CheatSheets of Common Attacks

Detection and Mitigation

JANUARY 18, 2024

CREATED BY IBRAHIM SALEH
LinkedIn

Contents

Denial of Service (DoS) Attack:

- Types: Ping Flood, SYN Flood, UDP Flood, Application Layer DoS.

Security Solution:

- Security Solution: DDoS Protection Services, Web Application Firewalls (WAFs), Intrusion Prevention Systems (IPS), and Traffic Analysis Tools

Detection:

- **Detection in SIEM:** Anomalies in network traffic, such as a sudden increase in connection attempts or high bandwidth usage.
- **SIEM Solution Features:** Threshold monitoring, anomaly detection, and real-time alerting based on abnormal patterns.

Mitigation:

- Implement rate limiting to control the number of requests from a single source.
- Use load balancing to distribute traffic across multiple servers.
- Employ Content Delivery Networks (CDNs) to absorb and filter traffic.

Examples:

Ping Flood:

Example: An attacker floods a target server with a massive number of ICMP echo requests using a tool like "hping" or "ping-of-death," overwhelming its resources and causing it to become unresponsive.

SYN Flood:

Example: Attackers send a flood of TCP SYN packets, overwhelming the target's ability to complete the three-way handshake, and exhausting its connection resources.

HTTP GET Flood:

Example: An attacker uses automated tools to flood a web server with a large number of HTTP GET requests, consuming server resources and causing it to slow down or crash.

DNS Amplification:

Example: An attacker spoofs the source IP address and sends a small DNS query to an open DNS server, which, in turn, responds with a larger response to the forged source IP, amplifying the traffic directed at the target.

Distributed Denial of Service (DDoS) Attack:

- Types: Botnets, Amplification Attacks, Reflective Attacks.

Security Solution:

- Security Solution: DDoS Protection Services, Content Delivery Networks (CDNs), and Traffic Scrubbing Services.

Detection:

- **Detection in SIEM:** Unusual spikes in traffic from multiple sources, patterns consistent with known DDoS attack signatures.
- **SIEM Solution Features:** Anomaly detection, correlation of traffic patterns, integration with DDoS protection services.

Mitigation:

- Utilize DDoS protection services provided by cloud service providers.
- Deploy appliances or services that specialize in detecting and mitigating DDoS attacks.
- Configure firewalls to block known malicious IP addresses.

Examples:

Mirai Botnet:

Example: Compromised IoT devices, such as cameras and routers, are used collectively as a botnet to flood a target with traffic, disrupting its services.

Man-in-the-Middle (MitM) Attack:

- Types: ARP Spoofing, DNS Spoofing, SSL Stripping.

Security Solution:

- Security Solution: SSL/TLS Encryption, Certificate Pinning, Network Monitoring Tools, Intrusion Detection/Prevention Systems (IDS/IPS).

Detection:

- **Detection in SIEM:** Unexpected changes in network traffic or ARP/DNS discrepancies.
- **SIEM Solution Features:** Network traffic analysis, log analysis, and anomaly detection for unexpected changes in communication patterns.

Mitigation:

- Use encryption (SSL/TLS) to secure communication channels.
- Implement secure Wi-Fi protocols (WPA3) for wireless networks.
- Regularly monitor and update network configurations to detect unauthorized changes.

Examples:

ARP Spoofing:

Example: An attacker sends falsified Address Resolution Protocol (ARP) messages to associate their MAC address with the IP address of a target, intercepting and manipulating the traffic**.**

DNS Spoofing:

Example: Manipulating DNS responses to redirect users from a legitimate website to a malicious one by providing false IP address information.

SSL Stripping:

Example: Downgrading a secure HTTPS connection to an unencrypted HTTP connection, allowing the attacker to intercept sensitive data.

Packet Sniffing:

- Types: Passive Sniffing, Active Sniffing.

Security solution:

- Security Solution: Encryption (SSL/TLS, VPNs), Network Segmentation, Intrusion Detection/Prevention Systems (IDS/IPS).

Detection:

- **Detection in SIEM:** Monitoring for unauthorized sniffing activities, and analyzing network traffic for abnormal patterns.
- **SIEM Solution Features:** Log analysis, real-time monitoring, and detection of unusual network behavior.

Mitigation:

- Encrypt sensitive data using protocols like SSL/TLS or VPNs.
- Implement network segmentation to limit access to sensitive information.
- Use intrusion detection/prevention systems to detect and block sniffing attempts.

Examples:

Wireshark:

Example: An attacker uses Wireshark to capture and analyze packets on a network, gaining unauthorized access to sensitive information, such as login credentials.

Port Scanning:

- Types: SYN Scan, ACK Scan, XMAS Scan.

Security Solutions:

- Security Solution: Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), Regular Security Audits.

Detection:

- **Detection in SIEM:** Unusual connection attempts to various ports, repeated scanning activities.
- **SIEM Solution Features:** Log analysis, correlation of events, and real-time alerting for suspicious port scanning activities.

Mitigation:

- Configure firewalls to block or rate limit suspicious scanning activities.
- Regularly audit and close unnecessary open ports.
- Implement intrusion detection/prevention systems to detect and block port scanning.

Examples:

Nmap SYN Scan:

Example: An attacker uses Nmap to perform a SYN scan, identifying open ports on a target system and potential vulnerabilities.

SQL Injection:

- Types: Classic SQL Injection, Blind SQL Injection.

Security Solution:

- Security Solution: Web Application Firewalls (WAFs), Input Validation, Parameterized Queries, Secure Coding Practices.

Detection:

- Detection in SIEM: Anomalies in database activity, unexpected query patterns.
- SIEM Solution Features: Log analysis of database activities, pattern recognition, and correlation with other events.

Mitigation:

- Use parameterized queries to prevent SQL injection.
- Implement input validation and sanitize user inputs.
- Regularly audit and patch database systems.

Examples:

Injecting Malicious SQL Code:

Example: Inputting SQL code into a web form to manipulate a database, potentially gaining unauthorized access or extracting sensitive information.

Cross-site Scripting (XXS):

- Types: Stored XSS, Reflected XSS, DOM-based XSS.

Security Solution:

- Security Solution: Content Security Policy (CSP), Input Validation, Web Application Firewalls (WAFs).

Detection:

- **Detection in SIEM:** Unusual web application behavior, logs indicating malicious script injection.
- **SIEM Solution Features:** Log analysis, integration with WAFs, and detection of abnormal web application activities.

Mitigation:

- Employ a Content Security Policy (CSP) to control script execution.
- Input validation and output encoding to prevent script injection.
- Regularly update and patch web applications.

Examples:

Script Injection:

Example: Embedding malicious scripts in user-generated content on a website, which execute in other users' browsers, stealing cookies or defacing pages.

Cross-Site Request Forgery (CSRF):

- Types: Same-Site CSRF, Cross-Site Request Forgery with Token.

Security Solution:

- Security Solution: Anti-CSRF Tokens, SameSite Cookie Attribute, Input Validation.

Detection:

- **Detection in SIEM:** Unusual patterns in web requests, identification of unauthorized transactions.
- **SIEM Solution Features:** Log analysis, monitoring of web application logs, and detection of CSRF indicators.

Mitigation:

- Implement anti-CSRF tokens in web applications.
- Use the SameSite cookie attribute to prevent CSRF attacks.
- Validate and secure user sessions.

Examples:

Unauthorized Form Submission:

Example: Forcing a logged-in user to submit a form that changes their email address or password without their knowledge.

Phishing Attacks:

- Types: Email Phishing, Spear Phishing, Vishing, Smishing.

Security Solution:

- Security Solution: Email Filtering, Anti-Phishing Software, User Training and Awareness, Domain-based Message Authentication, Reporting, and Conformance (DMARC).

Detection:

- **Detection in SIEM:** Analysis of email logs, and identification of phishing indicators.
- **SIEM Solution Features:** Email log analysis, correlation with threat intelligence feeds, and user behavior analytics.

Mitigation:

- Implement email filtering solutions to detect and block phishing emails.
- Educate users through security awareness training.
- Use Domain-based Message Authentication, Reporting, and Conformance (DMARC) to authenticate email sources

Examples:

Deceptive Email:

Example: Sending emails that appear to be from a trusted source, tricking users into clicking on malicious links, or providing sensitive information.

DNS spoofing/ Cashe Poisoning:

- Types: DNS Spoofing, DNS Cache Poisoning.

Security Solution:

- Security Solution: DNS Security Extensions (DNSSEC), DNS Filtering, Regular DNS Monitoring.

Detection:

- **Detection in SIEM:** Unusual DNS responses, and unexpected changes in DNS records.
- **SIEM Solution Features:** DNS log analysis, real-time monitoring, and integration with DNS security solutions.

Mitigation:

- Implement DNS Security Extensions (DNSSEC) to authenticate DNS responses.
- Regularly monitor and audit DNS configurations.
- Use DNS filtering services to detect and block malicious domains.

Eavesdropping:

- Definition: is the unauthorized act of secretly listening to or intercepting private conversations or communications without consent, often for gathering information. It can involve physical proximity, wiretapping, or electronic surveillance
- Types: Passive Eavesdropping, Active Eavesdropping.

Security Solution:

- Security Solution: Encryption (SSL/TLS, VPNs), Secure Wi-Fi Protocols (WPA3), Network Monitoring Tools.

Detection:

- **Detection in SIEM:** Monitoring for unauthorized interception, and analyzing network traffic for signs of eavesdropping.
- **SIEM Solution Features:** Network traffic analysis, intrusion detection, and monitoring for unusual network behavior.

Mitigation:

- Use encryption (SSL/TLS, VPNs) to secure sensitive communication.
- Regularly monitor and audit network traffic for unusual patterns.
- Implement secure Wi-Fi protocols and strong access controls.

Examples:

Unauthorized Wi-Fi Interception:

Example: Capturing unencrypted Wi-Fi traffic using tools like Wireshark to eavesdrop on sensitive data, such as login credentials.

Zero-Day Exploits:

- Types: Unknown vulnerabilities not publicly disclosed.

Security Solution:

- Security Solution: Intrusion Detection/Prevention Systems (IDS/IPS), Endpoint Protection (Antivirus, EDR), Regular Software Patching, Vulnerability Scanning.

Detection:

- **Detection in SIEM:** Anomalies in system or application logs, patterns consistent with known exploit techniques.
- **SIEM Solution Features:** Log analysis, correlation with threat intelligence feeds, and behavior analytics to identify suspicious activities.

Mitigation:

- Regularly update and patch software to address known vulnerabilities.
- Employ intrusion detection/prevention systems to detect and block suspicious activities.
- Implement application firewalls to filter and monitor incoming traffic.

Examples:

Exploiting Unknown Vulnerability:

Example: Leveraging a previously undisclosed vulnerability in a software application before a patch is released, allowing unauthorized access or system manipulation