GIAC GCIH Exam Master Cheat Sheet

Your Complete Guide to Incident Handling & Hacker Techniques

This cheat sheet provides a concise and comprehensive guide for cybersecurity professionals preparing for the GIAC GCIH (GIAC Certified Incident Handler) exam. It condenses critical information on incident handling processes, common attack types, hacker techniques, malware analysis, log analysis, and defensive strategies. Designed to be a quick reference, it covers the essential knowledge and practical skills required to effectively detect, respond to, and mitigate cyber threats, ensuring you are well-equipped to ace the GCIH certification.

Ionised

Incident Handling Process (SANS Model)

The SANS incident handling process is a structured approach to managing cybersecurity incidents, ensuring effective and systematic response from initial preparation to post-incident review.

1

Preparation

Establishing policies, procedures, and training for incident response. This includes setting up secure networks, systems, and tools.

2

Identification

Detecting and analyzing suspicious activities to confirm if an incident has occurred. This involves monitoring logs, alerts, and user reports.

3

Containment

Limiting the scope and impact of the incident. This involves isolating affected systems, segmenting networks, and disabling compromised accounts.

- **Short-term:** Preventing further damage (e.g., unplugging network cables).
- **Long-term:** Implementing temporary fixes to allow business operations to continue while a permanent solution is developed.

4

Eradication

Removing the root cause of the incident and eliminating malicious components from affected systems. This includes patching vulnerabilities, removing malware, and strengthening security controls.

5

Recovery

Restoring affected systems and services to full operation. This involves testing systems, restoring data from backups, and continuous monitoring.

6

Lessons Learned

Reviewing the incident response process to identify areas for improvement. This includes documenting the incident, conducting post-mortem analysis, and updating policies and procedures.

Ionised

Common Attack Types

Understanding various attack types is crucial for effective incident handling and proactive defense. Each attack targets different vulnerabilities and requires specific mitigation strategies.

Denial of Service (DoS/DDoS)

Overwhelming a system or network resource with traffic, making it unavailable to legitimate users.

Example: A **DDoS attack** using a botnet to flood a company's web server with millions of requests, causing it to crash.

Web Application Attacks

Exploiting vulnerabilities in web applications to gain unauthorized access, steal data, or deface websites.

Example: A **SQL Injection** where an attacker inserts malicious SQL code into input fields to access sensitive database information.

Password Attacks

Attempts to discover valid user credentials through various methods.

Example: Brute-forcing a login portal by trying every possible password combination until the correct one is found.

Insider Threats

Malicious acts or unintentional errors committed by current or former employees, contractors, or business partners who have authorized access to an organization's systems or data.

Example: A disgruntled employee intentionally deleting critical company files before leaving the organization.

Malware

Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.

- **Ransomware:** Encrypts data and demands payment for decryption.
- **Trojans:** Disguised as legitimate software, performs malicious actions.
- **Worms:** Self-replicating malware that spreads across networks.

Example: The **WannaCry ransomware** encrypting files on thousands of computers globally.

Hacker Techniques & Tools

Understanding the methodologies and tools used by attackers is vital for developing robust defensive strategies. This section outlines common techniques and associated tools.

Social Engineering

- **Phishing:** Deceptive emails or messages to trick victims into revealing sensitive info.
- **Spear Phishing:** Targeted phishing attacks on specific individuals or organizations.
- **Pretexting:** Creating a fabricated scenario to gain trust and information.

Tools: Social Engineering Toolkit (SET), custom email spoofing tools.

Credential Attacks

- **Password Spraying:** Using a few common passwords against many accounts.
- **Brute Force:** Systematically trying all possible password combinations.

Tools: Hydra, John the Ripper, Medusa.

Reconnaissance

- **OSINT (Open Source Intelligence):** Gathering information from public sources (social media, websites).
- **DNS Lookups:** Querying DNS records to map network infrastructure.

Tools: Maltego, NSLookup, Whois, Shodan.

Exploitation

- **Buffer Overflow:** Overwriting a buffer's memory to execute malicious code.
- **Session Hijacking:** Taking control of a user's authenticated session.

Tools: Metasploit, Burp Suite, Nmap (for vulnerability scanning).

Post Exploitation

- **Privilege Escalation:** Gaining higher-level access within a system.
- **Covering Tracks:** Removing evidence of an intrusion (logs, temporary files).

Tools: Mimikatz, PowerShell Empire, Rootkits, custom scripts.

Malware & Payload Types

Malware is a pervasive threat, and understanding its various forms, delivery methods, and common payloads is crucial for effective defense and incident response.

Malware Types

- **Ransomware:** Encrypts data and demands a ransom payment, often via cryptocurrency.
- **Spyware:** Secretly monitors and collects user information (e.g., keyloggers).
- **Rootkits:** Conceals the presence of malware and provides backdoor access.
- **Trojans:** Malicious software disguised as legitimate, performing hidden functions.
- **Worms:** Self-replicating malware that spreads across networks without human interaction.

Delivery Methods

- **Email:** Phishing attachments, malicious links, or embedded scripts.
- **USB Drives:** Infected removable media inserted into systems.
- **Drive-by Downloads:** Malicious code executing simply by visiting a compromised website.
- **Exploit Kits:** Bundles of exploits targeting various software vulnerabilities.

Common Payloads

- **Reverse Shells:** A connection initiated from the target machine back to the attacker, often bypassing firewalls.
-
- **Bind Shells:** A connection where the target machine listens for incoming connections from the attacker.
- **RATs (Remote Access Trojans):** Provides full remote control over a compromised system, including file management, webcam access, and keystroke logging.

Prevention Tips

- Regularly update OS and software.
- Use reputable antivirus/anti-malware solutions.
- Implement email filtering and security awareness training.
- Exercise caution with removable media.
- Employ network segmentation and strong access controls.

Log Analysis & Indicators of Compromise (IoCs)

Effective incident response heavily relies on thorough log analysis and the ability to identify Indicators of Compromise (IoCs) that signal a breach or ongoing malicious activity.

Common Logs to Review	- **Firewall Logs:** Connection attempts, blocked traffic, rule violations. - **IDS/IPS Logs:** Alerting on known attack signatures, anomalous behavior. - **Syslog:** Centralized logs from various systems (servers, routers). - **Web Server Logs:** HTTP requests, status codes, user-agent strings. - **Endpoint Logs:** Process execution, file modifications, registry changes.	- Splunk (SIEM) - ELK Stack (Elasticsearch, Logstash, Kibana) - Graylog
Indicators of Compromise (IoCs)	- **Suspicious IPs/Domains:** Known malicious IPs, C2 server domains. - **File Hashes:** MD5/SHA1/SHA256 hashes of known malware. - **Registry Changes:** Persistent keys for malware or abnormal entries. - **Port Scanning:** Multiple connection attempts to various ports. - **Unusual Outbound Traffic:** Data exfiltration, C2 communications. - **Abnormal Account Activity:** Login failures, logins from unusual locations.	- VirusTotal - Threat Intelligence Platforms - Packet Analyzers (Wireshark) - Endpoint Detection & Response (EDR)

IoCs are digital breadcrumbs left by attackers. Their timely identification and analysis are critical for early detection and rapid response to security incidents.

Defense Tools & Techniques

A multi-layered defense strategy, combining various tools and techniques, is essential for protecting against evolving cyber threats and ensuring robust security posture.

Firewalls

Control network traffic based on security rules.

- **Next-gen (NGFW):** Deep packet inspection, application awareness, IPS capabilities.
- **Host-based:** Protect individual endpoints.

Intrusion Detection/Prevention Systems (IDS/IPS)

Monitor network or system activities for malicious policies or policy violations.

- **IDS:** Detects and alerts.
- **IPS:** Detects and actively blocks.

Endpoint Detection & Response (EDR)

Continuously monitor and respond to cyber threats on endpoints.

- Real-time visibility
- Threat hunting
- Automated response

SIEM Tools

Security Information and Event Management (SIEM) aggregates and analyzes security alerts from various sources.

- Splunk
- IBM QRadar
- Elastic SIEM

Honeypots & Deception Tools

Decoy systems designed to attract and trap attackers to learn their methods and collect intelligence.

- Divert attackers
- Gather threat intelligence
- Early warning system

Best Practices for Detection & Response:

- Implement regular vulnerability scanning and penetration testing.
- Maintain up-to-date threat intelligence feeds.
- Develop and test incident response playbooks.
- Conduct continuous security awareness training for all employees.
- Automate security tasks where possible to improve response times.

Exam Tips & Study Checklist

Preparation is key to GCIH exam success. Use this checklist and tips to structure your study and maximize your performance on exam day.

Top Study Resources

- **SANS Books:** Comprehensive material, focus on concepts and labs.
- **Practice Labs:** Hands-on experience with tools and techniques (e.g., SANS OnDemand labs, Hack The Box, TryHackMe).
- **GCIH Blueprint:** Your primary guide for exam topics and weighting.
- **Index Creation:** Develop a detailed, searchable index for your course books.

Exam Day Tips

- **Time Management:** Allocate time per question. Don't dwell too long on one question.
- **Flagging Questions:** Mark difficult questions for review later.
- **Trust Your Index:** Use your created index efficiently to look up answers.
- **Read Carefully:** Pay close attention to keywords like "NOT," "ALWAYS," "BEST."
- **Breaks:** Utilize scheduled breaks to clear your head.

Final Checklist

- **Know Tool Categories:** Understand what each tool does and its purpose (e.g., Wireshark for packet analysis, Metasploit for exploitation).
- **Attack Phases:** Master the steps of an attack lifecycle (reconnaissance, exploitation, post-exploitation).
- **Indicators of Compromise:** Be able to identify and interpret various IoCs.
- **Response Process:** Memorize and understand each stage of the SANS Incident Handling Process.
- **Common Vulnerabilities:** Understand typical vulnerabilities and how they are exploited (e.g., OWASP Top 10).

> "Success is not final, failure is not fatal: it is the courage to continue that counts."
>
> - Winston Churchill