Cybersecurity Concepts and Network Discovery Techniques

Overview of Cybersecurity Concepts

- CIA Triad (Confidentiality, Integrity, Availability)

- Authentication & Authorization

Cybersecurity Tools

- ENCRYPTION (AES, RSA)

- FIREWALLS

- IDS/IPS

Common Cybersecurity Threats

- MALWARE (VIRUSES, WORMS, RANSOMWARE)

- PHISHING

- DDOS ATTACKS

Other Threats

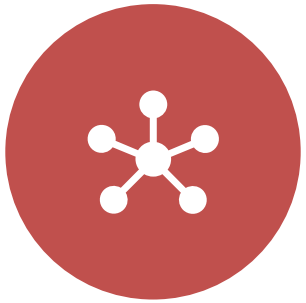
- Man-in-the-Middle (MITM)
- Insider Threats
- Zero-Day Exploits

Network Discovery Techniques

- PORT SCANNING (NMAP, NETCAT)

- PACKET SNIFFING (WIRESHARK)

Advanced Network Discovery



- NETWORK MAPPING

- BANNER GRABBING

- TRACEROUTE

Summary

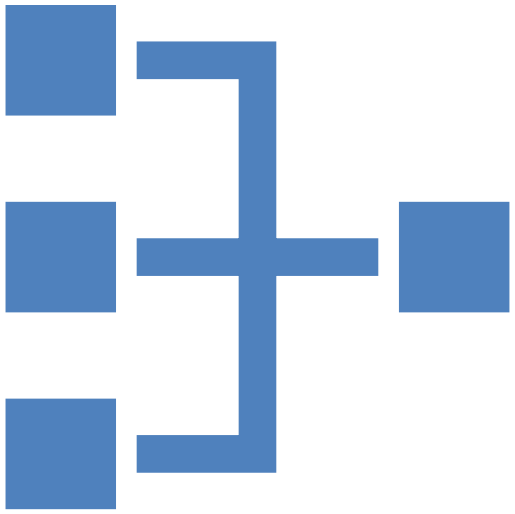
- IMPORTANCE OF CYBERSECURITY MEASURES

- KEY TOOLS AND TECHNIQUES FOR SECURING NETWORKS

Incident Response Planning

Introduction

- Failing to plan is planning to fail."
  A well-defined incident response plan minimizes damage, reduces downtime, and ensures a swift and organized response to cyberattacks.

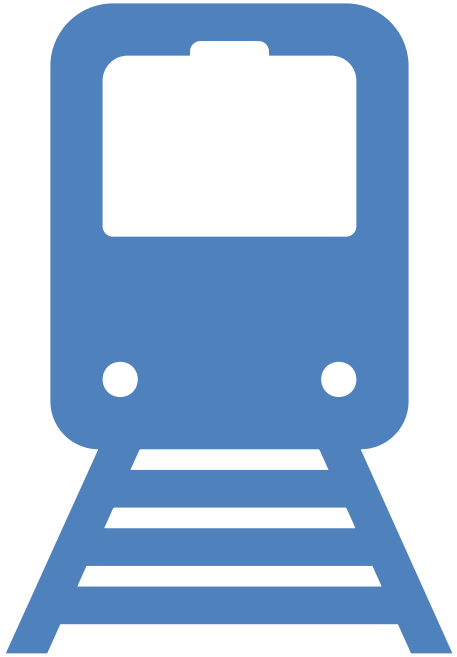


Scope and Roles

Scope: This plan covers all Target Company's systems, networks, and data assets. Key Roles: Incident Commander (leads response), Security Analysts (investigate), Forensic Investigators (gather evidence), Communication Team, Legal Counsel, Management.

Response Phases

1. Preparation
2. Detection
3. Containment
4. Eradication
5. Recovery
6. Post-Incident Activities



Preparation & Detection

- Preparation: Establish policies, train employees, harden systems (vulnerability scanning, strong passwords, MFA).
- Detection: Monitor systems, leverage threat intelligence, establish reporting mechanisms.

Containment & Eradication

Containment: Isolate affected systems, disrupt attacker activity, preserve evidence.

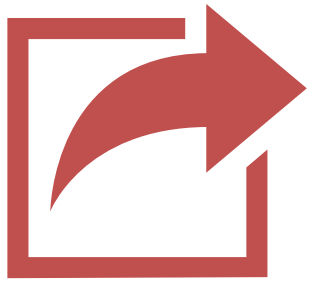
Eradication: Remove malware, restore from backups, patch vulnerabilities.

Recovery & Post-Incident Activities

Restore critical systems, validate functionality, communicate progress. Post-Incident

Activities: Review and analyze the incident, document findings, update the plan.

Communication and Legal Considerations



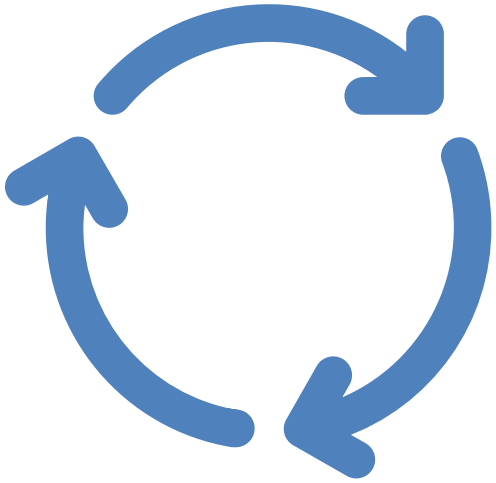
Communication: Establish clear internal and external communication channels.

Legal: Ensure compliance with data protection regulations (GDPR, CCPA), reporting requirements, and legal counsel involvement.

Training and Documentation:

Regular training and exercises are essential for preparedness. Key

Documentation: Incident Response Plan, System Hardening Reports, Incident Reports.



Review and Improvement

- Regularly review and update the plan based on lessons learned, evolving threats, and new technologies. Continuous improvement is key

Conclusion

- A robust incident response plan enables organizations to effectively manage cybersecurity incidents, minimizing their impact and ensuring business cosntinuit

Simulated Incident & Response

Ransomware Simulation – Introduction

Practical exercise using Splunk to analyze a simulated ransomware attack on a user's device.

Scenario and Tools

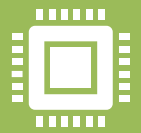
- Scenario: Keegan's machine is suspected of a ransomware attack. Files have unusual extensions, but the machine is operational. Tool: Splunk for log analysis and investigation

Attack Detection with Splunk

- Splunk searches reveal suspicious process execution (OUTSTANDING_GUTTER.exe), PowerShell activity, and network connections to a suspicious domain (ngrok.io).

Containment and Eradication - Simulation

Containment: In a real scenario, we would isolate Keegan's machine from the network.



Eradication: Splunk helps identify malicious files for removal. Antimalware scans would be performed.

Recovery and Lessons Learned

Recovery: Restoring Files From Backups Is Crucial. Verify Backup Integrity Before Restoring.

Lessons Learned: Importance Of System Monitoring, Strong Passwords, And Up-to-date Antivirus.

The Power of Data Analytics

- Splunk enables rapid identification of malicious activity, accelerates incident response, and provides valuable insights for future prevention.

Thanks