Post Initial Foothold

Monday, 19 September 2022 7:23 PM

Linux:

1. Check **sudo -l**
2. LinPEAS
3. **Horizontal privesc!**
4. Check **.bash_history**
5. Always **check /** directory
6. Check **SUID binaries** (carefully review all)
7. **uname -a**
8. *find / -f filename*
9. *find / -u user*
10. *find / -writable*
11. Try to **find processes** running for the next **target user**
12. *netstat -ano* (check for local service)
13. If local ports are open, try to **curl them locally**
14. Try to access user **home dirs** from **local web ports**
15. Check HTTP **directory for passwords**
16. Check **password reuse/null** password
17. Check **/etc/[service-config-files]** for other services found (web,ftp,etc)
18. **/etc/passwd**
19. **/etc/shadow**
20. **SNMP** can **execute scripts** with NET-SNMP-EXTEND-MIB/ExtendObjects, try to specify OID HTB pit)
21. **Drop** a shell with "bash" inside **msfconsole**
22. If another user **ssh is not working**, try password with **su**
23. /etc/crontab **(always check for crontab -l)**
24. Check for **mongodb scheduled tasks** (**node** machine, rana khalil)
25. Use **env variables/wildcards/symlinks** when path/file name filtering
26. **Pspy** (process spy, for recurring processes, check build for 32/64 bit)
27. Python **library hijack** (create import file on the same dir)
28. Create **symlinks** for files (or **subfiles** if **writeable**) running in **cron jobs**
29. For a **binary having BO**, use gdb (check HTB **Frolic**)
30. Check for **groups with id**, and find / -group [group] 2>/dev/null
31. For NetBSD, **sudo = doas**
32. If **SETENV** is set in **sudo**, you can **run** the command with **env variable** value (for eg, to chang program path variables, library hijacking etc, see HTB **admirer**)
33. Change **$PATH** value to execute **elevated binaries** with the custom one in pwd/sudo scripts
34. If **/usr/bin/screen** is elevated, run screen -x [user]/[sess_id] (see HTB backdoor)
35. For **shared objects:**
    a. Msfvenom -p payload -f elf-so -o utils.so LHOST= LPORT=
    b. Shared library path: /usr/local/lib/dev
    c. Check for custom **LD_LIBRARY_PATH** variables set in **crontab** to place so files
36. For **shared library**:
    a. Create rootshell c file
    b. Check function name and return type (void, _init())
    c. Check header files (stdlib, sys/types.h, stdio)
    d. Common ports
    e. Generic bash -I payload

Windows:

1. *Users\[user]\Desktop*
2. WinPEAS
3. **Horizontal privesc!**

4. **UAC Bypass (manual > msf > empire)**
5. **Powerup.ps1**
6. **Windows-exploit-suggester**
7. Check **powershell history** (winpeas)
8. Check **AlwaysInstallElevated** (winpeas sysinfo, create msf msi file)
9. Check **program files (x86)**
10. **JuicyPotatoNG** with simpersonate
11. For **windows <=2003**, and **SeImpersonate**, use **Churrasco.exe** (github)
12. Look around the **file system** for **sensitive strings**
13. *reg query*
14. Check Program Files for installed apps
15. *sc query list brief*
16. *sc qc [service_name]* ***(unquoted paths/autorun)***
17. *wmic service get name,startname*
18. *whoami /priv*
19. *net user /domain*
20. *tasklist*
21. *net localgroup user*
22. Check for **other users**, try to horizontal privesc (may have more privs)
23. Check fo**r LAPS access**
24. Check for files and folders permissions with **icacls**
25. **Decrypt PSCredential with CLiXml (HTB Omni)**
26. Use **psexec.exe** to upgrade to **SYSTEM** with **admin** privilege
27. **Grant file permission** inside a folder **with icacls /grant**
28. Use **printspoofer** for **seimpersonate** on win 10, else **juicypotato**
29. Check **AlwaysInstallElevated** (can **execute** any software **package installer** with **SYSTEM** p e.g. **msi**)
30. Check for **WSL path (rootfs)**

Active Directory:

1. *net user /domain*
2. *Horizontal!*
3. When found **other user creds**, run **service as another user** with powershell **PSCredential** a **Start-Process**
4. **cmdlist** for checking another user creds, use runas to login
5. Obtain **kerberos tickets** with **GetUserSPNs** with account details if **88 open**
6. If a **service account pass/hash** is found, try **silver ticket** with **ticketer.py/mimikatz** kerberos golden
7. If an account is allowed to **Delegate to domain**, we can **request service tickets** with **getST.p -impersonate administrator**, and **login with psexec -no-pass**
8. ADPEAS
9. *whoami /groups*