**Project Name: Vulnerability Exploitation**

**Technology: Metasploit**

**Market: Security**

**Name / Group: Gagneet S**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Potential Providers:**

Metasploit

Metasploitable Linux

**Intended Activities:**

Installation of Vulnerability Exploitation tool / suite.

Exploitation of a Host that You have access to AND the authorization to exploit (Metasploitable Linux).

Development of a report that details your actions taken to exploit the targeted vulnerability.

**Design:**

The goal of this lab is to begin to become familiar with exploiting vulnerabilities on hosts / network devices. In order to do so, we must become accustomed to installing and updating our vulnerability exploitation tools. Even if people have been working systems for a long period of time, they will notice changes in the evolution of systems over the years.

**Directions:**

Answer the questions below in preparation for the practical portion of your lab (in Section 3).

**Questions to Answer:**

**Section 0: Vulnerability Basics**

Explain the following terms:

Vulnerability - This is a weakness in system that can be exploited. Attackers can use

tools/techniques to gain unauthorized access of the system.

Exploit - A piece of software part of some data, or a series of commands that will take

advantage of a vulnerability. This often ends with gaining control of a system, but that is

not always the intended result.

Common Vulnerability and Exposure (CVE) - this a a public knowledge base of know

vulnerabilities and exposures. Each of these are given unique identifier for easier

research when an CVE is come across.

Private Exploit - An exploit that is discovered, but kept private. This prevents the exploit from

being patched and allows those with knowledge of it the exploit to take advantage of it.

Payload – this a script or malicious code used to take advantage on a hacked system. The most common use would be to transfer data two or from the hacked system.

**Section 1: Vulnerability Exploitation**

What is the difference between the following:

Nmap: a network mapping tool used to gain information about a network. This could be something on the same LAN or a completely unrelated network. It is great for giving detail such as open/closed ports, connected devices, and even firewall details. The level of information provided is limited by the level of access on the network being scanned.

Openvas: A vulnerability scanner tool. It allows for the scanning of a device to check it for known vulnerabilities. This could range from the OS not being up to date to bugs in software that allow for know exploits.

Metasploit – An exploit tool. This is takes advantages of vulnerabilities with known exploits

How does a vulnerability exploitation tool (like Metasploit) work?

These types of tools work by using known exploits of vulnerabilities. They allow for a slight autonomation of the exploitation process. You can set a target, choose parameters of the exploits and run it with the tool like Metasploit. This eliminates the need to write your script or have to reinvent the wheel.

How do these tools stay current?

These tools stay current through a combination of community and industry support

Does it seem logical to depend on a single well known tool?

Like most things in life, its best to choose the right tool for the job when possible. Metasploit is great for when it has a way to exploit the a system, but provides little use when it doesn’t. Other tools may work better, or a custom tool or script may be needed to reach the desired end goal.

**Section 2: Vulnerability Exploitation**

Vulnerability Exploitation tools provide a means of consolidating several tools into one typically offering a greater degree of usability and integration than using various tools in isolation. As with anything the abstractions that are offered by consolidated tools can both constrict options and increase tool usability. At the same time, the traditional options of the underlying tools are mostly available in the command line user interface of the meta tool.

What is the context of vulnerability exploration tools?

They are designed to give insight into the security and potential points of failure/exploitation. On their own, they are neither malicious are good.

Said differently, how are such tools used within an organization?

They are used for assessing the security vulnerabilities of an organization and developing strategies to either patch them or create a plan to detail with potential breaches.

How would you go about providing these exploitation details to a given IT team in order to inform them of the work that they need to carryout.

First and foremost is written permission with a detailed scope to protect yourself. Within this scope, you should provide the tools used, the vulnerabilities found, and a risk assessment of them. In addition, you could provide potential solutions as well. Something to note is that some vulnerabilities and risks may be considered acceptable. A camera system may be running on an outdated but denied all external traffic and have heavy limitations on internal traffic. This is a vulnerable system, but it would have lower risk and lower priority of getting dealt with than say it was able to access public networks.

How do organizations stay current (with regard to keeping abreast of vulnerabilities within their infrastructure)? (Hint: Automation)

Automation is a large way to stay current with ensuring systems are automatically patched and with security systems receiving frequent updates to threats. Another way in with internal and external audits. This comes in the form of pen-testing and assessing systems.

**Section 3: Practical**

Installation your chosen Vulnerability Exploitation Suite / Tool.

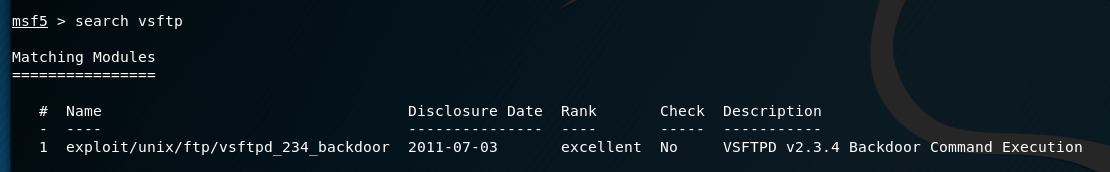
Assess a host that you have available AND have the authorization to exploit (i.e. a VM for CYB 201).

Develop a report demonstrates your exploit (include a write-up with screenshots).

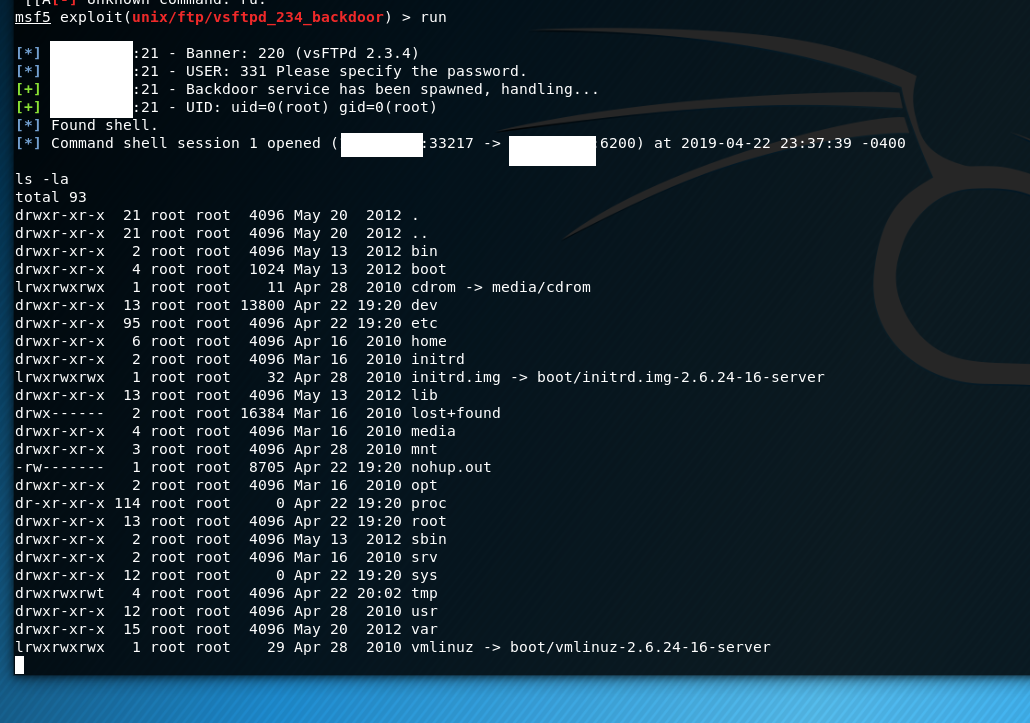
I chose to create a home lab and exploit a Metasploitable VM. To start, Openvas was used to scan the system for vulnerabilities. These vulnerabilities were checked against known exploits of Metasploit.



The above vulnerabilities were chosen to exploit. This was then verified that Metasploit had an exploit for this, see below.



From here I was able to select the exploit, set the options for it, set a target, and run the exploit itself. This gave shell access to the system and allowed me to explore some of the file on the system. The results of which are shown below.



**Useful Tips / Sites:**

https://metasploit.com