS/DDoS Incidents

The IH&R team must perform the following activities to recover the network after DoS/DDOS attacks:

- Determine the extent of the impact on different resources, their ability to function and risks involved in using the compromised resources
- Devise various methods of recovery depending on the severity of the incident, systems affected, critical systems and devices required to keep business running, and backup resources available
- Communicate with the incident response team to select the best recovery plan and obtain the required permissions from cybersecurity authorities
- Use the backup resources efficiently to replace the compromised systems
- Recover any lost data from backup files
- Restore all systems to their ready-to-work state
- Check the functionality of all restored systems
- Implement additional monitoring to look for related activity in future
- Formulate and regularly update security policies

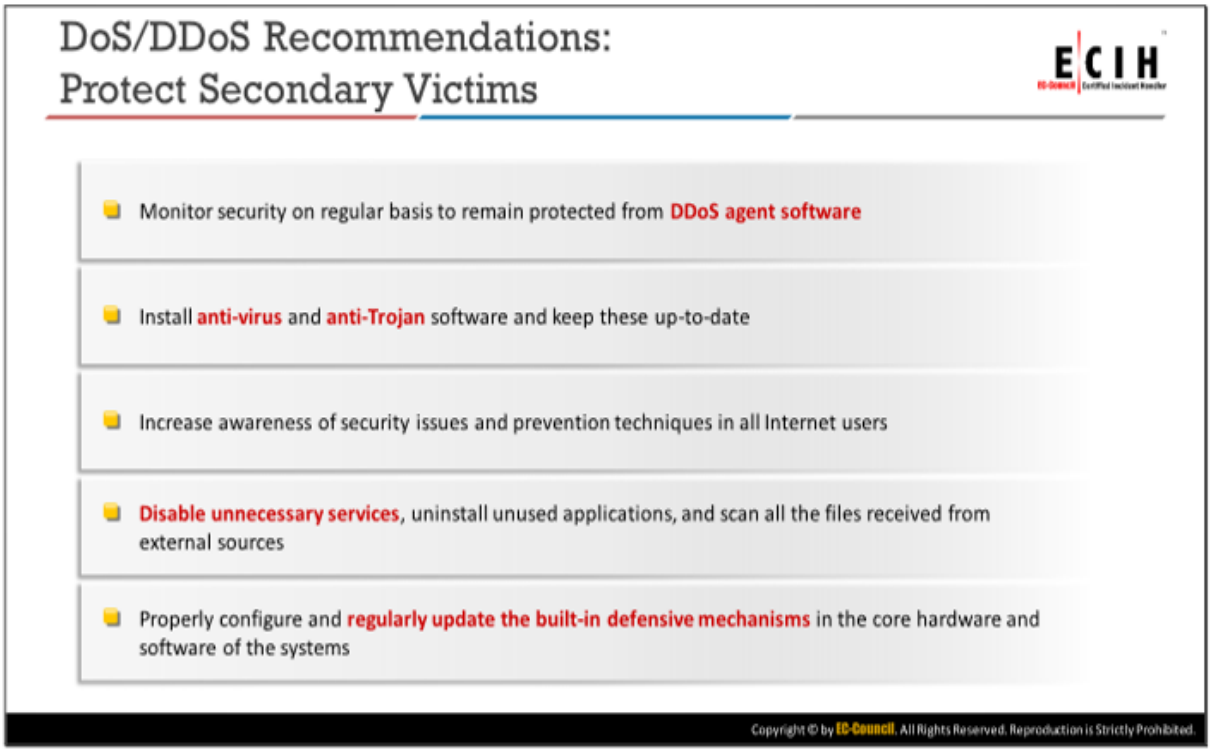


DoS/DDoS Recommendations

Implementing defensive mechanisms in appropriate parts of the network and following proper measures can increase organizational network security. The following are a list of countermeasures for combating DoS/DDoS attacks:

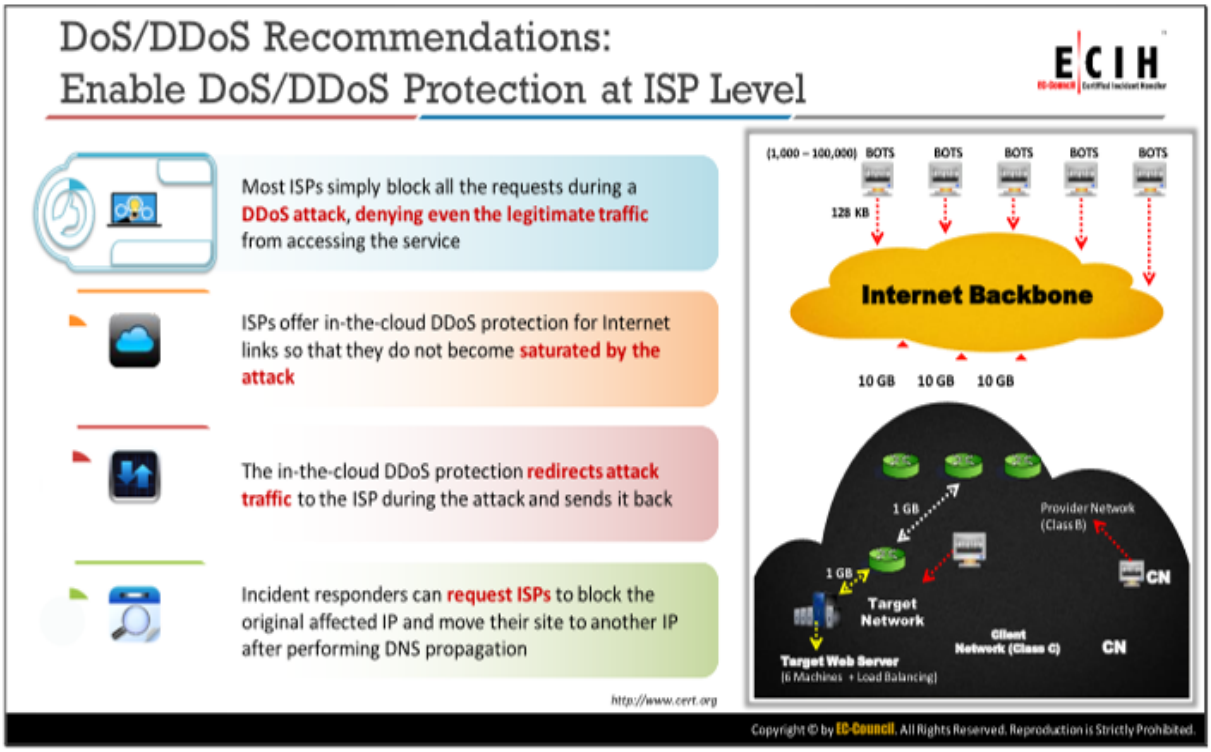
- Use strong encryption mechanisms such as WPA2 and AES 256 for broadband networks to evade eavesdropping
- Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior
- Disable unused and insecure services
- Block all inbound packets originating from the service ports to block traffic from reflection servers
- Update kernel to the latest release
- Enable TCP SYN cookie protection
- Prevent the transmission of fraudulently addressed packets at the ISP level
- Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
- Use a better network card that can handle larger number of packets
- Configure the firewall to deny external ICMP traffic access
- Perform thorough input validation
- Prevent use of unnecessary functions, such as gets and strcpy

- Secure the remote administration and connectivity testing
- Stop execution of data processed by the attacker
- Prevent overwriting of the return addresses



DoS/DDoS Recommendations: Protect Secondary Victims

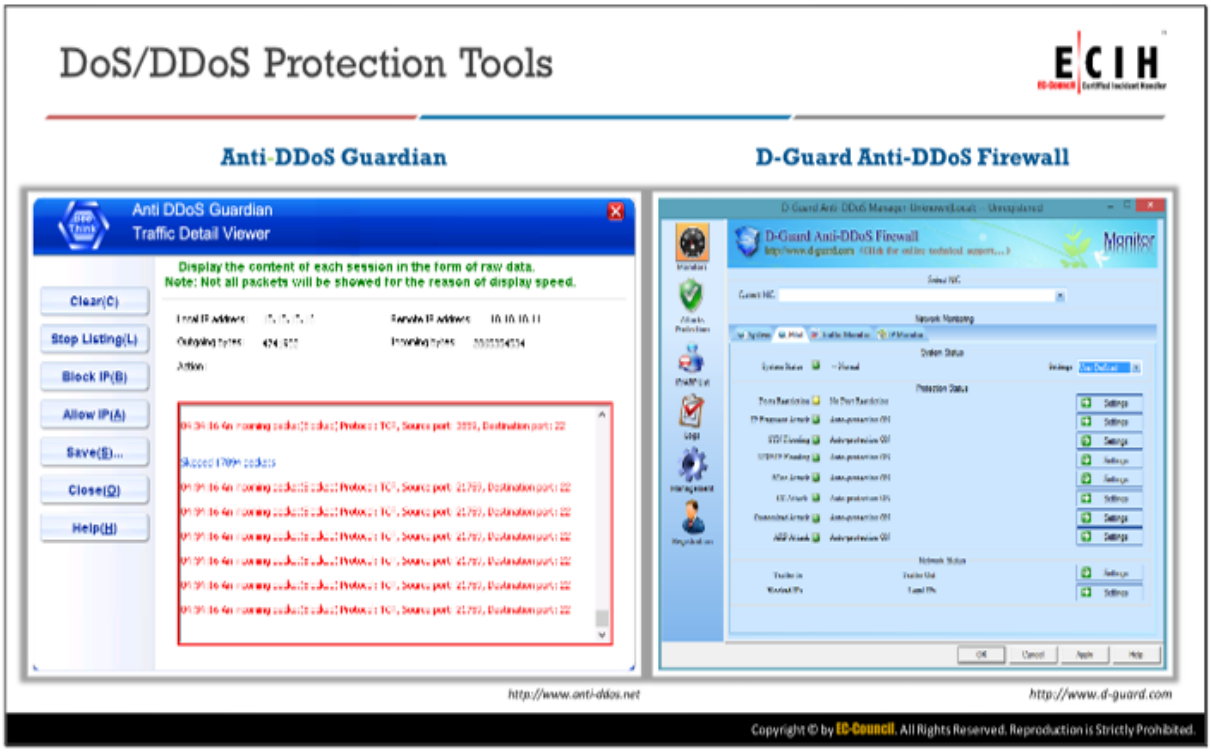
The best method for preventing DDoS attacks is to prevent secondary victim systems from taking part in the attack. This demands intensified security awareness and prevention techniques. Secondary victims must monitor their security on a regular basis to ensure that the system does not install any DDoS agent program and DDoS agent traffic is not transferred into the network. Antivirus and anti-Trojan software must be installed and updated on a regular basis, as well as software patches to fix known vulnerabilities. In addition, it is important to increase awareness of security issues and prevention techniques among all internet users, including disabling unnecessary services, uninstalling unused applications, and scanning all files received from external sources. Because these tasks may appear daunting to the average internet user, the core hardware and software of computing systems come with integrated mechanisms that defend against malicious code insertion. Hence, DDoS attacks are avoided by properly configuring and regularly updating the built-in defense mechanisms. Employing such countermeasures minimize the number of machines available from which attacks can be launched.

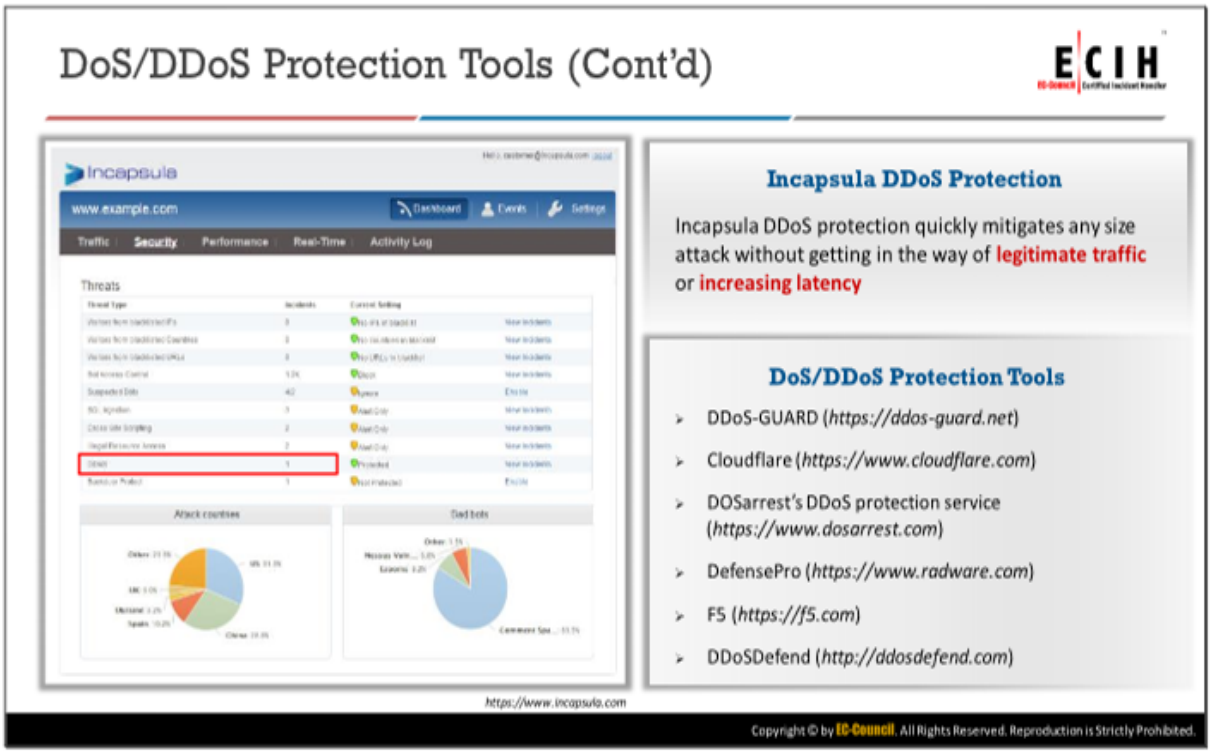


DoS/DDoS Recommendations: Enable DoS/DDoS Protection at ISP Level

Source: *http://www.cert.org*

One of the best ways to defend against DoS attacks is to block them at the gateway, which is the responsibility of the contracted ISP. ISPs offer "clean-pipe" SLAs that ensure a certain bandwidth of genuine traffic rather than total bandwidth of all traffic. Most ISPs simply block all requests during a DDoS attack, denying even legitimate traffic from accessing the service. If an ISP does not provide clean-pipe services, the user should choose subscription services provided by many cloud service providers. The subscription services serve as an intermediary, receive traffic destined for the network, filter it, and then pass it on only to trusted connections. Vendors such as Imperva and VeriSign offer services for cloud protection against DoS attacks. ISPs offer in-the-cloud DDoS protection for internet users to avoid saturation by the attack. This system redirects attack traffic to the ISP during the attack and sends it back to the attacker. Incident responders can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.





DoS/DDoS Protection Tools

The IH&R team can use the following tools to protect their networks from DoS/DDoS attacks.

- **Anti DDoS Guardian**

  Source: *http://www.anti-ddos.net*

  Anti DDoS Guardian protects Windows Servers from DDoS attacks. It detects and stops most DDoS/DoS attacks, including SYN attacks, IP flood, TCP flood, UDP flood, ICMP flood, slow HTTP DDoS attacks, Layer 7 attacks, Application attacks, and Windows Remote Desktop brute-force password guessing attacks. The DDoS protection system manages the network flows, client bandwidth, client TCP connection number, UDP/ICMP packet rate, and TCP half-open connection. This light and robust DDoS protection software can be successfully deployed on Windows website server machines in a production environment to ensure websites are protected against DDoS/DoS attacks.

- **D-Guard Anti-DDoS Firewall**

  Source: *http://www.d-guard.com*

  D-Guard Anti-DDoS Firewall provides DDoS protection for online enterprises, public and media services, essential infrastructure, and internet service providers. As a professional Anti-DDoS Firewall, D-Guard can protect against almost all kinds attacks, including DoS/DDoS, Super DDoS, DrDoS, Fragment attack, SYN flooding attack, IP Flooding attack, UDP, mutation UDP, random UDP flooding attack, ICMP, IGMP Flood attack, ARP Spoofing attack, HTTP Proxy attack, CC Flooding attack, CC Proxy attack, CC varieties attack, and zombie cluster CC attack. D-Guard Anti-DDoS Firewall is an excellent tool for mitigating DDoS attacks, with a design that focuses on passing legitimate traffic rather than discarding attack traffic, which allows it to handle severe attack scenarios without performance degradation.

  Features:

  - Protection against almost all kinds of attacks
  - Built-in intrusion prevention system
  - TCP flow control
  - IP blacklist and white list, ARP white list, and MAC binding
  - Multiple OSs supported

- **Incapsula DDoS Protection**

  Source: *https://www.incapsula.com*

  Incapsula DDoS protection quickly mitigates attacks of any size without compromising legitimate traffic or increasing latency. It is designed to provide multiple DDoS protection options and supports unicast and anycast technologies to power a many-to-many defense methodology. This tool automatically detects and mitigates attacks exploiting application and server vulnerabilities, hit-and-run events, and large botnets. Incapsula proxies all web requests to block DDoS attacks from being relayed to client origin servers. In addition, it detects and mitigates any type of attack, including TCP

SYN+ACK, TCP FIN, TCP RESET, TCP ACK, TCP ACK+PSH, TCP fragment, UDP, slowloris, spoofing, ICMP, IGMP, HTTP flood, brute-force, connection flood, DNS flood, NXDomain, mixed SYN + UDP or ICMP + UDP flood, ping of death, and smurf type attacks.

Additional DDoS protection tools are listed below:

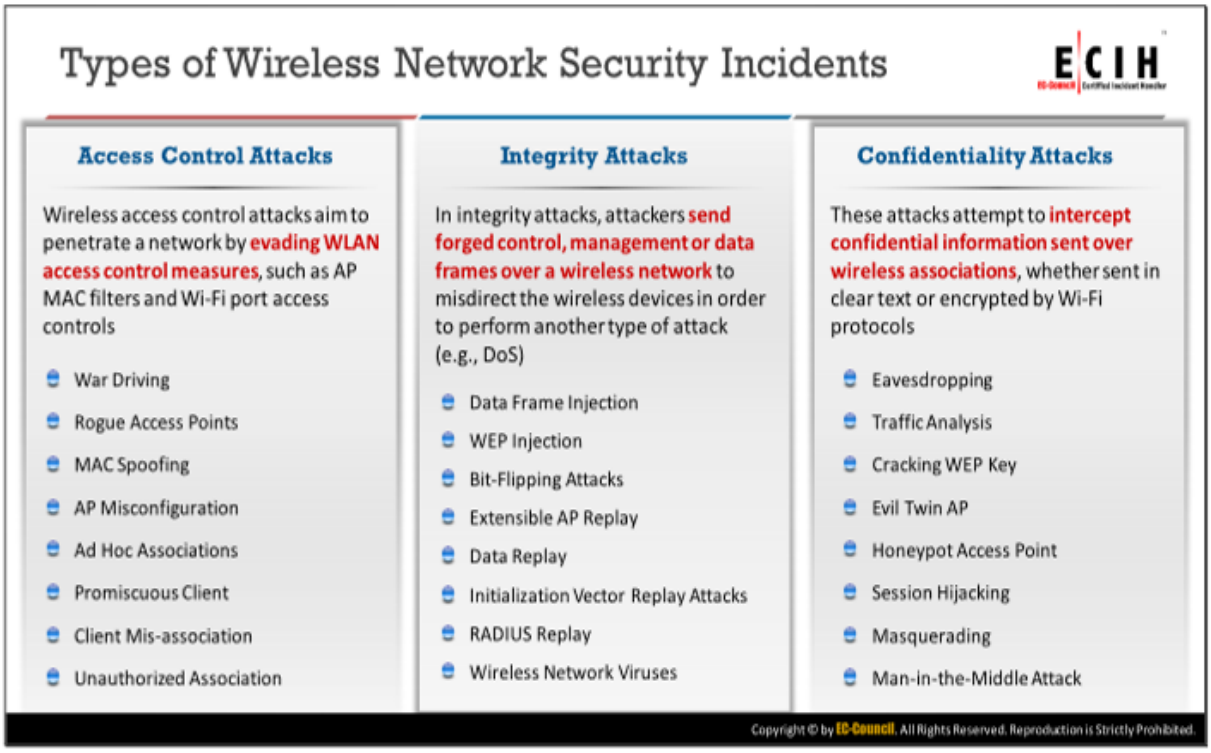
- DDoS-GUARD (*https://ddos-guard.net*)
- Cloudflare (*https://www.cloudflare.com*)
- DOSarrest's DDoS protection service (*https://www.dosarrest.com*)
- DefensePro (*https://www.radware.com*)
- F5 (*https://f5.com*)
- DDoSDefend (*http://ddosdefend.com*)
- NetFlow Analyzer (*https://www.manageengine.com*)
- Wireshark (*https://www.wireshark.org*)
- NetScaler AppFirewall (*https://www.citrix.com*)
- Andrisoft Wanguard (*https://www.andrisoft.com*)

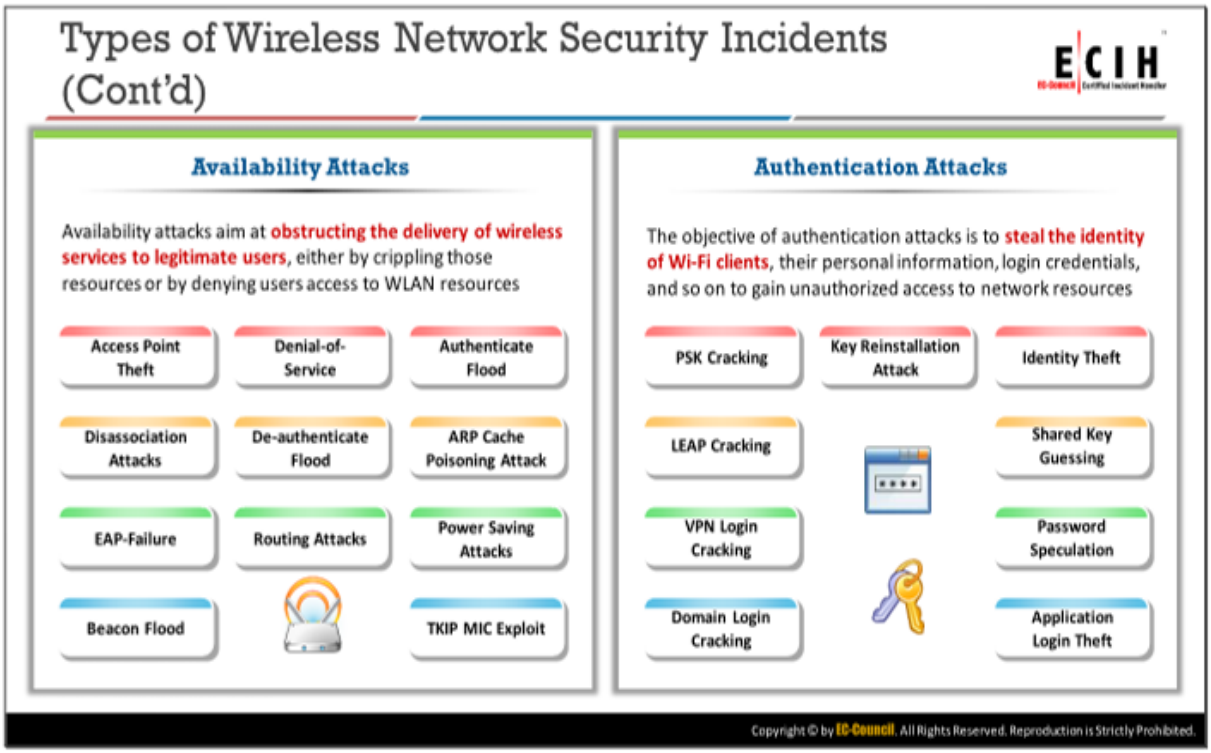
Handling Wireless Network Security Incidents

Wireless networks are inexpensive and easy to maintain compared to wired networks. An attacker can easily compromise a wireless network if proper security measures are not used or if there is no appropriate network configuration. Using a high-security mechanism for a wireless network can be expensive. Hence, it is advisable to determine critical resources, risks, or vulnerabilities associated with the network and ensure that the current security mechanism can protect the wireless network against all possible attacks. If not, the security mechanisms should be upgraded. This section includes an introduction to the types of wireless network security incidents, and the strategies for preparing for such incidents, and their detection, containment, eradication, and recovery.

Introduction to Wireless Network Security Incidents

A wireless network security incident refers to a security event that happens due to accidental or intentional activities in a wireless network. It can involve a software or hardware failure or a well-planned attack to compromise the resources of a wireless network. A wireless network is an unbounded data communication system that uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections by using electromagnetic waves to connect two individual points without establishing any physical connection between them. Wireless networks are inexpensive and easy to maintain compared to legacy networks, which has resulted in increased adoption of wireless technologies. However, this has led to wireless networks becoming a target for attackers, which is currently a major area of concern for organizations. Unlike wired networks, there is no built-in security for wireless networks; hence, wireless networks incidents can easily occur.





Types of Wireless Network Security Incidents

Wireless networks are used in nearly all organizations and are becoming more attractive for malicious cyberattacks. Wireless networks can be compromised by various types of attacks, including access control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks. These are described in detail in the following sections.

Access Control Attacks

Wireless access control attacks aim to penetrate a network by evading wireless LAN access control measures, such as AP MAC filters and Wi-Fi port access controls. There are several types of access control attacks, including:

- **War driving:** In a war driving attack, wireless LANS are detected either by sending probe requests over a connection or by listening to web beacons. An attacker who discovers a penetration point can launch further attacks on the LAN. KisMAC and NetStumbler and other tools can be used by the attacker in war driving attacks.
- **Rogue Access Points (APs):** To create a backdoor into a trusted network, an attacker may install an unsecured AP or fake AP inside a firewall. The attacker may also use any software or hardware APs to perform this kind of attack. A wireless AP (WAP) is a rogue AP when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue APs on a trusted network with malicious intent.
- **MAC Spoofing:** Using the MAC spoofing technique, an attacker can reconfigure a MAC address to appear as an authorized AP to a host on a trusted network. The attacker may use tools such as SMAC to perform this type of attack.
- **AP Misconfiguration:** If the user improperly configures any of the critical security settings at any of the APs, the entire network could be exposed to vulnerabilities and attacks. The AP cannot trigger alerts in most IDSs, as the system recognizes them as a legitimate device.
- **Ad hoc Associations:** An attacker may perform this type of attack using any USB adapter or wireless card. The attacker connects the host to an unsecured client to attack a specific client or avoid AP security.
- **Promiscuous Client:** Using a promiscuous client, an attacker exploits a behavior of 802.11 wireless cards, which always try to find a stronger signal with which to connect. An attacker places an AP near the target Wi-Fi network and gives it a common SSID name, and then offers an irresistibly strong signal and higher speed than the target Wi-Fi network. The intent is to lure the client to connect to the attacker's AP rather than the legitimate Wi-Fi network. Promiscuous clients allow an attacker to transmit target network traffic through a fake AP. It is very similar to the evil twin threat on a wireless network, in which an attacker launches an AP that poses as an authorized AP by beaconing the WLAN's SSID.
- **Client Misassociation:** The client may connect or associate with an AP outside the legitimate network, intentionally or accidentally. This is because the WLAN signals travel in the air, through walls and other obstructions. Such client misassociation can result in access control attacks.
- **Unauthorized Association:** Unauthorized association is a major threat to a wireless network. Prevention of this kind of attack depends on the method or technique that the attacker uses to become associated with the network.

Integrity Attacks

An integrity attack involves changing or altering data during transmission. In wireless integrity attacks, the attacker sends forged control, management, or data frames over a wireless network to misdirect wireless devices to perform another type of attack (e.g., DoS). Some examples of integrity attacks are listed in the table below.

Type of Attack	Description	Method and Tools
Data Frame Injection	Constructing and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
WEP Injection	Constructing and sending forged WEP encryption keys.	WEP cracking + injection tools
Bit-flipping Attacks	Capturing the frame and flipping random bits in the data payload, modifying ICV, and sending it to the user.	
Extensible AP Replay	Capturing 802.1X extensible authentication protocols (e.g., EAP identity, success, and failure) for later replay.	Wireless capture + injection tools between client and AP
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools
Initialization Vector Replay Attacks	Deriving the key stream by sending plain-text message.	
RADIUS Replay	Capturing RADIUS access-accept or reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	Viruses have a great impact on a wireless network as they are a simple method for compromising APs.	

Table 6.4: Wireless Threats - Integrity Attacks

Confidentiality Attacks

These attacks attempt to intercept confidential information sent over a wireless network, regardless of whether the system transmits data in clear text or encrypted format. If the system transmits data in encrypted format, an attacker will try to break the encryption (such as WEP or WPA). Examples of confidentiality attacks on wireless networks are listed in the table below.

Type of Attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
Traffic Analysis	Inferring information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, WepAttack, WepDecrypt
Evil Twin AP	Posing as an authorized AP by beaconing the WLAN's SSID to lure users.	CqureAP, HostAP, OpenAP
Honeypot AP	Resetting an AP's SSID to that of a legitimate AP.	Manipulating SSID
Session Hijacking	Manipulating the network so the attacker's host appears to be the desired destination.	Manipulating
Masquerading	Pretending to be an authorized user to gain access to a system.	Stealing login IDs and passwords, bypassing authentication mechanisms
MITM Attack	Running traditional MITM attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap

Table 6.5: Wireless Threats - Confidentiality Attacks

Availability Attacks

Availability attacks aim to obstruct the delivery of wireless services to legitimate users, either by crippling those resources or by denying them access to WLAN resources. Attackers can perform such attacks in various ways. Some examples are shown in the table below.

Type of Attack	Description	Method and Tools
AP Theft	Physically removing an AP from its installed location.	Stealth and/or speed
Disassociation Attacks	Destroying the connectivity between an AP and client, to make the target unavailable to other wireless devices.	Destroying the connectivity
EAP failure	Observing a valid 802.1X EAP exchange, and then sending the client a forged EAP failure message.	File2air and libradiate
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for clients to find a legitimate AP.	FakeAP
Denial-of-Service	Exploiting the CSMA/CA clear channel assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmissions
De-authenticate Flood	Flooding client(s) with forged de-authenticates or disassociates to disconnect users from an AP.	AirJack, Omerta, void11
Routing Attacks	Distributing routing information within the network.	RIP protocol
Authenticate Flood	Sending forged authenticates or associates from random MACs to fill a target AP's association table.	AirJack, File2air, Macfld, void11
ARP Cache Poisoning Attack	Creating many attack vectors.	
Power Saving Attacks	Transmitting a spoofed TIM or DTIM to the client while in power saving mode, making the client vulnerable to a DoS attack.	
TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject

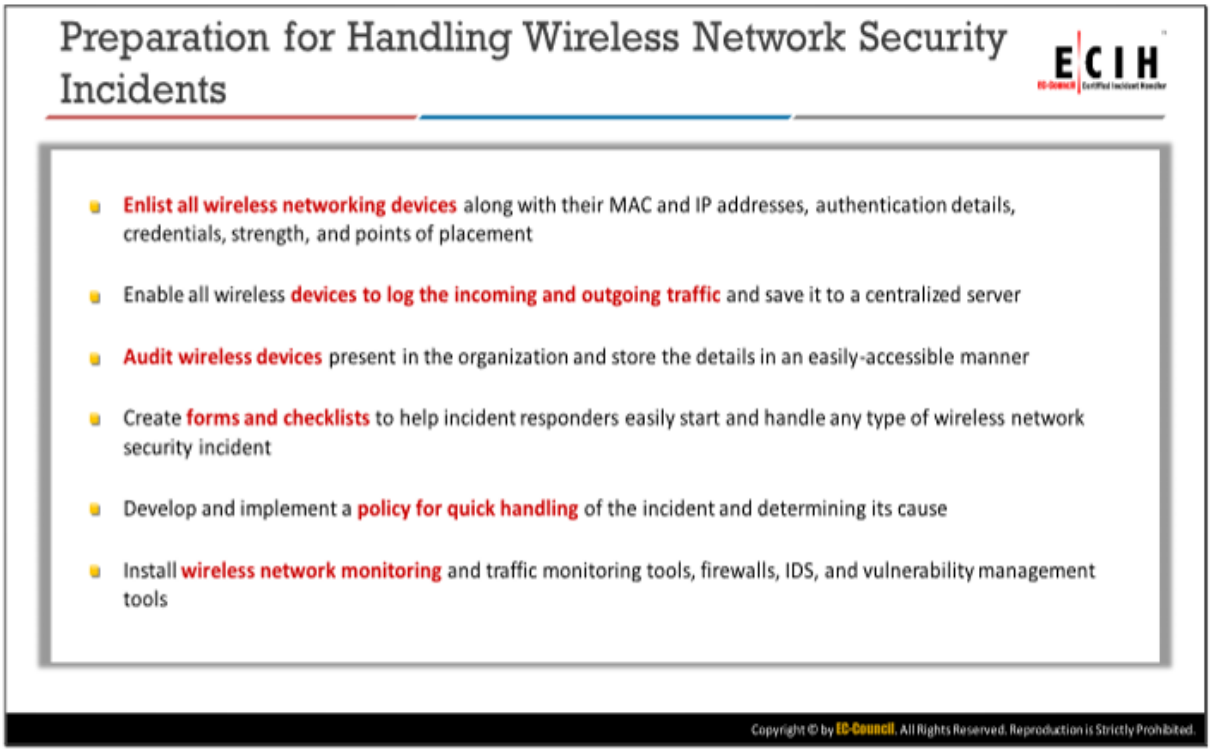
Table 6.6: Wireless Threats—Availability Attacks

Authentication Attacks

The objective of authentication attacks is to steal the identity of Wi-Fi clients, such as their personal information and login credentials, to gain unauthorized access to network resources.

Type of Attack	Description	Method and Tools
PSK Cracking	Obtaining a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
LEAP Cracking	Obtaining user credentials from captured 802.1X lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker
VPN Login Cracking	Gaining user credentials (e.g., PPTP password or IPsec preshared secret key) using brute-force attacks on VPN authentication protocols.	ike_scan and IKECrack (IPsec), Anger and THC-pptp-bruter (PPTP)
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain & Abel
Identity Theft	Capturing user identities from cleartext 802.1X identity response packets.	Packet capturing tools
Shared Key Guessing	Attempting 802.11 shared key authentication with guessed vendor default or cracked WEP keys.	WEP cracking tools
Password Speculation	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password dictionary
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, dsniff
Key Reinstallation Attack	Exploiting the 4-way handshake of the WPA2 protocol.	Nonce reuse technique

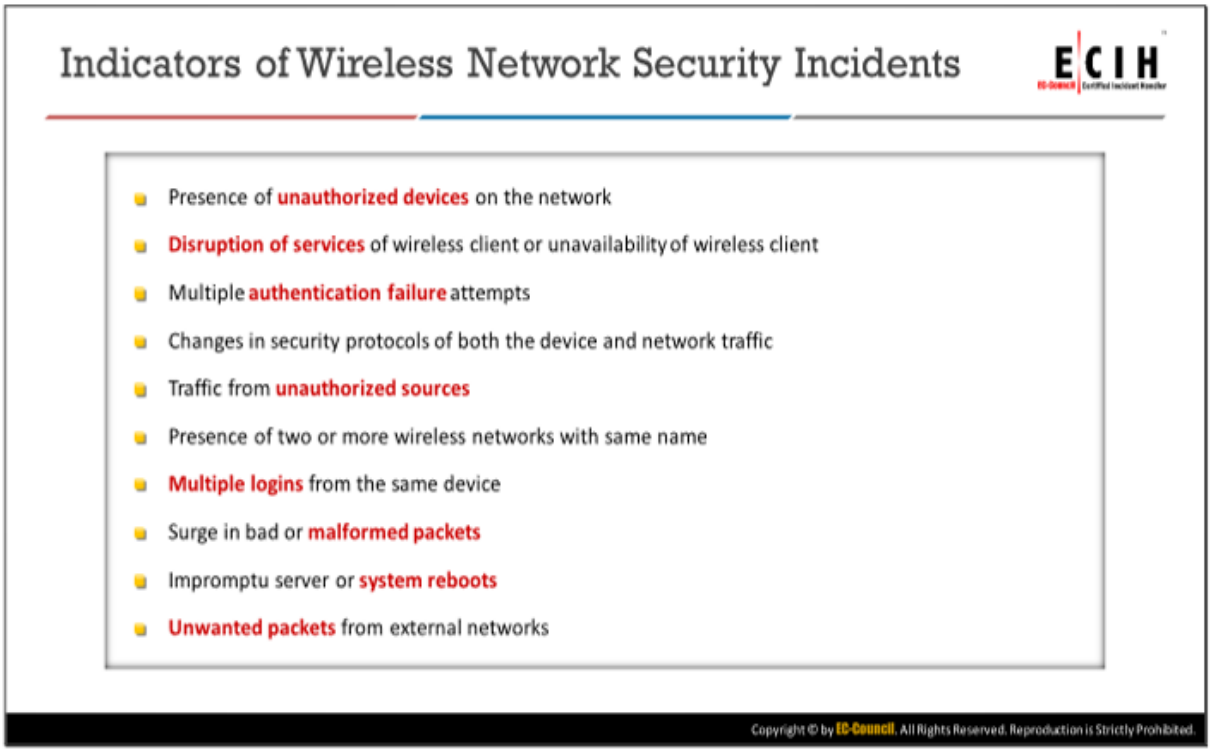
Table 6.7: Wireless Threats - Authentication Attacks



Preparation for Handling Wireless Network Security Incidents

The following preparation strategies are used to handle wireless security incidents.

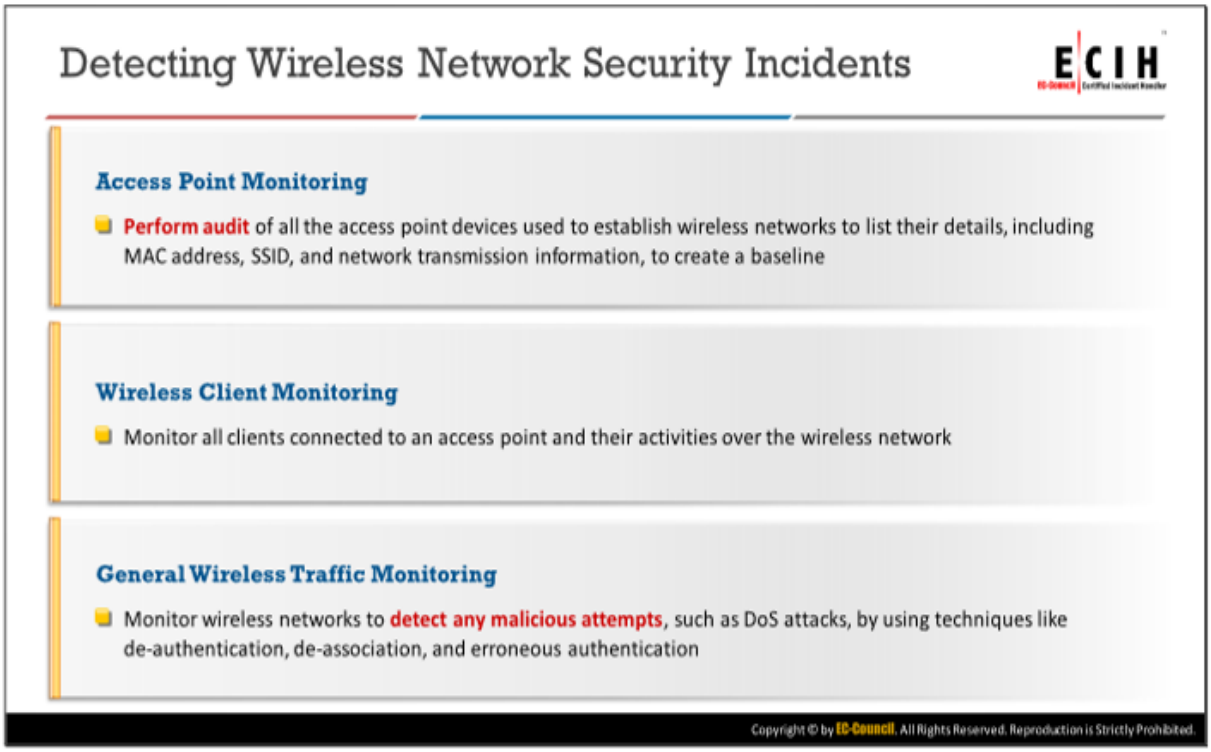
- Enlist all wireless networking devices, along with their MAC and IP addresses, authentication details, credentials, strength, and points of placement
- Enable all wireless devices to log the incoming and outgoing traffic and save it to a centralized server
- Audit the wireless devices present in the organization and store their details in easily accessible manner
- Create forms and checklists to help the IH&R team quickly respond to incidents
- Develop and implement a policy for handling the incident quickly and determining its cause
- Install wireless network and traffic monitoring tools, firewalls, IDS, and vulnerability management tools
- Obtain reports from wireless vulnerability management (WVM) systems installed on the wireless network.
- Inform the organization's security office that the organization should be capable of handling sensitive data
- Gather the tools required for performing IH&R procedures, such as detection, containment, and eradication of wireless network attacks



Indicators of Wireless Network Security Incidents

Indicators of wireless network incidents include:

- Presence of unauthorized devices on the network
- Disruption of services or unavailability of wireless client
- Multiple authentication failure attempts
- Changes in security protocols of the device and network traffic
- Traffic from unauthorized sources
- Presence of two or more wireless networks with the same name
- Multiple logins from the same device
- Surge in bad or malformed packets
- Impromptu server or system reboots
- Unwanted packets from external networks



Detecting Wireless Network Security Incidents

The incident responders can detect wireless network incidents using wireless client monitoring and general wireless traffic monitoring tools that record activity of the wireless devices.

- **Access Point Monitoring**

  The process includes performing audits of all AP devices used to establish wireless networks and obtaining their MAC address, SSID, and network transmission information to create a baseline. In addition, Wi-Fi monitoring tools, such as WifiChannelMonitor and PRTG Wi-Fi monitoring tools can be installed at the server level to monitor any changes in the baseline information of the AP. Incident responders should enable the device to listen to all possible traffic.

  Wi-Fi monitoring tools help incident responder access AP information, including the protocols used, signal strength, connected clients, admin status, and operation status. These tools also provide access reports of load, noise, and interference from the device. Incident responders can use this information to identify APs showing suspicious behavior. AP monitoring helps detect man-in-the-middle attacks by finding the new APs trying to connect to an already established channel, even if the spoofed AP has similar IP and MAC addresses to the original AP.

- **Wireless Client Monitoring**

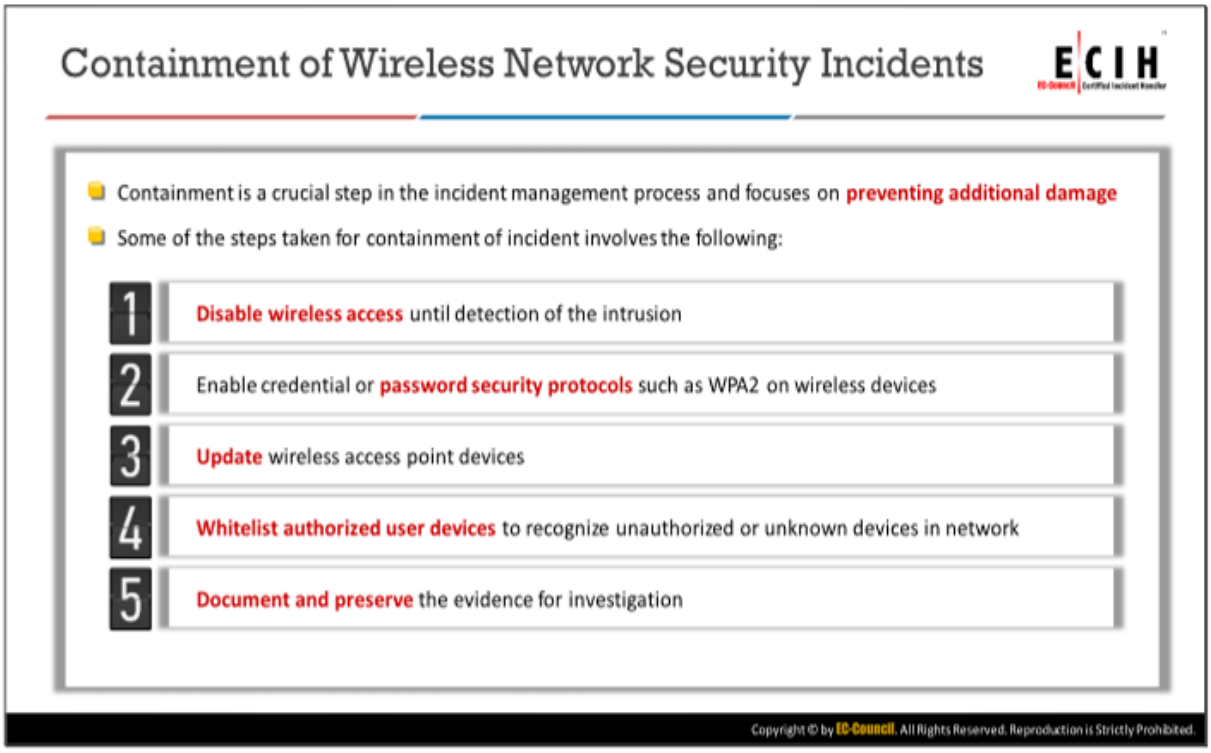
  The process involves monitoring all clients connected to an AP and their activities over the wireless network. This provides incident responders with information regarding the network performance, connection history, and usage statistics of all clients. Hence, incident responders can continuously monitor the clients connected to a particular AP and blacklist them using their MAC addresses. The incident responders can also use this

functionality to whitelist the clients that need to connect to the network through wireless APs. The process helps incident responders detect impersonation attacks.

- **General Wireless Traffic Monitoring**

  This method involves monitoring wireless networks to detect malicious attempts, such as DoS attacks using de-authentication, de-association, and erroneous authentication techniques. Such monitoring can also provide information about login failure attempts. Tools such as Wireshark are used to monitor the traffic of the wireless networks. Signal-to-noise ratio monitoring can also be performed to determine the frequency of the ongoing DoS attack. Incident responders can detect wireless network incidents using the following techniques.

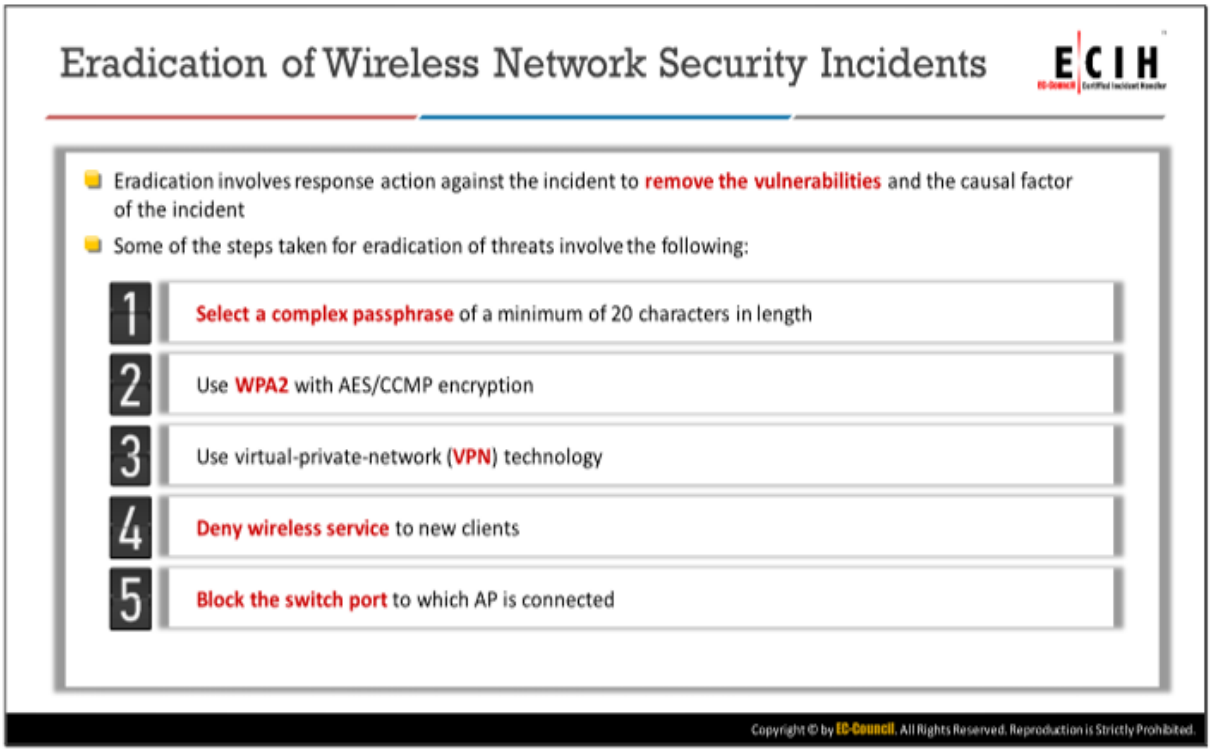
  - **Sniffing**: Sniffers installed on the wireless networks can store MAC address data along with their signal strength and timestamps. Incident responders can analyze anomalies in the MAC address timestamps of the APs to detect rogue APs and evil twins present on the network.
  - **Map of Physical Location**: Incident responders should develop a map of physical locations of the APs and their coverage area and look for signal mismatch points across the organization to locate rogue APs with spoofed MAC addresses, SSIDs, and passwords.
  - **Log Analysis**: Some attacks, such as brute force and password cracking, require the attacker's device to connect with the victim's AP. Incident responders need to analyze logs of all APs to locate new machines connected to them. Log data can be deleted in compromised devices, so incident responders can also detect the attacks by tracing the missing logs in the centralized log servers.
  - **Network Traffic Monitoring**: Incident responders should always monitor the network traffic to find illegitimate connections using IP address, MAC address, signal strength, and machine names. Tools such as NEtStumbler can be used to detect wireless network attacks.



Containment of Wireless Network Security Incidents

Containment is a crucial step in the incident management process that focuses on preventing additional damage. It includes planning strategies to avoid further losses, while ensuring that no forensic evidence related to the incident is destructed or tampered with. Organizations can contain wireless network security incidents by following the steps listed below.

- Disable wireless access until the intrusion is detected
- Use wireless access only in case of crucial business needs
- Enable credential or password security protocols such as WPA2 on wireless devices and change the key at regular intervals
- Check the devices connected to the victim's AP for traces of attack
- Change passwords of all devices across the organization
- Update the WAP devices, restoring the default settings and privileges
- Identify attacker details, such as IP address and MAC address, and block the devices used for the attack
- Whitelist authorized user devices so that no other devices can connect to the access points
- Implement additional security measures that are more difficult to compromise
- Document and preserve evidence for investigation

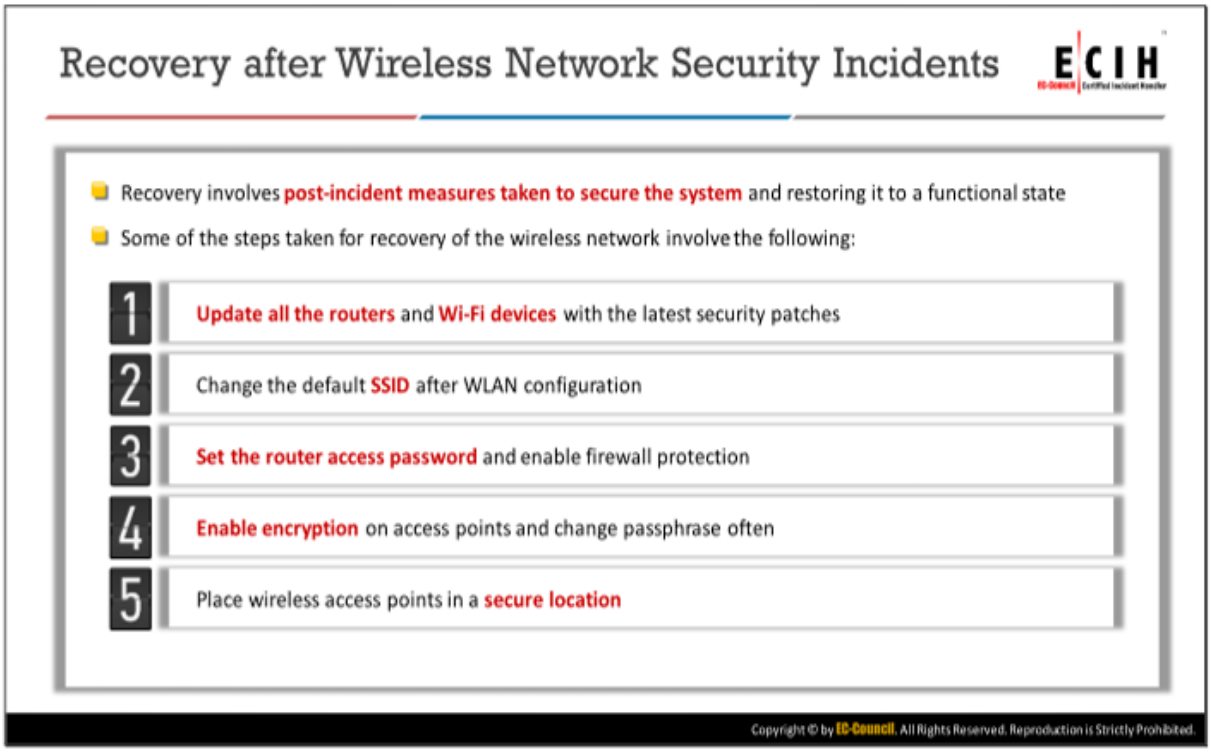


Eradication of Wireless Network Security Incidents

After a wireless network security breach attack is identified, controlled, and contained, the next step is to eradicate important aspects and causal factors related to the incident. These steps may involve removing the attacking agent from the wireless network, quarantining viruses and malware, and immobilizing compromised user accounts. In addition, the weaknesses and vulnerabilities present in the network system should be identified and resolved. The following steps can be used to eradicate wireless network security threats.

- Select a complex passphrase of a minimum of 20 characters in length and change it at regular intervals
- Use WPA2 with AES/CCMP encryption only
- Use virtual-private-network (VPN) technology such as remote access, extranet, and intranet VPN systems
- Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity
- Turn on auto updates for all wireless devices and patch the device firmware
- Avoid the use of public Wi-Fi networks
- Browse only secured websites and avoid accessing sensitive resources when the device is connected to an unprotected network
- In the case of internet-of-things devices, perform audits of devices and avoid connection to insecure Wi-Fi routers
- Enable HTTPS Everywhere extension and two-factor authentication

- Deny wireless service to new clients
- Block the switch port to which the AP is connected or manually locate the AP and physically remove it from the LAN
- Use non-regular patterns as PIN keys while pairing a device, and use key combinations which are non-sequential on the keypad
- Restrict any unknown and unexpected request for pairing of a device

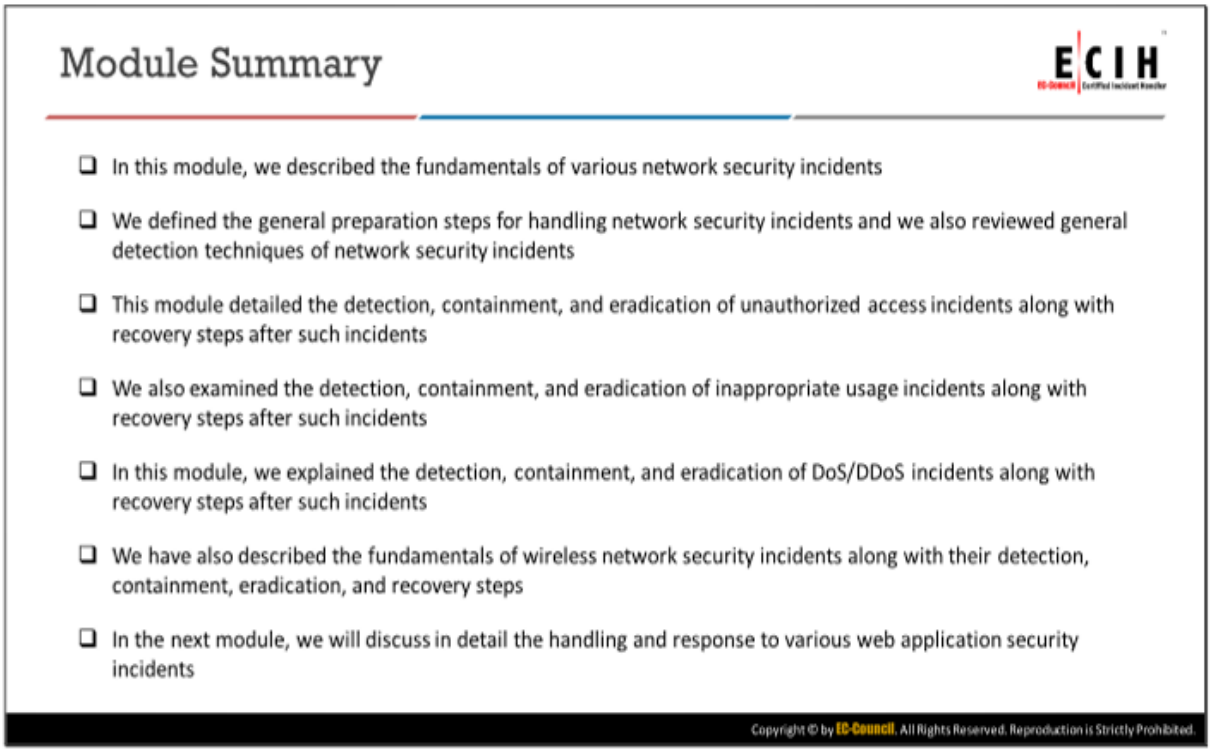


Recovery after Wireless Network Security Incidents

Recovering a system generally depends on the extent of the security breach. In the recovery step, restoration is started for the affected systems. When a wireless network security incident occurs, the IH&R teams decide whether to restore the existing system or completely replace it with system backups to rebuild the breached network system. The following are some of the steps that can be implemented when restoring the affected systems to their normal and secured functional state after a network security incident.

- Select a random passphrase that is not made up of dictionary words
- Properly set the client settings (e.g., validate the server, specify server address, do not prompt for new servers)
- Update all routers and Wi-Fi devices with the latest security patches
- Disable SSID broadcasts
- Change the default SSID after WLAN configuration
- Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone
- Avoid the use of SSID, company name, network name, or any easy-to-guess string in passphrases
- Set the router access password and enable firewall protection
- Place a firewall or packet filter in between the AP and the corporate intranet
- Disable the remote router login and wireless administration

- Enable MAC address filtering on the AP or router
- Enable encryption on the AP and change the passphrase often
- Limit the strength of the wireless network so it cannot be detected outside the bounds of the organization
- Regularly check the wireless devices for configuration or setup problems
- Implement an additional technique for encrypting traffic, such as IPSEC over wireless networks
- Choose Wi-Fi protected access (WPA) instead of WEP
- Implement WPA2 Enterprise wherever possible
- Disable the network when not required
- Place WAPs in a secure location
- Keep drivers on all wireless equipment updated
- Use a centralized server for authentication
- Keep Bluetooth in the disabled state, and enable it only when needed for the duration of the intended task
- Keep the Bluetooth device in non-discoverable (hidden) mode
- Check all Bluetooth devices that paired with the network in the past and delete any unknown devices
- Enable encryption when establishing Bluetooth connection to your PC
- Set the Bluetooth-enabled device to the lowest network range and perform pairing only in a secure area
- Install antivirus that supports host-based security software on Bluetooth-enabled devices
- Change the default settings of the Bluetooth-enabled device to the best security standard
- Use link encryption for all Bluetooth connections
- Use strong encryption on each link in the communication chain in the case of multiple wireless communication networks



Module Summary

In this module, we discussed the fundamental aspects of various network security incidents. We presented the general preparation steps and detection techniques for handling network security incidents. This module also gave a detailed discussion of the methods for the detection, containment, and eradication of various incidents (unauthorized access, inappropriate usage, DoS/DDoS, and wireless network security incidents), and strategies for recovery after such incidents.

In the next module, we present a detailed discussion of methods for handling and responding to various web application security incidents.

This page is intentionally left blank.