PEN Consultants

Network Penetration Testing Coverage - Comparison

DISCLAIMER: The following is an approximation of coverage for each tier. Exact tests are chosen based on technologies being used, client's risk concerns, current attacker trends, dynamic results of previous testing, etc.

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
[Sub]domain takeover/jacking	1) Full Coverage	1) Full Coverage
CMS	1) Full Coverage	1) Full Coverage
Dump hashes	1) Full Coverage	1) Full Coverage
Host discovery	1) Full Coverage	1) Full Coverage
Mail Relay	1) Full Coverage	1) Full Coverage
MFA	1) Full Coverage	1) Full Coverage
Password spraying	1) Full Coverage	1) Full Coverage
Port scans	1) Full Coverage	1) Full Coverage
Service Enumeration	1) Full Coverage	1) Full Coverage
User enumeration	1) Full Coverage	1) Full Coverage
VDP & Bug Bounty	1) Full Coverage	1) Full Coverage
Verify Accesses	1) Full Coverage	1) Full Coverage
Verify Scope	1) Full Coverage	1) Full Coverage
Vulnerability Analysis	1) Full Coverage	1) Full Coverage
Vulnerability Scanning (Network)	1) Full Coverage	1) Full Coverage
WAF	1) Full Coverage	1) Full Coverage
Active Directory / LDAP	2) Partial Coverage	1) Full Coverage
AD checks - Kerberoasting, privEsc, etc.	2) Partial Coverage	1) Full Coverage
Admin Interfaces	2) Partial Coverage	1) Full Coverage
AS-REP Roast	2) Partial Coverage	1) Full Coverage
Attacking the Endpoint	2) Partial Coverage	1) Full Coverage
Attacking the User	2) Partial Coverage	1) Full Coverage
Authentication	2) Partial Coverage	1) Full Coverage
Blocks	2) Partial Coverage	1) Full Coverage
Brute Force	2) Partial Coverage	1) Full Coverage
Certificate transparency searches	2) Partial Coverage	1) Full Coverage
Citrix VDI / xendesktop	2) Partial Coverage	1) Full Coverage
Cloud resources	2) Partial Coverage	1) Full Coverage
Cryptography	2) Partial Coverage	1) Full Coverage
Default password checks	2) Partial Coverage	1) Full Coverage
Detect & Respond	2) Partial Coverage	1) Full Coverage
DHCP and DNS poisoning	2) Partial Coverage	1) Full Coverage
Disabled NLA / CredSSP	2) Partial Coverage	1) Full Coverage
DNS	2) Partial Coverage	1) Full Coverage
Exploit file permissions	2) Partial Coverage	1) Full Coverage
Familiarization	2) Partial Coverage	1) Full Coverage
File uploads	2) Partial Coverage	1) Full Coverage
Fingerprinting	2) Partial Coverage	1) Full Coverage
FTP	2) Partial Coverage	1) Full Coverage
Fuzzing	2) Partial Coverage	1) Full Coverage
Gaining Access	2) Partial Coverage	1) Full Coverage
GPO / Group Policy	2) Partial Coverage	1) Full Coverage
Hidden folders/files	2) Partial Coverage	1) Full Coverage

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
HTTP/HTTPS Services	2) Partial Coverage	1) Full Coverage
Insecure Protocols/Unencrypted	2) Partial Coverage	1) Full Coverage
IPMI	2) Partial Coverage	1) Full Coverage
Kerberoast	2) Partial Coverage	1) Full Coverage
Network Configuration	2) Partial Coverage	1) Full Coverage
Network Shares	2) Partial Coverage	1) Full Coverage
NTLM relaying	2) Partial Coverage	1) Full Coverage
NTLM_theft	2) Partial Coverage	1) Full Coverage
Open Directory Browsing	2) Partial Coverage	1) Full Coverage
OSINT	2) Partial Coverage	1) Full Coverage
Password and lockout policies	2) Partial Coverage	1) Full Coverage
Penetration	2) Partial Coverage	1) Full Coverage
Portals	2) Partial Coverage	1) Full Coverage
Public Exploits	2) Partial Coverage	1) Full Coverage
QUIC	2) Partial Coverage	1) Full Coverage
RDP / mstsc	2) Partial Coverage	1) Full Coverage
Reconnaissance	2) Partial Coverage	1) Full Coverage
Redis	2) Partial Coverage	1) Full Coverage
Remote Access Channels	2) Partial Coverage	1) Full Coverage
RMI / Java Deserialization	2) Partial Coverage	1) Full Coverage
Services on the endpoint	2) Partial Coverage	1) Full Coverage
SMB/samba/network shares	2) Partial Coverage	1) Full Coverage
SMTP	2) Partial Coverage	1) Full Coverage
SNMP	2) Partial Coverage	1) Full Coverage
SQLi	2) Partial Coverage	1) Full Coverage
SSDP / UPnP	2) Partial Coverage	1) Full Coverage
SSH	2) Partial Coverage	1) Full Coverage
SSL/TLS	2) Partial Coverage	1) Full Coverage
Stored passwords	2) Partial Coverage	1) Full Coverage
Threat Modeling	2) Partial Coverage	1) Full Coverage
Token Stealing and Reuse	2) Partial Coverage	1) Full Coverage
User permissions	2) Partial Coverage	1) Full Coverage
Username Predictability	2) Partial Coverage	1) Full Coverage
VPN	2) Partial Coverage	1) Full Coverage
Business impact attacks	3) Coverage if time permits	1) Full Coverage
DNS and ICMP tunnels	3) Coverage if time permits	1) Full Coverage
Email	3) Coverage if time permits	1) Full Coverage
Group policy restrictions	3) Coverage if time permits	1) Full Coverage
Outbound internet/content filtering	3) Coverage if time permits	1) Full Coverage
Outbound/egress ports	3) Coverage if time permits	1) Full Coverage
Password Reuse	3) Coverage if time permits	1) Full Coverage
VoIP / SIP	3) Coverage if time permits	1) Full Coverage
Database Enumeration	4) No Coverage	1) Full Coverage
Device Search Engines	4) No Coverage	1) Full Coverage
Email addresses	4) No Coverage	1) Full Coverage
Geolocation	4) No Coverage	1) Full Coverage
HSTS	4) No Coverage	1) Full Coverage
Leakage areas	4) No Coverage	1) Full Coverage
Session control	4) No Coverage	1) Full Coverage
Source code repos	4) No Coverage	1) Full Coverage
Tracked changes	4) No Coverage	1) Full Coverage

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
Versions	4) No Coverage	1) Full Coverage
Video Cameras	4) No Coverage	1) Full Coverage
VoIP channels	4) No Coverage	1) Full Coverage
Data Exfiltration	3) Coverage if time permits	2) Partial Coverage
Golden ticket	3) Coverage if time permits	2) Partial Coverage
Loggers/SEIMs	3) Coverage if time permits	2) Partial Coverage
MiTM	3) Coverage if time permits	2) Partial Coverage
Pass the ticket	3) Coverage if time permits	2) Partial Coverage
Password dumps	3) Coverage if time permits	2) Partial Coverage
Protection mechanisms	3) Coverage if time permits	2) Partial Coverage
Shared web hosting	3) Coverage if time permits	2) Partial Coverage
Silver ticket	3) Coverage if time permits	2) Partial Coverage
Vulnerability Scanning (Web)	3) Coverage if time permits	2) Partial Coverage
Web related vulnerabilities	3) Coverage if time permits	2) Partial Coverage
Wifi Infrastructure	3) Coverage if time permits	2) Partial Coverage
Backups	4) No Coverage	2) Partial Coverage
Custom apps	4) No Coverage	2) Partial Coverage
Defense Evasion	4) No Coverage	2) Partial Coverage
Detection Bypass	4) No Coverage	2) Partial Coverage
DoS	4) No Coverage	2) Partial Coverage
History/Logs	4) No Coverage	2) Partial Coverage
Persistence	4) No Coverage	2) Partial Coverage
Social Media	4) No Coverage	2) Partial Coverage
AMSI evasion	4) No Coverage	3) Coverage if time permits
Audio Capture	4) No Coverage	3) Coverage if time permits
Autoruns	4) No Coverage	3) Coverage if time permits
Backdoored binaries	4) No Coverage	3) Coverage if time permits
Countermeasure Bypass	4) No Coverage	3) Coverage if time permits
Custom Exploitation	4) No Coverage	3) Coverage if time permits
Custom malware and RATs	4) No Coverage	3) Coverage if time permits
DLP	4) No Coverage	3) Coverage if time permits
Fax	4) No Coverage	3) Coverage if time permits
iSCSI	4) No Coverage	3) Coverage if time permits
Key loggers	4) No Coverage	3) Coverage if time permits
Passive Collection	4) No Coverage	3) Coverage if time permits
Restricted console / kiosk escape	4) No Coverage	3) Coverage if time permits
Reverse Shell	4) No Coverage	3) Coverage if time permits
RF Access	4) No Coverage	3) Coverage if time permits
Sandbox Testing	4) No Coverage	3) Coverage if time permits
Screen scrapers	4) No Coverage	3) Coverage if time permits
Social engineering	4) No Coverage	3) Coverage if time permits