Implement and Explain Advanced Cybersecurity Defense Strategies

1. Application of Zero Trust Architecture

To enforce Zero Trust Architecture, access controls were applied across the following two security layers:

Network Layer

- Implemented network segmentation using VLANs and firewalls with strict Access Control Lists (ACLs).
- Deployed Intrusion Detection and Prevention Systems (IDPS) to monitor and block unauthorized traffic.
- Established a VPN with strict authentication to ensure encrypted remote access.

Data Layer

- Enforced encryption for sensitive data at rest and in transit.
- Implemented Data Loss Prevention (DLP) controls to prevent unauthorized data exfiltration.
- Applied strict access control and classification policies to regulate data access and handling.

.

---

2. Defense in Depth Implementation

Three distinct layers of security were implemented to establish a Defense in Depth strategy:

Perimeter Security

- Firewalls were configured to filter incoming and outgoing traffic based on predefined rules.
- Deployed Intrusion Detection Systems (IDS) to identify and respond to malicious activities.
- VPN implementation to secure remote connections and prevent unauthorized network access.

Endpoint Security

- Installed Endpoint Detection and Response (EDR) tools to monitor and mitigate threats.
- Enforced device authentication and policy-based access controls.
- Regular security patching and system hardening to reduce vulnerabilities.

Application Security

- Deployed Web Application Firewalls (WAF) to prevent SQL injection and XSS attacks.
- Conducted secure code reviews and vulnerability assessments.
- Implemented input validation and output encoding to prevent common web-based attacks.

---

3. Supply Chain Security

Example of Risk Identification & Mitigation

Risk Identified: A third-party software dependency introduced a critical vulnerability that could be exploited remotely.

Mitigation Strategy:

- Implemented a Software Bill of Materials (SBOM) to track all dependencies and their security status.
- Conducted vendor security assessments before integrating third-party software.
- Established a regular patch management process to ensure timely updates and vulnerability fixes.

---

4. Advanced Security Model: Clark-Wilson Model

Application to Secure a System

The Clark-Wilson model was applied to enforce integrity constraints within a database system.

- **Well-formed Transactions:** Ensured data modification could only occur through controlled procedures (e.g., using stored procedures and application-layer controls).
- **Separation of Duties:** Restricted direct database access and implemented a layered approval process for changes.

- **Integrity Verification:** Regular audit logs and integrity checks to ensure compliance with security policies

Implement Incident Response and Handling

Incident Response Plan

Preparation

- Establish security policies and response procedures.
- Ensure staff is trained in incident handling.
- Maintain updated backups and security tools.

Identification

- Monitor logs and alerts for anomalies.
- Use IDS/IPS to detect suspicious activities.
- Confirm and classify the incident type.

Containment

- Isolate affected systems to prevent spread.
- Disable compromised accounts.
- Apply temporary security controls.

Eradication

- Remove malicious files or unauthorized access.
- Patch vulnerabilities.
- Perform forensic analysis.

Recovery

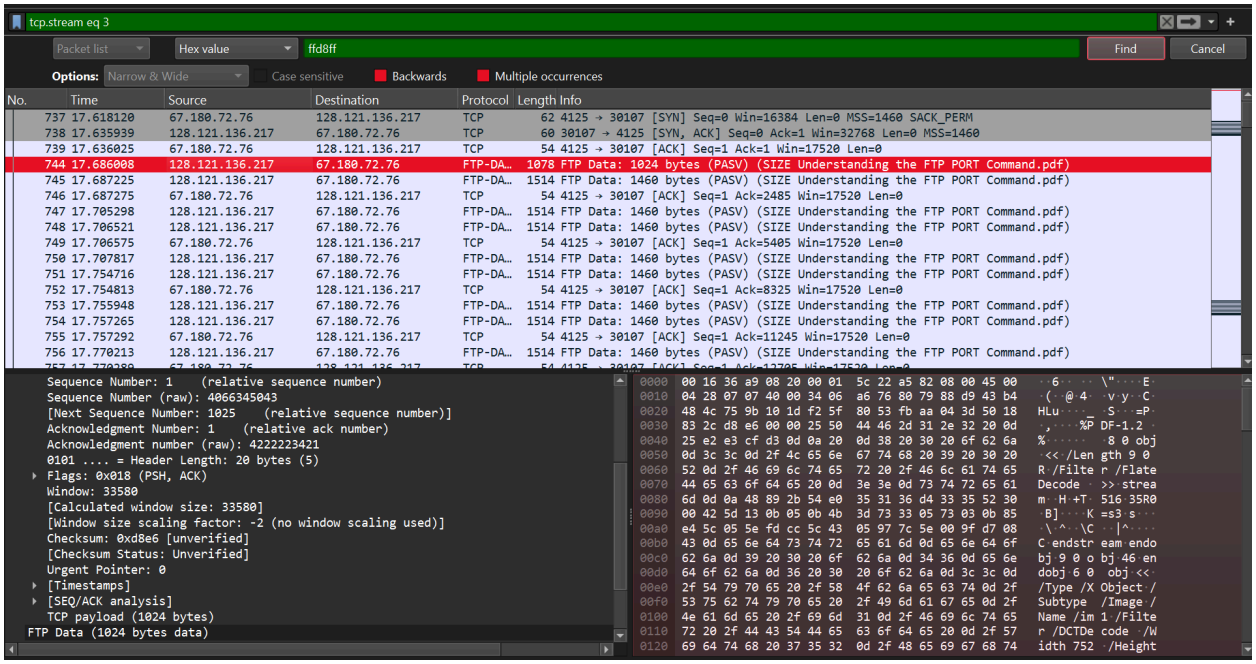
- Restore systems from clean backups.
- Validate security measures.
- Resume normal operations with monitoring.

Digital Forensics

1) Picked out package shown below

2) Went through follow -> TCP Stream -> Show as: Raw -> Save file as..

3) Uncovered real PDF file from package, opening it in Adobe Acrobat



Understanding the FTP PORT Command

Laura Chappell, Sr. Protocol Analyst
Protocol Analysis Institute
www.packet-level.com; www.podbooks.com

Note: HP Certified Professionals may attend a free course online "**Detecting and Preventing Network Scans - Part 1 and Part 2; approx. time: 90 mins. total**" at ftp://ftp.hp.com/pub/hpcp/chappel.html.

==========

You may already know that when FTP (File Transfer Protocol) commands cross the wire, they use port 21 by default. You may also know that port 20 is assigned to FTP data. Unfortunately, most FTP data sessions do not actually use port 20.

So you have just taken a trace of an FTP session and noticed that a PORT command crossed the wire. When you looked at the decode, you saw the strangest command sequence:

PORT 10,2,0,2,4,31

[We have several FTP trace files online at http://www.packet-level.com/traceFiles.htm.]

What does this mean? First let us take a look at the purpose of the PORT command. Then we will decipher the numbers following the command.

THE PORT COMMAND

FTP communications use two port number values – one for commands (port 21 by default) and

Incident Triage

Incident Type	Severity Level	Business Impact	Description
Unauthorized File Transfer (PDF Extraction)	Medium	Potential data leak	A PDF file was transferred via FTP and extracted from a PCAP file. Possible unauthorized data exfiltration
Malware in PDF	High	Security Breach	If the PDF contains embedded malware (e.g., JavaScript, exploits), it could compromise systems.
Failed Unauthorized FTP Login Attempts	Low	Minimal risk	Multiple failed login attempts could indicate a reconnaissance attempt.

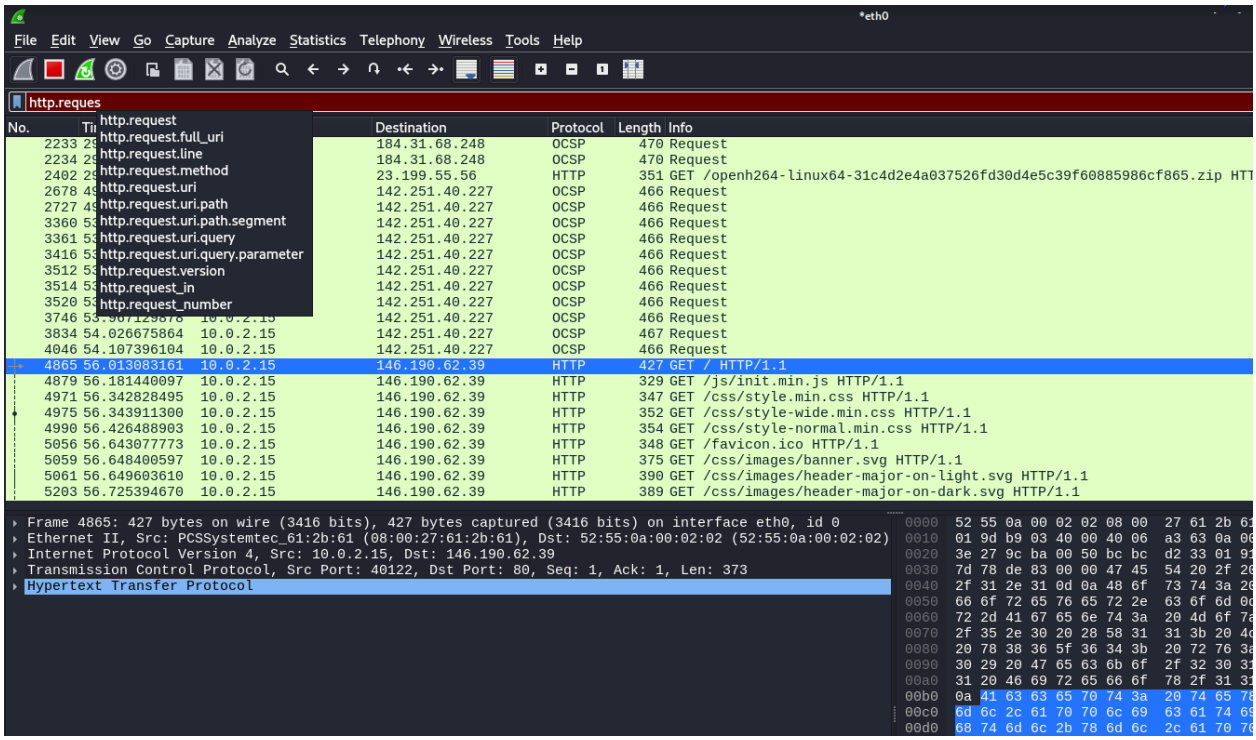
Demonstrate SOC (Security Operations Center) Fundamentals

Primary SOC Roles & Responsibilities

- SOC Analyst (Tier 1): Monitors alerts, performs triage, and escalates incidents.
- Incident Responder (Tier 2): Investigates security alerts, contains threats, and coordinates remediation.
- SOC Manager (Tier 3): Oversees SOC operations, sets policies, and leads major incident response efforts.

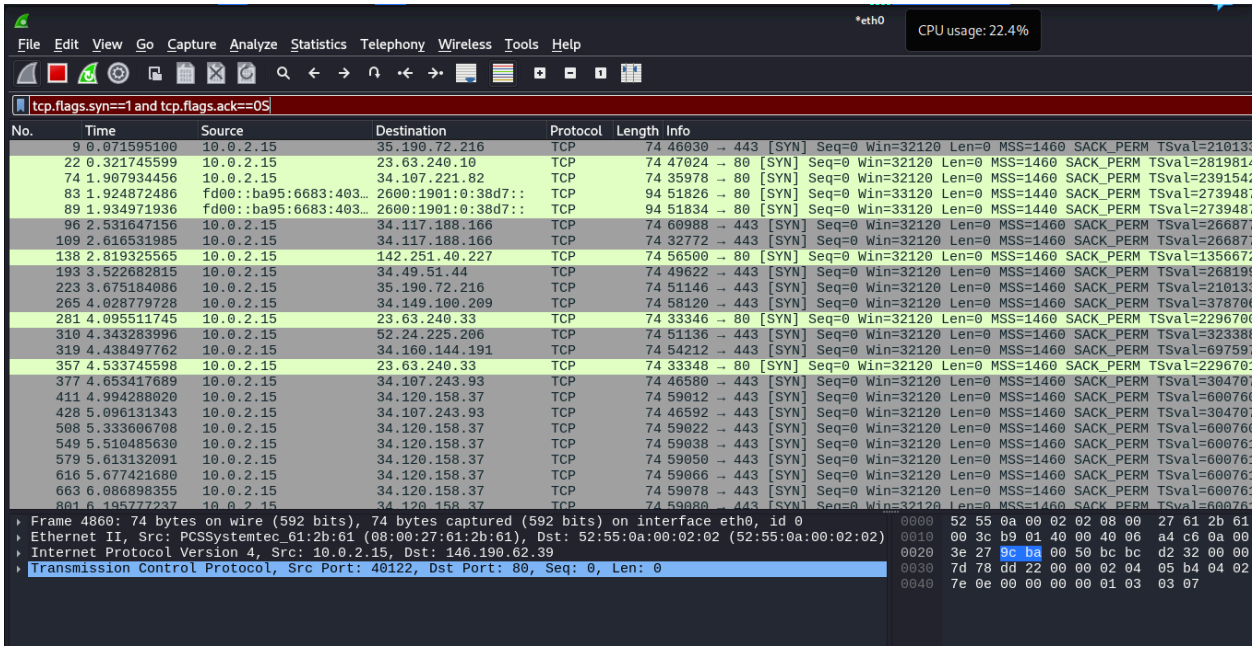
Wireshark Network Activities

1) Basic HTTP Website monitoring



- Clearly shows the GET request and the IP address of the destination of http://httpforever.com/

2) Suspicious Network Scan example



- Simulated a suspicious network port scan by using another VM to simulate the command “nmap -sS <target_IP> “ onto this VM
- Used the filter “tcp.flags.syn==1 and tcp.flags.ack==0” to discover SYN packets to confirm suspicious activity.

Develop and Implement Security Policies and Governance

1. Access Control Policy

Objective: Ensure only authorized individuals access systems and data.

Policy:

- User authentication must be enforced using multi-factor authentication (MFA).
- Role-based access control (RBAC) is implemented, granting access based on job responsibilities.
- Accounts must follow the principle of least privilege (PoLP).
- Inactive accounts will be disabled after 30 days of inactivity.
- Logs of access events must be maintained and reviewed weekly.

Enforcement:

- System administrators are responsible for enforcing access policies.
- Regular access reviews will be conducted every quarter.

2. Data Protection Policy

Objective: Protect the confidentiality, integrity, and availability of sensitive data.

Policy:

- All sensitive data must be encrypted at rest (AES-256) and in transit (TLS 1.2+).
- Data classification levels (e.g., public, internal, confidential) must be defined.
- Regular data backups must be performed and tested monthly.
- Data access must be logged and monitored.
- Employees handling sensitive data must undergo annual security awareness training.

Enforcement:

- Data protection officers oversee encryption compliance.
- IT teams conduct regular audits to ensure policy adherence.

3. System Use Policy

Objective: Define acceptable use of organizational IT resources.

Policy:

- Company systems must only be used for authorized activities.
- Personal use of company systems should be limited and must not interfere with work.
- Installation of unauthorized software is strictly prohibited.
- External devices (USB drives, external hard drives) require IT approval before use.
- Employees must report security incidents immediately.

Enforcement:

- IT administrators will monitor system usage logs.
- Non-compliance may result in access revocation or disciplinary action.

Governance Structure

- **Chief Information Security Officer (CISO):** Oversees policy development and enforcement.
- **IT Security Team:** Implements security measures and conducts audits.
- **Department Managers:** Ensure team compliance with policies.
- **Employees:** Adhere to security policies and report violations.

Compliance with Security Standards

NIST Cybersecurity Framework (CSF) guidelines, specifically:

- **PR.AC-1:** Identities and credentials are managed for authorized users.
- **PR.DS-1:** Data-at-rest is protected.
- **PR.PT-1:** Removable media use is restricted.

Produce Effective Security Documentation

Multi-Factor Authentication (MFA)

1. Security Control Implementation

1.1 Overview Multi-Factor Authentication (MFA) enhances security by requiring users to provide multiple forms of verification before accessing systems. This reduces the risk of unauthorized access due to compromised credentials.

1.2 Implementation Steps

1. **Define MFA Policies**
    - Require MFA for all administrative accounts.
    - Enforce MFA for remote access.
    - Select supported authentication methods (e.g., TOTP, biometric, hardware token).
2. **Select an MFA Solution**
    - Choose an MFA provider (e.g., Microsoft Authenticator, Google Authenticator, Duo Security).
    - Ensure integration with existing authentication systems.
3. **Deploy MFA**
    - Enable MFA in identity management settings.
    - Configure MFA enforcement policies for users.
    - Conduct initial testing with a pilot group before organization-wide deployment.
4. **User Enrollment and Training**
    - Provide step-by-step enrollment instructions.
    - Offer training on MFA usage and recovery options.
    - Implement a support channel for troubleshooting.
5. **Monitor and Maintain MFA**
    - Regularly review authentication logs for suspicious activity.
    - Update MFA policies based on security assessments.
    - Reassess MFA configurations periodically to align with security best practices.

2. Process Documentation: Patch Management

2.1 Purpose Patch management ensures that software vulnerabilities are promptly addressed, reducing the risk of exploitation.

2.2 Step-by-Step Guide

1. **Identify Systems Requiring Patching**
    - Use vulnerability scanners to detect outdated software.
    - Prioritize patches based on severity.
2. **Test Patches**
    - Deploy patches in a controlled environment.
    - Monitor for compatibility issues.
3. **Schedule Patch Deployment**
    - Establish maintenance windows to minimize disruption.
    - Notify users of potential downtime.
4. **Apply Patches**
    - Deploy patches using automated tools.
    - Verify successful installation.
5. **Monitor and Validate**
    - Conduct post-patch testing.
    - Roll back patches if issues arise.

3. Security Playbooks

3.1 Incident Response Scenario 1: Phishing Attack

Steps to Follow:

1. **Detect and Report**
    - Identify suspicious emails reported by users.
    - Use email security tools to analyze headers and links.
2. **Contain and Mitigate**
    - Block malicious domains and revoke compromised credentials.
    - Alert affected users and provide security awareness training.
3. **Investigate and Document**
    - Analyze logs to trace the source.
    - Identify affected accounts or systems.
4. **Recovery and Lessons Learned**
    - Restore any compromised systems.
    - Update email filtering policies.
    - Review and enhance phishing awareness programs.

3.2 Incident Response Scenario 2: Unauthorized System Access

Steps to Follow:

1. **Detect and Alert**
    - Monitor authentication logs for unusual access attempts.
    - Notify security teams of anomalies.
2. **Contain the Threat**
    - Disable compromised accounts.
    - Restrict access to critical systems.
3. **Investigate the Breach**
    - Review logs to identify attack vectors.
    - Conduct forensic analysis if necessary.
4. **Remediate and Improve Security**
    - Enforce stricter access controls.
    - Require password resets and MFA activation.
    - Update security policies and conduct a security audit.

---

4. Knowledge Base Management

4.1 Structured Document Repository A centralized repository ensures that cybersecurity documentation is easily accessible. The repository includes:

1. **Authentication and Access Control**
    - MFA implementation guides
    - Password policy documents
    - Single Sign-On (SSO) best practices
2. **Incident Response**
    - Security playbooks
    - Incident report templates
    - Log analysis techniques
3. **System Hardening and Patch Management**
    - Secure configuration guides
    - Patch deployment policies
    - Vulnerability scanning procedures