Cybersecurity Essentials (Modules 1–3)

Threats & Attacks — Securing Networks — Attacking the Foundation (TCP/IP)

Instructor Name

Undergraduate Lecture

December 24, 2025

How this lecture works

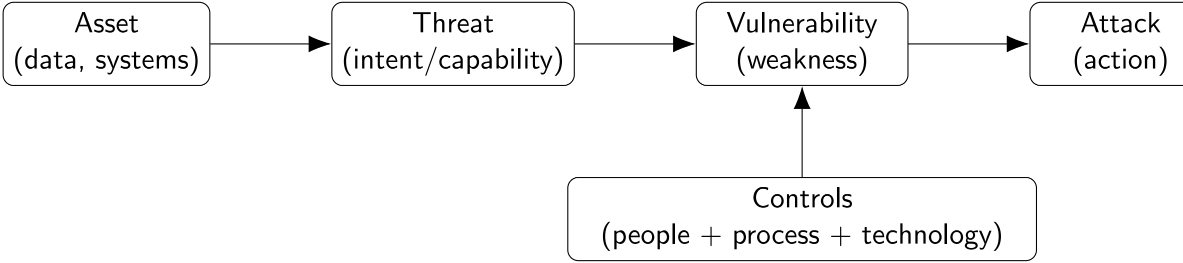
- We build a mental model first: **assets** → **threats** → **vulnerabilities** → **attacks** → **controls**.
- Each module ends with: quick check, mini-scenarios, and what to remember for exams.
- Goal: you should be able to **explain** an attack, **recognize** it in a scenario, and **suggest** defenses.

Module 1 objectives

By the end of this module, you should be able to:

- Explain what a **threat domain** is and why it matters.
- Distinguish **internal vs external** threats.
- Describe common **deception (social engineering)** techniques.
- Describe common **malware** and **attack** categories and defenses.

Core model: asset → threat → vulnerability → attack



Key idea: attackers don't "break security" directly; they exploit **weaknesses**.

Threat domains (where attackers can enter)

A **threat domain** is an area of control, authority, or protection attackers can exploit. Examples:

- Physical access to systems
- Wireless beyond boundaries (Wi-Fi)
- Bluetooth / NFC devices
- Email attachments / links
- Supply chain weaknesses
- Social media accounts
- Removable media (USB drives)
- Cloud-based apps (SaaS/PaaS/IaaS)

Internal vs external threats

Internal threats

- Current/former employees, contractors
- Accidental (mistakes) or intentional (malice)
- Often high-impact: already inside

External threats

- Amateur to skilled attackers
- Exploit vulnerabilities or use deception
- Often at scale (phishing, scanning)

Exam cue: always mention **motive + access level + typical impact**.

User threats: why people are the easiest target

Users are often the weakest link affecting **confidentiality, integrity, availability (CIA)**.

- No security awareness / policy violations
- Weak policy enforcement
- Data theft / unauthorized downloads
- Risky browsing, VPN misuse, unsafe installs
- Destruction of systems/applications/data

Threats to devices and networks (examples)

Devices

- Unattended logged-in machines
- Vulnerable/outdated software
- Untrusted downloads; infected removable media
- Lack of IT policies

Local Area Network (LAN)

- Unauthorized access to wiring closets / servers
- Misconfigured firewalls; port scanning
- Data-in-transit exploitation (sniffing/MitM)
- Rogue wireless access

Cloud threats (private vs public)

Private cloud (single organization): unauthorized access, probing/scanning, device vulnerabilities, config errors, remote data exfiltration.

Public cloud (shared provider): understand service models:

- **SaaS**: use software hosted by provider
- **PaaS**: build/run apps on provider platform
- **IaaS**: rent compute/storage/network resources

Exam cue: tie each model to who manages what (customer vs provider).

Threat complexity: beyond simple malware

Software vulnerabilities happen due to:

- Programming mistakes
- Protocol weaknesses
- Misconfiguration

Two advanced examples:

- **APT**: long-running, stealthy, multi-step intrusion
- **Algorithm attacks**: exploit unintended behavior from legitimate algorithms

Backdoors and rootkits

Backdoor

- Bypasses authentication to give unauthorized access
- Often installed via a **RAT** (remote administrative tool) on a victim machine

Rootkit

- Modifies the OS to hide attacker presence + create backdoor
- Often uses **privilege escalation** to access restricted resources

Threat intelligence basics (what defenders watch)

Common concepts:

- **CVE**: standardized vulnerability identifiers
- **IOC**: evidence of compromise (hashes, domains, IPs, filenames)
- **AIS / STIX / TAXII**: structured, automated sharing of indicators
- **Dark web**: markets/forums not indexed by normal search

Why it matters: defense improves when organizations share signals early.

Social engineering (deception) definition

Social engineering is a non-technical strategy that manipulates people into actions or revealing confidential info.

- **Pretexting**: lying to gain access to data
- **Quid pro quo**: exchange something for personal info
- **Identity fraud**: using stolen identity to obtain goods/services

Social engineering tactics (why it works)

Attackers exploit human shortcuts:

- Authority
- Intimidation
- Consensus (everyone is doing it)
- Scarcity (limited time/stock)
- Urgency (act now)
- Familiarity
- Trust

Exam cue: pick 2–3 tactics and show how they appear in a real message/call.

Physical-world deception: shoulder surfing and dumpster diving

Shoulder surfing

- Observing PINs, codes, card details (even via cameras/binoculars)

Dumpster diving

- Searching trash for sensitive info
- Mitigation: shredding, burn bags, secure disposal process

Piggybacking, tailgating, and mantraps

Piggybacking/tailgating: attacker follows an authorized person into restricted areas.

Common methods:

- Pretend escort / blend into a crowd
- Target careless employees

Defense: **mantrap** (two-door system; one must close before the next opens).

Defending against deception (high-yield points)

Practical habits:

- Never disclose credentials via email/chat/phone to unknown parties
- Avoid clicking enticing links; verify sender and URL
- Beware auto-downloads and unexpected attachments
- Train employees; enforce clear policies
- Encourage reporting without blame
- Don't give in to pressure tactics

Malware: the big three

- **Virus**: attaches to files/programs; replicates when executed
- **Worm**: self-replicates by exploiting network vulnerabilities
- **Trojan**: looks legitimate, performs hidden malicious actions

Exam cue: define each in one line + a differentiator (attachment vs self-spread vs disguise).

Ransomware

- Encrypts data and demands payment for decryption/unlock
- Often spreads via phishing attachments or unpatched software
- Paying doesn't guarantee recovery

Defenses (conceptual):

- Patch management
- Backups (offline/immutable)
- Email filtering + user training

Denial of Service (DoS) vs Distributed DoS (DDoS)

DoS: overwhelms a target so legitimate users can't access services.

Two common approaches:

- **Volume flood**: too much traffic to handle
- **Malformed packets**: trigger crashes or resource exhaustion

DDoS: same idea, but traffic comes from many sources (harder to block).

Application attacks: XSS, injection, buffer overflow, RCE

XSS

- Attacker injects scripts; victim's browser runs them
- Can steal cookies/session tokens and impersonate users

Injection (SQL/XML/etc.)

- Exploits weak input handling in databases/parsers

Buffer overflow / RCE

- Writes beyond memory bounds; may crash or enable code execution

Email and browser attacks: spam and phishing

Spam: unsolicited bulk email; may include malicious links/attachments.
Phishing: pretending to be legitimate to steal info or install malware.

- **Spear phishing**: targeted, personalized
- **Vishing**: voice-based
- **Pharming**: redirecting to fake websites
- **Whaling**: targets high-profile individuals

Module 1 quick check (write 1–2 lines each)

1. Define **threat domain** and give two examples.
2. One internal threat example and one external threat example.
3. Name two social engineering tactics and how they show up.
4. Differentiate virus vs worm vs trojan.
5. Give two defenses against ransomware.

Module 2 objectives

By the end, you should be able to:

- Explain why network security ties directly to **business continuity**.
- Define **attack vector** and give examples.
- Distinguish hacker vs threat actor; describe common threat actor types.
- Explain **threat indicators** (IOC vs IOA) and why sharing matters.

Why network security matters (business impact)

Network breaches can:

- Disrupt e-commerce and operations
- Cause data loss (customer, financial, IP)
- Harm privacy and trust
- Trigger lawsuits and regulatory action
- In some contexts, threaten public safety

Exam cue: always link technical failure → business consequence.

Attack vectors (paths into the network)

An **attack vector** is the path a threat actor uses to access a host/server/network.

- Inside: careless or malicious employee, infected USB, misconfig changes
- Outside: phishing, scanning/exploitation, credential stuffing, DDoS

Threat, vulnerability, and risk (keep them distinct)

- **Threat**: something capable of causing harm (actor/event)
- **Vulnerability**: weakness that can be exploited
- **Risk**: likelihood × impact of exploitation

Risk decisions often fall into four buckets:

- Avoid, Reduce/Mitigate, Transfer, Accept

Hacker vs threat actor (language matters)

“Hacker” can mean:

- Skilled programmer/optimizer
- Security professional (ethical testing)
- Person attempting unauthorized access

Threat actor is clearer: anyone who can conduct attacks (criminal, insider, state, etc.).

White hat, grey hat, black hat

White hat

- Legal/ethical testing
- Finds vulnerabilities to fix them

Grey hat

- May break rules/laws
- Not always for direct gain

Black hat

- Malicious + illegal
- Profit, disruption, espionage

Threat actors you should recognize

Examples (high-level):

- Script kiddies
- Vulnerability brokers
- Hacktivists
- Cybercriminal groups
- State-sponsored actors

Exam cue: map each to motivation (fun, money, ideology, intelligence).

Indicators: IOC vs IOA

Indicator of Compromise (IOC): evidence something already happened (hashes, domains, IPs).
Indicator of Attack (IOA): behavior suggesting an attack strategy (lateral movement pattern, repeated login failures).

Why IOA matters: helps you defend against the **strategy**, not just the one sample.

Why sharing matters (AIS example)

Organizations reduce harm when they share indicators early.

- Faster detection for everyone
- Better blocking and hunting
- Builds shared awareness across users and teams

Module 2 quick check

1. Explain business continuity in one sentence.
2. Define attack vector and give two examples.
3. Threat vs vulnerability vs risk (one line each).
4. IOC vs IOA: what's the difference?

Module 3 objectives

By the end, you should be able to:

- Explain why IP is **connectionless** and what that implies for security.
- Identify key fields in IPv4/IPv6 headers (conceptually).
- Explain ICMP abuse (recon + DoS).
- Explain spoofing, amplification/reflection, and transport-layer attacks (TCP/UDP).

IP at Layer 3: the security takeaway

IP is designed for **delivery**, not trust:

- Connectionless: does not manage flow or reliability (TCP often does)
- Does not verify the source IP truly belongs to the sender
- Attackers can spoof source IP and manipulate header fields

IPv4 vs IPv6 (big picture)

- IPv4 header: more fields, widely used, common in legacy networks
- IPv6 header: fewer base header fields; uses extension headers

You don't need to memorize every bit, but you must explain how attackers leverage headers.

ICMP: what it is and how it is abused

ICMP provides diagnostics and error messages.

- **Ping** uses ICMP echo request/reply to test reachability

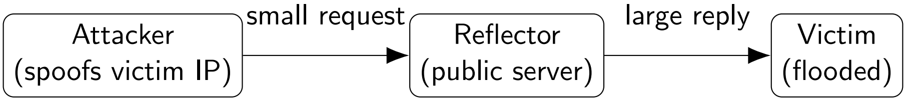
Threat actor uses:

- Recon/scanning: map topology, find live hosts, fingerprint OS, test firewall behavior
- Flooding: DoS/DDoS (ICMP flood)

Amplification and reflection (idea)

Attackers try to:

- Send small requests that trigger much larger replies (amplification)
- Trick third-party systems into replying to the victim (reflection)



Address spoofing: non-blind vs blind

IP spoofing: forging source IP to hide identity or impersonate.

- **Non-blind spoofing**: attacker can see traffic; can help session hijacking
- **Blind spoofing**: attacker cannot see traffic; often used for DoS-style attacks

Also common internally: **MAC spoofing** (pretend to be another device on LAN).

TCP services (why TCP is different)

TCP provides:

- Reliable delivery (ACK + retransmission)
- Flow control
- Stateful communication (3-way handshake)

Trade-off: reliability can add delay and overhead.

TCP SYN flood (classic resource exhaustion)

Exploit: TCP three-way handshake.

1. Attacker sends many SYNs (often with spoofed IPs)
2. Target replies SYN-ACK and waits for ACK
3. ACK never arrives → many half-open connections
4. Legitimate users get denied (resources exhausted)

TCP reset and session hijacking (conceptual)

TCP reset attack

- Inject a segment with RST flag to tear down a connection

TCP session hijacking

- Take over an authenticated session by spoofing IP + predicting sequence numbers
- Can send data as victim; receiving data may be limited depending on position

UDP: lightweight and common, but easy to abuse

UDP is connectionless and low-overhead (used by DNS, DHCP, SNMP, streaming/VoIP).

- No built-in reliability like TCP
- Encryption is not inherent by default
- Checksum can be optional in some contexts; attackers may tamper and recompute

UDP flood (what happens)

- Attacker floods UDP packets to many ports
- Closed ports trigger ICMP “port unreachable” replies
- Bandwidth and host resources get consumed → DoS-like outcome

Defenses (high level, exam-friendly)

For network-layer and transport-layer attacks:

- Keep patches current; reduce known vulnerabilities
- Harden configurations (firewalls, rate limiting, ICMP policies)
- Monitor for abnormal traffic patterns (baseline → anomaly)
- Segment networks; reduce blast radius
- Use redundancy and load distribution for resilience

Module 3 quick check

1. Why is IP spoofing possible?
2. How can ICMP be used for recon?
3. Explain SYN flood in 4 steps.
4. Why is UDP attractive for attackers?

How to answer scenario questions (template)

When given an incident/scenario, write in this order:

1. **Identify**: attack type (and where it happens: user, app, network, transport).
2. **Mechanism**: 3–5 steps of how the attack works.
3. **Impact**: CIA (confidentiality/integrity/availability) + business consequence.
4. **Controls**: prevention + detection + response (at least 2 each if possible).

One-slide recap (what to memorize)

- Threat domain, internal vs external threats, CIA triad.
- Social engineering types + tactics + defenses.
- Malware: virus vs worm vs trojan; ransomware basics.
- Attack vector, risk vocabulary, threat actors, IOC vs IOA.
- IP is connectionless and spoofable; ICMP abuse; SYN flood; UDP flood.

References (course decks)

- Cybersecurity Essentials 3.0 Instructor Materials, Module 1: Cybersecurity Threats, Vulnerabilities, and Attacks. :contentReference[oaicite:3]index=3
- Cybersecurity Essentials 3.0 Instructor Materials, Module 2: Securing Networks. :contentReference[oaicite:4]index=4
- Cybersecurity Essentials 3.0 Instructor Materials, Module 3: Attacking the Foundation. :contentReference[oaicite:5]index=5

Case Study (M1): Threat Domains & Internal vs External Threats

Scenario (Campus Lab):
A university computer lab has shared logins for “quick access”. Students often plug in USB drives to print. The lab Wi-Fi password is posted on the wall. One evening, several PCs start showing pop-ups and files disappear from a shared folder. The next day, the same lab account is used to access the department’s cloud storage from an off-campus IP.

C3 (Apply):

- Identify **3 threat domains** present (e.g., physical, removable media, wireless, cloud) and **1 control** for each.
- Classify the likely threats as **internal, external, or both** and justify in 2 lines.

C4 (Analyze):

- Draw an **attack chain** (entry → privilege → action on objectives) and mark where detection would be easiest.
- Which single weakness is the **highest leverage fix** and why (impact + likelihood)?

Case Study (M1): Social Engineering (Deception)

Scenario (Finance Office Email):
An email claims to be from the university IT Helpdesk: “Mailbox storage exceeded. Click to re-validate or your account will be disabled in 2 hours.” The link goes to a page that looks identical to the real login portal. A staff member logs in. Within minutes, that staff member’s account sends similar emails to all contacts.

C3 (Apply):

- List **4 red flags** in the message and write **the correct response procedure** (steps).
- Rewrite the message into a **safe internal alert** that IT could send legitimately.

C4 (Analyze):

- Identify the **social engineering principles** used (authority, urgency, scarcity, etc.) and explain how each pushes behavior.
- Propose a **layered defense** (people + process + tech): minimum **2 controls per layer**.

Case Study (M1): Malware & Ransomware

Scenario (Small Business):

A small company receives an invoice spreadsheet. After opening it, the user notices the system becomes slow, then files start changing extensions, and a note appears demanding payment. The shared drive is also affected. Backups exist but are stored on a permanently connected external drive.

C3 (Apply):

- Classify the malware behavior and list **immediate incident-response actions** in order (first 5 actions).
- Recommend a **backup strategy** that would reduce damage next time (give 3 concrete rules).

C4 (Analyze):

- Explain **why the connected backup failed as a protection** and how the attacker likely reached it.
- Build a short **risk table** (3 risks, likelihood, impact, mitigation) focusing on ransomware pathways.

Case Study (M1): DoS/DDoS

Scenario (Online Booking Site):
A flight-training school's booking website becomes unreachable during peak enrollment. Monitoring shows traffic spikes from thousands of IPs. The database is healthy, but the web server CPU is maxed, and inbound bandwidth is saturated.

C3 (Apply):

- Decide if this is more consistent with **DoS or DDoS** and state the evidence.
- List **4 mitigation actions** the team can apply quickly (technical + operational).

C4 (Analyze):

- Separate symptoms into **volume** vs **application-layer** attack indicators.
- Propose an **architecture-level improvement** that increases resilience (explain how it changes the bottleneck).

Case Study (M1): Web/Application Attacks (XSS & Injection)

Scenario (Student Portal):
Students report that after viewing a forum post, their accounts randomly log out and their profiles show changes they did not make. Logs show many requests with unusual parameters in URL query strings, and multiple failed database queries.

C3 (Apply):

- Choose the **most likely attack type(s)** (XSS, SQL injection, session hijack) and justify using the symptoms.
- List **3 secure coding fixes** and **2 immediate compensating controls**.

C4 (Analyze):

- Explain the **difference between data theft vs session theft** in this scenario and what evidence would confirm each.
- Design a simple **test plan** to verify the fix (inputs, expected outputs, and logging).

Case Study (M2): Attack Vectors & Risk

Scenario (Branch Office Network):
A branch office uses default router settings and has remote management enabled. Staff reuse passwords across systems. One morning, VPN access logs show repeated login attempts, then a successful login from a new location. Soon, internal file shares are scanned.

C3 (Apply):

- Identify **two attack vectors** used and propose **one immediate hardening step** for each.
- Calculate and explain **risk ranking** for three assets (e.g., file server, email, VPN) using likelihood × impact (qualitative is fine).

C4 (Analyze):

- Infer the attacker's **goal** (data theft, persistence, disruption) from the behavior and justify.
- Recommend a **risk treatment plan** (avoid/reduce/transfer/accept) for each of the three risks.

Case Study (M2): Threat Actors & Motivation

Scenario (Public Leak + Defacement):
A company website is defaced with a political message. Customer data is later posted online. The attacker claims it was "for the people", but the leaked database includes payment records and personal identifiers.

C3 (Apply):

- Classify the likely threat actor category (hacktivist, cybercriminal, etc.) and give **2 reasons**.
- List **3 controls** that reduce defacement risk and **3 controls** that reduce data exfiltration risk.

C4 (Analyze):

- Argue whether this is **mixed-motive** (ideology + profit) using the evidence.
- Propose **two competing hypotheses** and what logs/evidence would confirm each.

Case Study (M2): IOC vs IOA (Detection Thinking)

Scenario (Security Operations):
Your SIEM flags a known malicious file hash on one laptop (IOC). Separately, you see a pattern: multiple hosts attempt lateral movement using remote admin tools and repeated authentication failures across departments (IOA).

C3 (Apply):

- Write **2 IOC-based** detection rules and **2 IOA-based** detection rules (plain English is fine).
- Prioritize response: which alert do you handle first and why?

C4 (Analyze):

- Explain how attackers can **evade IOC-only** defenses and why IOA can still catch them.
- Propose a **sharing plan**: what to share (fields), with whom, and what to avoid sharing (privacy/overexposure).

Case Study (M3): IP Spoofing & ICMP Abuse

Scenario (Network Discovery):
A network admin notices many ICMP echo requests across multiple subnets at unusual times. Some packets have unusual TTL values and inconsistent source IP patterns. Soon after, there are targeted connection attempts to a few critical servers.

C3 (Apply):

- Identify **two reconnaissance goals** the attacker may have and map them to the ICMP behavior.
- Propose **3 firewall/ACL policy changes** that reduce recon while maintaining diagnostics where needed.

C4 (Analyze):

- Explain why **spoofing is feasible at Layer 3** and what network features make it harder.
- Design a **detection strategy** using baselines (what normal looks like vs abnormal).

Case Study (M3): Amplification & Reflection

Scenario (Sudden Bandwidth Saturation):
A victim network experiences inbound traffic far larger than outbound. Logs show responses from many public servers that the victim never contacted. The inbound packets are valid replies to requests the victim did not send.

C3 (Apply):

- Explain how **reflection** works in 4 steps, using this case.
- Suggest **2 upstream** and **2 local** mitigations (ISP/CDN vs on-prem).

C4 (Analyze):

- Identify what evidence indicates **spoofed source IP** was used.
- Evaluate the trade-off between **blocking** and **availability** (what might you accidentally break?).

Case Study (M3): TCP SYN Flood

Scenario (Web API Outage):
An API becomes slow, then stops accepting connections. Packet captures show a high rate of SYN packets with few completed handshakes. The server's connection table fills, and CPU usage increases due to connection tracking.

C3 (Apply):

- Describe the **SYN flood mechanism** and propose **3 technical mitigations**.
- Propose a **monitoring dashboard** (3 metrics) that would catch this early.

C4 (Analyze):

- Distinguish between a SYN flood and a genuine traffic spike using **handshake completion rate** evidence.
- Analyze how mitigations shift the bottleneck (server → firewall → upstream).

Case Study (M3): UDP Flood

Scenario (VoIP Degradation):
During business hours, VoIP calls become choppy. Network monitoring shows heavy UDP traffic across many ports. Many ICMP "port unreachable" messages appear, and edge router CPU spikes.

C3 (Apply):

- Explain why UDP floods can create ICMP storms and **two immediate mitigations**.
- Propose a **QoS approach** to protect VoIP during the incident.

C4 (Analyze):

- Identify which symptoms suggest **resource exhaustion at router** vs at end hosts.
- Recommend a longer-term design change that improves resilience without harming legitimate UDP apps.

Case Study (M3): TCP Reset & Session Hijacking (Conceptual)

Scenario (Remote Admin Session Drops):
A remote admin session repeatedly disconnects. Wireshark shows RST packets arriving unexpectedly. Separately, another user reports that after logging in, actions appear in their account that they did not perform, while their password remains unchanged.

C3 (Apply):

- Match the symptoms to likely causes: **RST injection** vs **session hijack**.
- List **3 protections** that reduce session hijacking risk in web apps.

C4 (Analyze):

- Propose **evidence** that distinguishes hijacking from stolen credentials (cookies/tokens vs password login logs).
- Analyze how encrypted transport (e.g., TLS) changes feasibility of RST injection and hijacking attempts.

Solution (M1): Threat Domains & Internal/External Threats

C3 – Apply

Threat domains and controls

- Physical domain: unattended lab PCs
  Control: automatic screen lock, individual user accounts
- Removable media domain: infected USB drives
  Control: disable autorun, USB scanning and device control
- Wireless domain: exposed Wi-Fi password
  Control: WPA2/WPA3 Enterprise or frequent password rotation
- Cloud access domain: off-campus login misuse
  Control: multi-factor authentication and geo-login alerts

Threat classification

- Internal: students using shared credentials and USB devices
- External: attacker accessing cloud storage from off-campus IP
- Overall: combined internal–external threat chain

C4 – Analyze

Solution (M1): Social Engineering

C3 – Apply

Red flags

- Urgent deadline ("2 hours")
- Generic sender identity
- Suspicious URL
- Credential request via email

Correct response

1. Do not click the link
2. Report email to IT security
3. Verify via official IT portal
4. Change password if credentials entered
5. Scan device for malware

C4 – Analyze

Principles exploited

- Authority, urgency, fear, trust

Solution (M1): Malware & Ransomware

C3 – Apply

Malware type: ransomware (file encryption + payment demand)

Immediate response

1. Isolate infected system
2. Disconnect shared drives
3. Notify security team
4. Preserve evidence
5. Scan other endpoints

Backup strategy

- Offline or immutable backups
- 3-2-1 rule
- Regular restore testing

C4 – Analyze

Why backup failed: permanently connected backup was encrypted like normal storage.

Risk analysis

Solution (M1): DoS / DDoS

C3 – Apply

Attack type: DDoS (traffic from many IPs)

Immediate mitigations

- Rate limiting
- CDN/WAF activation
- Traffic filtering
- Load balancing

C4 – Analyze

Indicators

- Volume-based: bandwidth saturation
- Application-layer: high CPU with normal bandwidth

Improvement: upstream traffic absorption using CDN shifts bottleneck away from origin server.

Solution (M2): Attack Vectors & Risk

C3 – Apply

Attack vectors

- Exposed remote management
- Password reuse on VPN

Hardening

- Disable public remote admin
- Enforce MFA and strong passwords

Risk ranking

- VPN – high
- File server – high
- Email – high

C4 – Analyze

Attacker goal: lateral movement and data discovery.

Risk treatment

- VPN: reduce

Solution (M3): TCP SYN Flood

C3 – Apply

Mechanism

1. Large number of SYN packets sent
2. Server replies with SYN-ACK
3. ACK not returned
4. Connection table fills

Mitigations

- SYN cookies
- Rate limiting
- Upstream DDoS protection

C4 – Analyze

Detection

- High SYN-to-ACK ratio
- Many half-open connections

Effect of controls: shifts load from server to firewall or ISP-level defenses.