eJPT notes

Scripts and notes from eJPT certification

Host discovery:

```
nmap -sn -T4 <IP/24>
```

Discovers all up hosts on network

```
arp -a
```

Prints arp table

Routing/ pivoting:

```
ip route show
```

Shows current routing table of hosts

```
route
```

Similar output as above

```
ip route add <target network/24> via <IP>
```

Adds static route to access other network

Enumeration:

```
nmap -sV -sC -p- -T4 <IP>
```

Standard nmap scan to show port services and versions with verbose

```
nmap -sU -sC -sV -p- -T4 <IP>
```

Same as above but with UDP option

```
gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt
```

Standard Gobuster scan used

Sqlmap:

```
sqlmap -u "http://<URL>/" -D <database> --tables
```

```
sqlmap -u "http://<URL>/" -D <database> -T <table> --columns
```

```
sqlmap -u "http://<URL>/" -D <database> -T <table> --dump
```

```
‘ or 1=1; – -
```

Hydra

```
hydra <http://<URL>> "/login.php:username=^USER^&password=^PASS^:invalid credentials" -L usernames.txt -P passwords.txt -f -V
```

Burpsuite

Setup burp on browser: HTTP Proxy: 127.0.0.1 Port: 8080

XSS

```
<script>alert(1)</script>
```

Checks for XSS

ftp

```
ftp <IP>
```

SMB

```
smbclient -L //<IP> -N
```

Checks for available shares

```
smbclient //<IP>/IPC$ -N
```

Connecting to a share

```
enum4linux -a <IP>
```

Other tools that I forgot to take notes on during the test:

Metasploit

Wireshark

John the Ripper