Identifying and Exploiting Vulnerabilities (3e)

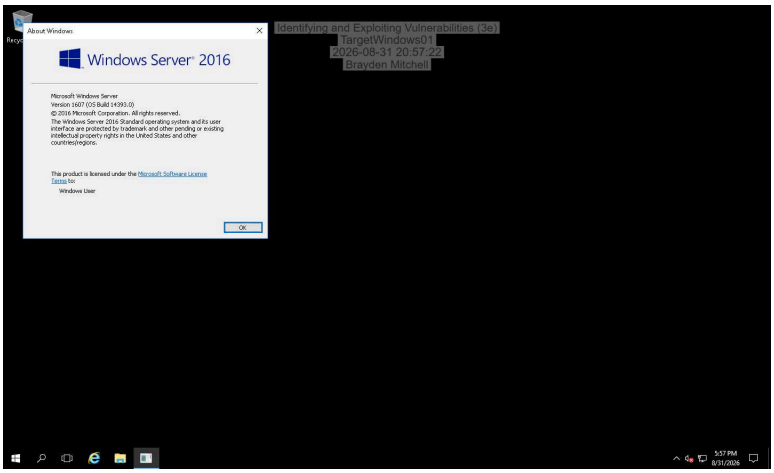
Managing Risk in Information Systems, Third Edition - Lab 01

Student: Brayden Mitchell
Email: brayden.m.mitchell@gmail.com
Time on Task: 1 hour, 16 minutes
Progress: 100%
Report Generated: Monday, August 31, 2026 at 10:08 PM

Guided Exercises

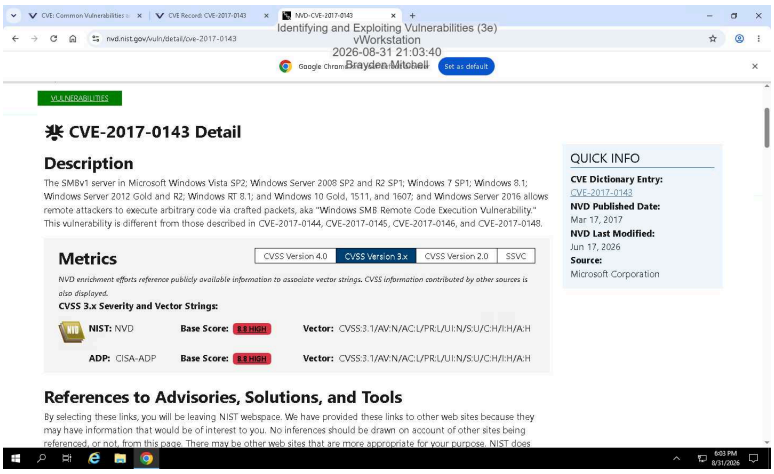
Part 1: Identify the Version and Build of a Windows System

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

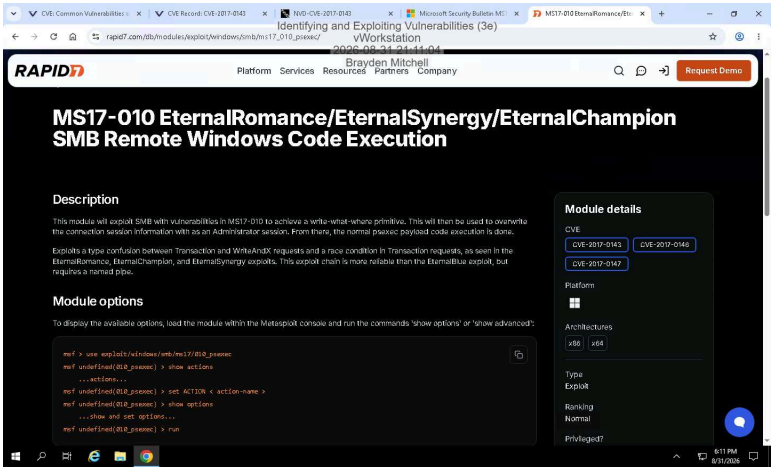


Part 2: Research and Identify Vulnerabilities and Exploits

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

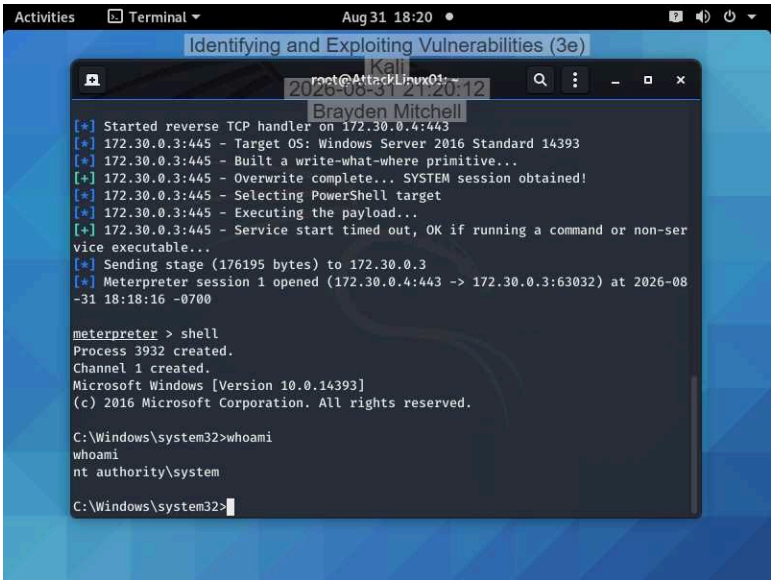


21. **Make a screen capture** showing the ***MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution*** **module in the Rapid7 Vulnerability and Exploit Database**.

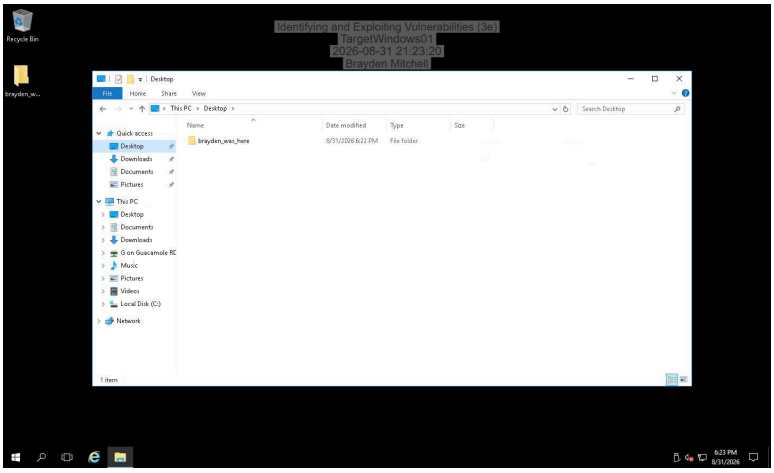


Part 3: Use the Metasploit Framework to Exploit a Vulnerability

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

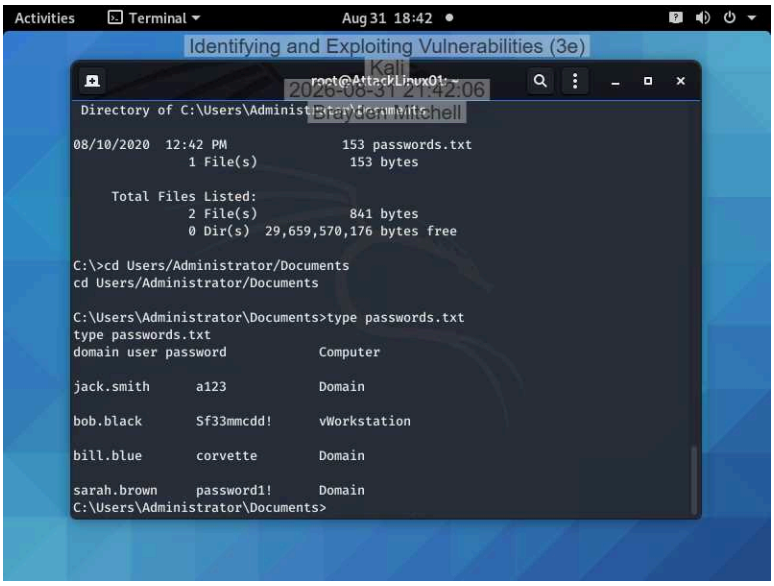


18. **Make a screen capture** showing the **TargetWindows01 Desktop and the *yourname*_was_here folder**.

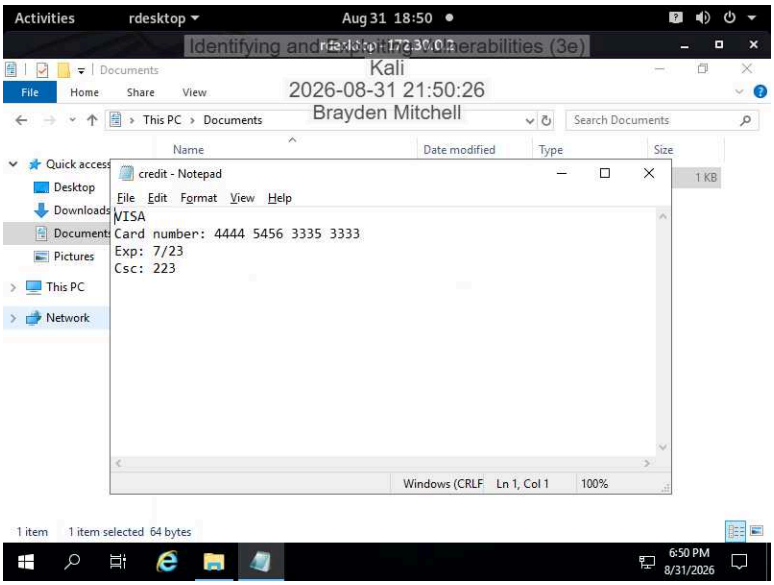


Part 4: Retrieve Sensitive Files

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



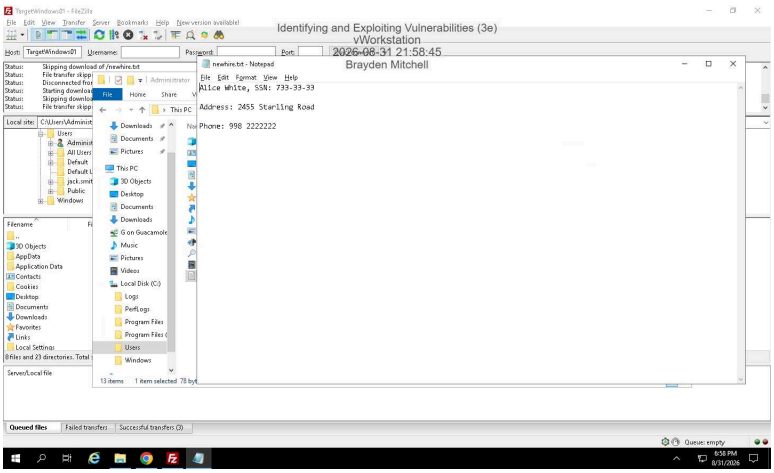
12. **Make a screen capture** showing the **contents of the file containing sensitive information**.



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?

It is easy to quickly open when someone is telling you information or in a meeting and you need to jot something down quick a text pad is often the easiest place to do it. It requires no password or special setup and you can store it in a convenient place on your computer.

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

As they say, if it ain't broke don't fix it and legacy FTP must not have been broke for ACME. I know first hand that employees don't like change so it is often easier to stick with what you have rather than changing to a new modern approach.

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

This could have been the default configuration that never got changed. It could have been a convenience factor once again. Convenience comes up a lot, security and convenience almost never go together, until they do when a system has been hacked or broke into but you were untouched or safe because of the security in place. At my job the Information Security Profesional before my boss was thrown into the position from a Construction Safety and Helicopter Pilot Position. You never know who may have setup the system and how much security knowledge they did or did not have.