

OLD DOMINION UNIVERSITY

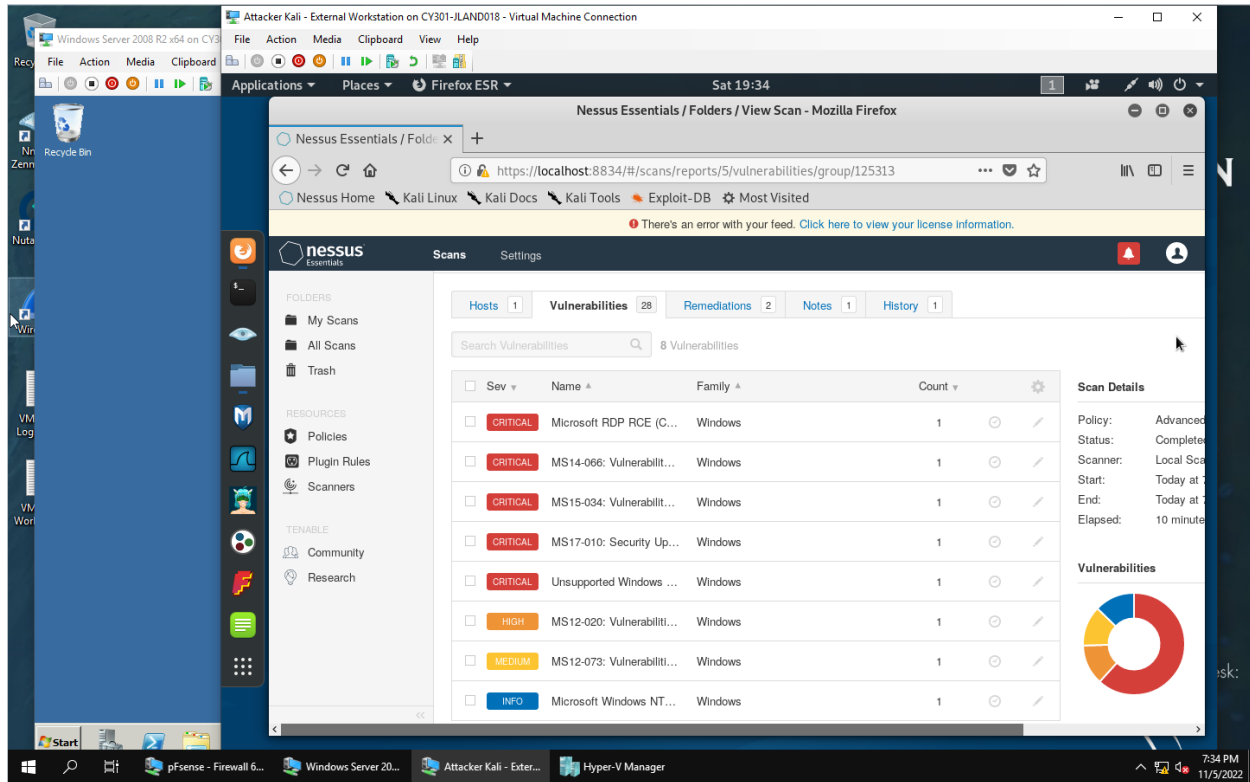
**CYSE 301 CYBERSECURITY TECHNIQUES
AND OPERATIONS**

Assignment #4 Ethical Hacking

Justin Landolina

UIN: 01214163

Task A:



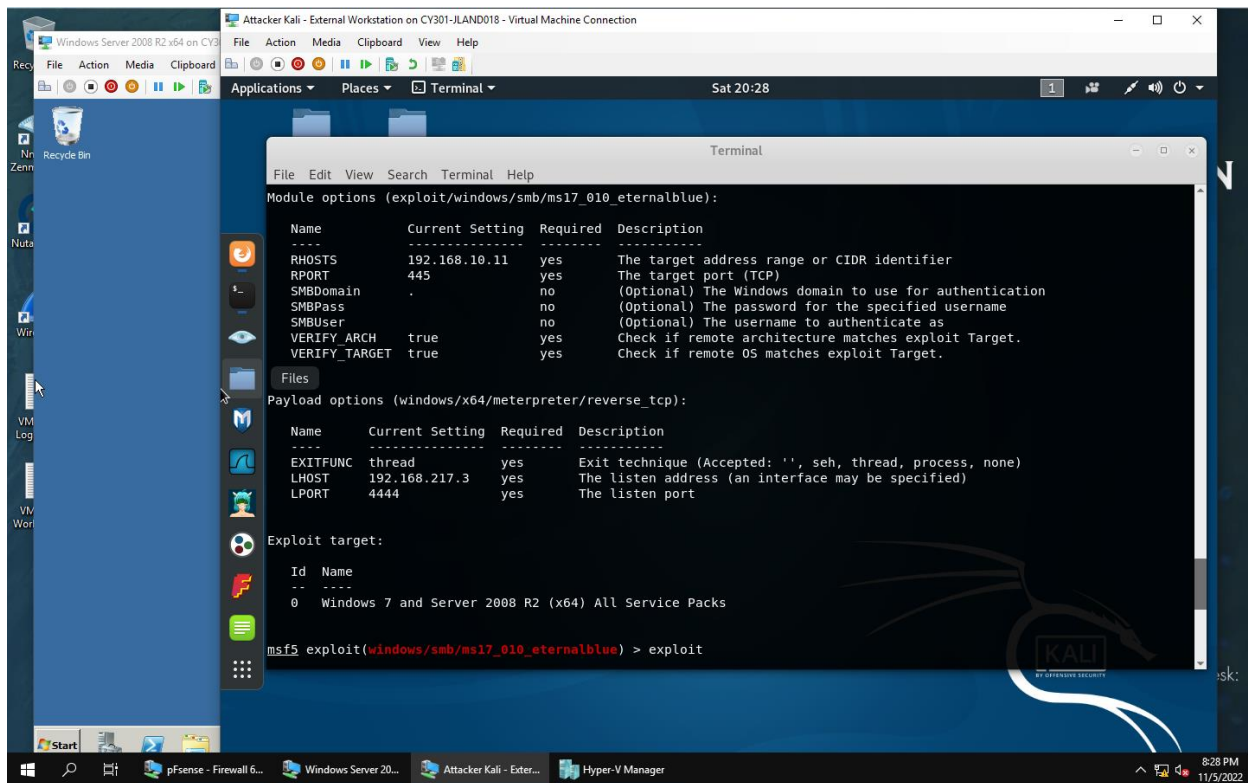
The screenshot shows a Windows Server 2008 R2 desktop environment. A Firefox browser window is open, displaying the Nessus Essentials interface. The browser's address bar shows the URL `https://localhost:8834/#/scans/reports/5/vulnerabilities/group/125313`. The Nessus Essentials interface has a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Scanners', 'Community', and 'Research'. The main content area shows a list of vulnerabilities under the 'Vulnerabilities' tab. The list includes 8 vulnerabilities, with 5 marked as 'CRITICAL'. The scan details on the right indicate the scan was completed today at 7:34 PM, took 10 minutes, and was performed by a local scanner. A donut chart shows the distribution of vulnerability severity levels: 5 Critical (red), 1 High (orange), 1 Medium (yellow), and 1 Info (blue).

Sev	Name	Family	Count
CRITICAL	Microsoft RDP RCE (C...	Windows	1
CRITICAL	MS14-066: Vulnerabliti...	Windows	1
CRITICAL	MS15-034: Vulnerabliti...	Windows	1
CRITICAL	MS17-010: Security Up...	Windows	1
CRITICAL	Unsupported Windows ...	Windows	1
HIGH	MS12-020: Vulnerabliti...	Windows	1
MEDIUM	MS12-073: Vulnerabliti...	Windows	1
INFO	Microsoft Windows NT...	Windows	1

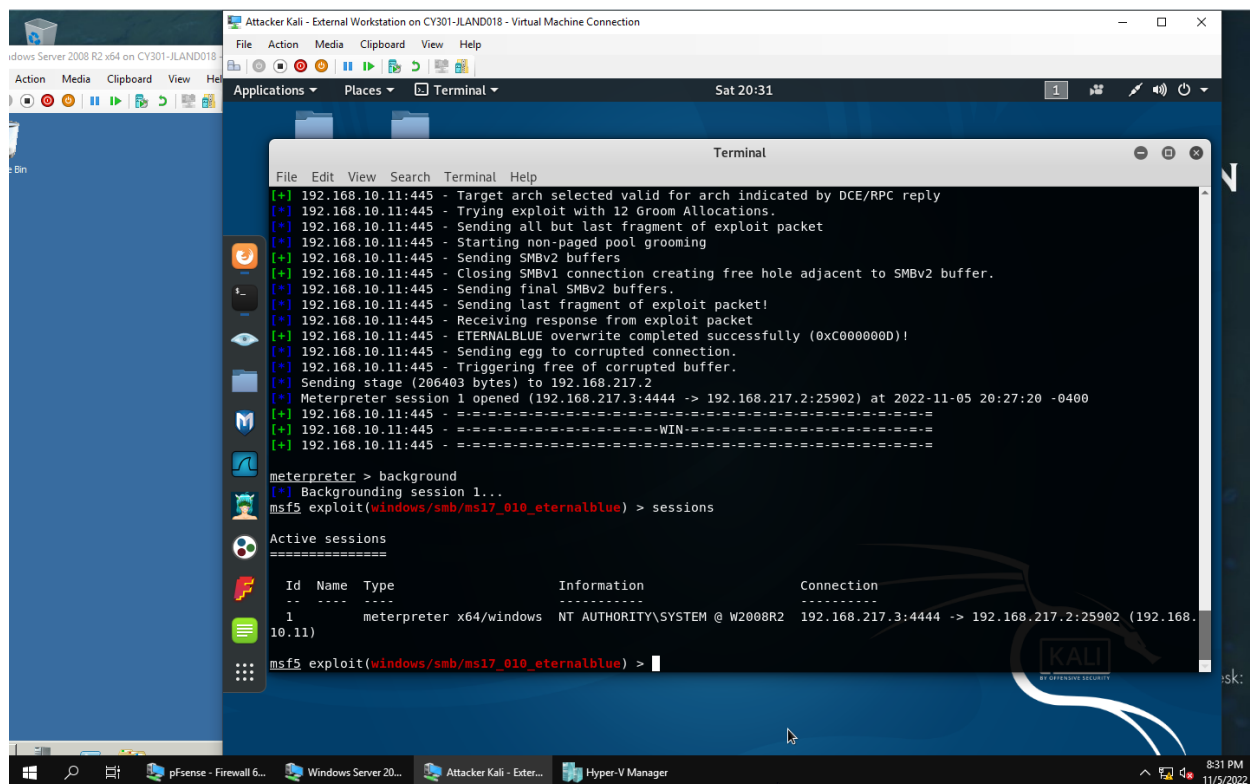
Part 1. In the above screenshot I discover the 5 critical vulnerabilities after running an advanced nessus scan.

Part 3. In the above screenshot I show the exploit I chose, oracle_reports_rce. It is one that allows for remote code execution through misconfigurations in oracle reports. Some of the configuration information is: PAYDIR (folder to download payload), RHOSTS, RPORT, SRVHOST (local host to listen on), SRVPORT (local port to listen on), SSL, and SSLCert (path to a custom SSL certificate).

Task B:

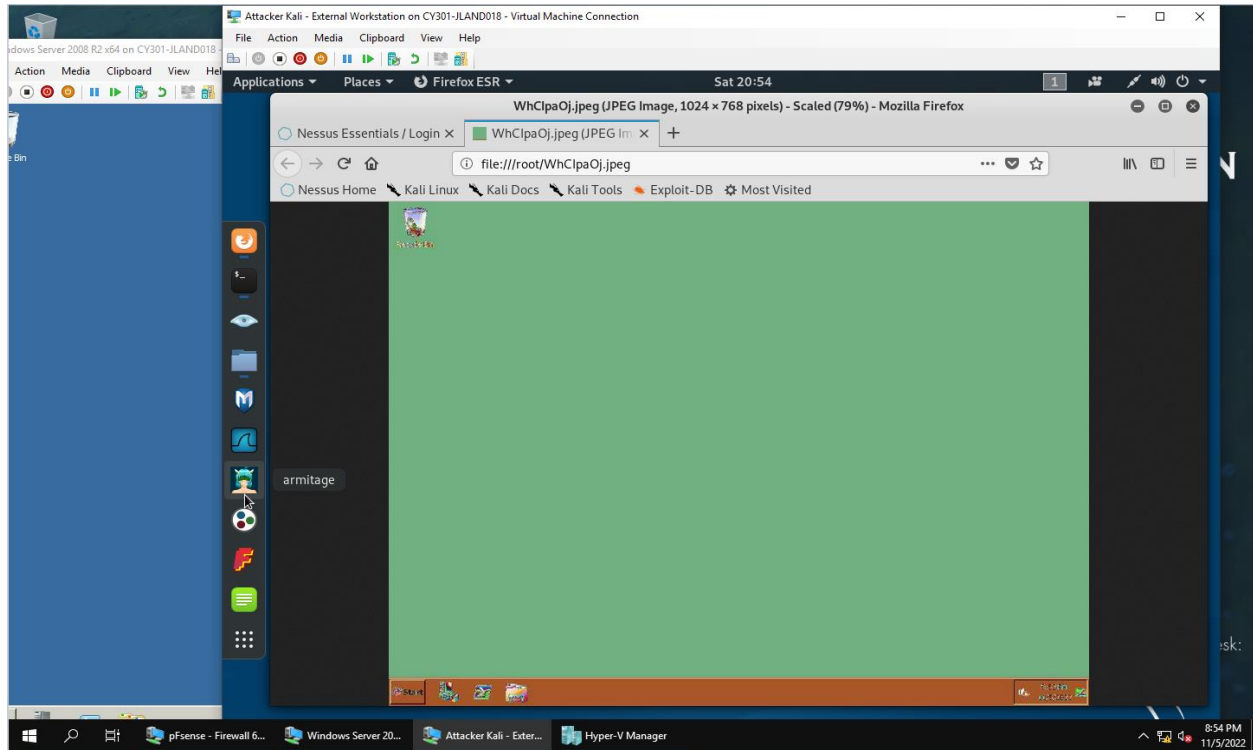


Part 1. In this screenshot I show the configuration for the ms17_010_eternalblue exploit (using a smaller port number as discussed in class).

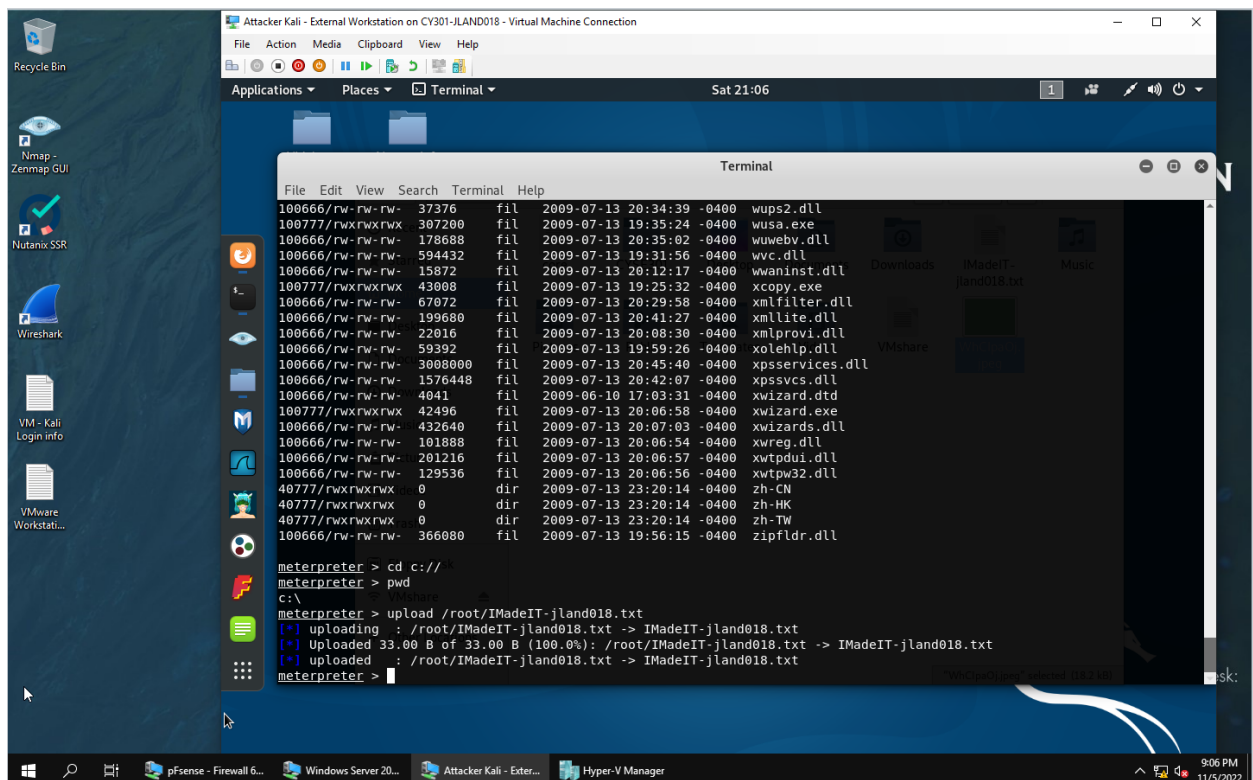


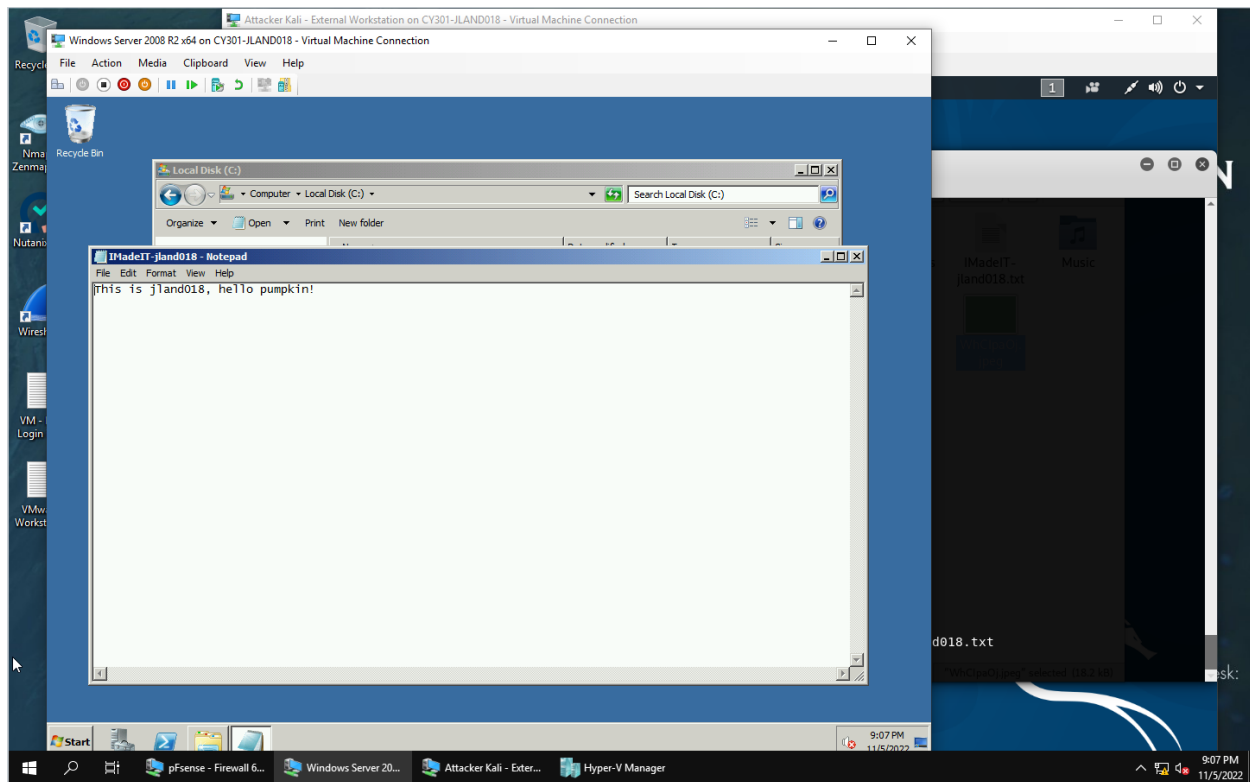
Part 2. Here I show the ms17_010_eternalblue successfully exploited the Win 2008 server and the reverse TCP session is running in the background

Task C:

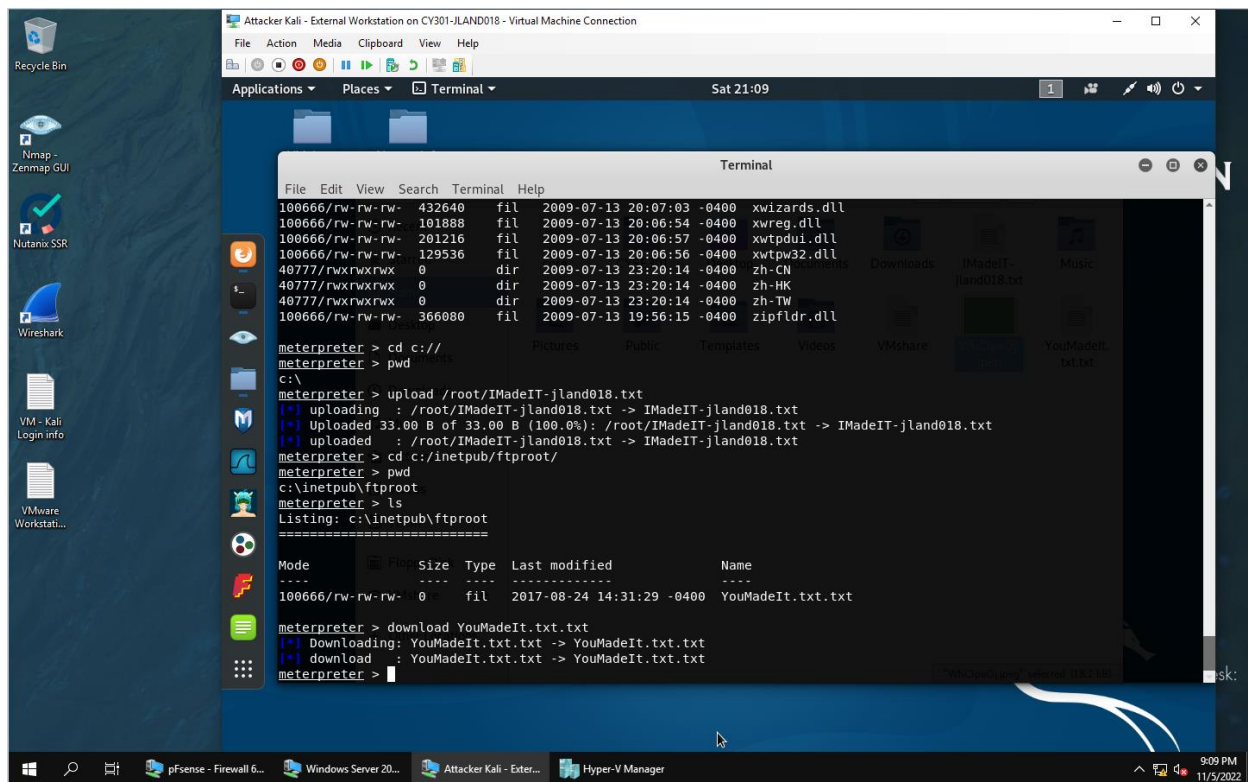


Part 1. The above screenshot shows the screengrab taken from the target Windows 2008 machine through the meterpreter shell.





Part 2. In the above two screenshots I first upload the text file I created on External Kali to the target Windows Server 2008. Then I check to see if the file exists on the Windows machine.



Part 3. This screenshot shows me use the ‘download’ meterpreter command to steal the YouMadeIt.txt file.