combined

nmap

```
nmap -sC -sV 172.217.27.174
```

gobuster

- directories

```
gobuster dir -u https://example.com -w /wordlists/Discovery/Web-
Content/big.txt -t 4 --delay 1s -o results.txt
```

- DNS

```
gobuster dns -d emample.com -t 50 -w
/usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --wildcard
```

- Virtual Hosts

```
gobuster vhost -u http://devvortex.htb -w
/usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
```

dirsearch

simple use

```
python3 dirsearch.py -u https://target
```

threading

```
python3 dirsearch.py -e php,htm,js,bak,zip,tgz,txt -u https://target -t 20
```

File Search

- exiftool Authors

```
find . -type f -exec exiftool {} \; | grep Author
```

- awk (get 7th element of each line)

```
awk '{print $7}'
```

- jq

```
echo '[ {"data":[ {"id": 1, "name": "jeff", "active": false}, {"id": 2, "name": "noah", "active": true} ]} ]' | jq '.[].data.[] | (.id|tostring) + ":" + .name + ":" + (.active|tostring) '
```

- see encoding

```
| xxd
```

- change encoding (for powershell)

```
| iconv -t utf16le
```

- base64

```
| base64 -w 0
```

- simple python server

```
python3 -m http.server
```

- spaces

```
echo {hello,hi}
```

Docker

```
docker run -it -v $(pwd):/mnt mcr.microsoft.com/dotnet/sdk:6.0 bash
```

Kerbrute

- Kerbrute
  - set sys date to domain date

  ```
  sudo ntpdate dc.absolute.htb
  ```

  - check user valid with users.txt

  ```
  ./kerbute userenum --dc dc.absolute.htb -d absolute.htb -o users.txt
  ```

  - check user validate (-k to use Kerberos)

  ```
  cme smb 10.10.11.181 -k -u d.klay -p Darkmoonsky248girl
  ```

  - generate access token

  ```
  getTGT.py absolute.htb/d.klay
  ```

  - blood hound scrape

  ```
  KRB5CCNAME=d.klay.ccache ./bloodhound.py -k -dc dc.absolute.htb -ns
  10.10.11.181 -c all -d absolute.htb -u d.klay
  ```

  - Scan shares

  ```
  cme smb 10.10.11.181 -u d.klay -p Darkmoonsky248girl -k --shares
  ```

  - ldapsearch

  ```
  ldapsearch -H ldap://dc.absolute.htb -Y GSSAPI -s base

  ldapsearch -H ldap://dc.absolute.htb -Y GSSAPI -b
  "cn=users,dc=absolute,dc=htb" "user" "description"
  ```

- Kerbrute

  ```
  KRBSCCNAME=/home/accesstoken.ccache ./smbclient.py -k
  absolute.htb/user_goview@dc.absolute.htb -target -ip 10.10.11.181
  ```

Joomscan

```
joomscan --url http://joomdns.htb
```

db files

cat /etc/passwd
/var/www/contact

hashcat

- bcryp `$2*$` blowfish (unix)

```
hashcat -m 3200 -o cracked-hashes hashes /usr/share/wordlists/rockyou.txt
```

Windows

- Get hostname (add hostname.domain & hostname to etc/hosts)

```
cme smb 10.10.11.187
```

Test