STUDENT HANDOUT · WEEK 6

Indicators of Malicious Activity and Mitigation Techniques

SY0-701 objectives 2.4, 2.5. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

1. Identify the nine malware types in objective 2.4 from their behavior and indicators.
2. Recognize physical, network, and application attacks from evidence in a scenario.
3. Explain downgrade, collision, and birthday attacks, and password spraying versus brute force.
4. Interpret indicators such as impossible travel, account lockout, and missing logs.
5. Choose mitigation techniques that fit a given attack and explain their purpose.
6. Apply the hardening techniques from objective 2.5 to a workstation or server.

KEY IDEAS

Each malware type leaves its own trail

Malware	What it does	Indicator
Ransomware	Encrypts files and demands payment	Mass file renames, ransom notes, high disk use
Trojan	Hides inside software that looks legitimate	New outbound connections after an install
Worm and virus	Worm spreads alone; virus needs a host and a user	Sudden scanning traffic; altered files
Spyware and keylogger	Watch activity and record keystrokes	Data sent out on a schedule, odd processes

Malware	What it does	Indicator
Rootkit	Hides itself with admin or kernel access	Tools disagree; processes or logs missing
Logic bomb, bloatware	Waits for a trigger; unwanted preinstalled apps	Damage on a date or event; wasted resources

Attacks on doors, airwaves, and wires

Physical attacks	Network attacks
Brute force: forcing doors, locks, or windows	DDoS, often both reflected and amplified
RFID cloning: copying a badge to a blank card	DNS: cache poisoning, hijacking, tunneling
Environmental: attacking power, HVAC, or fire systems	Wireless: evil twins, rogue APs, deauthentication
	On-path: ARP poisoning to sit between two hosts
	Credential replay and malicious code

Application attacks show up in the logs

Attack	What it does	Log clue
Injection	Input runs as SQL, OS, or LDAP commands	Quotes, OR 1=1, or semicolons in fields
Buffer overflow	Oversized input corrupts memory	Very long inputs, then a crash
Replay	Captured valid traffic or a token is resent	The same token or request seen twice
Privilege escalation	A user gains rights they were not given	New admin rights with no change ticket
Forgery	CSRF or SSRF makes a trusted party send it	Requests from an unexpected origin
Directory traversal	../ sequences reach files outside the web root	../ or %2e%2e%2f in the URL

Cryptographic and password attacks

Cryptographic attacks	Password attacks
Downgrade: force an older, weaker protocol	Spraying: a few common passwords, many accounts
Collision: two inputs that produce the same hash	Brute force: many guesses against one account
Birthday: probability makes collisions easier	Offline cracking of stolen hashes avoids lockout
Defense: disable old versions, use SHA-256 or better	Defense: MFA, lockout, long passwords, salted hashes

Indicators that something is wrong

Indicator	What it can mean
Account lockout	Brute force or spraying against that account
Concurrent session usage	One account in use in two places at once
Impossible travel	Logins too far apart for the time between them
Blocked content	Malware or a user reaching a banned site or file
Resource use or inaccessible	Cryptomining, DDoS, or ransomware at work
Out-of-cycle or missing logs	Tampering, or an attacker hiding tracks

Mitigation techniques limit the damage

Technique	What it does	Clinic example
Segmentation	Splits the network so a breach stays small	Medical devices on their own VLAN
Access control	ACLs and permissions decide who reaches what	Only billing staff can open the billing share
Application allow list	Only approved programs may run	Front desk PCs run only approved apps
Isolation	Cuts a system off entirely or nearly so	Quarantine an infected laptop
Patching	Fixes known flaws on a schedule	Critical patches within 14 days
Encryption	Makes stolen data unreadable	Full disk encryption on laptops

Watch, limit, enforce, and retire

Monitoring	Logs and alerts reveal an attack while it is under way. (SIEM alert on mass lockouts)
Least privilege	Each account gets only the access its job requires. (No admin rights for daily work)
Config enforcement	Tools push the approved baseline and undo drift. (Group Policy, MDM profiles)
Decommissioning	Retire fully: wipe data, remove access and DNS entries. (Old server wiped, not just unplugged)

Harden every host the same way

1. Encrypt	Turn on full disk encryption, keys escrowed

2. Protect	Install endpoint protection and a HIPS
3. Firewall	Enable the host firewall, deny inbound by default
4. Close ports	Disable unused ports and protocols such as Telnet
5. Change defaults	Replace every default password before go-live
6. Remove	Uninstall software the system does not need

EXERCISE 1: NAME THE ATTACK FROM THE EVIDENCE

8 MINUTES · PAIRS

For each piece of evidence, name the most likely attack and the indicator or clue that points to it.

#	Prompt	Your answer
1	Fifty accounts each show one failed login with Winter2026!	
2	A user signs in from Ohio, then Singapore 20 minutes later	
3	Web logs show GET /../../../etc/passwd	
4	Every file on the file server ends in .locked by morning	
5	DNS answers for the bank's site point to an unknown IP	
6	One victim receives huge NTP replies it never asked for	
7	The firewall log is empty from 2:00 to 2:45 a.m.	
8	A browser and server that support TLS 1.3 settle on SSL 3.0	

EXERCISE 2: MATCH EACH ATTACK TO A MITIGATION

6 MINUTES · SMALL GROUPS

For each Lakeside incident, choose the two mitigation techniques from 2.5 that would have helped most, and say why.

#	Prompt	Your answer
1	Ransomware spread from one front desk PC to the file server	
2	A former employee's VPN account was used last week	
3	A staff member ran a cracked PDF editor that held a trojan	
4	An attacker replayed a stolen session cookie on the portal	
5	A retired server in the closet still answers on the network	
6	Password spraying locked out six staff accounts on Monday	

REVIEW QUESTIONS

1. What is the difference between a reflected and an amplified DDoS attack?

2. How does password spraying differ from brute force, and which one avoids account lockout?

3. What is impossible travel?

4. Name three hardening techniques from objective 2.5.

5. How is segmentation different from isolation?

KEY TAKEAWAYS

- **Know malware by behavior.** Worms spread alone, viruses need a user, rootkits hide, trojans disguise.
- **Indicators prompt a look.** Impossible travel, lockouts, and log gaps call for investigation.
- **MFA beats password attacks.** Spraying avoids lockout; a second factor stops a guessed password.
- **Layer prevent and detect.** Pair a control that stops an attack with one that reveals it.

LAB 6: PACKET CAPTURE ANALYSIS OF AN ATTACK IN WIRESHARK

60 MINUTES

You need Wireshark on your Linux analysis VM and one attack capture your instructor assigns, from the Wireshark wiki's SampleCaptures page or a malware-traffic-analysis.net training exercise. Captures of malware traffic can contain live malware: open them only inside the isolated lab VM, never copy extracted files to your host, and never run anything you extract.

Steps

1. Take a snapshot of your analysis VM. Switch its adapter to NAT just long enough to install Wireshark (sudo apt install wireshark) and download the assigned capture, then set it back to host-only before you unzip or open anything. If it is a password-protected zip from malware-traffic-analysis.net, unzip it inside the VM only, using the password the site publishes.
2. Record the capture's hash with sha256sum capture.pcap so your report identifies exactly which file you analyzed.
3. Get the big picture in Wireshark: Statistics > Capture File Properties for the time span, Statistics > Protocol Hierarchy, and Statistics > Conversations (IPv4 tab, sorted by bytes).
4. Identify the hosts: apply the dhcp or nbns display filter to find the victim's hostname and MAC address, and note which internal and external addresses exchange the most traffic.
5. Hunt for the attack with display filters: dns for lookups, http.request for web requests, tls.handshake.extensions_server_name for HTTPS sites, and tcp.flags.syn == 1 && tcp.flags.ack == 0 for scanning.
6. Right-click a suspicious packet and choose Follow > TCP Stream or HTTP Stream to read the exchange. Note downloaded file names, user agents, and any credentials sent in clear text.
7. Build a timeline of at least five events, each with a timestamp, source, destination, and what happened, from first contact to the last suspicious connection.
8. Match your findings to the attack types and indicators in objective 2.4, and name two mitigation techniques from objective 2.5 that would have stopped or limited the attack.
9. Close Wireshark, delete the capture, and revert the VM to your snapshot.

Hand in

A lab report with the capture's file name and SHA-256 hash, screenshots of the Protocol Hierarchy, the Conversations view, and one followed stream, your timeline table, the attack and indicators you identified, and answers to the lab questions.

Questions to answer in your report

1. Which host was the victim, and what evidence in the capture identifies it?
2. What was the first sign of malicious activity, and when did it occur?
3. Which indicators from objective 2.4 appear in this capture, and which would only appear in host or authentication logs?

4. Which two mitigation techniques from objective 2.5 would have prevented or limited this attack at Lakeside Family Clinic, and why?
5. Why must this capture be analyzed only inside an isolated VM?