Beauvais Security Consulting, Inc.

Penetration Testing Report

Business Confidential

Submitted by: Berline BEAUVAIS
Date: June 1st, 2023
Cohort: 8/8/2022

Confidentiality Statement, Disclaimer, and Contact Information

Document Control

Issue Control			

Owner Details	**Title**	**Contact Information**	

Revision History			
Issue	Date	Author	Comments
	6/1/2023	Berline BEAUVAIS	

Executive Summary

Beauvais Security Consulting conducted a penetration test from May 20th, 2023 to June 1st, 2023 in order to determine Metasploit3's exposure to a targeted attack, by leveraging a series of attacks. All activities were conducted in a manner that simulated a malicious actor engaged against the target. With the goals of:

- Identifying if a remote attacker could penetrate the target's defenses

Test Scope

Evaluate the security posture of the infrastructure compared to current industry best practices, that included an external penetration test. The scope excluded Denial of Service(DoS) attacks during testing.

Results

Beauvais Security Consulting Inc, found critical level vulnerabilities that may allow full internal network access to metasploit3.

Finding Severity Ratings

The severity is rate based on the CVSS v3.1 which attempts to assign severity scores to vulnerabilities. The scores are calculated on a formula that depends on several metrics that approximate ease and impact of an exploit. Scores range from 0 to 10, with 10 being the most severe.

Severity	CVSs.v3 Score Range
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

The table below includes the scope of the test performed, as well as the overall results of penetration testing these environments.

Environment Tester	Testing Results based on CVSs.v3 Score Range
Dictionary attack	6.8

Vulnerability Reconnaissance	8.9
Exploit Execution	9.5

Assessment Overview and Assessment Components

Overview

Metasploitable3 is a VM that is built from the ground up with a large amount of security vulnerabilities. It is intended to be used as a target for testing exploits with metasploit. Metasploitable3 is released under a BSD-style license[1].

Beauvais Security Consulting, emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. To gather intelligence, our staff attempts to gather sensitive information about the target through open-source intelligence (OSINT).

Penetration Testing Results

Reconnaissance

During the test, Beauvais Consulting created a Metasploitable3 VM. Then we proceed with some Open Source information by using Tools, like the Recon-ng. We were able to see some valuable information through this tool. See figures 1, 2, 3, and 4.

First, we used recon-ng to do a detailed reconnaissance of the Metasploitable3 VM.

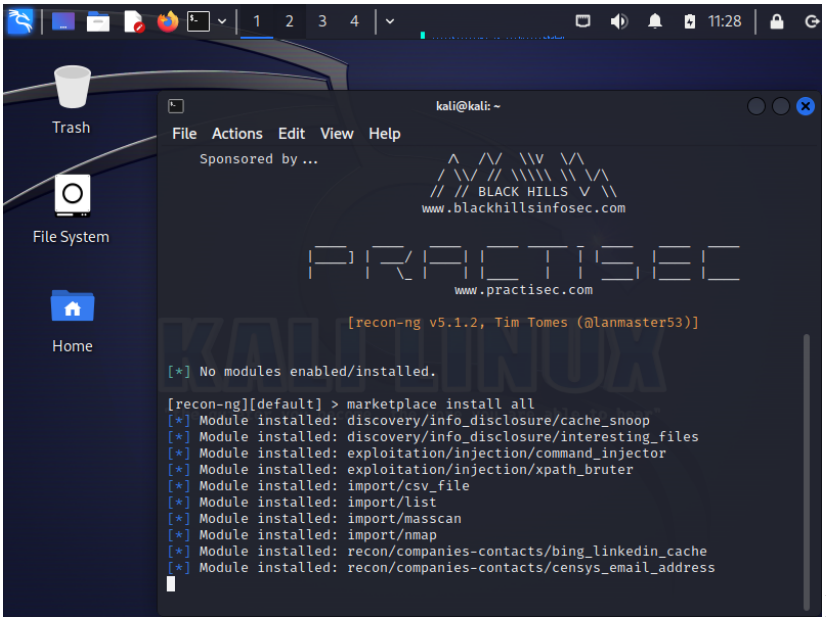


Figure 1.

[1] https://github.com/rapid7/metasploitable3#

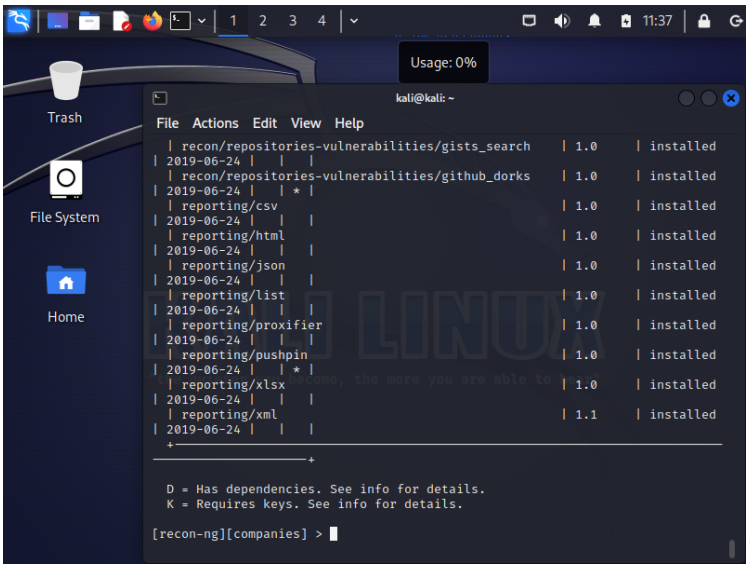


Figure 2.

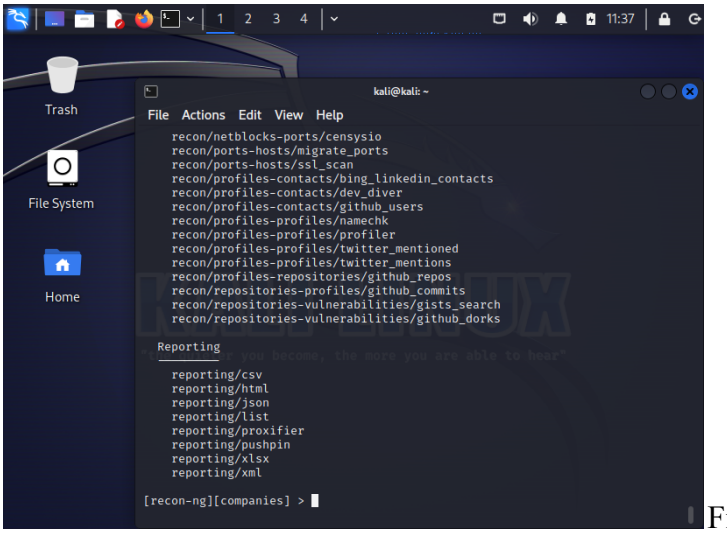


Figure 3.

Figure 4.

Dictionary attack

Our team conducts a dictionary attack by trying to create an ssh session, then to find a protected password. Although we got far in the process, we could not enter the metasploit 3 session, which is a positive point for the VM. Below are the figures that demonstrate the session. Figures: 5, 6, 7.

Figure 5

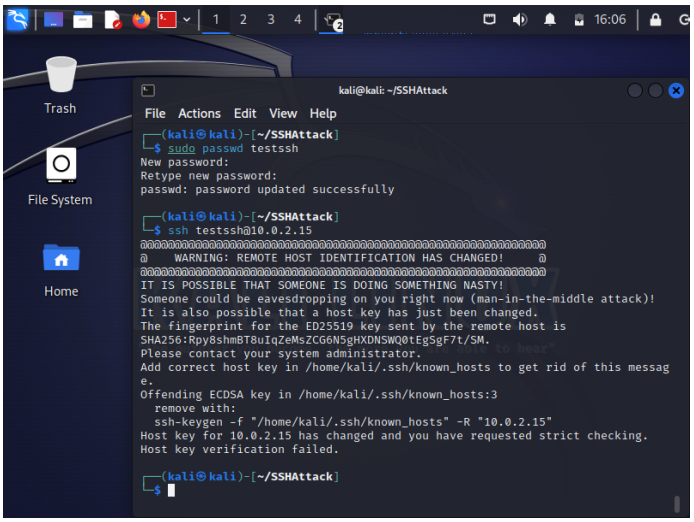


Figure 6.

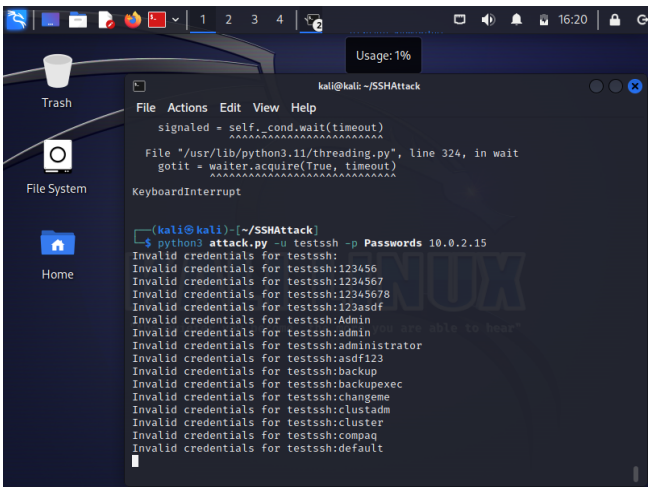
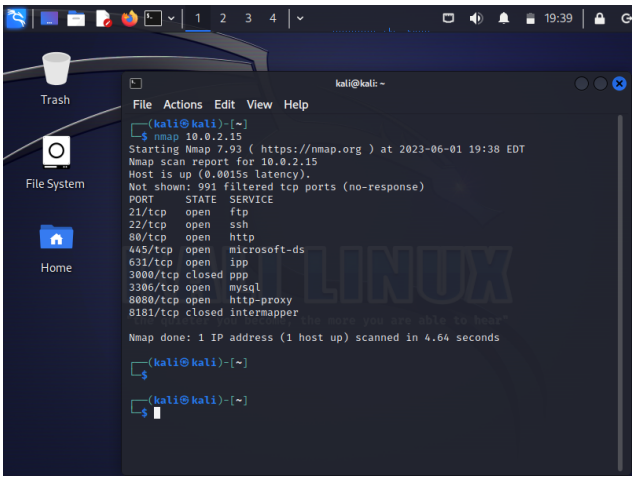


Figure 7.

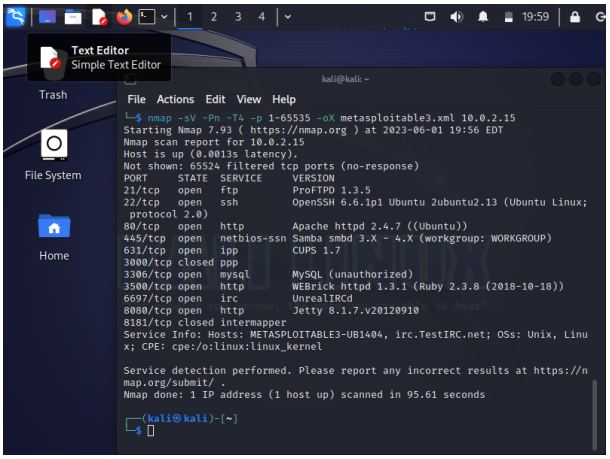
Vulnerability Exploit Execution

The Penetration team tester at Beauvais Security Consulting, used a Kali VM to exploit vulnerability of the metasploit 3 machine. We proceed to port scanning. However, some key ports were not open, like the port of the NFS 2049.At the same time we found some very important ports open like 22, 80, 6697. Moreover, we proceed to exploit some of the vulnerabilities found on the backdoor. But, we were not completely successful in creating the secession inside the target machine. See figures 8, 9. 10. 11. and 12.

We did vulnerability scanning by using nmap. We were able to see the ports that were opened. Figure 8.



We looked at the version information to know where the system may be vulnerable. So we can look for a matching, published, vulnerability. Figure 9.



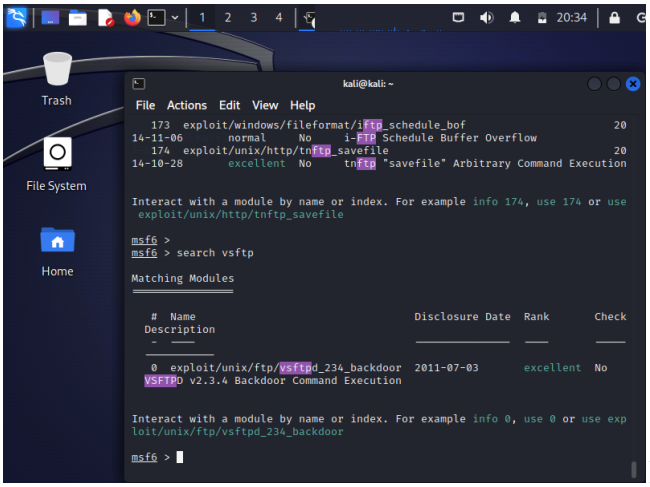


Figure 10.

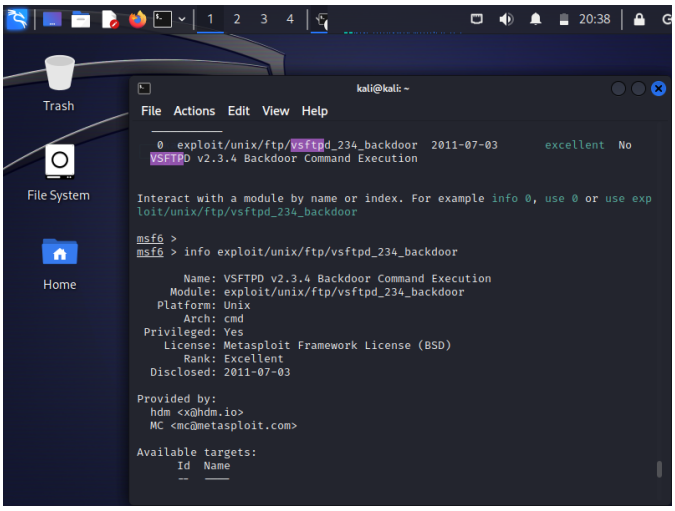
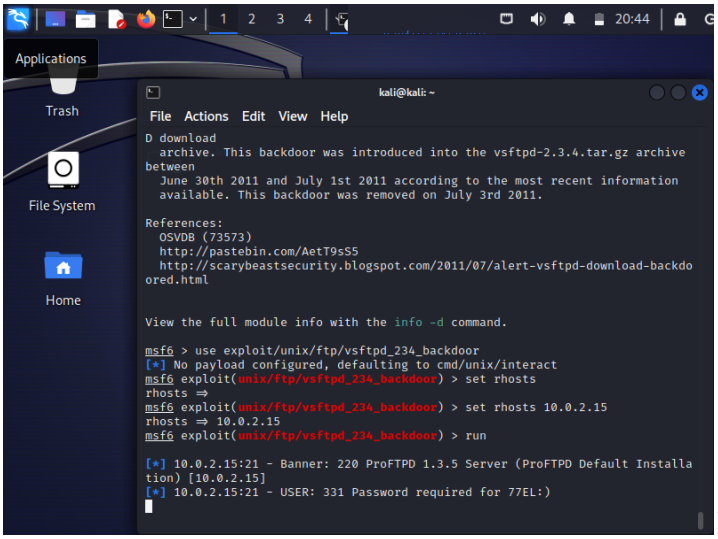


Figure 11.


Applications
Trash
File System
Home
1 2 3 4
20:44
kali@kali: ~
File Actions Edit View Help
D download
archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
June 30th 2011 and July 1st 2011 according to the most recent information
available. This backdoor was removed on July 3rd 2011.
References:
OSVDB (73573)
http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
View the full module info with the info -d command.
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts
rhosts =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.15:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
[*] 10.0.2.15:21 - USER: 331 Password required for 77EL:)
Figure 12.