Cybersecurity Essentials (Undergraduate Lecture Slides)

Attacking What We Do (Module 4) + Wireless Network Communication (Module 5) with Bloom C3/C4 analytical caselets + solved problems (Washington Accord aligned)

Instructor

Department / University

December 24, 2025

What we will cover today

1. IP Services attacks and mitigations: ARP, DNS, DHCP
2. Enterprise services attacks: web attack chain, HTTP exploits, email threats, web databases, XSS
3. Operational visibility: reading logs (why logs matter)
4. Defending the network: practical mitigation playbook
5. Wireless networks: WLAN operation, threats, and securing WLANs

Learning style: we learn each topic, then solve one applied (C3) and one analytical (C4) question.

Learning outcomes (Washington Accord aligned)

By the end, students should be able to:

- Explain how local network protocols can be abused to enable man-in-the-middle attacks.
- Apply packet-level observations (ports, addresses, message types) to diagnose suspicious behavior.
- Analyze multi-stage attack narratives and identify controls that break the chain.
- Recommend mitigations that are actionable: policy, configuration, monitoring, and segmentation.
- Troubleshoot wireless association/security failures and propose secure WLAN configurations.

Module 4 goal

Module objective: Recommend measures to mitigate threats.
Core focus: IP services + enterprise services attack surfaces and how defenders reason about them.

Key instructor emphasis includes ARP vulnerabilities, DNS attacks, DHCP spoofing, web attack stages, and mitigation practice.[1]

[1] Source: Cybersecurity Essentials 3.0 Module 4 slides.

IP Services: why these protocols matter

ARP, DNS, and DHCP are foundational. They exist to make networks usable, but they were not designed with hostile LANs in mind.

That creates a practical reality:

- If an attacker can influence *who you think you are talking to*, they can intercept or reroute traffic.
- Defenders must understand normal protocol behavior to spot abnormal patterns.

ARP basics (what it does)

- ARP maps an IPv4 address to a MAC address on the local network.
- A host broadcasts an ARP request; the matching host replies with its MAC.

This is routine LAN plumbing. The problem is trust: ARP has no built-in authenticity checks.[2]

[2] ARP request/reply and broadcast nature described in Module 4 slides.

ARP vulnerability: gratuitous ARP and cache poisoning

- Any client can send an unsolicited ARP reply (gratuitous ARP).
- Hosts may store the IP/MAC pair from that unsolicited message in their ARP tables.
- A threat actor can claim ownership of an IP/MAC pair they do not actually own.

Goal in many attacks: bind the attacker MAC to the default gateway IP in victim ARP caches, placing the attacker in the path (MiTM).[3]

[3] Source: Module 4 ARP Vulnerabilities and ARP Cache Poisoning slides.

ARP cache poisoning: what passive vs active means

- **Passive ARP poisoning**: attacker intercepts and steals information.
- **Active ARP poisoning**: attacker modifies data in transit or injects malicious content.

Defender mindset: treat this as a *path manipulation* problem, not just a single packet problem.[4]

[4] Source: Module 4 ARP Cache Poisoning continuation slide.

ARP: Defender playbook (practical)

- **Switch protections**: Dynamic ARP Inspection (DAI) + DHCP snooping (where supported).
- **Segmentation**: reduce attacker reach on the same L2 segment.
- **Monitoring**: sudden ARP table changes, many gratuitous ARPs, gateway MAC flapping.
- **Endpoint hardening**: host firewalling and EDR detections for ARP spoof tools.

Think in layers: prevention + detection + response.

Caselet (ARP): “The disappearing gateway”

A small lab network has:

- Default gateway IP: `192.168.10.1`
- Multiple student PCs on the same switch

Students report:

- Internet works intermittently
- Some HTTPS sites show certificate warnings

Your job: reason like a defender.

ARP Questions (Bloom C3/C4)

C3 (Apply): A PC shows its ARP table now maps `192.168.10.1` to an unfamiliar MAC. List **three** immediate actions you would take on the PC and switch.

C4 (Analyze): Analyze the symptoms. Why do you see **intermittent** connectivity and **certificate warnings**? Provide a plausible attack flow.

ARP Solutions (worked)

C3 solution (actions):

1. On PC: clear ARP cache, re-check gateway MAC; capture ARP traffic for rapid repeats.
2. On switch: identify the port sending gratuitous ARPs; apply port shutdown/quarantine.
3. Enable/verify protections (where available): DAI + DHCP snooping; lock down unused ports.

C4 solution (analysis):

- Intermittent connectivity often happens when the attacker forwards traffic unreliably (misconfig, overload, or selective forwarding).
- Certificate warnings can occur if a MiTM tries SSL interception or breaks end-to-end integrity.
- Flow: attacker poisons victim ARP $\rightarrow$ traffic redirected $\rightarrow$ attacker relays/inspects/optionally alters $\rightarrow$ user experiences unstable paths and trust failures.

DNS: what defenders must remember

DNS translates names to records (A, AAAA, CNAME, TXT, etc.). It is also a high-value control point: if DNS lies, users go to the wrong place.

In the Module 4 material, DNS attacks are discussed in the context of open resolvers, stealth techniques, and tunneling.[5]

[5] Source: Module 4 DNS attacks and tunneling slides.

DNS open resolver and abuse

A **DNS open resolver** answers queries from clients outside its administrative domain, which makes it vulnerable to multiple malicious activities.[6]

Defensive principle:

- Recursive resolution should be restricted to authorized clients.
- Publicly exposed resolvers must be hardened and monitored.

[6] Source: Module 4 DNS Attacks slide.

Domain shadowing (DNS stealth technique)

- Threat actor steals domain account credentials.
- Creates many subdomains quietly.
- Uses them in attacks while the parent domain owner may not notice quickly.

7

[7] Source: Module 4 DNS stealth and domain shadowing note.

DNS tunneling: how it works (defender view)

DNS tunneling can be used by malware/botnets to send commands or exfiltrate data.
Mechanism described in the module:

- Data is split into encoded chunks.
- Chunks are placed into lower-level DNS query labels (often TXT queries).
- Queries pass to recursive resolvers and ultimately to attacker-controlled authoritative DNS.
- Responses carry encoded commands; malware recombines and executes.

[8]

[8] Source: Module 4 DNS Tunneling slides.

Stopping DNS tunneling: detection cues

- Use DNS inspection filters to stop tunneling attempts.
- Pay attention to queries longer than average or suspicious domains.
- Domains associated with Dynamic DNS services should be treated as high risk.

9

[9] Source: Module 4 DNS Tunneling (Cont.) slide.

Lab tie-in: Exploring DNS traffic (Wireshark)

A standard defensive workflow:

- Capture DNS packets and filter `udp.port == 53`.
- Compare query vs response: MAC/IP/ports swap direction.
- Validate DNS responses match `nslookup` results.
- Remember: packet details can reveal sensitive network information if traffic is not encrypted.

10

[10] Source: 4.1.7 Lab "Exploring DNS Traffic" (Instructor Version).

Caselet (DNS): “Strange long queries”

A campus SOC sees spikes of outbound DNS queries:

- Many queries have extremely long subdomain labels
- Repeated TXT queries to domains the university has never used
- Endpoints do not show obvious large file uploads

You suspect covert data movement.

DNS Questions (Bloom C3/C4)

C3 (Apply): Propose a **3-step** triage plan using DNS logs and packet captures to validate whether this is DNS tunneling.

C4 (Analyze): Given the module's tunneling mechanism, analyze **why** you might see (1) long labels and (2) many repeated queries with small payloads instead of one big transfer.

DNS Solutions (worked)

C3 solution (triage plan):

1. Baseline: compute typical query length, record types, and NXDOMAIN rates; flag outliers.
2. Packet confirm: capture DNS traffic; inspect TXT queries, label entropy/length, and authoritative destinations.
3. Containment: block suspicious domains at DNS security layer; isolate top-talking hosts; run endpoint investigation.

C4 solution (analysis):

- Long labels fit the "encoded chunk in subdomain" strategy.
- Many small queries reduce detection by volume-based controls and blend into normal DNS behavior.
- DNS is often allowed outbound; tunneling abuses that trusted egress path.

DHCP: what it does and why it's targeted

DHCP dynamically provides IP configuration to clients.[11]

Attackers target DHCP because it controls:

- Default gateway (where traffic goes)
- DNS server (how names resolve)
- IP assignment (who gets to communicate)

[11] Source: Module 4 DHCP slide.

DHCP spoofing / rogue DHCP server

A DHCP attack occurs when a rogue DHCP server provides false configuration to legitimate clients:

- Wrong default gateway: enables MiTM.
- Wrong DNS server: redirects users to malicious sites.
- Wrong IP settings: can create DoS for clients.

12

[12] Source: Module 4 DHCP Attacks slide.

DHCP defenses (practical)

- DHCP snooping on managed switches; trust only uplink ports.
- Port security and network access control for user ports.
- Segment critical systems; do not let arbitrary endpoints sit on the same broadcast domain.
- Monitor: sudden gateway/DNS changes across many clients.

Caselet (DHCP): “Everyone’s DNS changed”

After lunch, many PCs suddenly:

- Receive a new DNS server IP
- Start getting redirected when typing familiar sites

No firewall rule changes were made. The switch logs show a new device came online on a student port.

DHCP Questions (Bloom C3/C4)

C3 (Apply): List the configuration items you would check on a client to confirm a rogue DHCP issue.

C4 (Analyze): Analyze how **wrong DNS server** and **wrong gateway** lead to different attacker capabilities. Compare the impact.

DHCP Solutions (worked)

C3 solution: Check client:

- DHCP lease details: offered IP, gateway, DNS server, lease time.
- Compare against known-good values for that subnet.
- Identify DHCP server identifier (where available) from lease metadata or packet capture.

C4 solution:

- Wrong DNS: attacker controls name-to-IP mapping, enabling phishing and traffic steering even without full MiTM.
- Wrong gateway: attacker can become the path for all off-subnet traffic (stronger for interception/modification).
- Combined: very powerful, because attacker controls both destination selection and traffic path.

Typical web attack chain (high-level)

The module outlines a common web attack flow:

- Victim visits compromised page
- Redirected through multiple servers to malicious code
- Exploit kit scans victim software for vulnerabilities
- Downloads exploit and runs malicious code
- Victim connects to malware server and downloads payload

[13]

[13] Source: Module 4 HTTP/HTTPS "common stages of a typical web attack" slide.

Why defenders care about HTTP status codes

Server connection logs reveal clues. The module highlights categories:

- 1xx informational, 2xx success
- 3xx redirection (watch for loops)
- 4xx client error, 5xx server error

14

[14] Source: Module 4 HTTP/HTTPS (Cont.) slide on status codes.

Common HTTP exploits (defender perspective)

The module calls out:

- **Malicious iFrames**: injected into pages to load attacker-controlled content.
- **HTTP 302 cushioning**: repeated redirects until the browser lands on exploit content.

[15]

Defender hint: many attacks look like "normal browsing" unless you correlate redirection patterns and destinations.

[15] Source: Module 4 Common HTTP Exploits slide.

Domain shadowing in web attack chains

Attack sequence described:

- Compromise a parent domain account
- Create many malicious subdomains
- Use redirects (e.g., 302) to route victims through subdomains to exploit infrastructure

16

[16] Source: Module 4 Domain Shadowing slide.

Caselet (Web): “The redirect maze”

Web proxy logs show a user clicked a legitimate-looking link. Within 2 seconds, the browser hit **8 different domains**, mostly via **302 redirects**, then downloaded a file.
The user says: “I only clicked once.”

Web Questions (Bloom C3/C4)

C3 (Apply): Using only proxy logs, list the **minimum evidence** you would extract to support a suspected redirect-based attack (fields you want and why).

C4 (Analyze): Analyze how repeated 302 redirects make detection harder. What correlation strategy would you use to identify these chains at scale?

Web Solutions (worked)

C3 solution (minimum evidence):

- Timestamped URL sequence + status codes (to reconstruct chain)
- Referrer headers (to link steps)
- Destination domain/IP + reputation/age (to flag shadowed domains)
- User agent + device ID (scope and containment)
- Download indicators: content-type, file hash if available

C4 solution (analysis):

- Each hop looks "normal" alone; chain behavior is the anomaly.
- Use sessionization: group requests by user+tab time window; build redirect graphs; alert on unusually long chains, new domains, and rapid hop timing.

Email threats (what the module highlights)

Email is a major threat surface, especially HTML email across many devices. Examples include:

- Attachment-based attacks
- Email spoofing
- Spam email
- Open mail relay abuse
- Homoglyph tricks in text

17

[17] Source: Module 4 Email slides.

Email defenses (practical)

- Patch and harden SMTP infrastructure.
- Use dedicated email security controls (filtering, sandboxing, URL rewriting).
- User training: suspicious links, spoofed senders, homoglyph detection.
- Authentication: SPF/DKIM/DMARC (conceptually: prove sender domain authorization).

Caselet (Email): “The CFO request”

A finance intern receives an email:

- Sender display name matches the CFO
- Email asks for urgent payment and a “new bank account”
- Link goes to a “document” login page

No malware attachment. Just urgency and a link.

Email Questions (Bloom C3/C4)

C3 (Apply): Write a **short checklist** the intern can apply in 60 seconds before acting.

C4 (Analyze): Analyze which controls reduce this risk most: technical controls vs process controls. Justify with the attack mechanics.

Email Solutions (worked)

C3 checklist:

- Verify sender address (not just display name)
- Hover link: domain spelling, odd characters, mismatched destination
- Look for urgency/pressure language patterns
- Confirm via second channel (call known CFO number)
- Report to security mailbox; do not forward externally

C4 analysis:

- This is identity deception; process control (out-of-band verification) is extremely strong.
- Technical controls help (spoof detection, URL filtering), but attackers iterate. A mandatory verification step breaks the payoff.

Web-exposed databases: what can go wrong

Web apps commonly connect to relational databases holding sensitive data. The module highlights:

- Code injection at OS level via vulnerable web apps
- SQL injection as a common database attack

18

Defender job: recognize suspicious queries/behaviors, and reduce blast radius.

[18] Source: Module 4 Web-Exposed Databases slide.

Defending against SQL injection (safe, practical)

- Parameterized queries / prepared statements (primary control).
- Input validation and output encoding (supporting controls).
- Least-privilege DB accounts (reduce impact).
- WAF rules and anomaly detection (detect exploitation attempts).
- Monitoring: unusual query patterns, error spikes, new user agents.

Lab tie-in (safe): analyzing an SQLi capture

A lab can involve viewing PCAP traffic and following an HTTP stream to see abnormal input patterns and DB responses.[19]
In class, treat this as **forensics**: identify indicators, not how to exploit.

[19] Source: 4.2.8 Lab "Attacking a mySQL Database" (Instructor Version).

Caselet (SQLi): “Why is the DB returning extra rows?”

A web login page should return either:

- “Login failed” OR
- a single user record after success

Instead, logs show:

- Many requests returning multiple user records
- Sudden increase in 500 errors right before the weird successes

SQLi Questions (Bloom C3/C4)

C3 (Apply): List **three** log sources you would correlate to validate SQL injection suspicion.

C4 (Analyze): Analyze why you might see a burst of errors (5xx) before the attacker starts getting useful data.

SQLi Solutions (worked)

C3 solution (log sources):

- Web server access logs (URI, parameters, status codes, user agent)
- Application logs (auth failures, DB query exceptions)
- Database logs/auditing (query patterns, permission failures)

C4 solution (analysis):

- Attackers often probe inputs; malformed payloads trigger errors.
- They iterate until they discover an input pattern that changes query logic and yields valid output.
- Errors are a feedback channel; suppress detailed error messages to users, keep them in internal logs.

Client-side scripting attacks: XSS

The module describes:

- **Stored (persistent)**: malicious script stored on server; served to many visitors.
- **Reflected (non-persistent)**: script delivered via a crafted link; triggers when user clicks.

[20]

[20] Source: Module 4 Client-Side Scripting slide.

XSS defenses (practical)

- Output encoding (context-aware) is the workhorse.
- Input validation helps but is not sufficient alone.
- Content Security Policy (CSP) limits script sources and reduces impact.
- Security testing: code review, SAST/DAST, and dependency checks.

Caselet (XSS): “The comment box incident”

A course forum allows comments. Some users report:

- When viewing a specific thread, they get logged out
- Then they see posts made from their accounts that they did not create

No server breach is found. The database is intact.

XSS Questions (Bloom C3/C4)

C3 (Apply): Give **two** immediate mitigation steps you can apply quickly while a full fix is developed.

C4 (Analyze): Analyze whether this is more consistent with stored XSS or reflected XSS, and explain why based on the symptom pattern.

XSS Solutions (worked)

C3 quick mitigations:

- Temporarily disable rendering of user-supplied HTML in comments (escape everything).
- Invalidate sessions and rotate auth cookies; enable HTTPOnly/SameSite where appropriate.

C4 analysis:

- If the issue appears whenever anyone views a specific thread, it suggests the payload is stored with the content.
- Reflected XSS usually needs each victim to click a unique crafted link; stored XSS spreads via normal navigation.

Defending the network: baseline best practices

The module emphasizes best practices such as:

- Written security policy + employee education
- Physical access control
- Strong passwords and regular changes
- Encryption of sensitive data
- Firewalls, IPS, VPN, antivirus, content filtering
- Backups (and tests)
- Shut down unnecessary services/ports
- Frequent patching
- Security audits

21

[21] Source: Module 4 Defending the Network slide.

Mitigation thinking: break the attack chain

A useful mental model:

1. **Prevent** initial access (hardening, patching, training)
2. **Limit** movement (segmentation, least privilege)
3. **Detect** early (logs, anomaly alerts, endpoint telemetry)
4. **Respond** quickly (isolate, eradicate, recover)

What this really means: perfect prevention is rare; resilience is mandatory.

Caselet (Mitigation): two real-ish incident narratives

Use structured thinking: conditions → actions → controls.
Examples of incident narratives include:

- Malware introduced via infected USB media, then data exfiltration using DNS tunneling
- Third-party access leading to payment server compromise and customer data theft

22

[22] Source: 4.3.7 Lab "Recommend Threat Mitigation Measures" (Instructor Version).

Mitigation Questions (Bloom C3/C4)

C3 (Apply): For a DNS-tunneling exfiltration scenario, propose **four** controls that would have stopped or detected it earlier.

C4 (Analyze): Analyze which single control gives the best leverage if budget only allows **one** major improvement. Explain your choice.

Mitigation Solutions (worked)

C3 controls:

- Block/inspect outbound DNS; alert on long/odd queries and suspicious domains
- Patch management for servers and content management systems
- Endpoint security + removable media scanning and policy enforcement
- Network monitoring for internal scanning and abnormal DNS volumes

C4 best-leverage choice (example): Outbound DNS control is high leverage because it can detect and stop covert command/exfil channels even when endpoint compromise has already happened.

Module 5 goal

Module objective: Troubleshoot a wireless network.[23]

We focus on:

- How WLANs work (association, 802.11 frames, CSMA/CA)
- Common threats (interception, intruders, DoS, rogue AP)
- Secure configuration (WPA2/WPA3, enterprise AAA/RADIUS)

[23] Source: Module 5 objectives slide.

Wireless vs wired: what changes

Wireless is a shared medium, and clients often cannot detect collisions while transmitting. Result: WLANs use a different access method than Ethernet.

In practice: more control frames, more negotiation, and more ways an attacker can observe or disrupt the medium.

802.11 frame structure (conceptual)

802.11 frames have header + payload + FCS, similar to Ethernet, but with more fields:

- Frame control, duration
- Multiple address fields (receiver, transmitter, distribution)
- Sequence control, optional address4 (ad hoc)

24

[24] Source: Module 5 802.11 Frame Structure slide.

CSMA/CA: how Wi-Fi avoids collisions

Workflow described in the module:

1. Listen to channel (carrier sense)
2. Send RTS to request access
3. Receive CTS granting access (or wait random time and retry)
4. Transmit data
5. Expect acknowledgments; if missing, assume collision and retry

25

[25] Source: Module 5 CSMA/CA slide.

Client association: 3-stage process

Wireless devices typically:

1. Discover an AP
2. Authenticate with AP
3. Associate with AP

Parameters must match (SSID, password, security mode, channel, standard).[26]

[26] Source: Module 5 Wireless Client and AP Association slides.

Discovery: passive vs active scanning

- **Passive**: AP sends beacon frames advertising SSID and capabilities.
- **Active**: client sends probe requests; AP responds if SSID matches.

27

[27] Source: Module 5 Passive and Active Discovery Mode slide.

AP management: autonomous vs controller-based

- Autonomous APs: configured individually.
- WLC model: central management; APs become lightweight (LWAPs) forwarding to controller.

28

[28] Source: Module 5 AP/LWAP/WLC slide.

Caselet (WLAN ops): “It connects, but no internet”

A student connects to campus Wi-Fi:

- Wi-Fi shows “Connected”
- No websites load
- Another student nearby works fine

WLAN Ops Questions (Bloom C3/C4)

C3 (Apply): Map the likely fault to one of the three association stages (discover/authenticate/associate) or post-association (IP/DNS). Explain the quickest check for each.

C4 (Analyze): Analyze two different root causes that would produce the same symptom, and show how you would distinguish them using observations.

WLAN Ops Solutions (worked)

C3 mapping/checks:

- Discover: can the SSID be seen? signal strength ok?
- Authenticate: does it ask for credentials and accept them?
- Associate: does it get an IP? check DHCP lease + gateway + DNS
- Post-association: ping gateway, test DNS resolution

C4 analysis:

- Cause A: DHCP failure (connected to Wi-Fi but no valid IP). Distinguish: IP is self-assigned / missing gateway.
- Cause B: DNS misconfiguration (IP works, names fail). Distinguish: ping IP works, but name lookup fails.

Wireless threat surface

Wireless networks are susceptible to:

- Interception of data (if not encrypted)
- Wireless intruders (unauthorized access)
- DoS attacks (malicious or accidental interference)
- Rogue APs (unauthorized APs attached to a corporate network)

[29]

[29] Source: Module 5 Wireless Security Overview slide.

DoS in WLANs (three common causes)

Wireless DoS can come from:

- Improper configuration errors
- Malicious interference
- Accidental interference (e.g., other devices; 2.4 GHz is more prone than 5 GHz)

30

[30] Source: Module 5 DoS Attacks slide.

Rogue APs and evil twins (MiTM pattern)

- **Rogue AP**: unauthorized AP connected to corporate network.
- **Evil twin**: rogue AP configured with the same SSID as a legitimate AP to lure clients.
- Clients often choose stronger signal; traffic can be captured and forwarded.

31

[31] Source: Module 5 Rogue APs and Man-in-the-Middle Attack slides.

Caselet (WLAN threats): “The coffee shop SSID”

Students connect to “CampusWiFi” at a cafe near campus. Some get:

- Very fast connection but repeated login prompts
- Occasional pop-ups asking to “install a certificate”

On campus, the same SSID works normally.

WLAN Threat Questions (Bloom C3/C4)

C3 (Apply): List **five** indicators a user or helpdesk can check to suspect an evil twin / rogue AP situation.

C4 (Analyze): Analyze why "strong signal" can be a trap. How should enterprise WLAN design and monitoring reduce this risk?

WLAN Threat Solutions (worked)

C3 indicators:

- Unexpected certificate install requests
- Repeated captive portal prompts for known SSID
- Different security mode than expected (open vs WPA2-Enterprise)
- BSSID/AP MAC differs from known campus APs (if visible)
- Location anomaly: works on campus, fails nearby with same SSID

C4 analysis:

- Clients often auto-select strongest signal; attackers exploit proximity/power.
- Enterprise mitigation: use WPA2/3-Enterprise (802.1X), certificate validation, WLC rogue AP detection policies, and spectrum monitoring.[32]

[32] Module 5 recommends rogue AP detection via management software/policies.

Early controls: SSID cloaking and MAC filtering

The module notes two early security features still seen today:

- SSID cloaking (disable SSID beacon)
- MAC address filtering (allow/deny based on MAC)

These are not strong by themselves: SSIDs can be discovered and MACs can be spoofed.[33]

[33] Source: Module 5 Secure WLANs slides on SSID cloaking and MAC filtering.

Authentication and encryption: the real security

The best way to secure a WLAN is proper authentication + encryption:

- Prefer WPA2 (AES/CCMP) or WPA3 where available
- Avoid weak/legacy modes

34

[34] Source: Module 5 encryption methods slide.

Home vs Enterprise authentication

- **WPA2-Personal**: pre-shared key (PSK) for home/small office
- **WPA2-Enterprise**: uses AAA with a RADIUS server (802.1X/EAP)

[35]

[35] Source: Module 5 “Authenticating a Home User” slide.

AAA and RADIUS (what you must know)

Enterprise WLAN typically uses a RADIUS server for:

- Authentication and Accounting ports (commonly UDP 1812/1813)
- Shared secret between AP and RADIUS
- Per-user authentication via 802.1X/EAP

36

[36] Source: Module 5 Authentication in the Enterprise slide.

WPA3 note

The module notes:

- WPA3 is recommended if available
- WPA2 is no longer considered secure

37

[37] Source: Module 5 WPA3 slide.

Caselet (Secure WLAN): “Dorm network redesign”

A dorm WLAN currently uses:

- One shared WPA2-Personal password for 500 students
- Password leaks every semester

The university wants better control and auditability.

Secure WLAN Questions (Bloom C3/C4)

C3 (Apply): Propose a target configuration using Enterprise authentication. List the minimum components needed.

C4 (Analyze): Analyze the risk difference between WPA2-Personal (shared PSK) and WPA2-Enterprise (per-user auth). Focus on accountability and blast radius.

Secure WLAN Solutions (worked)

C3 solution (target config):

- WPA2-Enterprise or WPA3-Enterprise SSID
- RADIUS/AAA server integrated with university identity (directory)
- 802.1X/EAP profiles for clients, with certificate validation
- WLC policies for rogue AP detection and consistent configuration

C4 analysis:

- Shared PSK: one leak compromises everyone; no per-user accountability; difficult offboarding.
- Enterprise: per-user credentials, better logging/accounting, smaller blast radius, faster revocation.

Hands-on reinforcement (safe labs/activities)

Suggested practice activities include:

- Configuring basic wireless security (WPA2-Personal) and verifying connectivity
- Troubleshooting a wireless connection by correcting misconfigurations

38

[38] Source: Module 5 Packet Tracer activity slides.

Exam-style integrated problem (C3 + C4)

A medium office reports:

- Users sometimes get redirected to fake login pages
- DNS logs show long TXT queries to unknown domains
- Wi-Fi network has multiple APs and one was recently added by a staff member

You must produce: (1) immediate response plan, (2) root cause analysis hypothesis, (3) longer-term controls.

Integrated Solution (Step-by-step)

1) Immediate response (containment):

- Block suspicious DNS domains and inspect outbound DNS for tunneling patterns (long queries).
- Identify top clients generating those queries; isolate them for endpoint inspection.
- Disable/locate unauthorized AP; verify SSID/security mode consistency across APs.

2) Root cause hypothesis (analysis):

- Rogue AP/even an evil twin can enable credential interception.
- Compromised hosts can use DNS tunneling for command/exfiltration, which matches long TXT queries.

3) Long-term controls:

- WPA2/3-Enterprise with 802.1X + RADIUS, strong rogue AP monitoring via WLC.
- DNS security controls + logging baselines, and strict patching + least privilege.
- User training for phishing and certificate prompts.

Quick recap

- ARP, DNS, DHCP are powerful because they control *identity and routing* inside a LAN.
- Enterprise attacks often look like normal traffic unless you correlate stages and logs.
- WLANs add new risks: shared medium, rogue APs, and association weaknesses.
- Best outcomes come from layered controls: hardening + monitoring + response readiness.

End

Questions?