GSDC
Global Skill Development Council

ETHICAL HACKING TOOLS REFERENCE GUIDE

www.gsdcouncil.org

How to Use This Guide

Each tool entry is structured to give you everything you need — from plain-language descriptions to exam-ready facts. Whether you are studying for a certification or preparing for your first professional engagement, this guide will help you understand not just *what* each tool does, but *why* it matters and *how* to use it responsibly.

1

What It Is

Plain language description of the tool and its core purpose

2

Phase It Belongs To

Which stage of the 5-phase hacking lifecycle it supports

3

What It Finds or Does

The output the tool produces and why that output has value

4

Ethical Boundary

How to use the tool responsibly within authorized engagements

5

What to Know for the Exam

The key fact or concept that examiners most commonly test

CATEGORY 1

Reconnaissance Tools

Reconnaissance is the foundation of every penetration test. Before any scanning, exploitation, or post-exploitation activity can begin, the tester must understand who and what they are dealing with. Reconnaissance tools help build that picture — mapping the target's digital footprint, identifying key personnel, discovering internet-facing assets, and uncovering publicly available information that informs every subsequent phase of the engagement.

Passive Reconnaissance

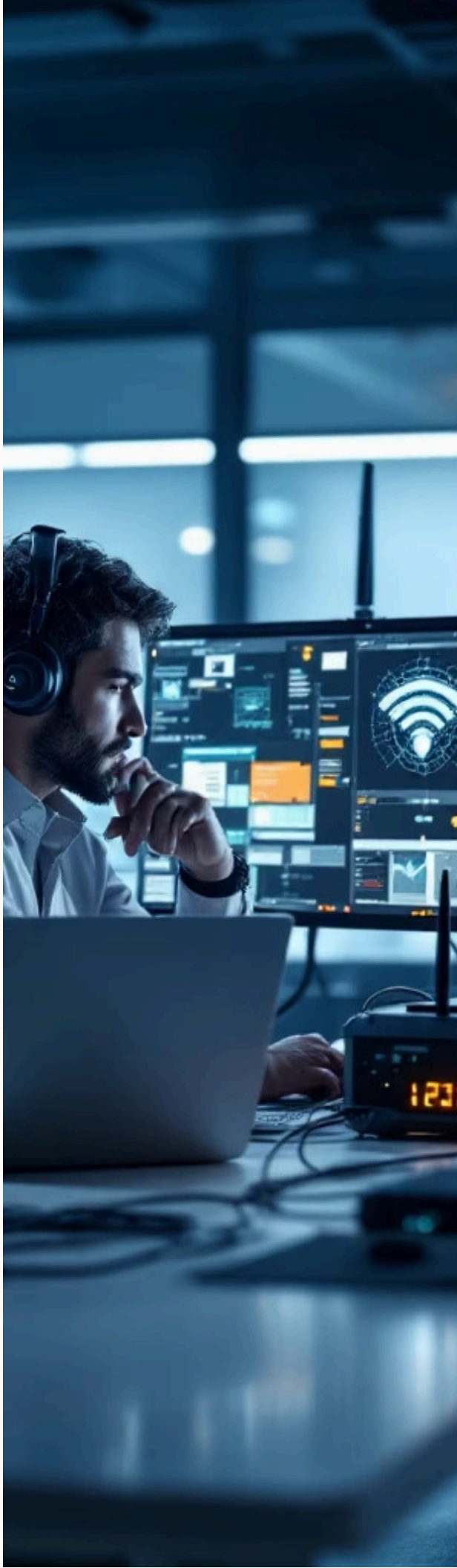
Gathering information without sending packets directly to the target — querying public databases, search engines, and third-party records

Active Reconnaissance

Directly interacting with the target system to extract information — DNS queries, banner grabbing, and direct host probing

OSINT

Open Source Intelligence — gathering intelligence exclusively from publicly available sources without accessing private or restricted data



Maltego

PASSIVE RECONNAISSANCE | OSINT

What It Is

Maltego is an open-source intelligence (OSINT) and link analysis tool that maps relationships between people, organizations, domains, IP addresses, and social networks. It transforms disconnected public data points into a rich, visual intelligence picture — making it one of the most powerful reconnaissance tools available to ethical hackers and threat intelligence professionals alike.

What It Finds

Maltego visualizes connections — linking a company's domain to its IP addresses, its IP addresses to its hosting provider, its employees to their social media profiles, and those profiles to other organizations. It turns a single known data point into a sprawling web of related entities, each one a potential avenue for further investigation or exploitation.

Why It Matters

Manual reconnaissance can miss connections that are immediately obvious when visualized. Maltego automates the gathering of public information and presents it in a graph format that reveals attack surface breadth quickly. What might take hours of manual searching can be surfaced in minutes through Maltego's automated transforms against public data sources.

Ethical Boundary

Maltego queries public data sources only — it does not access private systems or restricted databases. However, "public" does not mean "unrestricted use." Maltego must be used only for targets you are explicitly authorized to investigate. Using OSINT tools against unauthorized targets can still constitute unauthorized surveillance depending on jurisdiction and context.

Exam Key Fact: Maltego is primarily an OSINT and reconnaissance tool. It is used for **passive information gathering and relationship mapping** before any direct target interaction. Examiners often pair it with questions about link analysis and attack surface visualization.

Shodan

PASSIVE RECONNAISSANCE | DEVICE DISCOVERY

Shodan is a search engine for internet-connected devices — it continuously crawls and indexes servers, routers, webcams, industrial control systems, medical devices, and any other device with an internet-facing presence. Unlike traditional web search engines that index web page content, Shodan indexes the banners and metadata returned by services running on exposed ports.

What It Finds

Shodan reveals internet-facing devices and their exposed services — including devices that should never be directly internet-facing in the first place. A targeted search can reveal a company's exposed database servers, unprotected industrial control systems, misconfigured cloud storage buckets, and webcams with no authentication. The tool is famously called "the world's most dangerous search engine" for exactly this reason.

Why It Matters

Shodan lets an ethical hacker see the target's internet exposure without sending a single packet to the target. What Shodan has already indexed is public information — querying it is pure passive reconnaissance. This means a tester can build a detailed picture of a target's attack surface with zero risk of detection and with no authorization concerns for the query itself.

Ethical Boundary

Shodan reveals what is already indexed and publicly accessible — the query itself is passive. However, using Shodan findings to actively attack or access discovered systems is an entirely separate matter that requires explicit, written authorization for each specific target system. Discovery does not equal permission.

Exam Key Fact: Shodan is often called **"the world's most dangerous search engine"** because it reveals internet-connected devices and their exposed services without requiring active scanning of the target. It is passive reconnaissance by nature.

WHOIS

PASSIVE RECONNAISSANCE | DOMAIN INTELLIGENCE

WHOIS is both a protocol and a command-line tool that queries the public database of domain name registrations. Every domain registered on the internet has an associated WHOIS record — a public entry containing registration details submitted at the time of purchase. It is one of the simplest, oldest, and most consistently useful tools in passive reconnaissance.

Identity Data

Domain owner name, organization name, and administrative and technical contact information — revealing who is behind a target domain

Registration Timeline

Registration date, last update date, and expiry date — an expiring domain can be a social engineering angle or indicate organizational changes

Technical Infrastructure

Name servers and registrar details — revealing which DNS provider manages the domain and potentially other hosted domains under the same provider

Contact Channels

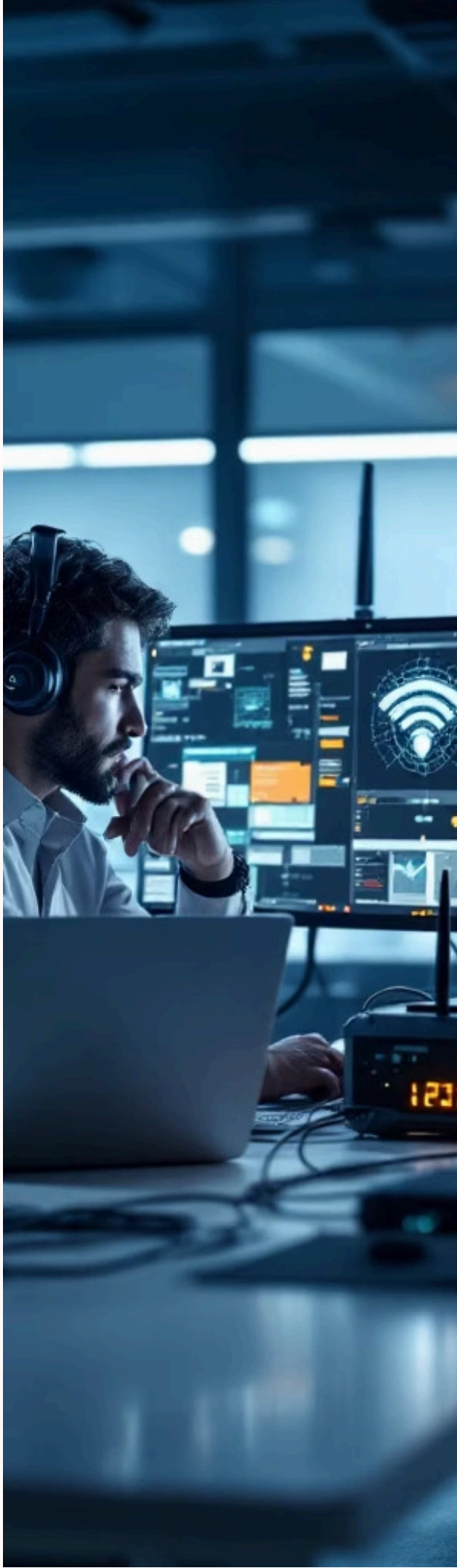
Contact email addresses and phone numbers (where not redacted) — potential targets for social engineering and spear phishing campaigns

Exam Key Fact: WHOIS is entirely passive — no authorization is required to perform a WHOIS lookup. Note that **GDPR has led many registrars to redact personal contact information** for European registrants, which is a meaningful limitation testers must be aware of in modern assessments.

CATEGORY 2

Scanning Tools

Once reconnaissance is complete, the ethical hacker moves into the scanning phase — actively probing the target to build a technical map of its attack surface. Scanning tools identify live hosts, open ports, running services, software versions, and known vulnerabilities. This is where passive intelligence gathering transitions to active technical assessment, and where authorization becomes critically important. Every tool in this category sends packets directly to target systems — making scope, timing, and written authorization non-negotiable.



Nmap (Network Mapper)

SCANNING & ENUMERATION | INDUSTRY STANDARD

Nmap is the most widely used network discovery and port scanning tool in ethical hacking. It is the industry standard for mapping what is on a network and what services are running — and has been for over two decades. Before you can exploit anything, you need to know what is there, and Nmap provides that foundational inventory.

What It Finds

- Which hosts are alive on a network
- Which ports are open on each host
- What services are running on each open port
- What version those services are running
- What operating system a host is running
- Network topology and device relationships

Ethical Boundary

Port scanning without authorization can be considered unauthorized access in many jurisdictions. Nmap must always be used within the defined scope and authorized time window — and never against systems not listed in the rules of engagement.

Scan Types

SYN Scan

Stealthy — does not complete TCP connections. Default scan type.

Full Connect Scan

Completes TCP connections — more detectable but works without root privileges.

UDP Scan

Finds UDP services frequently missed by TCP-only scans.

Version & OS Detection

Identifies specific software versions and operating systems via fingerprinting.

Exam Key Fact: Nmap is the industry-standard port scanner. **SYN scan is the default and most common scan type.** Nmap can also perform OS fingerprinting and service version detection.

Nessus

VULNERABILITY SCANNING | CVE MAPPING

Nessus is a professional vulnerability scanner that checks systems against a continuously updated database of thousands of known vulnerabilities. Where Nmap tells you what is on the network, Nessus tells you what is *wrong* with what is on the network — cross-referencing discovered services against CVE identifiers and providing severity ratings and remediation guidance for each finding.

Nmap vs. Nessus — Know the Difference

Nmap discovers what is on the network — live hosts, open ports, running services, OS and version information. It maps the attack surface.

Nessus checks what is on the network for known vulnerabilities — comparing discovered services against a database of CVEs. It assesses the attack surface for weakness.

They are used in sequence: Nmap first to map the surface, Nessus to scan for known weaknesses in what was found.

What It Finds

Known vulnerabilities in operating systems, applications, and services — each cross-referenced with a CVE identifier, assigned a severity score, and accompanied by remediation guidance. Manual testing cannot realistically check thousands of known vulnerabilities. Nessus automates this comprehensively.

Ethical Boundary

Vulnerability scanning is significantly more intrusive than port scanning. Some vulnerability checks can crash vulnerable services — this must be discussed with the client before running. Confirm whether the risk of service disruption is acceptable within the engagement terms before proceeding.

Exam Key Fact: Nessus is a **vulnerability scanner** — it identifies known vulnerabilities. Nmap is a **port scanner** — it identifies open ports and services. These are different tools with different purposes used together in sequence.

Nikto

WEB SERVER SCANNING | NOT STEALTHY

Nikto is an open-source web server scanner that checks web servers for dangerous files, outdated software, and misconfigurations. Web servers are constantly exposed to the internet and represent one of the most frequently attacked surfaces in any organization. Nikto quickly identifies the most common web server security issues — providing a rapid baseline assessment without requiring deep manual testing.

Outdated Software

Identifies web server software versions that are out of date and known to be vulnerable to published exploits

Default & Dangerous Files

Finds default configuration files, test scripts, and sample files that should be removed from production servers

Misconfigurations

Detects SSL configuration weaknesses, insecure HTTP methods, and server headers that unnecessarily expose version information

Not Stealthy

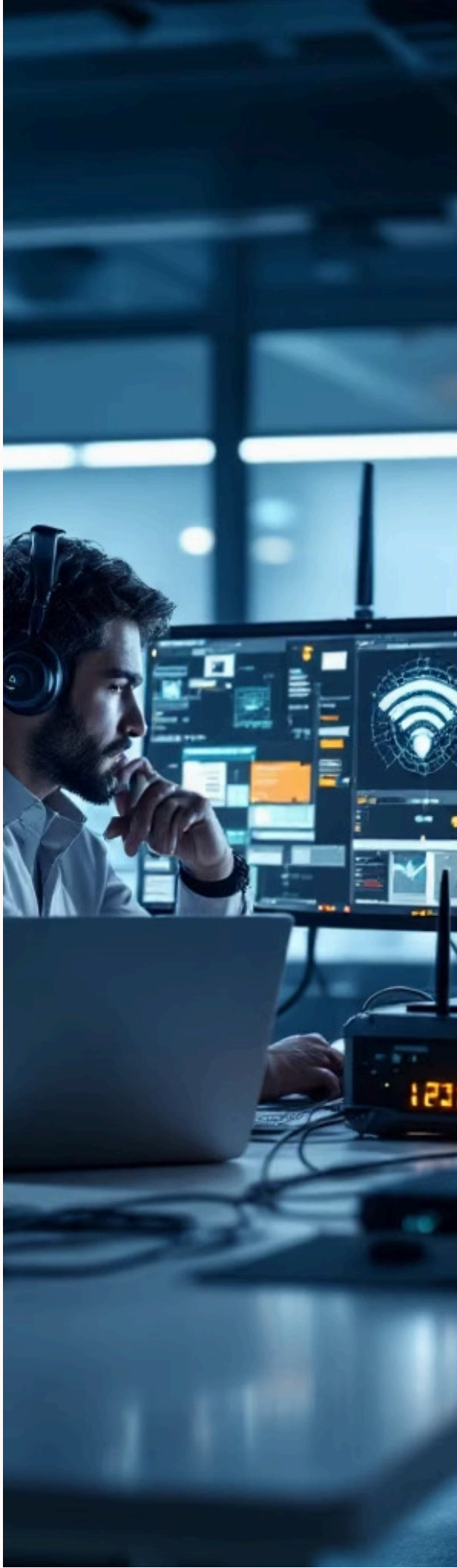
Nikto generates significant traffic that any reasonable security monitoring system will detect — it is loud by design and not suitable for covert assessments

Exam Key Fact: Nikto is specifically a **web server scanner** — not a general-purpose vulnerability scanner and not a web *application* logic tester. It is **not stealthy**. If the client has an active SOC, coordinate before running Nikto to avoid triggering unnecessary incident response.

CATEGORY 3

Exploitation Tools

Exploitation tools are the instruments used to take advantage of discovered vulnerabilities — turning theoretical weaknesses into demonstrated access. This is the phase that defines penetration testing: proving that a vulnerability is actually exploitable, not just present. The tools in this category are the most powerful in the ethical hacker's toolkit — and accordingly require the highest level of authorization, discipline, and care. Exploitation without authorization is not ethical hacking; it is criminal unauthorized access.



Metasploit Framework

GAINING ACCESS | POST-EXPLOITATION | INDUSTRY STANDARD

Metasploit is the world's most widely used penetration testing framework. It provides a structured, organized environment for exploiting vulnerabilities, managing payloads, maintaining access to compromised systems, and reporting exploitation activities. It dramatically reduces the technical barrier to exploitation by providing ready-made, tested exploit code — allowing ethical hackers to demonstrate real exploitability of discovered vulnerabilities quickly and consistently.

Core Concepts You Must Know

Exploit

The code that takes advantage of a specific vulnerability in a target system or application

Payload

The code that executes on the target after the exploit succeeds — opens a shell, creates a user account, establishes a connection back to the attacker

Module

A self-contained unit of functionality — exploit modules, auxiliary modules, and post-exploitation modules

Session

An active connection to a compromised system — the persistent foothold maintained after successful exploitation

What It Does

- Provides a library of exploit modules for thousands of known vulnerabilities
- Manages payloads — the code executed on the target after successful exploitation
- Provides post-exploitation modules for privilege escalation and lateral movement
- Manages active sessions on compromised systems
- Generates structured reports of exploitation activities

Ethical Boundary

Metasploit is powerful enough to cause real damage if misused. It must only be used against authorized targets. Destructive payloads — file deletion, disk encryption, service disruption — must **never** be used without explicit, written authorization from the client.

Exam Key Fact: Metasploit is the primary exploitation framework. **Meterpreter** is Metasploit's advanced payload providing extensive post-exploitation capabilities including file system access, privilege escalation, and pivoting.

Burp Suite

WEB APPLICATION TESTING | INTERCEPTING PROXY

Burp Suite is the industry-standard platform for web application security testing. It intercepts, analyzes, and manipulates the HTTP/HTTPS traffic flowing between a browser and a web application — giving the tester complete visibility into every request and response. In an era where web applications represent the most common attack surface in modern organizations, Burp Suite is an indispensable tool.

What It Does

- **Intercepting Proxy** — sits between the browser and the web application, capturing every request and response for inspection and modification
- **Scanner** — automatically detects common vulnerabilities including XSS, SQL injection, CSRF, and authentication issues
- **Repeater** — manually replays and modifies captured requests to test parameter manipulation
- **Intruder** — automates custom attack patterns including brute force and fuzzing
- **Spider/Crawler** — discovers hidden directories, files, and endpoints not linked from the visible application

Why It Matters

Burp Suite is the definitive tool for understanding exactly what a web application sends and receives — and for systematically testing every input for vulnerabilities. Without an intercepting proxy, many web application vulnerabilities simply cannot be properly tested or demonstrated.

Ethical Boundary

Burp Suite's automated scanner can generate a very high volume of requests in a short time. Automated scanning must be within the authorized time window and coordinated with the client to avoid triggering incident response or overloading production systems.

Exam Key Fact: Burp Suite's defining feature is its **intercepting proxy** — allowing complete visibility and manipulation of all web traffic. Burp Community is free; Burp Professional includes advanced automated scanning capabilities.

John the Ripper

POST-EXPLOITATION | PASSWORD CRACKING

John the Ripper is a password cracking tool that attempts to recover plaintext passwords from password hashes. When an ethical hacker obtains a database of password hashes from a compromised system, the plaintext passwords are needed to demonstrate the real-world impact — can these credentials be reused on other systems? Can they access email, VPN, or cloud services? John the Ripper answers that question by working to reverse the hash.

1

Dictionary Attack

Tests passwords from wordlists — highly effective against common or predictable passwords

2

Rule-Based Attack

Applies transformation rules to wordlist entries — adding numbers, capitalizing, appending special characters

3

Brute Force

Tries all combinations within defined character sets and lengths — exhaustive but time-intensive

4

Hybrid Attack

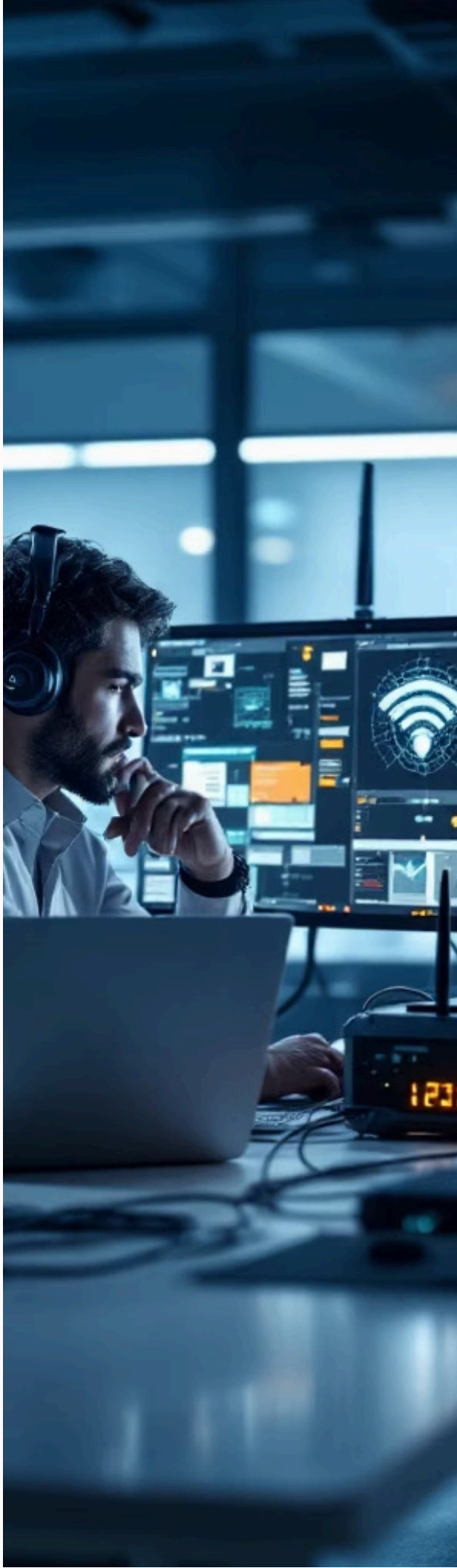
Combines dictionary and brute force approaches for maximum coverage against complex passwords

Exam Key Fact: John the Ripper **cracks password hashes** — it does not bypass live authentication directly. It works *after* hashes have been obtained from a compromised system. Cracked passwords must be reported to the client and not used beyond the authorized engagement scope.

CATEGORY 4

Network Analysis Tools

Network analysis tools give the ethical hacker insight into what is actually being communicated across the network — the real data in motion. While scanning tools tell you what is on the network and where, network analysis tools tell you what those systems are saying to each other. This phase is critical for identifying plaintext protocols, capturing credentials in transit, understanding application behavior, and validating encryption implementations. Access to network traffic is sensitive and must be handled with exceptional care.



Wireshark

RECONNAISSANCE | POST-EXPLOITATION | PROTOCOL ANALYSIS

Wireshark is the world's most widely used network protocol analyzer — a tool that captures and analyzes all network traffic visible to a network interface. It operates in promiscuous mode, meaning it captures all traffic passing through the interface, not just traffic addressed to the testing machine. Its ability to decode hundreds of protocols and reconstruct full conversations makes it an essential tool for both reconnaissance and post-exploitation analysis.

What It Does

- Captures all packets passing through a network interface in real time
- Decodes hundreds of protocols — HTTP, DNS, FTP, SMTP, Telnet, and many more
- Filters traffic by protocol, IP address, port, content, and dozens of other criteria
- Reconstructs TCP sessions to view complete conversations end-to-end
- Reveals credentials and sensitive data transmitted in plaintext
- Identifies insecure protocols that should be replaced with encrypted alternatives

Why It Matters

Finding that a web application transmits session tokens or credentials over unencrypted HTTP is a critical finding that Wireshark makes immediately visible. It provides undeniable, packet-level evidence that a communication is insecure — the kind of evidence that drives organizational change.

Ethical Boundary – Special Attention Required

Network sniffing in promiscuous mode captures traffic from **all** devices on the network segment — not just the authorized target. This means Wireshark will inevitably capture sensitive data from non-target systems, including other users' credentials, personal communications, and business-sensitive traffic.

Authorization must explicitly cover network sniffing. Captured traffic files must be stored securely, handled according to the data management provisions in the engagement agreement, and destroyed properly after the engagement concludes.

Exam Key Fact: Wireshark operates in **promiscuous mode** to capture all visible traffic, not just traffic addressed to the testing machine. It is used to identify plaintext protocols, find credentials in transit, and analyze protocol behavior.

TCPDump

SCANNING | POST-EXPLOITATION | COMMAND LINE

TCPDump is the command-line packet capture tool — the text-based, server-friendly alternative to Wireshark for environments where a graphical interface is not available or practical. It provides the same core functionality as Wireshark through a terminal interface, making it indispensable for work on Linux servers, remote systems accessed via SSH, and any production environment without a desktop GUI.

What It Does

- Captures packets from a network interface directly from the command line
- Filters traffic based on protocol, port, IP address, and many other criteria
- Saves captures to `.pcap` files for later analysis in Wireshark
- Works on servers and systems without graphical interfaces
- Supports the same BPF filter syntax as Wireshark for flexible traffic filtering

Why It Matters

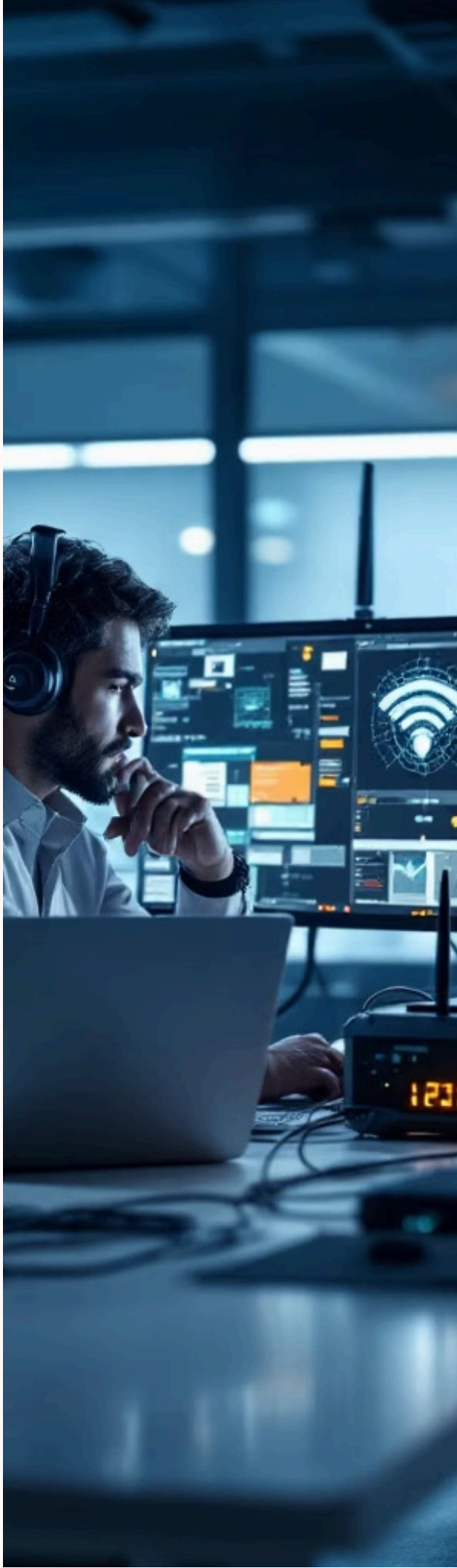
Many production servers and remote systems accessed during a penetration test will not have graphical interfaces. TCPDump enables packet capture in these environments — and the resulting capture files can be transferred to a workstation for deep analysis in Wireshark. This makes it a critical bridge tool in post-exploitation scenarios.

Exam Key Fact: TCPDump is the **command-line equivalent of Wireshark**. It captures packets and can save them to `.pcap` files for later Wireshark analysis. It is particularly essential on Linux servers where no graphical interface is available.

CATEGORY 5

Wireless Testing Tools

Wireless networks introduce a unique attack surface — one that exists in the air rather than behind physical perimeters. A vulnerable wireless network extends the organization's attack surface to anyone within radio range, potentially including a parking lot or an adjacent building. Wireless penetration testing assesses whether that radio boundary is properly secured. This category requires particular care around scope, as wireless signals do not respect property lines and can inadvertently capture traffic from neighboring organizations and individuals.



Aircrack-ng

GAINING ACCESS | WIRELESS EXPLOITATION

Aircrack-ng is a comprehensive suite of tools for assessing wireless network security — specifically focused on testing the strength and correctness of wireless encryption implementations. It is the standard toolkit for wireless penetration testing and covers the full workflow from packet capture to encryption cracking.

What It Does

- Captures wireless packets from nearby networks using a monitor-mode wireless adapter
- Performs deauthentication attacks — forcibly disconnecting clients to capture the WPA/WPA2 four-way handshake during reconnection
- Cracks WEP encryption — definitively and quickly, regardless of password complexity
- Attempts to crack WPA/WPA2 pre-shared keys by testing captured handshakes against wordlists
- Tests wireless adapter capabilities for monitor mode and packet injection

WEP vs. WPA/WPA2

WEP is a broken encryption standard — aircrack-ng can crack WEP in minutes regardless of password strength. Any organization still using WEP has a critical vulnerability. **WPA/WPA2** cracking requires capturing a four-way handshake and testing it against a wordlist — success depends on the strength of the passphrase, not the protocol's mathematical weakness.

Ethical Boundary – Physical Scope Challenge

Wireless signals do not respect physical boundaries. When testing in a dense urban or office environment, aircrack-ng will inevitably capture traffic from neighboring networks that are outside the scope of the engagement. Capture and testing must be strictly limited to authorized SSIDs. The physical testing location must be chosen carefully to minimize capture of out-of-scope wireless traffic.

Exam Key Fact: Aircrack-ng is the primary wireless security testing tool. **WEP can be cracked very quickly regardless of password complexity** — it is a broken protocol. WPA/WPA2 cracking requires capturing a four-way handshake and testing it against a wordlist — password strength matters significantly.

CATEGORY 6

Password & Credential Tools

Password and credential tools are used primarily in the post-exploitation and gaining access phases to recover or test passwords through a variety of attack strategies. These tools serve a critical purpose in penetration testing: demonstrating the real-world impact of password hash exposure and weak password policies. When a client sees that their domain administrator's password hash was cracked in under an hour, the argument for stronger password policies and better hashing algorithms becomes impossible to dismiss.

Hashcat

POST-EXPLOITATION GPU-ACCELERATED

Hashcat is the world's fastest password recovery tool — built around GPU-accelerated processing that delivers dramatically faster cracking speeds than any CPU-based alternative. Where traditional password crackers rely on the computer's central processor, Hashcat leverages the massively parallel architecture of modern graphics cards to perform billions of hash comparisons per second.

Speed Advantage

On modern consumer-grade GPU hardware, Hashcat can test billions of MD5 or NTLM hashes per second — orders of magnitude faster than CPU-based tools. This speed difference means that a password that might take days to crack on a CPU can be recovered in minutes with Hashcat on a capable GPU. Cloud-based cracking rigs can push these numbers even further.

Hash Type Support

Hashcat supports over 300 hash types including MD5, SHA-1, SHA-256, NTLM, bcrypt, Argon2, and many more. This breadth means it is applicable to nearly every password hash format encountered in real-world assessments — from Windows Active Directory NTLM hashes to Linux shadow file SHA-512 hashes to web application MD5 password databases.

Hashcat vs. John the Ripper

Hashcat	John the Ripper
GPU-accelerated. Orders of magnitude faster for supported hash types. Best for rapid cracking of large hash databases on capable hardware.	More versatile. Works across more platforms including those without capable GPUs. Excellent for complex rule-based attacks and less common formats.

Exam Key Fact: Hashcat is the **GPU-accelerated password cracker** — significantly faster than CPU-based tools. The speed advantage is greatest for weak algorithms like MD5 and NTLM. **bcrypt resists GPU acceleration by design** — its intentional slowness makes it far more resistant to cracking.

Hydra

GAINING ACCESS | ONLINE BRUTE FORCE

Hydra is a fast, parallel network login cracker that attempts to brute force authentication to live, running network services. Unlike Hashcat and John the Ripper — which work against offline password hashes captured from compromised systems — Hydra attacks services that are actively running, testing actual login attempts against real authentication systems in real time.

Network Protocol Attacks

Brute forces authentication to SSH, FTP, RDP, SMTP, IMAP, Telnet, and dozens of other network protocols — testing credential lists against live services

Web Application Attacks

Tests HTTP and HTTPS login forms — including both GET and POST-based authentication — against web application login pages

Parallel Processing

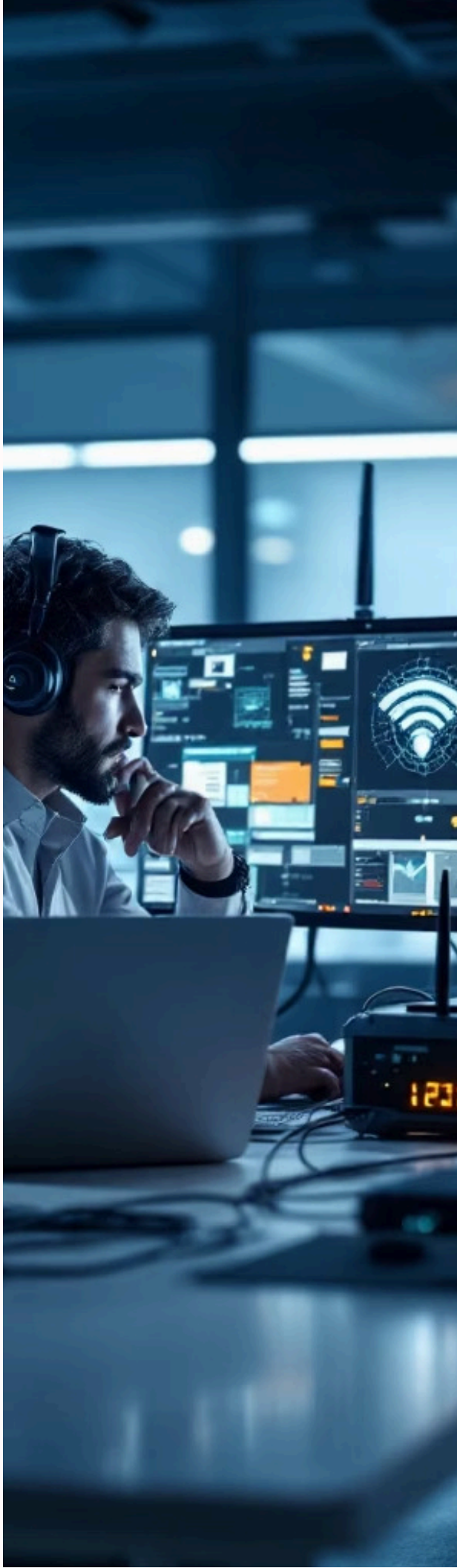
Runs multiple authentication attempts simultaneously across configurable connection threads — significantly faster than sequential testing approaches

Exam Key Fact: Hydra is an **online password attack tool** — it attacks live, running services. This critically distinguishes it from **offline crackers** like Hashcat and John the Ripper. Online attacks generate logs, can trigger account lockouts, and can cause service availability issues — always review lockout policies before running.

CATEGORY 7

Social Engineering Tools

Social engineering attacks target the human layer — the layer that no technical control can fully protect. Even organizations with perfect patch management, robust firewalls, and comprehensive monitoring can be compromised through a convincing phishing email or a carefully crafted pretexting call. Social engineering testing is an essential component of a comprehensive security assessment, revealing how an organization's people respond to manipulation attempts and whether security awareness training is effective in practice.



Social Engineer Toolkit (SET)

GAINING ACCESS | SOCIAL ENGINEERING | PHISHING

The Social Engineer Toolkit (SET) is an open-source framework specifically designed for conducting and automating social engineering attacks in authorized penetration testing contexts. It provides the infrastructure to run professional phishing campaigns, credential harvesting operations, and malicious payload delivery — all targeted at the human layer of an organization's security posture.

What It Does

- Creates convincing phishing websites that visually mirror legitimate sites to capture entered credentials
- Generates phishing emails with malicious attachments or embedded links targeting specific individuals
- Harvests credentials entered on cloned phishing pages in real time
- Creates malicious payloads delivered through social engineering vectors
- Supports spear phishing campaigns targeting specific, named individuals with personalized content

Why It Matters

Social engineering is often the most effective attack vector in a real-world penetration test because it bypasses technical controls entirely by targeting human behavior. SET provides the infrastructure to run these tests professionally, consistently, and with full logging of what was captured — enabling meaningful reporting to the client about human vulnerability exposure.

Ethical Boundary — Highest Sensitivity

SET creates realistic phishing attacks that can cause genuine distress, confusion, and embarrassment for the individuals targeted. These tests must be conducted within strictly defined scope — specific individuals or departments authorized for testing, with clear pre-agreement on what information may be collected and how it will be handled after the engagement.

The purpose of social engineering testing is **awareness and improvement** — not shame or punitive action. Results must be reported with sensitivity, framing findings as organizational training opportunities rather than individual failures.

Exam Key Fact: SET is the primary social engineering testing framework. It supports **credential harvesting through cloned websites** — creating exact visual copies of legitimate login pages to capture credentials entered by phishing targets during authorized tests.

Tools Mapped to Phases — Quick Reference

Every tool in the ethical hacker's toolkit belongs to a specific phase of the five-phase penetration testing lifecycle. Understanding which tool belongs to which phase — and why — is essential both for real-world engagements and for certification examinations. Use this reference to quickly locate the right tool for each phase of your assessment.

Phase	Primary Tools	Purpose
Reconnaissance	Maltego, Shodan, WHOIS, Google Dorking	Gather intelligence about the target from public and passive sources without direct interaction
Scanning	Nmap, Nessus, Nikto	Actively map the attack surface, identify live hosts, open ports, running services, and known vulnerabilities
Gaining Access	Metasploit, Burp Suite, Hydra, Aircrack-ng, SET	Exploit discovered vulnerabilities to gain unauthorized access to target systems and applications
Maintaining Access	Metasploit (Meterpreter), custom backdoors	Establish persistence on compromised systems to simulate an advanced persistent threat scenario
Post-Exploitation	John the Ripper, Hashcat, Wireshark	Crack captured password hashes, analyze network traffic, escalate privileges, and demonstrate full impact
Covering Tracks	Built-in OS commands, log manipulation utilities	Test detection and logging capabilities by simulating attacker attempts to remove evidence of access

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