HACKTHEBOX

FOOTPRINTING

CHEAT SHEET

Infrastructure-based Enumeration

Command	Description
curl -s https://crt.sh/\?q\=<target-domain>\&output\=json | jq .	Certificate transparency.
for i in $(cat ip-addresses.txt);do shodan host $i;done	Scan each IP address in a list using Shodan.

Host-based Enumeration

FTP

Command	Description
ftp <FQDN/IP>	Interact with the FTP service on the target.
nc -nv <FQDN/IP> 21	Interact with the FTP service on the target.
telnet <FQDN/IP> 21	Interact with the FTP service on the target.
openssl s_client -connect <FQDN/IP>:21 -starttls ftp	Interact with the FTP service on the target using encrypted connection.

Command	Description
`wget -m --no-passive ftp://anonymous:anonymous@<target>`	Download all available files on the target FTP server.

SMB

Command	Description
`smbclient -N -L //<FQDN/IP>`	Null session authentication on SMB.
`smbclient //<FQDN/IP>/<share>`	Connect to a specific SMB share.
`rpcclient -U "" <FQDN/IP>`	Interaction with the target using RPC.
`samrdump.py <FQDN/IP>`	Username enumeration using Impacket scripts.
`smbmap -H <FQDN/IP>`	Enumerating SMB shares.
`crackmapexec smb <FQDN/IP> --shares -u '' -p ''`	Enumerating SMB shares using null session authentication.
`enum4linux-ng.py <FQDN/IP> -A`	SMB enumeration using enum4linux.

NFS

Command	Description
`showmount -e <FQDN/IP>`	Show available NFS shares.
`mount -t nfs <FQDN/IP>:/<share> ./target-NFS/ -o nolock`	Mount the specific NFS share to ./target-NFS
`umount ./target-NFS`	Unmount the specific NFS share.

DNS

Command	Description
`dig ns <domain.tld> @<nameserver>`	NS request to the specific nameserver.
`dig any <domain.tld> @<nameserver>`	ANY request to the specific nameserver.
`dig axfr <domain.tld> @<nameserver>`	AXFR request to the specific nameserver.
`dnsenum --dnsserver <nameserver> --enum -p 0 -s 0 -o found_subdomains.txt -f ~/subdomains.list <domain.tld>`	Subdomain brute forcing.

SMTP

Command	Description
`telnet <FQDN/IP> 25`	

IMAP/POP3

Command	Description
`curl -k 'imaps://<FQDN/IP>' --user <user>:<password>`	Log in to the IMAPS service using cURL.
`openssl s_client -connect <FQDN/IP>:imaps`	Connect to the IMAPS service.
`openssl s_client -connect <FQDN/IP>:pop3s`	Connect to the POP3s service.

SNMP

Command	Description
`snmpwalk -v2c -c <community string> <FQDN/IP>`	Querying OIDs using snmpwalk.
`onesixtyone -c community-strings.list <FQDN/IP>`	Bruteforcing community strings of the SNMP service.

Command	Description
`braa <community string>@<FQDN/IP>:.1.*`	Bruteforcing SNMP service OIDs.

MySQL

Command	Description
`mysql -u <user> -p<password> -h <FQDN/IP>`	Login to the MySQL server.

MSSQL

Command	Description
`mssqlclient.py <user>@<FQDN/IP> -windows-auth`	Log in to the MSSQL server using Windows authentication.

IPMI

Command	Description
`msf6 auxiliary(scanner/ipmi/ipmi_version)`	IPMI version detection.
`msf6 auxiliary(scanner/ipmi/ipmi_dumphashes)`	Dump IPMI hashes.

Linux Remote Management

Command	Description
`ssh-audit.py <FQDN/IP>`	Remote security audit against the target SSH service.
`ssh <user>@<FQDN/IP>`	Log in to the SSH server using the SSH client.
`ssh -i private.key <user>@<FQDN/IP>`	Log in to the SSH server using private key.

Command	Description
`ssh <user>@<FQDN/IP> -o PreferredAuthentications=password`	Enforce password-based authentication.

Windows Remote Management

Command	Description
`rdp-sec-check.pl <FQDN/IP>`	Check the security settings of the RDP service.
`xfreerdp /u:<user> /p:"<password>" /v:<FQDN/IP>`	Log in to the RDP server from Linux.
`evil-winrm -i <FQDN/IP> -u <user> -p <password>`	Log in to the WinRM server.
`wmiexec.py <user>:"<password>"@<FQDN/IP> "<system command>"`	Execute command using the WMI service.

Oracle TNS

Command	Description
`./odat.py all -s <FQDN/IP>`	Perform a variety of scans to gather information about the Oracle database services and its components.
`sqlplus <user>/<pass>@<FQDN/IP>/<db>`	Log in to the Oracle database.
`./odat.py utlfile -s <FQDN/IP> -d <db> -U <user> -P <pass> --sysdba --putFile C:\\insert\\path file.txt ./file.txt`	Upload a file with Oracle RDBMS.