Initial Foothold

Wednesday, 21 September 2022 3:42 PM

General:

1. Always try to **guess directories** (common names, machine name, smb share, ftp dirs name)
2. When founds mysql/mssql creds, try to get a **shell with sqsh**
3. **DNSrecon** when DNS 53 is open (try **UDP scan** too)
   a. nslookup -> server IP -> IP
   b. dig axfr domain @IP
4. Try **SQLi on login** page
5. Try **NoSQLi** on login
6. Try to **add payload** in **exiftool comment** when uploading images
7. Try **$() for command injection** if there is filtering
8. Enum SNMP with **snmpwalk**
9. Try to **bypass 403** in a url with **/;/**
10. Check for **port banners with LFI (/proc/PID/cmdline)**
11. **For Oracle TNS, use odat (HTB Silo)**

Redis:

1. Try **redis rogue server** RCE (github)
2. If 1 doesn't work, try **uploading** custom **module.so** file and use redis-cli **MODULE LOAD (hacktricks)**
3. Try **config set dir** and **config set dbname** manually
4. If **non persistent** on disk, try **adding ssh keys** (see HTB **Postman**)

Linux:

1. **Enumerate all** ports
2. **Upload** files via **ftp/access** via **web**
3. **Bruteforce** FTP/SSH/MYSQL/ with **given usernames** atleast or apply common default creds
4. Try to **chain issues**
5. **Searchsploit** software **name + version**
6. Search on google for **better PoC on github**
7. Check **null passwords**

Linux Reverse shell:

1. **Change** ports to **well known ports**
2. Check **nc version** with '**which**','**whereis**'
3. Try **nc mkfifo**, **python**, **python3**
4. **Host a server** on your machine, **curl exploit file** on target and system

Windows Reverse shell:

1. Try **powershell base64**
2. **Libreoffice** for **client side macro** attacks
3. URL **Encode** enabled
4. msfvenom -p windows/**shell_reverse_tcp**

Windows:

1. **Mount smb shares** with **mount -t cifs -u anonymous**
2. **Mount vhd files** with **guestmount** (HTB **bastion**)

Active Directory:

1. Use responder when SSRF (point to non listening port for hashes)
2. **Crackmapexec** to check for **allowed types** (smb/evil-winrm/ssh)
3. **Enum4linux**

4. From a **list of users**, find **valid** users with **kerbrute**
5. Search for **service accounts** through **LDAPsearch**
6. Check for **service account permissions** with bloodhound
7. Use **bloodhound-python** if no interactive shell
8. If a domain is being hit by target, use python **DNSUpdate** and **responder** (HTB intelligence)
9. GPP Passwords are inside Policies\ID\MACHINE\Preferences\Groups
10. **AS-REP roasting** with list of users with GetNPUsers.py