Hackviser Secure Command Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Secure Command isimli Isınmayı çözeceğiz

Başlangıçta bize ssh hakkında bilgi vermiş

SSH (Secure Shell), bir ağ üzerindeki cihazlara güvenli bir şekilde erişmek ve yönetmek için kullanılan bir protokoldür. Gizliliği ve bütünlüğü korumak için verileri şifreler, bu da SSH'ı uzaktan yönetim için Telnet'e göre tercih edilen bir seçenek haline getirir.

Bizden toplamda 7 sorunun cevabını istiyor sırasıyla:

- Hangi port(lar) açık?
- Çalışan hizmet adı nedir?
- SSH'a hackviser:hackviser oturum bilgileri ile bağlanırken "Master's Message" nedir?
- Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?
- root kullanıcısının parolası nedir?
- ls komutunun gizli dosyaları gösteren parametresi nedir?
- Master’in tavsiyesi nedir?

Taramayla başlayalım

rustscan -a <ip adresi>

```
┌──(root㉿berk)-[~/Documents/Hackviser/Secure_Command]
└─# rustscan -a 172.20.6.121
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
0day was here ♥

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.20.6.121:22
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 17:11 EDT
Initiating Ping Scan at 17:11
Scanning 172.20.6.121 [4 ports]
Completed Ping Scan at 17:11, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:11
Completed Parallel DNS resolution of 1 host. at 17:11, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 17:11
Scanning 172.20.6.121 [1 port]
Discovered open port 22/tcp on 172.20.6.121
Completed SYN Stealth Scan at 17:11, 0.11s elapsed (1 total ports)
Nmap scan report for 172.20.6.121
Host is up, received echo-reply ttl 63 (0.091s latency).
Scanned at 2024-09-22 17:11:26 EDT for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (72B)
```

22 portunun açık olduğunu görüyoruz (ilk sorumuzun cevabı)

Daha detaylı bilgi için nmap çalıştıralım

nmap -Pn -n -O -sV -p 22 <ip adresi> -oN nmapV.txt

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

```
┌──(root㉿berk)-[~/Documents/Hackviser/Secure_Command]
└─# nmap -Pn -n -p 22 172.20.6.121 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 17:13 EDT
Nmap scan report for 172.20.6.121
Host is up (0.099s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

22 de ssh (secure shell) çalıştığını görüyoruz (2. sorumuzun cevabı)

ssh a giriş yapmak için bi kullanıcı adı ve şifreye ihtiyacımız var 3. soruda bunu vermiş ve bizde Master's Mesagge'in ne olduğunu sormuş ssh'a bağlanıp bakalım

ssh hackviser@<ip adresi>

Master's Mesagge'in **W3lc0m3 t0 h4ck1ng w0rld** olduğunu görüyoruz bu da 3. sorumuzun cevabı.

4. soruda bize kullanıcı değiştirmek için hangi komutu kullanırız diye sorulmuş cevap **su** olacak (4. sorunun cevabı). En yetkili kullanıcı olan root'a giriş yapmamız gerekiyor bize su komutunun ipucunu verdiğine göre basit şifreler deneyerek root olmaya çalışalım

su root

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

şifreyi root olarak denediğimde root olmayı başardım (5. sorunun cevabı)

6. soruda bize ls komutuyla gizli dosyaları görmek için hangi parametreyi kullanmamız gerektiğini sormuş doğru cevap ls -la (6. sorunun cevabı)

Şimdi kök dizine gidip gizli dosya varmı diye kontrol edelim

```
root@secure-command:~# cd /root
root@secure-command:~# ls -la
total 24
drwx------  4 root root 4096 Sep 22 17:26 .
drwxr-xr-x 18 root root 4096 Sep 12  2023 ..
-rw-r--r--  1 root root   13 Nov 18  2023 .advice_of_the_master
-rw-r--r--  1 root root  697 Nov 18  2023 .bashrc
drwxr-xr-x  3 root root 4096 Nov 18  2023 .local
drwx------  2 root root 4096 Sep 22 17:08 .ssh
root@secure-command:~# cat .advice_of_the_master
st4y cur10us
root@secure-command:~#
```

Ve evet burada da 7. sorunun cevabı olan master'in tavsiyesini okuyoruz

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş