Detection

Willard Rafnsson

IT University of Copenhagen

In this assignment, we will put ourselves in the shoes of system administrators, and audit a server for vulnerabilities. Concretely, we will *scan* the server for known vulnerabilities, and *exploit* them. The goal is to realize the imporance of engineering security into software; isolation, hardening, and auditing, while important, turn out to be insufficient for securing systems.

Setup a Vulnerable Server

Server: Download the Metasploitable 2[1] VM-image from SourceForge[2]. Create a new VirtualBox VM from an image[3]. The resulting VM will henceforth be referred to as "the server". Do *not* start the server yet! (the Internet must never touch the server).

Network: Make sure both Kali and the server are powered off (Did you power on the server by accident before this point? If so, then destroy the foul thing, and redo **Server**). You protect the server from the Internet by creating a NAT-network, and putting the server (and Kali) into it. You do this in VirtualBox by heading to File → Preferences (on a mac: VirtualBox → Preferences). In the network settings of Kali and the server, configure it to use the NAT-network you just created. Start both Kali and the server; you'll see that the IP address of Kali has changed (and is likely `10.0.2.?`); Kali and the server are now on the same network, and neither are reachable by the Internet (since your VM host does not forward its ports to Kali or the server).

Problem 1 : nmap

Find the server (by scanning the network using `nmap`). What is the IP address of the server? (~1 sentence) Which ports are open, and which services are running on them? (~1 sentence, plus a text dump).

Note: Screenshots are welcome.

[1] not to be confused with Metasploit (the framework, and its console interface).

[2] `https://sourceforge.net/projects/metasploitable/`

[3] `https://securingninja.com/how-to-install-metasploitable-in-virtualbox/`

Problem 2 : gvm

Scan the server with `gvm`, by following the instructions provided in the exercises for lecture 4 (takes ~1 hour). Examine the result of the scan.

Note: Screenshots are welcome.

Part 1 Explain the output format; what is *location*? (~1 sentence) *QoD*? (~1 sentence) What do each of the *solution types* mean? (~3 sentence)

Part 2 Explain the `vsftpd` vulnerability, in your own words. (~2 sentence)

Part 3 Explain another high-severity vulnerability of your own choice (~2 sentence)

Problem 3 : metasploit

Use `msfconsole` to launch your chosen exploits.

Part 1 Exploit the `vsftpd` vulnerability on the server. (~7 sentence)

Part 2 Exploit the other chosen vulnerability on the server. (~7 sentence)

Note: Explain every step; include each `msfconsole` command, explain what it does, explain why you are executing it (i.e. to what end). Finally, once the exploit is launched, demonstrate what you can do with it (run commands (as what user?), exfiltrate files, etc.) Screenshots are welcome.

Note: This particular server is well known; there are tutorials available online on how to do many of the exploits reported by `gvm`. You are more than welcome to follow such a tutorial. However, if you do, you **must** state that you did so, cite the tutorial (i.e. provide URL), and explain each step with your own words.

Problem 4 : Reflection

Let's consider the ramifications of what we have learned.

Part 1 Through the `vsftpd` exploit, which *asset(s)* are vulnerable to what kind of *harm* (i.e. which *aspect of security* (CIA) is violated)? (~ 3 sentences)

Hint: which user is `vsftpd` running as?

Part 2 How can logging & intrusion detection reveal the `vsftpd` exploit? (~ 2 sentences)

Part 3 How can a firewall stop the `vsftpd` exploit? Pros/Cons? (~ 2 sentences)

Part 4 How can containerization limit the impact of the `vsftpd` exploit? (~ 2 sentences)

Part 5 What is hardening? How can it improve security on the server? (~ 2 sentences)