

Final Project

ITSC304: Operating Systems Exploitation

Table of Contents

[Project Objectives(s) 2](#_Toc473929636)

[Readings/References 2](#_Toc473929637)

[Project Requirements 2](#_Toc473929638)

[Project Instructions 3](#_Toc473929639)

The project should be submitted in week 15 during exam week. It can be completed in groups of maximum of two students. The final document should be a pdf with requested screen captures, reports and references.

I certify that the work submitted in this assignment is my own and that it has not been taken in whole or in part from any other source. I understand that the penalty for plagiarism will include a grade of zero (0) for this assignment plus disciplinary action in accordance with SAIT policies.

**EVALUATION**

|  |  |  |
| --- | --- | --- |
| Setup and connect vulnerable machines (targets) | 5 |  |
| Vulnerability Assessment – Nessus | 25 |  |
| Exploitation, Post-exploitation, Attack | 20 |  |
| Report | 10 |  |
| TOTAL MARK | 60 |  |

Final Project Objectives

* Assess vulnerabilities
* Exploit and post-exploit Windows and Linux target systems
* Implement an attack from Mitre@attack framework
* Generate reports

Reading and References

* Vulnerable machines <https://github.com/rapid7/metasploitable3>
* <https://www.vulnhub.com/resources/>
* Vulnerability Assessment Nessus <https://www.tenable.com/> or OpenVAS <https://www.openvas.org/#about>
* Attacks Framework <https://attack.mitre.org/>
* Pentest Reports <http://www.pentest-standard.org/index.php/Reporting>
* <https://www.pentesteracademy.com/>

Requirements

1. Virtualbox or VMware
2. Virtual Kali , Windows and Linux machines

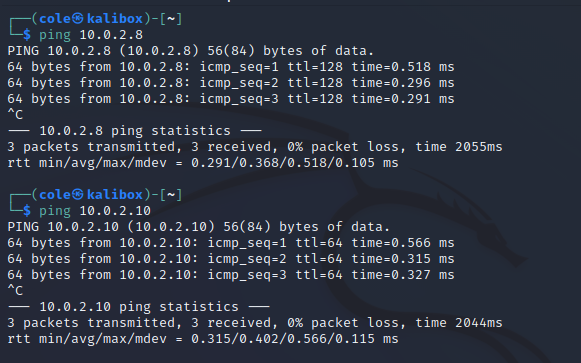
**Project Instructions**

**I. ( 5 marks)** **Setup and connect 3 virtual machines**. Kali virtual machine, the attacker and two victim machines (Windows and Linux). You can use virtual machines used in the Labs or download Metasploitable machines from github such as:

<https://github.com/rapid7/metasploitable3> or

<https://www.offensive-security.com/metasploit-unleashed/requirements/>.

Make sure the target machines are vulnerable (critical and high)



**II. (25 marks) Vulnerability Assessment.** The commercial vulnerability scanner most widely used by the industry is Nessus

1. Install Nessus Essentials (free version)

1. Access the web site: <https://www.tenable.com/products/nessus/nessus-essentials>
2. Register providing your email account to get the activation code
3. Click on Download and browse it to identify the version for the respective OS we want to install it in this case for kali 64 bit should be Nessus-8.12.1\_debian6\_amd64.deb
4. Accept the license
5. Install the package .deb using the following command:

dpkg –i Nessus-8.12.1-debian6\_amd64.deb

1. It will take few seconds. Read the instructions on how to start the service and access it
2. Start the service: /bin/systemctl start.service and use ps command to verify if the service nessusd is running
3. To access it open a browser and use URL: https://localhost:8834/
4. For certificate click on Advanced and Accept the Risk and Continue
5. Install Nessus Essentials and Register. If you already registered then skip it and provide the activation code you got via e-mail
6. Create a user account and password
7. Enter the activation code when requested
8. It will validate the code and initialize compiling plugins. Depending of your network speed it may take an hour to compile plugins

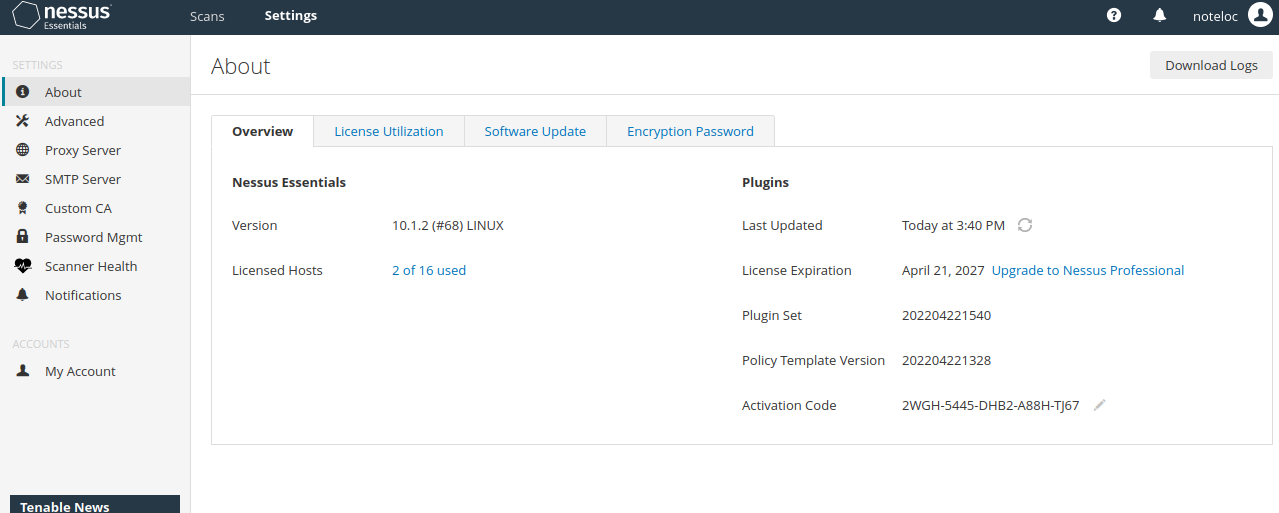
**Note:** Make sure nessusd service is running when accessing Nessus, otherwise will not work

1. After installation is completed use [https://localhost:8834/#](https://localhost:8834/)/ to login. After few minutes of initialization you should see a login screen. Use the login credentials you created before
2. Explore Settings to verify Nessus Essentials settings such as: License Utilization, Software Updates, Advanced settings, Scanner Health (Check Network, Alerts), Password Management. This version has limited functionality. Explore your Account settings. You can change the password or generate PKI keys
3. Explore Scans Folders and Resources. Under My Scans Folder create two scans one for Windows and one for Linux target machines
4. Under My Scans click on **Host Discovery** and configure the respective settings to scan target machines
5. Under Discovery select type of scan e.g. Host Enumeration or Port Scan. Perform two different types of scan
6. Schedule one of the scans
7. Configure the setting for report output.
8. Configure Advanced options if necessary
9. Provide target IP address or subnet to scan
10. Scan the target machines –Launch or wait for configured schedule time
11. Verify Host, Vulnerabilities detected and History
12. Generate a Custom CSV report for each scan for each target and analyze the results. Explain how these reports can be useful for you. Provide the most important information of the reports that you can use for analysis.
13. Nessus’s policy wizards will help you to create policy that will be useful for scanning. Under resources explore Policies templates and create a new Advanced Scan policy for each target machine.
14. For each policy configure the Basic settings, Host, Port Scanning and Service Discovery.
15. Under Assessment configure General and Windows settings for Windows target and for Linux target you can try brute force.
16. Configure report settings and if required Advanced options
17. Explore Credentials categories and configure Host credentials SSH for Linux and Windows for Windows target. Explore Authentication methods and select password. Provide the username and password for authentication
18. Explore Plugins and select the plugins for respective operating systems. Click on Plugin Family to select the respective plugins for each target. To disable plugins that are not required click on status (ENABLE)
19. Once the policies are created. Click on scan Templates > User Define and provide targets IP address or subnet. Now you can launch or implement the policy on selected targets and capture results
20. Select or click on a critical or high vulnerability for each target machine (windows and Linux) and read the details (Description, Plugins details, Risk, Vulnerability and reference information, solution and output) of the vulnerability and use that information to investigate more about this vulnerability. You can also access <https://cve.mitre.org/> or <https://www.exploit-db.com/> or <https://nvd.nist.gov/>

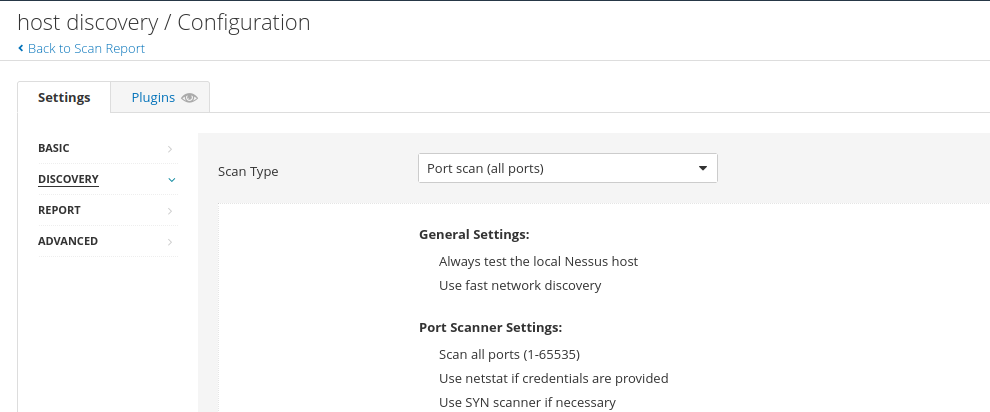
to find more information about the vulnerability. Provide remediation(s) of

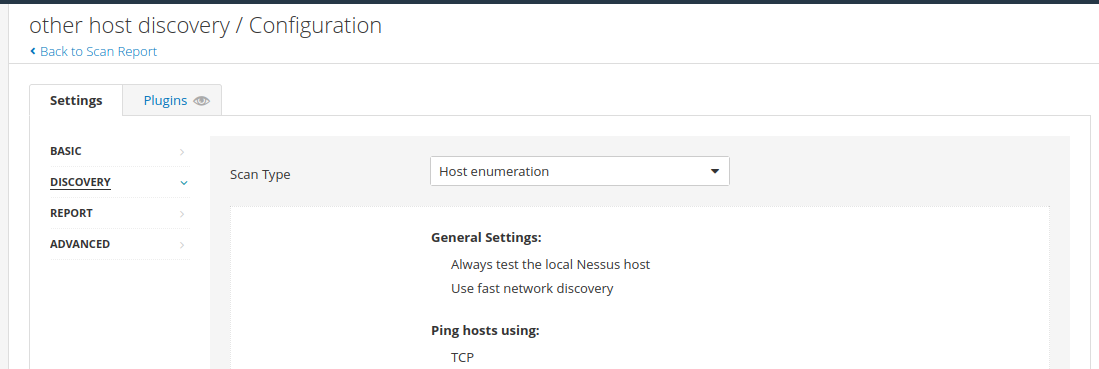
vulnerabilities selected

1. Generate Executive and Custom pdf reports for each target machine
2. Create a second policy on your own choice. Configure and implement it for each target
3. Provide screen captures that demonstrates:
4. ( 2 marks) Nessus installed and explored settings

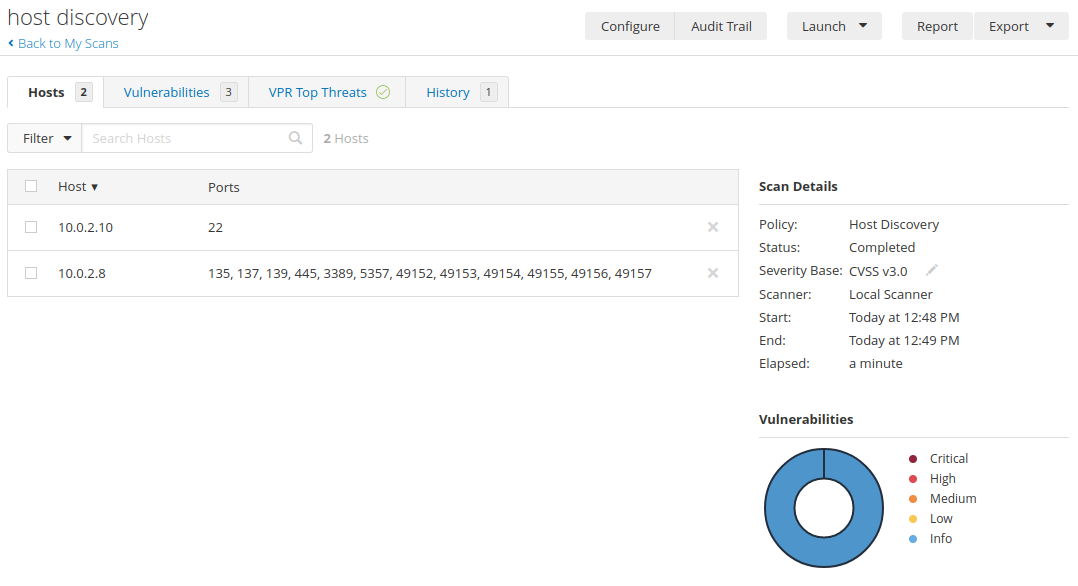


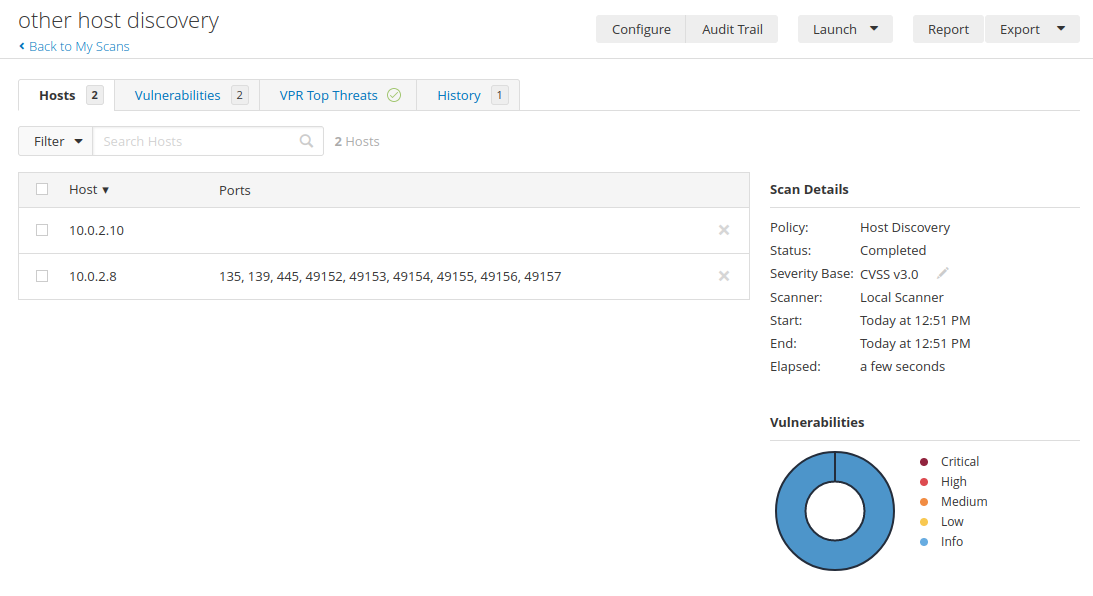
1. ( 2 marks) Configuration of two scans: for Windows and Linux





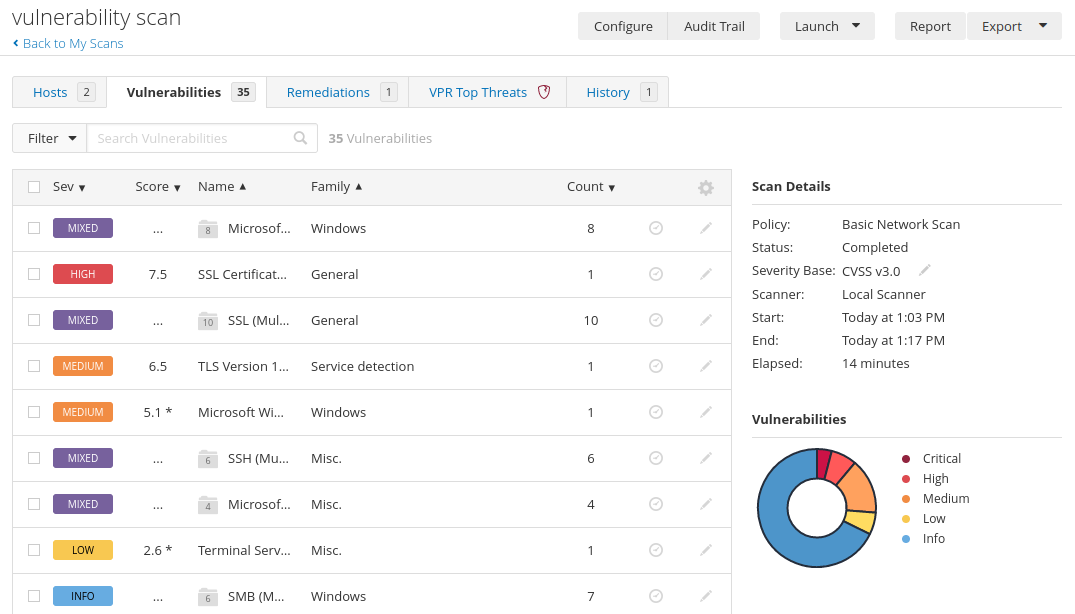
1. ( 2 marks) Results of scanning Windows and Linux target machines

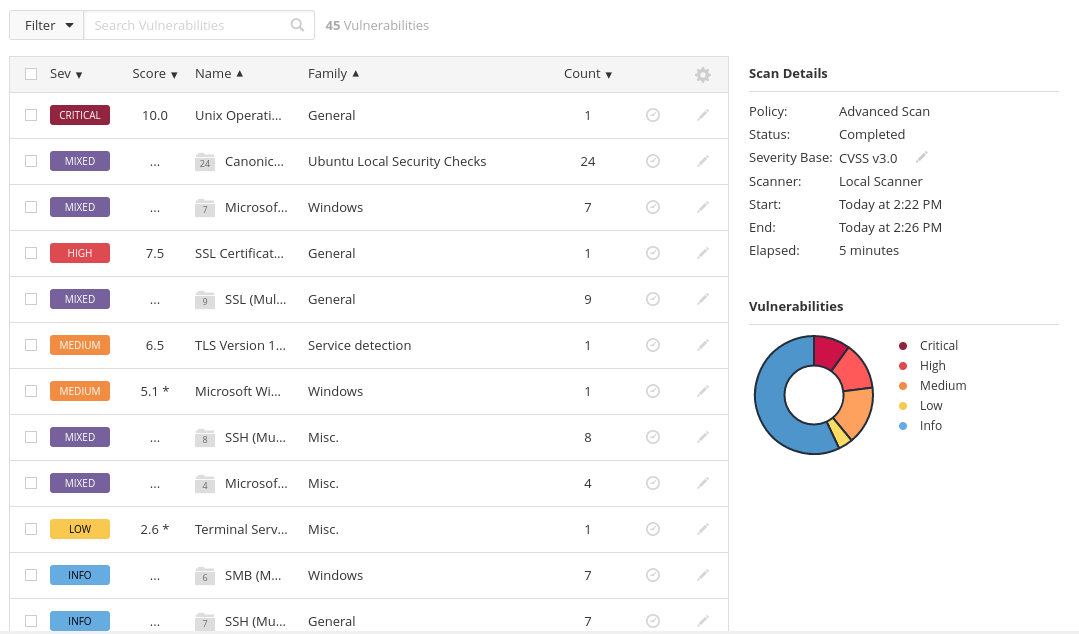




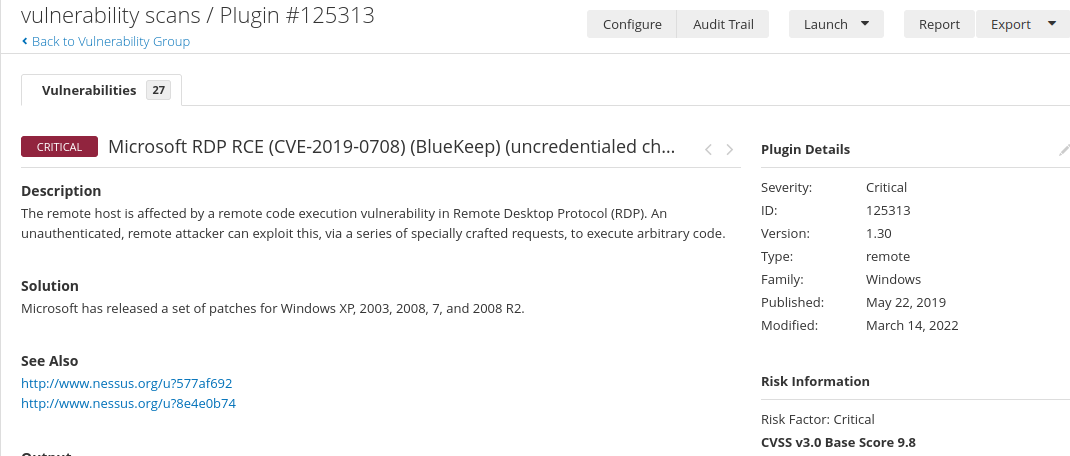
1. ( 2 marks) List of vulnerabilities detected in each target machine

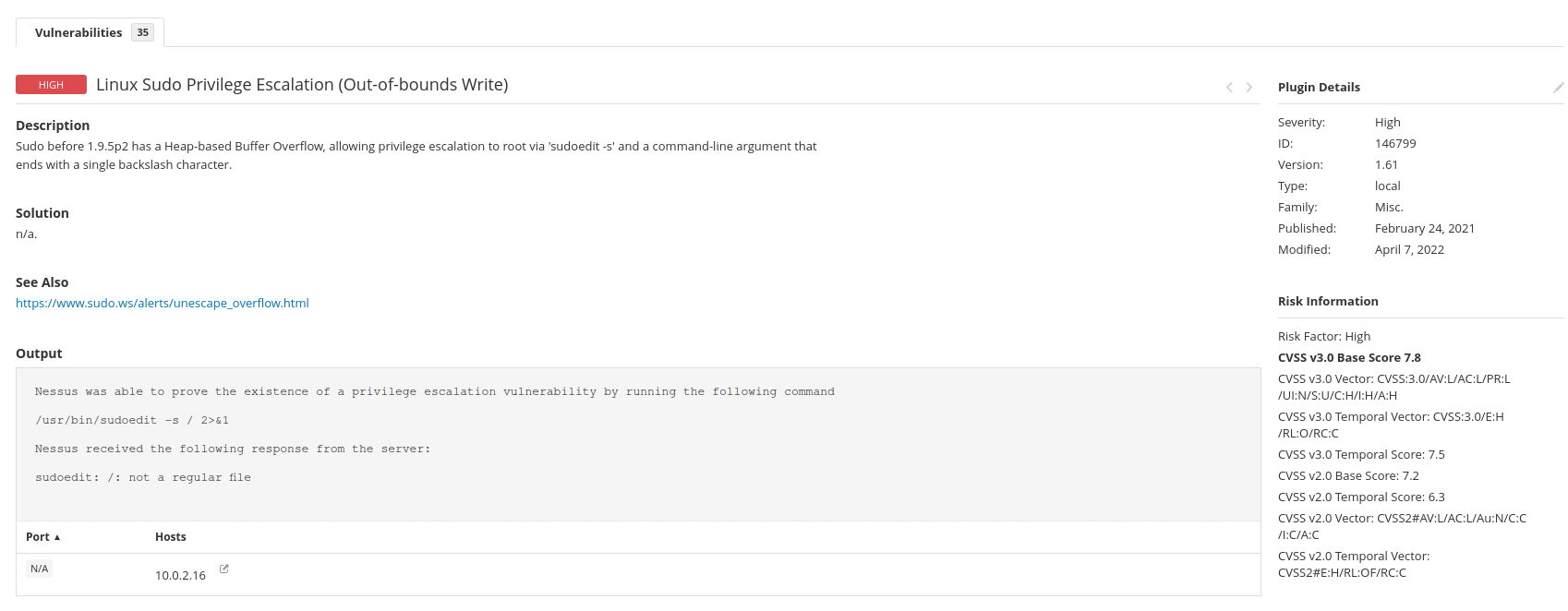
SEE ATTACHED DOCUMENTS – cvs1 & cvs2



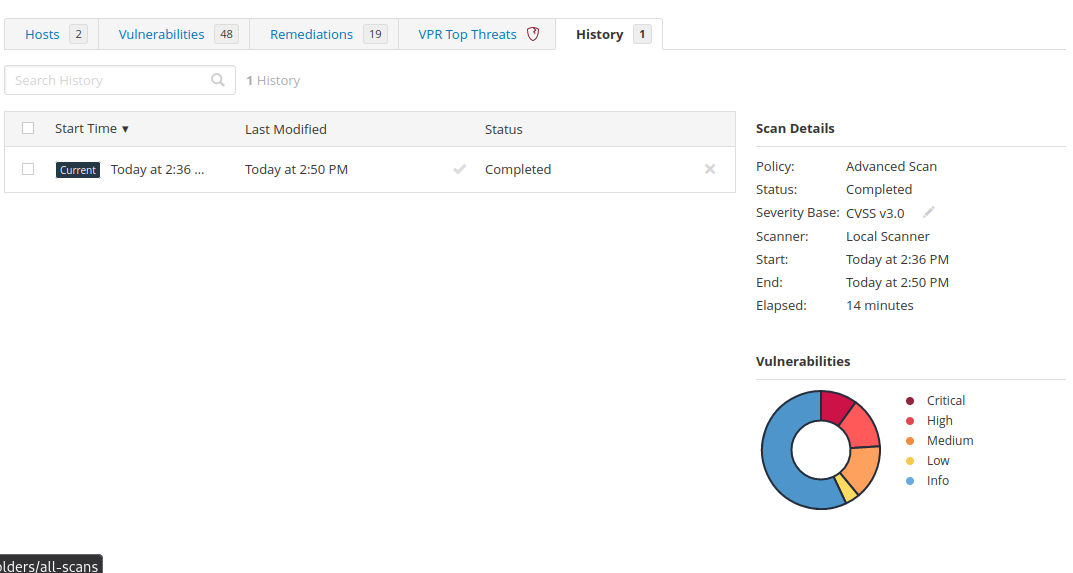


1. ( 4 marks) Details of selected critical or high vulnerabilities in each target machine and provided vulnerabilities remediation(s)

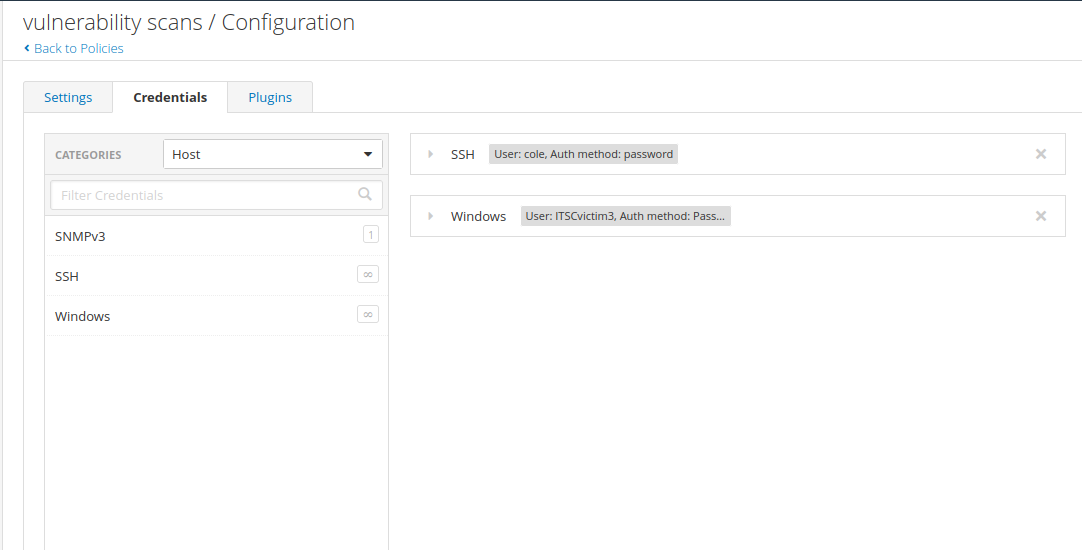


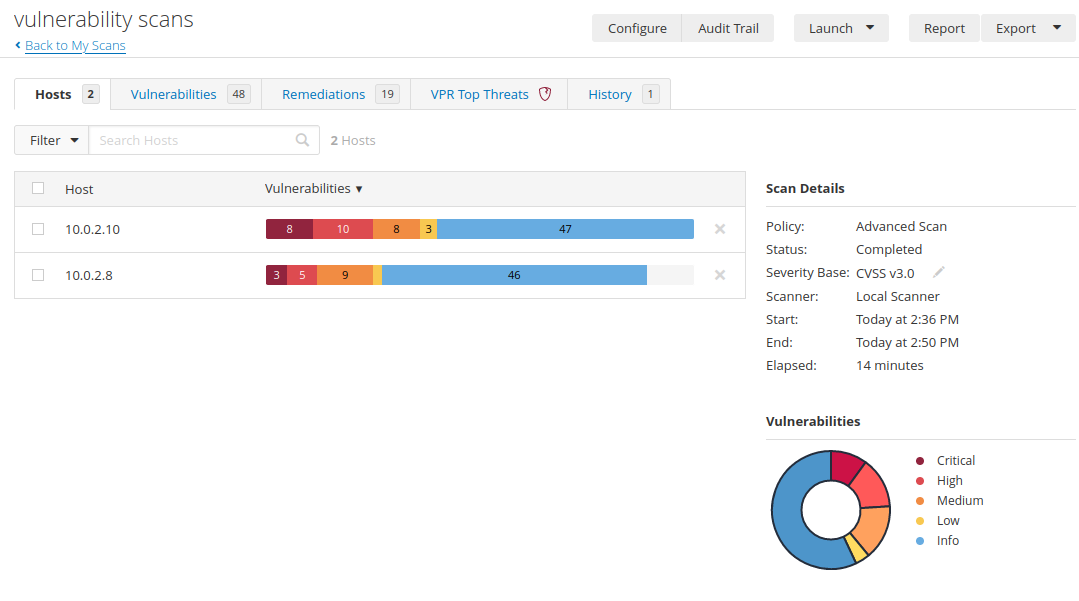


1. ( 2 marks) History screen after completing scanning targets

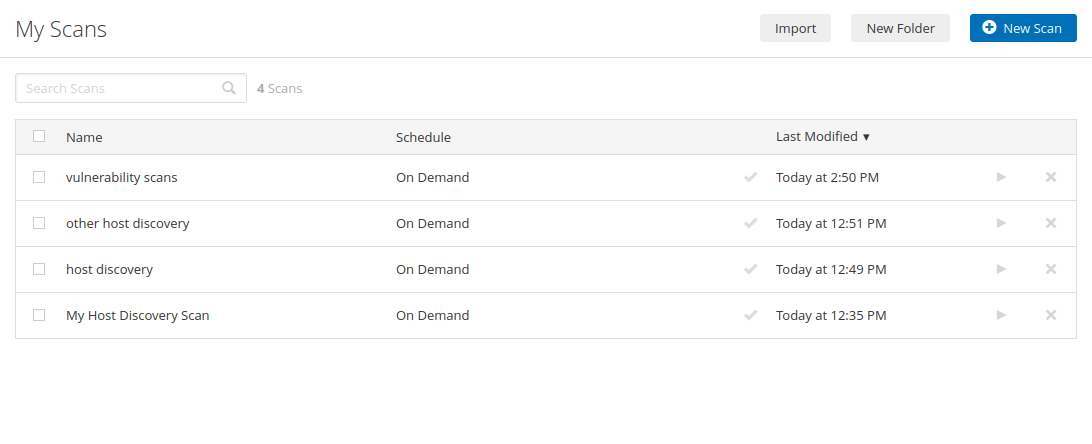


1. ( 5 marks) Two policies implemented (Advanced Scan and the one you selected) in each target machine and respective results





1. ( 2 marks) All scans you performed (My Scans screen)



1. ( 4 marks) Attach one Executive Summary pdf report and one Custom pdf report for each target machine and underline important areas to focus for analysis.

SEE ATTACHED DOCUMENT – vuln.pdf – ALL PDFS COMBINED INTO ONE

**III. (20 marks) Exploitation and Post-Exploitation**

1. Implement one Attack from framework attacks

Mitre Att@ck is one of the most complete frameworks used by Red and Blue Teams. It contains tactics/techniques attackers use before exploiting a target system. Based on gathered information and vulnerability assessment reports for Windows and Linux target machines use an attack framework such as <https://attack.mitre.org/> to identify and implement one technique (attack) in each target machine.

e.g. <https://attack.mitre.org/techniques/T1068/> or <https://attack.mitre.org/techniques/T1210/> or <https://attack.mitre.org/techniques/T1212/>

Another resource for Red Team in this Att@ck framework is the Group Directory that contains a list of known hacker group with the tools and techniques used to infiltrate their targets

Provide selected attack details and detailed reason for this selection

<https://attack.mitre.org/techniques/T1021/001/>

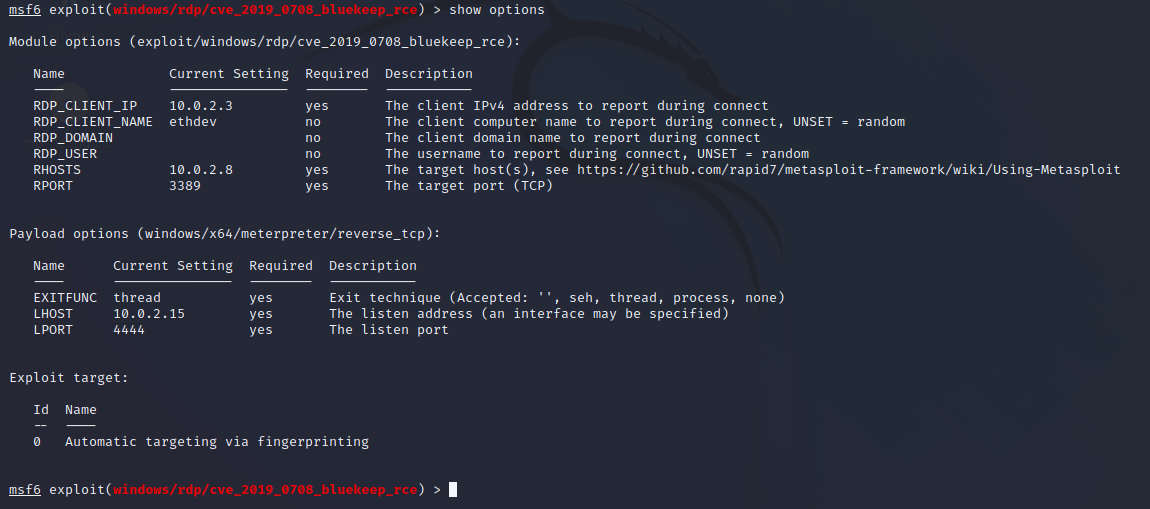
For exploitation of the windows machine this is a remote code execution attack for windows. It is a critical vulnerability and seems simple to exploit. For the post-exploitation I chose to use meterpreter post exploitation.

<https://attack.mitre.org/techniques/T1548/003/>

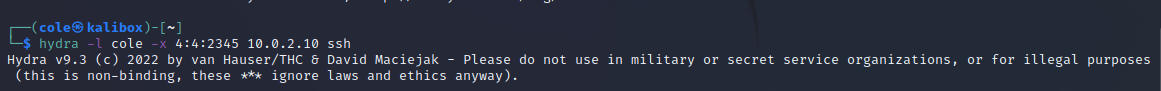
For the exploitation of the Ubuntu machine, even though this is vulnerable machine there wasn’t any exploits found, so I chose to use Hydra to bruteforce into ssh. For post-exploitation I chose a privilege escalation attack for Linux. I chose this as it was the only high/critical vulnerability to be found that I believe can be exploited given our scope.

1. After identifying the techniques to implement, use tools and techniques learnt and Metasploit to exploit each target machine and perform post-exploitation.
2. Provide screen captures that demonstrates:
   1. ( 5 marks) Technique implemented to exploit vulnerabilities in each target machine

Windows

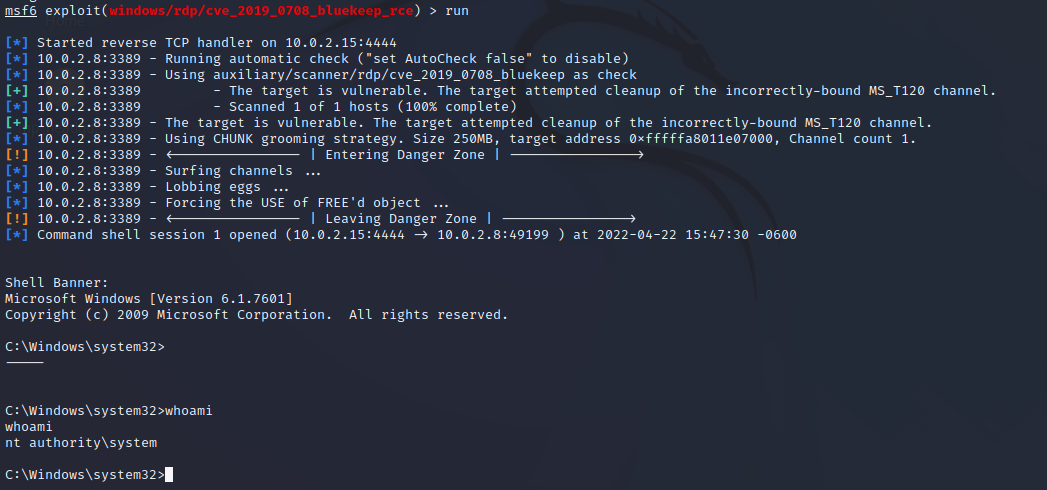


Linux

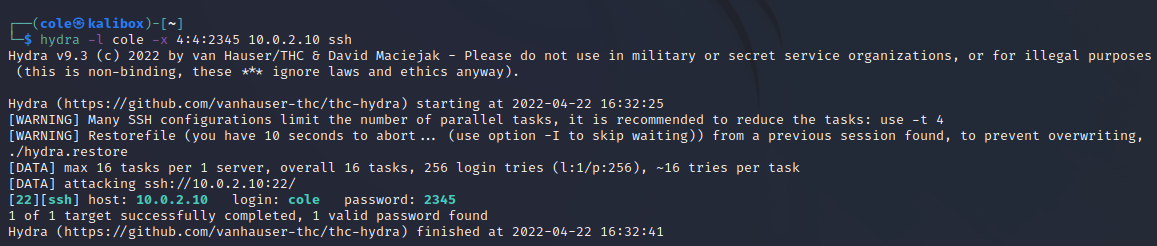


* 1. ( 5 marks) Exploitation results (compromised target machines)

Windows



Linux

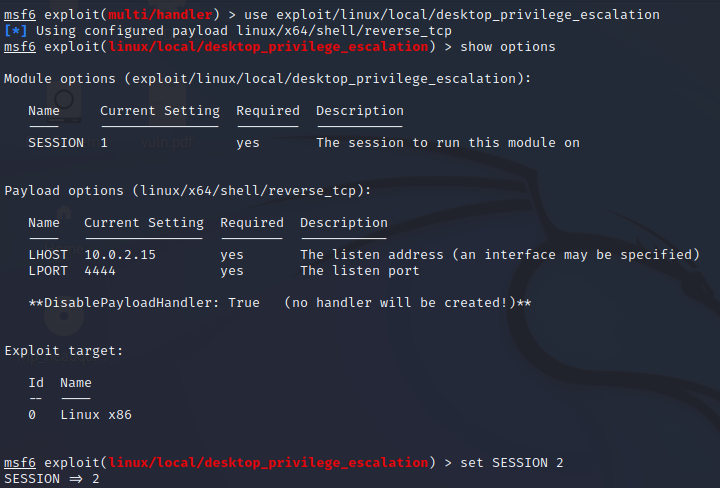


* 1. ( 5 marks) Technique implemented for post-exploitation in each target machine

Windows

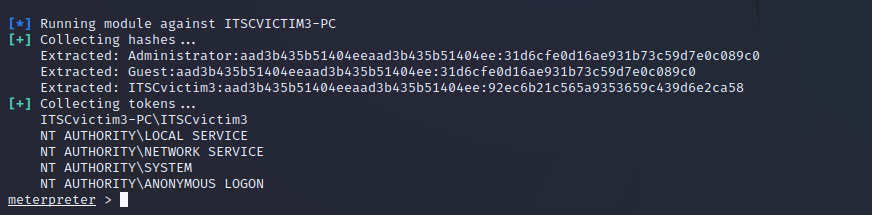


Linux

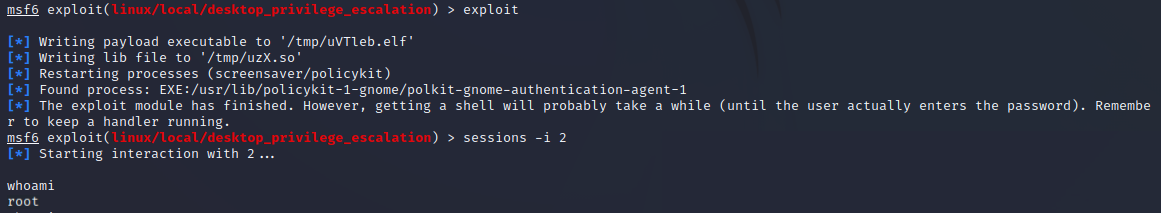


* 1. ( 5 marks) Post-exploitation results

Windows



Linux



**IV. (10 marks) Create a technical report**

1. Used gathered information, vulnerability assessment reports , Mitre Att@ck framework information and the following report reference <http://www.pentest-standard.org/index.php/Reporting> to create a technical report that contains the following sections:
   1. Introduction
   2. Information gathering
   3. Vulnerability assessment
   4. Exploitation/Vulnerability confirmation
   5. Post-Exploitation
   6. Conclusion
2. Upload technical reports with project results to D2L

**See attached document – report.docx**