GSDC
Global Skill Development Council

ETHICAL HACKING QUICK REFERENCE

GUIDE - CHEAT SHEET

www.gsdcouncil.org

What Is Ethical Hacking?

Ethical hacking is the authorized, legal practice of attempting to penetrate a computer system, network, or application with the owner's explicit permission — to find vulnerabilities before malicious attackers do. The ethical hacker thinks and acts like an attacker, but works within defined legal and ethical boundaries.

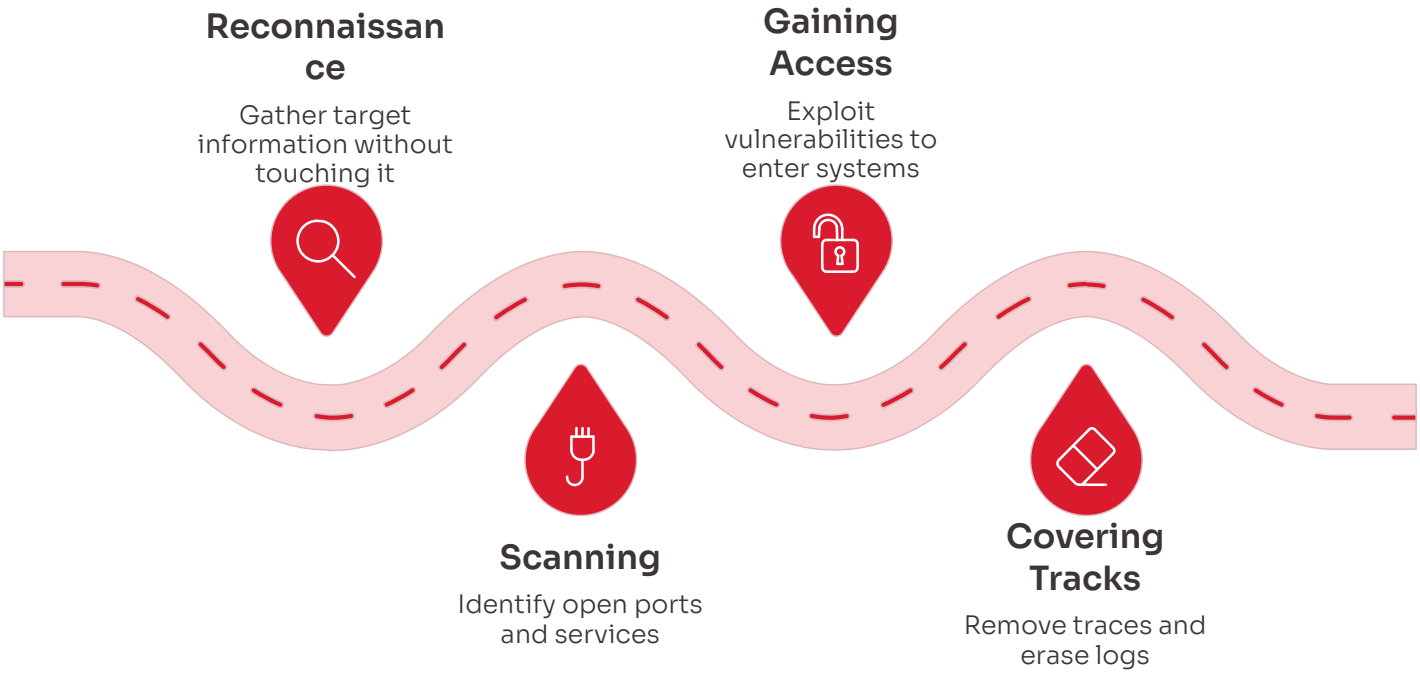
The Three Types of Hackers

Type	Who They Are	Authorization
White Hat	Ethical hackers, security professionals	Full written authorization
Black Hat	Malicious hackers, cybercriminals	None — illegal
Grey Hat	Hack without permission but without malicious intent	None — still illegal without authorization

The Golden Rule: No authorization = no ethical hacking. Written permission is the line between a security professional and a criminal.

The 5 Phases of Ethical Hacking

Every ethical hacking engagement follows this sequence. Know each phase, what happens in it, and what the goal is.



Phase 1: Reconnaissance

Goal: Gather as much information about the target as possible without touching it.

Passive Reconnaissance

Gathering information **without directly interacting** with the target system. The target never knows you are looking.

- Searching public websites, social media, job postings
- WHOIS lookups to find domain ownership
- DNS record lookups
- Google dorking — using advanced search operators to find exposed information
- Searching public code repositories for leaked credentials

Active Reconnaissance

Directly interacting with the target system to gather information.

- Ping sweeps to find live hosts
- Port scanning to find open services
- Banner grabbing to identify software versions
- Network topology mapping

What Attackers Look For

Network Info
IP address ranges, domain names and subdomains

People
Employee names and email formats

Technology
Technology stack being used

Physical
Physical locations, partner organizations and suppliers

Phase 2: Scanning & Enumeration

Goal: Identify specific vulnerabilities, open ports, active services, and system details.

Scanning finds what is there. **Enumeration** extracts specific details about what was found.

What Is Scanned

- Open ports — each open port is a potential entry point
- Running services and their versions
- Operating system type and version
- Network topology and firewall rules
- Live hosts on the network

What Is Enumerated

- User accounts on the system
- Network shares and accessible resources
- Routing tables and network paths
- Applications and their versions
- Security policies in place

Key Scanning Types

Port Scan

Which ports are open?

Vulnerability Scan

Which known vulnerabilities exist?

Network Scan

What devices are on the network?

OS Fingerprinting

What operating system is running?

Phase 3: Gaining Access

Goal: Exploit discovered vulnerabilities to enter the target system.

This is the exploitation phase — where the actual attack happens. Every exploitation attempt must be within the defined scope and authorization.

Common Exploitation Techniques

- Password attacks — brute force, dictionary attacks, credential stuffing
- Exploiting unpatched software vulnerabilities
- SQL injection on web applications
- Cross-site scripting (XSS) to execute malicious scripts
- Social engineering — manipulating people rather than systems
- Man-in-the-middle attacks — intercepting communications
- Buffer overflow attacks — sending more data than a system can handle
- Phishing — deceptive emails that steal credentials

What Success Looks Like

Shell Access

Access to the target system

Database Access

Direct access to stored data

Admin Privileges

Administrative control

Sensitive Data

Access to confidential information

Phase 4: Maintaining Access

Goal: Simulate what a real attacker would do to stay inside the system undetected.

Real attackers do not leave immediately after gaining access. They establish **persistence** — mechanisms that let them return even if the initial vulnerability is patched.

Persistence Techniques

- **Installing backdoors** — hidden access points
- **Creating new user accounts** with administrator privileges
- **Installing rootkits** — software that hides the attacker's presence
- **Planting Trojans** that appear to be legitimate software
- **Modifying startup scripts** to execute malicious code on reboot

Why this phase matters for ethical hackers: Testing whether an organization can detect sustained access is as important as testing whether initial access can be prevented. Many breaches go undetected for months.

Phase 5: Covering Tracks

Goal: Simulate how an attacker would erase evidence of their presence.

What Attackers Erase

Log Files

Log files that record their activity

Temporary Files

Temporary files created during the attack

Installed Tools

Evidence of installed tools and backdoors

Timestamps

Timestamps that reveal when access occurred

For ethical hackers: This phase tests whether the organization's logging and monitoring systems would detect the attack. If an ethical hacker can erase their tracks completely, the organization has a logging and detection problem that needs to be reported.

Key Ethical Hacking Concepts

Attack Types — Know These Cold

Attack Type	What It Is	Target
Phishing	Deceptive emails to steal credentials	People
Spear Phishing	Targeted phishing at a specific person	Individual
Vishing	Voice phishing — phone calls	People
Smishing	SMS-based phishing	People
SQL Injection	Inserting malicious SQL into input fields	Databases
XSS (Cross-Site Scripting)	Injecting scripts into web pages	Web browsers
CSRF	Forcing a user to perform unintended actions	Web sessions
MITM (Man-in-the-Middle)	Intercepting communication between two parties	Network traffic
DoS / DDoS	Overwhelming a system to make it unavailable	Servers/Networks
Brute Force	Trying every possible password combination	Authentication
Dictionary Attack	Using common words/passwords to crack authentication	Authentication
Credential Stuffing	Using breached username/password pairs on other sites	Authentication
Social Engineering	Manipulating people to reveal information	Humans
Zero-Day Exploit	Exploiting a vulnerability with no existing patch	Any system
Ransomware	Encrypting data and demanding payment	Data
Rootkit	Software that hides attacker presence and maintains access	OS level
Keylogger	Records keystrokes to capture passwords and data	Endpoints
Backdoor	Hidden access point installed for future access	Systems
Trojan	Malware disguised as legitimate software	Endpoints
Buffer Overflow	Sending more data than a system can handle	Applications

Malware Types — The Ecosystem

Malware Type	How It Spreads	Primary Purpose
Virus	Attaches to legitimate files	Damage and spread
Worm	Self-replicates across networks	Spread and overload
Trojan	Disguised as legitimate software	Backdoor access
Ransomware	Email attachments, exploits	Extortion
Spyware	Bundled with software	Surveillance
Adware	Bundled with free software	Revenue generation
Rootkit	Exploits, Trojans	Persistence and hiding
Keylogger	Physical or software install	Credential theft
Botnet	Malware on compromised machines	DDoS, spam, mining

Network Security Fundamentals

OSI Model — Why Ethical Hackers Must Know It

Each layer is an attack surface. Understanding which layer an attack targets helps you understand both the attack and the defense.

Layer	Name	What It Does	Common Attacks
7	**Application**	User-facing protocols (HTTP, DNS, FTP)	XSS, SQL injection, phishing
6	**Presentation**	Data formatting and encryption	SSL stripping
5	**Session**	Managing connections	Session hijacking
4	**Transport**	TCP/UDP — end-to-end delivery	SYN flood, port scanning
3	**Network**	IP addressing and routing	IP spoofing, MITM
2	**Data Link**	MAC addressing	ARP poisoning
1	**Physical**	Physical cables and signals	Physical access attacks

Key Protocols Ethical Hackers Must Understand

TCP/IP

The foundation of internet communication

HTTP / HTTPS

Web traffic — the most attacked protocol

DNS

Domain name resolution — target of DNS poisoning

FTP

File transfer — often insecure, transmits in plaintext

SSH

Secure remote access — target of brute force

SMTP

Email — used in phishing and spam attacks

SNMP

Network management — often misconfigured and exposed

ARP

Maps IP addresses to MAC addresses — target of ARP poisoning

Web Application Security — The OWASP Top 10

The OWASP Top 10 is the most widely referenced list of critical web application security risks. Know all ten for the exam.

Rank	Risk	What It Is
1	**Broken Access Control**	Users access data they should not be able to
2	**Cryptographic Failures**	Sensitive data not properly encrypted
3	**Injection**	SQL, command, LDAP injection attacks
4	**Insecure Design**	Security not considered in the design phase
5	**Security Misconfiguration**	Default settings, open cloud storage, verbose errors
6	**Vulnerable Components**	Using libraries with known vulnerabilities
7	**Authentication Failures**	Weak passwords, missing MFA, session issues
8	**Integrity Failures**	Software updates without integrity verification
9	**Logging Failures**	Attacks not logged — cannot detect or investigate
10	**Server-Side Request Forgery**	Server tricked into making unintended requests

Cryptography Basics

Encryption Types

Type	How It Works	Use Case
Symmetric	Same key encrypts and decrypts	Fast — bulk data encryption
Asymmetric	Public key encrypts, private key decrypts	Secure key exchange, digital signatures
Hashing	One-way transformation — cannot reverse	Password storage, file integrity

Common Algorithms

AES

Advanced Encryption Standard — symmetric, industry standard

RSA

Asymmetric — used in SSL/TLS, email encryption

SHA-256

Hashing algorithm — used in certificates and password storage

MD5

Hashing algorithm — considered weak, do not use for security

3DES

Older symmetric encryption — being phased out

Key Terms

Plaintext — Readable, unencrypted data

Ciphertext — Encrypted, unreadable data

Key — The secret used to encrypt and decrypt

Salt — Random data added to a password before hashing to prevent rainbow table attacks

PKI — Public Key Infrastructure — the system that manages certificates and trust

SSL/TLS — Protocols that secure web traffic (HTTPS)

Certificate — Digital document that proves identity and contains a public key

Social Engineering — Hacking Humans

Why it matters: The most sophisticated technical defenses can be bypassed by tricking the right person into giving up their credentials or opening a malicious attachment.

Techniques

Pretexting

Creating a fabricated scenario to manipulate a target (pretending to be IT support)

Baiting

Leaving infected USB drives in a parking lot hoping someone plugs them in

Quid Pro Quo

Offering something in exchange for information (fake IT help in exchange for login)

Tailgating / Piggybacking

Physically following an authorized person into a restricted area

Watering Hole

Compromising a website frequently visited by the target group

Dumpster Diving

Searching physical trash for useful information

Defense Against Social Engineering

- Security awareness training for all employees
- Clear verification procedures before sharing any sensitive information
- Physical security controls for building access
- Strict policies for USB and removable media

Wireless Security

Wireless Security Protocols — Weakest to Strongest

1

WEP

Very Weak — Deprecated — cracked in minutes

2

WPA

Weak — Deprecated — significant vulnerabilities

3

WPA2

Moderate — Still widely used — vulnerabilities exist

4

WPA3

Strong — Current standard — recommended

Common Wireless Attacks

Evil Twin Attack

Setting up a rogue access point with the same name as a legitimate one

Deauthentication Attack

Forcing devices off a network to capture reconnection traffic

WPS Attack

Exploiting vulnerabilities in Wi-Fi Protected Setup

Packet Sniffing

Capturing wireless traffic to analyze or steal data

KRACK Attack

Key Reinstallation Attack targeting WPA2

Penetration Testing Types

Type	What Is Tested	Who Conducts It
Black Box	Tester has no prior knowledge of the system	External attacker simulation
White Box	Tester has full knowledge — architecture, source code, credentials	Internal deep testing
Grey Box	Tester has partial knowledge — like a privileged user	Insider threat simulation
Network Pen Test	Network infrastructure and devices	Network security team
Web Application Pen Test	Web applications for OWASP vulnerabilities	Application security team
Social Engineering Test	Employee susceptibility to manipulation	Security awareness team
Physical Pen Test	Physical security controls	Physical security team
Wireless Pen Test	Wireless networks and access points	Wireless security team

Legal Framework — What Every Ethical Hacker Must Know

The Authorization Requirement: Every ethical hacking engagement requires explicit written authorization. This document must specify the scope (which systems), the time window, the techniques permitted, and the rules of engagement. Without this document, any testing is illegal regardless of intent.

Key Laws

CFAA — USA

Computer Fraud and Abuse Act — Primary federal law covering unauthorized computer access

IT Act 2000 — India

Governs cybercrime and unauthorized access in India

Computer Misuse Act — UK

Criminalizes unauthorized computer access

GDPR — EU

Data protection regulation affecting how discovered data must be handled

Scope Creep — Testing systems outside the defined scope, even if vulnerabilities are found, is illegal. If you discover an out-of-scope vulnerability, report it through the proper channel — do not test it.

Exam Day Quick Recall

- [ ] Reconnaissance has **two types** — passive (no target contact) and active (direct contact)
- [ ] **5 Phases** — Reconnaissance → Scanning → Gaining Access → Maintaining Access → Covering Tracks
- [ ] **3 hat types** — White (ethical), Black (malicious), Grey (unauthorized but no malicious intent)
- [ ] **OWASP Top 10** — Know all 10 — injection, broken access control, and cryptographic failures are most tested
- [ ] **WEP is broken** — always. WPA3 is the current secure standard
- [ ] **Social engineering targets humans** — not systems — the most effective attack vector
- [ ] **Written authorization** is the dividing line between ethical hacking and cybercrime
- [ ] **Rootkit** = hiding presence. **Backdoor** = maintaining access. **Trojan** = disguised malware
- [ ] **Symmetric** = same key. **Asymmetric** = public/private key pair. **Hashing** = one-way
- [ ] **Zero-day** = no patch exists yet. **CVE** = Common Vulnerabilities and Exposures identifier

GSDC
Global Skill Development Council

CERTIFIED ETHICAL HACKING FOUNDATION (CEHF)

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org