

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

4 hours, 6 minutes

Progress:

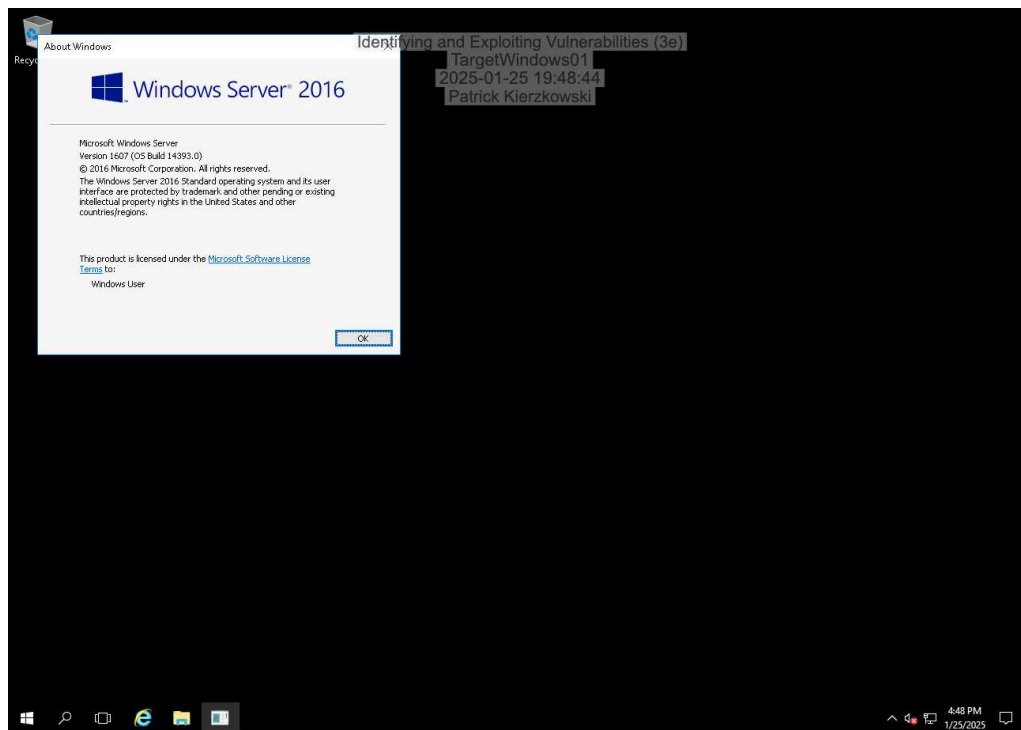
100%

Report Generated: Monday, July 7, 2025 at 9:37 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**.



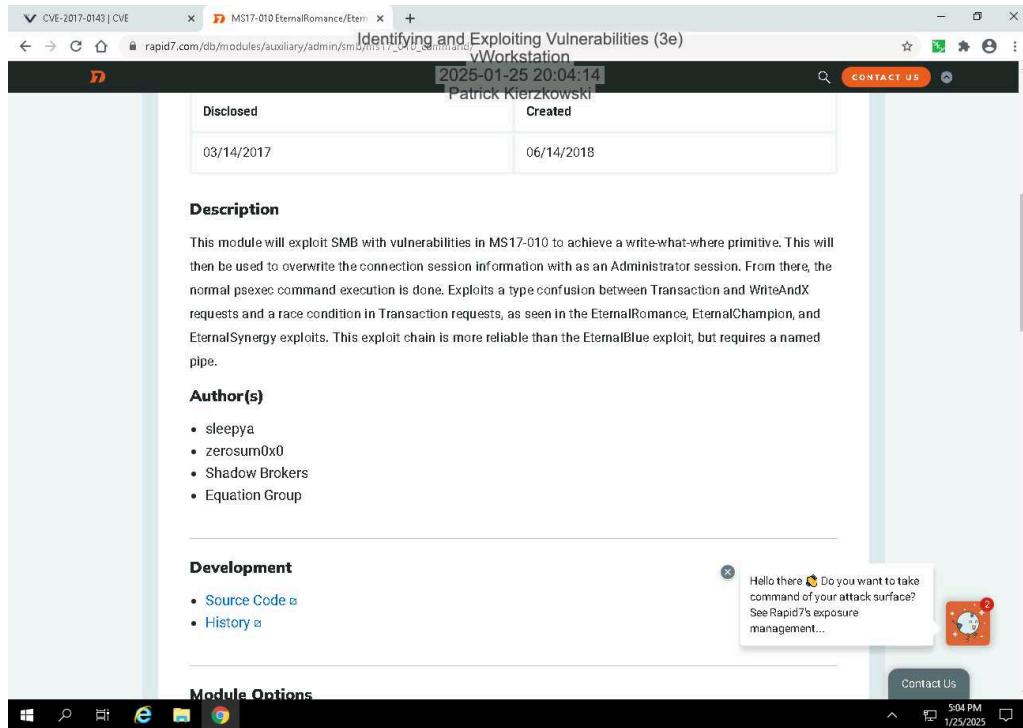
Part 2: Research and Identify Vulnerabilities and Exploits

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

The screenshot shows a web browser window with the URL nvd.nist.gov/vuln/detail/CVE-2017-0143. The page title is "Identifying and Exploiting Vulnerabilities (3e) Workstation". The page content includes a "Metrics" section with tabs for CVSS Version 4.0, CVSS Version 3.x, and CVSS Version 2.0. The CVSS 3.x Severity and Vector Strings section shows a Base Score of 8.8 HIGH and a Vector of CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H. Below this is a "References to Advisories, Solutions, and Tools" section with a table of hyperlinks and resources.

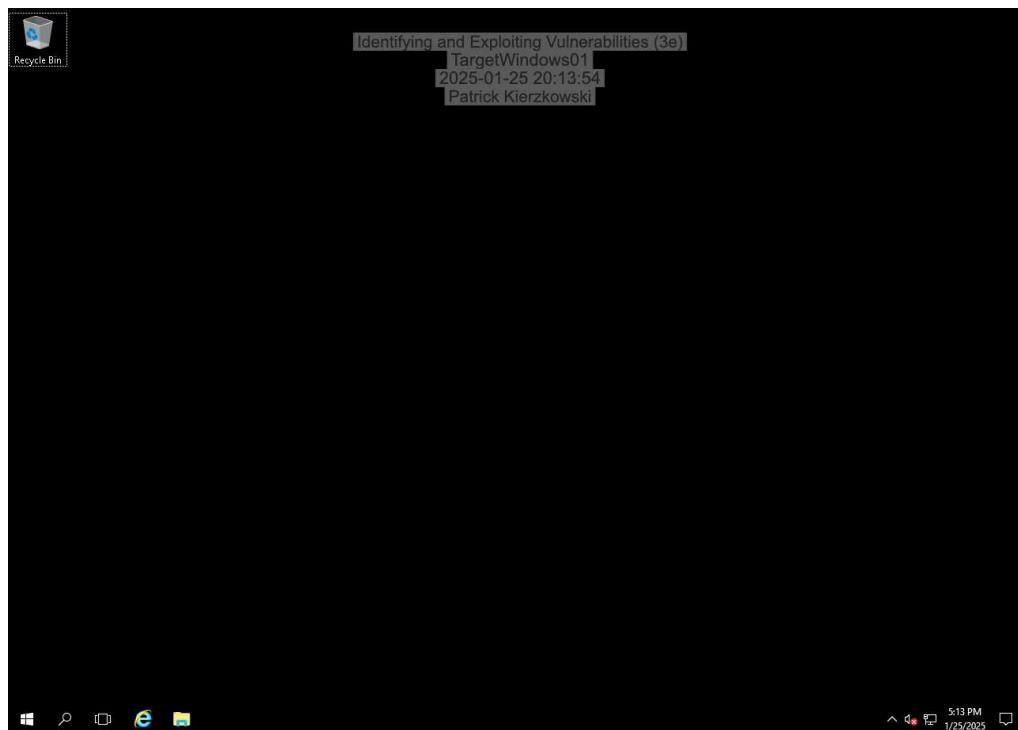
Hyperlink	Resource
http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html	Exploit Third Party Advisory VDB Entry
http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html	Exploit Third Party Advisory VDB Entry
http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html	Exploit Third Party Advisory VDB Entry
http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html	Exploit Third Party Advisory VDB Entry
http://www.securityfocus.com/bid/96703	Broken Link Third Party Advisory

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.

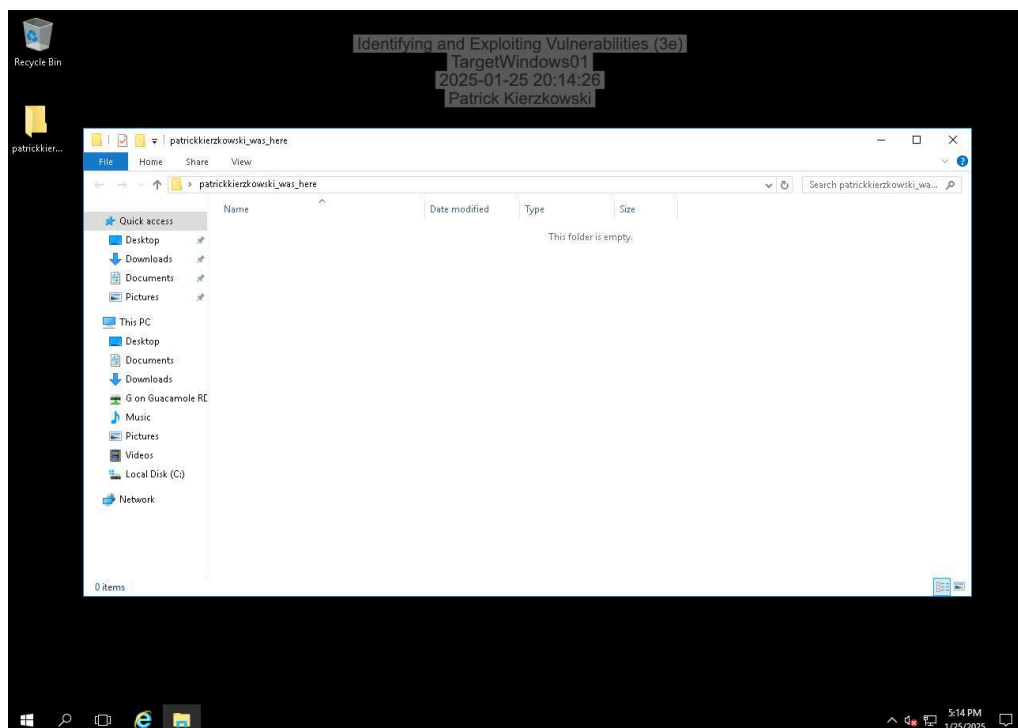


Part 3: Use the Metasploit Framework to Exploit a Vulnerability

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

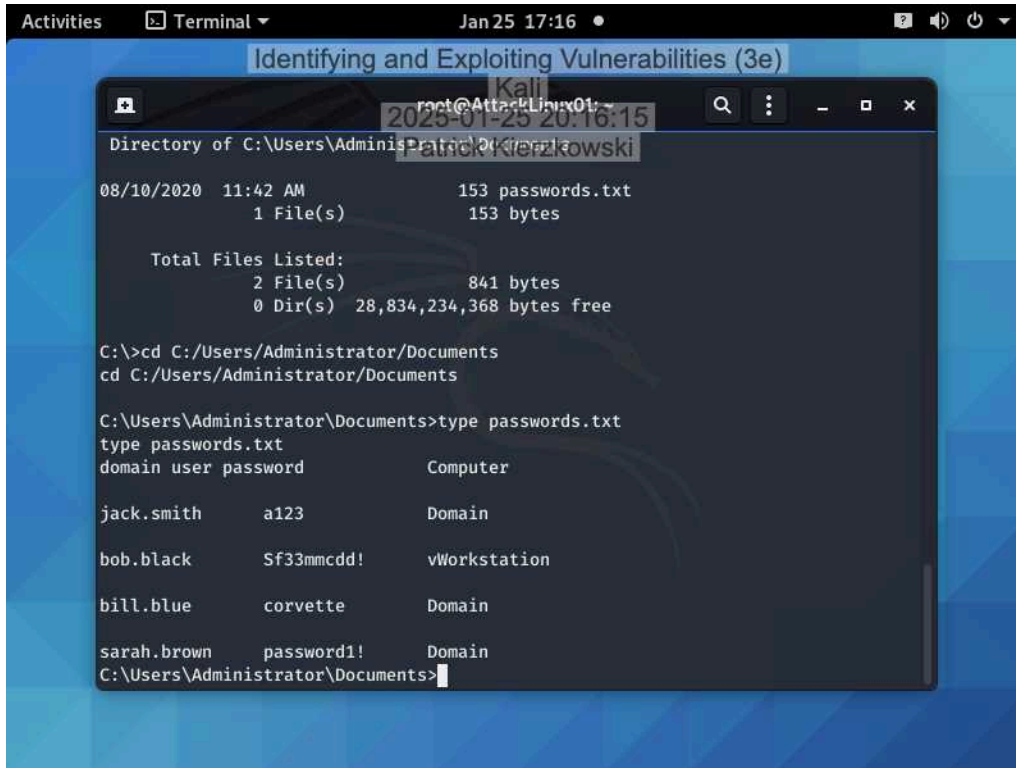


18. Make a screen capture showing the **TargetWindows01 Desktop and the *yourname_was_here* folder**.



Part 4: Retrieve Sensitive Files

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



```
Activities Terminal Jan 25 17:16
Identifying and Exploiting Vulnerabilities (3e)
root@AttackLinux01:~#
2025-01-25 20:16:15
Patrick Kierzkowski

Directory of C:\Users\Administrator\Documents
08/10/2020 11:42 AM 153 passwords.txt
1 File(s) 153 bytes

Total Files Listed:
2 File(s) 841 bytes
0 Dir(s) 28,834,234,368 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

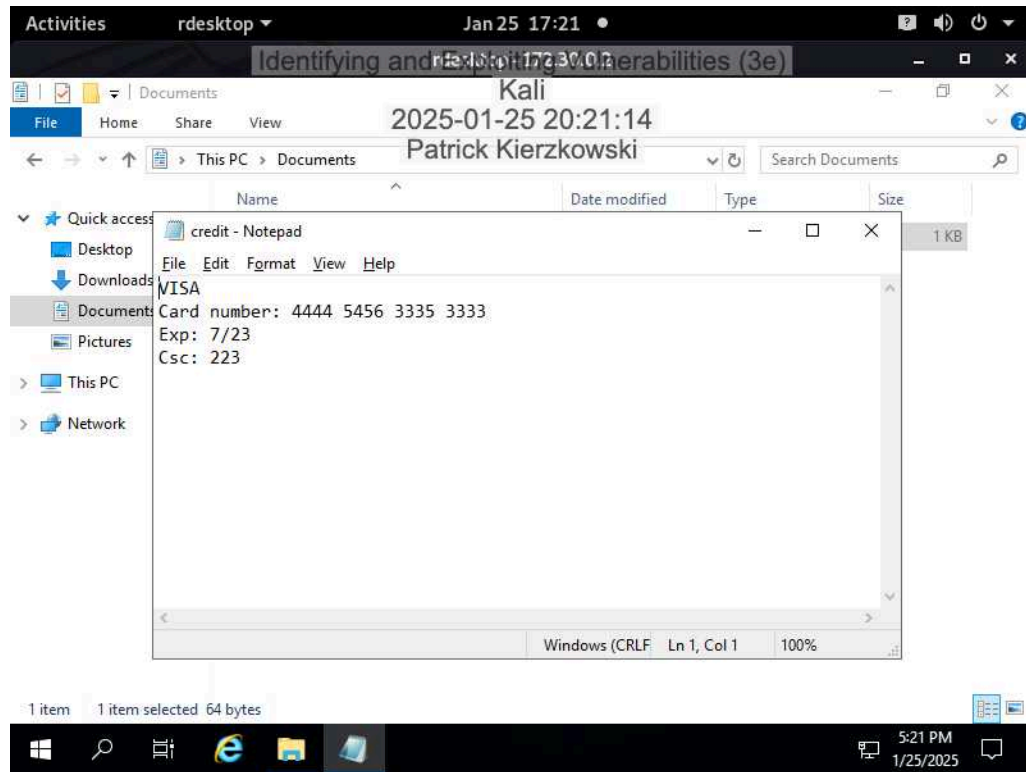
jack.smith a123 Domain

bob.black Sf33mmcdd! vWorkstation

bill.blue corvette Domain

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

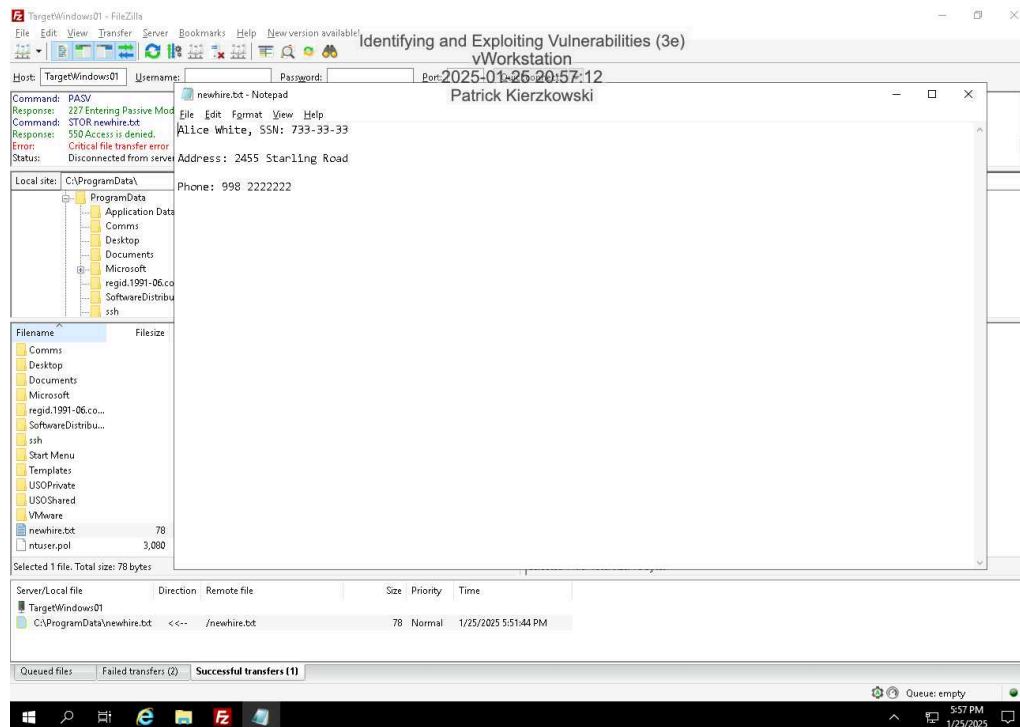
12. **Make a screen capture** showing the **contents of the file** containing sensitive information.



Challenge Exercises

Part 1: Use FTP to Extract Sensitive Information

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



Part 2: Identify Root Causes

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

They could be unaware of the risk that comes from it, or they're just unbothered. Bad security practices can be to blame as well

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

The company can be using outdated systems, such as using FTP services, which are known to not be secure. This is because it is simple to use, which makes it more convenient and more likely for people to use. They could also underestimate the drawbacks of using FTP

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

FTP could have been set up with settings that would allow an anonymous to work. Employees are most likely unaware the risk of enabling an anonymous login, which can lead to serious breaches of data.