

# Identifying and Exploiting Vulnerabilities (3e)

Managing Risk in Information Systems, Third Edition - Lab 01

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

4 hours, 6 minutes

Progress:

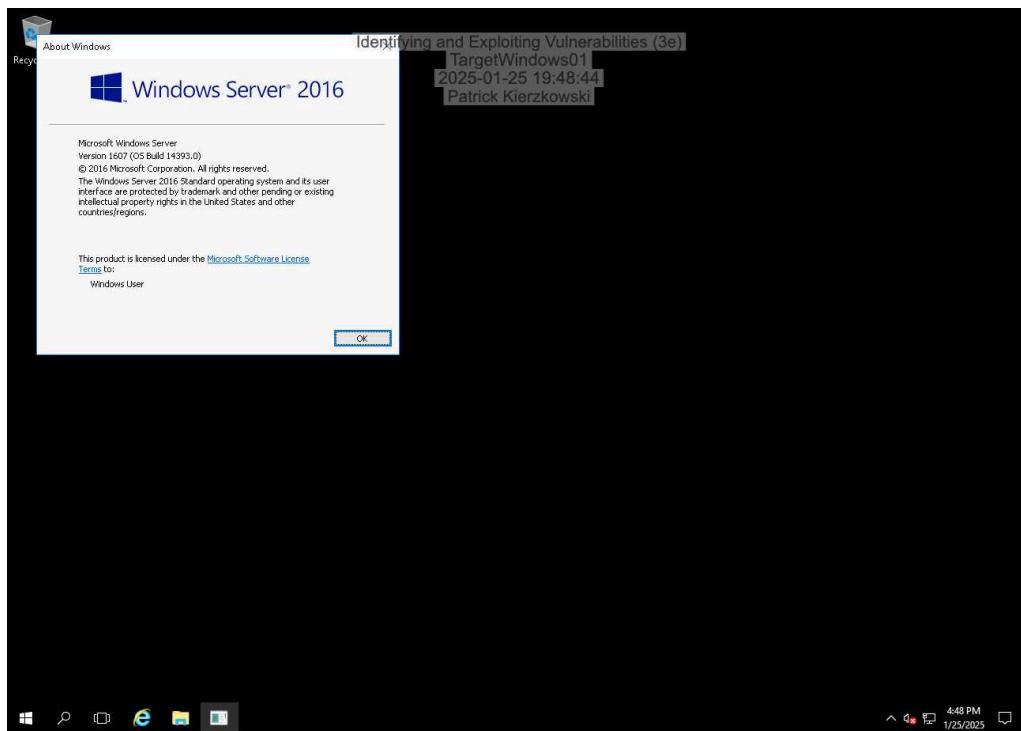
100%

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 two tabs open: 'CVE-2017-0143 | CVE' and 'NVD - CVE-2017-0143'. The main content area is titled 'Identifying and Exploiting Vulnerabilities (3e)' and 'Workstation'. It displays the following information:

This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148.

Patrick Kierzkowski

**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]

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

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
<a href="http://packetstormsecurity.com/files/154690/DOPPELPULSAR-Payload-Execution-Neutralization.html">http://packetstormsecurity.com/files/154690/DOPPELPULSAR-Payload-Execution-Neutralization.html</a>	[Exploit] [Third Party Advisory] [VDB Entry]
<a href="http://packetstormsecurity.com/files/154690/DOPPELPULSAR-Payload-Execution-Neutralization.html">http://packetstormsecurity.com/files/154690/DOPPELPULSAR-Payload-Execution-Neutralization.html</a>	[Exploit] [Third Party Advisory] [VDB Entry]
<a href="http://packetstormsecurity.com/files/156196/SMB-DOPPELPULSAR-Remote-Code-Execution.html">http://packetstormsecurity.com/files/156196/SMB-DOPPELPULSAR-Remote-Code-Execution.html</a>	[Exploit] [Third Party Advisory] [VDB Entry]
<a href="http://packetstormsecurity.com/files/156196/SMB-DOPPELPULSAR-Remote-Code-Execution.html">http://packetstormsecurity.com/files/156196/SMB-DOPPELPULSAR-Remote-Code-Execution.html</a>	[Exploit] [Third Party Advisory] [VDB Entry]
<a href="http://www.securityfocus.com/bid/96703">http://www.securityfocus.com/bid/96703</a>	[Broken Link] [Third Party Advisory] [VDB Entry]

# Identifying and Exploiting Vulnerabilities (3e)

Managing Risk in Information Systems, Third Edition - Lab 01

## 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.**

The screenshot shows a web browser displaying the Rapid7 Vulnerability and Exploit Database. The URL is [rapid7.com/db/modules/auxiliary/admin/smb/ms17\\_010\\_eternalblue](https://rapid7.com/db/modules/auxiliary/admin/smb/ms17_010_eternalblue). The page title is "Identifying and Exploiting Vulnerabilities (3e)". The module details are as follows:

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 an Administrator session. From there, the normal psexec command 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

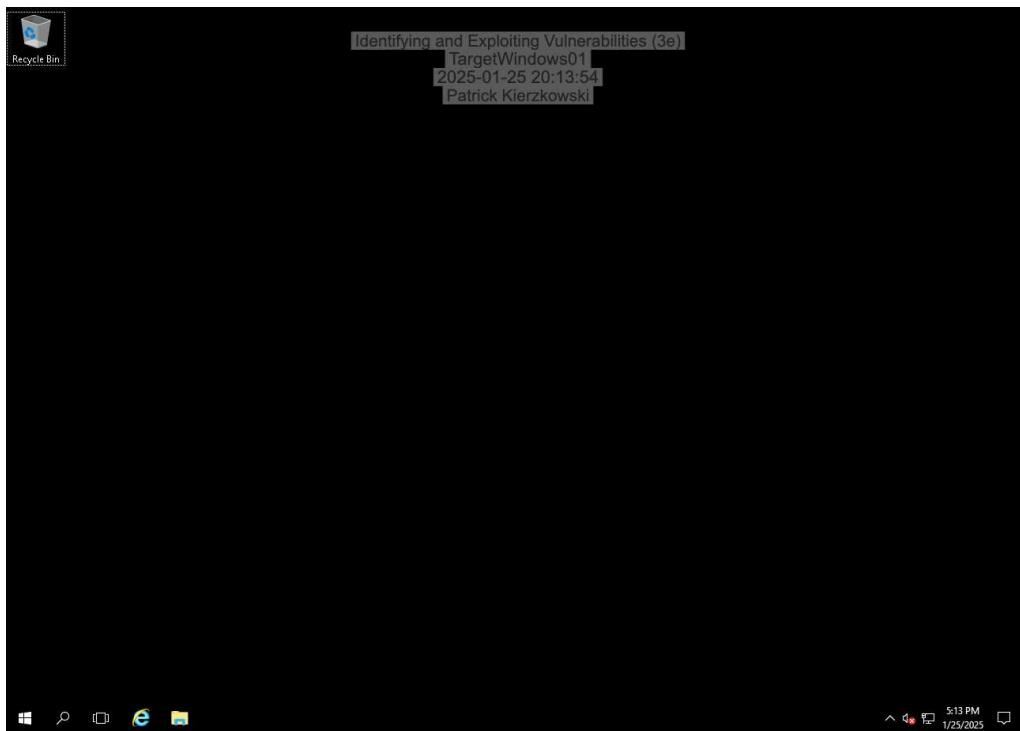
**Development**

- Source Code
- History

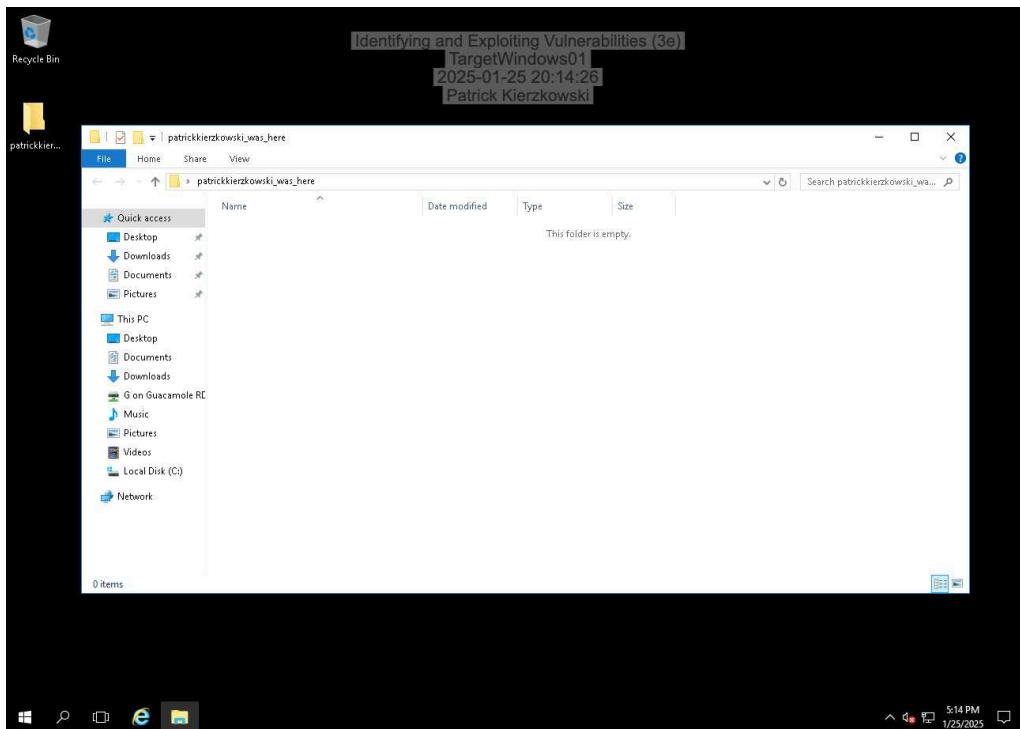
A tooltip message from a bot icon says: "Hello there! Do you want to take command of your attack surface? See Rapid7's exposure management..."

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

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

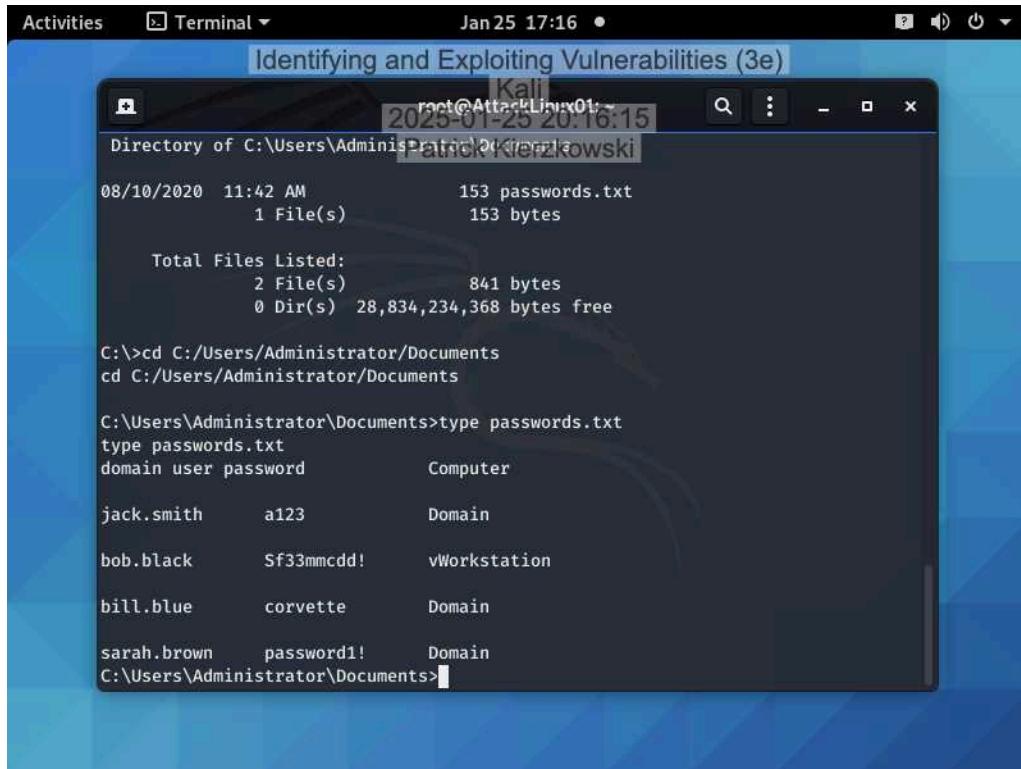


18. Make a screen capture showing the **TargetWindows01 Desktop and the *yourname\_was\_here* folder**.



## Part 4: Retrieve Sensitive Files

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



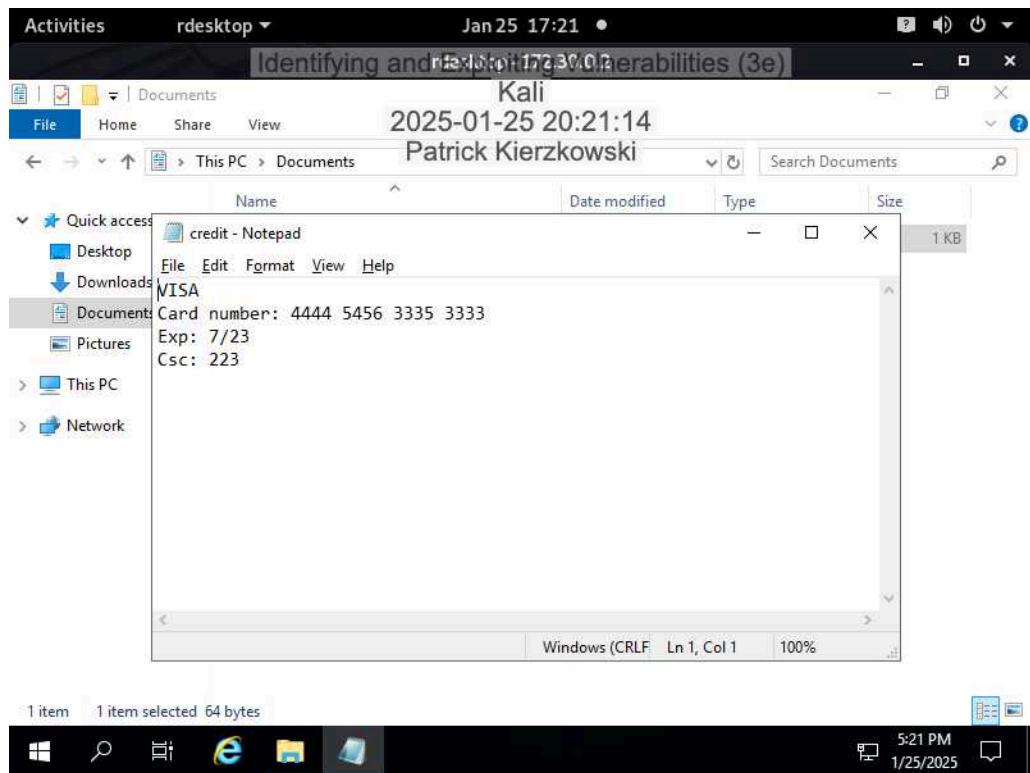
The screenshot shows a terminal window titled "Identifying and Exploiting Vulnerabilities (3e)" running on Kali Linux. The terminal displays the following output:

```
root@AttackLinux01:~# cd C:/Users/Administrator/Documents
root@AttackLinux01:~/Documents# type password.txt
password.txt
domain user password
jack.smith      a123          Domain
bob.black       SF33mmcdd!    vWorkstation
bill.blue       corvette     Domain
sarah.brown    password1!   Domain
root@AttackLinux01:~/Documents#
```

# Identifying and Exploiting Vulnerabilities (3e)

Managing Risk in Information Systems, Third Edition - Lab 01

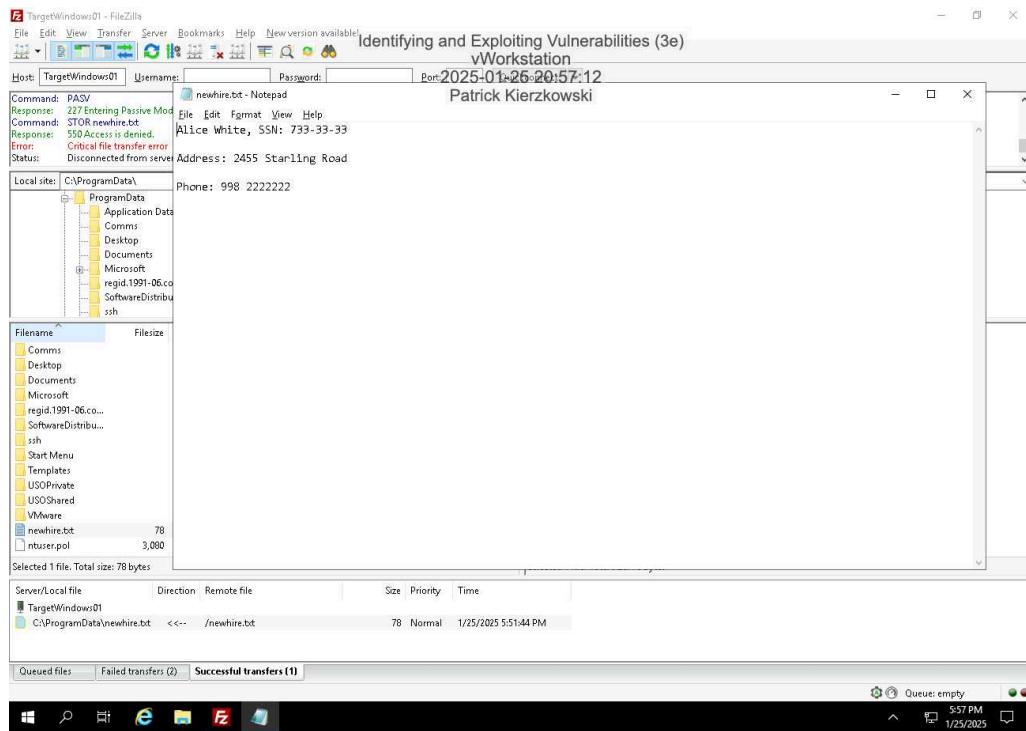
## 12. Make a screen capture showing the contents of the file containing sensitive information.



## 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

## **Identifying and Exploiting Vulnerabilities (3e)**

Managing Risk in Information Systems, Third Edition - Lab 01

---

- 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.