Secure Command Write-up

SSH Nedir?

SSH (Secure Shell) servisi, güvenli bir şekilde ağ üzerinden bir başka bilgisayara erişim sağlamak için kullanılan bir protokoldür. Temelde, kullanıcıların uzaktaki bir sunucuya veya bilgisayara şifreli bir ağ bağlantısı üzerinden erişimini sağlar. Bu erişim genellikle komut satırı aracılığıyla gerçekleşir ve kullanıcıya uzak makineyi komut satırı üzerinden kullanma imkanı sunar.

SSH servisi iki ana bileşenden oluşur: bir SSH istemcisi ve bir SSH sunucusu. SSH istemcisi, kullanıcının bulunduğu bilgisayarda çalışır ve uzaktaki SSH sunucusuna bağlanmak için kullanılır. SSH sunucusu ise, uzaktaki bilgisayarda çalışır ve gelen SSH bağlantılarını kabul eder. İstemci ve sunucu arasındaki iletişim, güvenliği sağlamak amacıyla şifrelenmiştir. Bu şifreleme, iletilen verilerin üçüncü şahıslar tarafından okunmasını veya değiştirilmesini engeller.

SSH, kullanıcı adı ve parola ile kimlik doğrulamasının yanı sıra daha güvenli olan anahtar tabanlı kimlik doğrulamasını da destekler. Anahtar tabanlı kimlik doğrulamasında, her kullanıcının bir "private key" ve bir "public key" dosyası olur. Kullanıcı, private key dosyasını gizli tutar ve bu key ile kimliğini doğrular. Public key ise SSH sunucusuna önceden yüklenir. Kullanıcı sunucuya bağlandığında, sunucu public key ile private key in eşleşip eşleşmediğini kontrol ederek kimlik doğrulaması yapar.

SSH, sadece uzaktan komut satırı erişimi sağlamakla kalmaz, aynı zamanda dosya transferi için de kullanılır. SCP (Secure Copy) ve SFTP (SSH File Transfer Protocol) gibi araçlar, SSH'nin güvenli kanalını kullanarak dosyaları güvenli bir şekilde transfer etmeye olanak tanır. Bu, hassas verilerin veya önemli dosyaların güvenli bir şekilde aktarılmasını sağlar.

Özetle, SSH servisi, ağ üzerinden güvenli iletişim ve veri transferi için önemli bir araçtır. Kullanıcıların uzaktaki sistemlere güvenli bir şekilde erişmesini, dosya transferi yapmasını ve sistem yönetimi görevlerini yerine getirmesini sağlar.

SSH servisine bağlanmak için aşağıdaki komut dizisi kullanılır.

```
ssh <username>@<hostname or ip address> -p <port-number>
```

Not: Eğer SSH servisi varsayılan olarak 22 portunu kullanıyorsa bağlanırken port numarası belirtmemize gerek yoktur.

SSH servisi açık olan bir uzak bilgisayara SSH ile bağlanmayı deneyelim.

```
root💀hackerbox:~# ssh root@10.0.0.88
root@10.0.0.88's password:
Linux debian 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~#
```

Yukarıdaki örnekte görüldüğü üzere uzaktaki bir bilgisayara **SSH** servisi ile kullanıcı adı ve parola bilgilerini girerek bağlandık.

Bilgi Toplama

Hedef makinemize yönelik port taraması gerçekleştirelim.

Görev 1, Görev 2

```
root💀hackerbox:~# nmap 10.0.0.10
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-19 01:07 +03
Nmap scan report for 10.0.0.10
Host is up (0.059s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh

Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds
```

Sisteme Erişim

Hedef makinemize SSH ile bağlanmayı deneyelim.

Görev 3

Hedef makinemize SSH ile bağlanırken, bize görev içerisinde verilen **`hackviser:hackviser`** oturum bilgilerini kullanmamız gerekiyor. Bu bilgiler ile giriş yapmaya çalışırken **`Master's Message`**'yi görüyoruz.

```
root💀hackerbox:~# ssh hackviser@10.0.0.10
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-19 01:07 +03
──────────────────────────────────────
Secure Command
──────────────────────────────────────

Master's Message: W3lc0m3 t0 h4ck1ng w0rld
```

```
hackviser@10.0.0.10's password:
Linux secure-command 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1
(2023-09-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hackviser@secure-command:~$
```

Bu aşamada hedef makinemize **hackviser** kullanıcısı olarak bağlanmış bulunuyoruz.

Görev 4, Görev 5
Makine içerisinde yetkimizi yükseltmek için, en yetkili kullanıcı olan root kullanıcısına geçmeye çalışalım. Linux dağıtımlarında kullanıcı değiştirmek için kullanabileceğimiz komut **su** komutudur. Bu komut "Switch User" anlamına gelmektedir.

```
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

Makine içerisinde root kullanıcısına geçmek istediğimizde bizden parola istedi. Her zaman işe yarayabilecek bir yöntem olan basit parolaları denemek ya da varsayılan parolaları denemek bu aşamada işe yarayabilir.

root kullanıcısına bağlanırken **root** parolasını denedik ve ve root kullanıcısı olmayı bu şekilde başardık.

Görev 6
Linux bilgisayarlarda adının başında **.** karakteri olan dosya ya da klasörler gizli dosya olarak kabul edilirler. Gerekli parametreyi vermeden **ls** komutunu çalıştırdığımızda bu gizli dosyaları görüntüleyemeyiz.

Gizli dosyaları görüntüleyebilmek için ls komutuna **-a** parametresi eklememiz gerekmektedir.

```
ls -a
```

Görev 7
Görevimiz; master'in yani ustanın tavsiyesini öğrenmek. Bunun için dosya sisteminde biraz gezinerek bir şeyler yakalamayı deneyelim.

```
root@secure-command:/home/hackviser# ls -a
. .. .bashrc
root@secure-command:/home/hackviser# cd ..
root@secure-command:/home# ls -a
. .. hackviser
root@secure-command:/home# cd ..
root@secure-command:/# ls -a
. bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
.. boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old
root@secure-command:/# cd
root@secure-command:~# ls -a
. .. .advice_of_the_master .bashrc .local .ssh
```

Dosyalar arasında biraz dolaştıktan sonra root kullanıcısının **`home dizininde`** "**`.advice_of_the_master`**" adlı ilginç bir gizli dosya bulduk.

Şimdi bu dosyanın içeriğini cat komutu ile okuyalım.

```
root@secure-command:~# cat .advice_of_the_master
st4y cur10us
```

-

Tebrikler 🙌

✨ Bu ısınma makinesindeki tüm görevleri başarıyla tamamladınız.