UNLV CYBER SECURITY CLUB

Agenda

Who We Are

Purpose and Mission

What to Expect in Layer Zero

Schedule

Demo (TBD)

Challenge (TBD)

Who We Are

First Cyber Security RSO at UNLV

Started in March 2018

Advisor is Dr. Yoohwan Kim (CISSP, CISA, CEH, CPT) - C.S. Department

2018-19 Officers:
- Phillipe Austria
- Jinger Siu
- Matt Lazeroff
- Matt Lyle

Consultant
- Daniel Ainsworth

Layer Zero Purpose

1. Gain interest to fill the huge demand in Cyber Security jobs source

2. National Cyber League (NCL) & Capture the Flag* (CTF)

3. Certifications
    - CompTIA Security+
    - Certified Ethical Hacker (CEH)

4. Continue officially representing UNLV Cyber Security in NCL and other national competitions

National Cyber League: Fall Season Information

Registration Fee: $35

- Layer Zero will cover $20

Gym Training: 03/28 - 05/24

Preseason: 04/01 - 04/08

Regular Season Competition (Solo): 04/12 - 04/14

Postseason Competition (Team): 04/26 - 04/28

Spring ‘19 (Fridays) Schedule //the short version

-Training and Lab

February 15th - Password Cracking, Cryptography & Steganography

March 8th - Open Lab

March 1st - Network, Traffic & Log Analysis

March 15th - Wireless, Scanning & Web Exploitation

March 22nd - Open Lab (during spring break)

April 5th - Enumerations

April 11th - Open Lab

April 19th - Open Lab/debrief/tips && tricks (between competition phases)

Spring ‘19 (Fridays) Schedule //the short version

-Guest Speakers

Friday, February 22nd

-Penetration testing and how it fits into the cybersecurity philosophy

Friday, March 29th

-Network traffic, NSM, SIEM, log analysis

Friday, May 3rd (post-competition)

-Cyber career advice, general “what it’s like to be in cyber”

Spring ‘19 (Fridays) Schedule //extended version

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
				Feb 08	Feb 09	Feb 10
				General Meeting		
Feb 11	Feb 12	Feb 13	Feb 14	Feb 15	Feb 16	Feb 17
				Training – Password Cracking, Cryptography & Steganography		
Feb 18	Feb 19	Feb 20	Feb 21	Feb 22	Feb 23	Feb 24
				Guest Speaker - (pen testing and how it fits into the cyber philosophy)		
Feb 25	Feb 26	Feb 27	Feb 28	Mar 01	Mar 02	Mar 03
NCL registration begins (until 03/30, then late Reg. Til 04/02)				Training - Network, Traffic & Log Analysis		
Mar 04	Mar 05	Mar 06	Mar 07	Mar 08	Mar 09	Mar 10
				Open Lab – Daniel		
Mar 11	Mar 12	Mar 13	Mar 14	Mar 15	Mar 16	Mar 17
				Training – Wireless, Scanning & Web Exploitation		Spring Break BEGINS
Mar 18	Mar 19	Mar 20	Mar 21	Mar 22	Mar 23	Mar 24
				Open Lab – Daniel		Spring Break ENDS
Mar 25	Mar 26	Mar 27	Mar 28	Mar 29	Mar 30	Mar 31
			NCL gym opens (practice area for learning, open all season)	Guest Speaker - (network traffic, NSM, SIEM, etc)		
Apr 01	Apr 02	Apr 03	Apr 04	Apr 05	Apr 06	Apr 07
NCL Preseason BEGINS - "try-outs" where your results place you into 'brackets' of difficulty for later				Training – Enumeration/Reverse Engineering		
Apr 08	Apr 09	Apr 10	Apr 11	Apr 12	Apr 13	Apr 14
NCL Preseason ENDS			Open Lab – Daniel	NCL Individual BEGINS (3 days)		NCL Individual ENDS
Apr 15	Apr 16	Apr 17	Apr 18	Apr 19	Apr 20	Apr 21
				Open Lab – Daniel; Discuss/Debrief Individual Event; Prep/Tips for Team Event		
Apr 22	Apr 23	Apr 24	Apr 25	Apr 26	Apr 27	Apr 28
				NCL Team BEGINS (3 days) - //Sign-up teams by 04/25		NCL Team ENDS
Apr 29	Apr 30	May 01	May 02	May 03	May 04	May 05
				Guest Speaker - (post competition, career/general cyber advice)		

Tips for success && avoiding catastrophic failure

*__Stay motivated__ - people in this field *LOVE* this field

*__Experiment and learn on your own__ - the internet is a wealth of knowledge

*__Be realistic__ - the internet is a cache of misinformation and garbage

*Running unknown code of the internet - __don't do it!__

*__Be prepared__ - primarily, be equipped, and have a backup plan (laptop failure!)

*__Be prepared (*again*)__ - if you haven't tried the tool, how do you know it works?

*__Be confident__ - everyone starts somewhere, and fellow competitors are college students!

NCL rules && legalities -

Don’t cheat - success is earned, not stolen

Material is copyrighted -

*instructors and professors can only go over problems *post-event*

*instruction material of past events *cannot be publicly distributed*

For Next Training Session ...

If you can, please show up on time

If you can't, don't ask what you missed, that takes away from everyone else

You will want to bring a functioning computer. By next session -

*Either have Kali installed (see **https://github.com/layer-zero-unlv** tutorial)

OR

*Have your files backed up, and we will walk you through the install

Option 1 - 'Live' disk (run off a USB) //not recommended

Option 2 - Virtual Machine (VMWare or VirtualBox) //sufficient but limited

Option 3 - Full install (single OS, or dual-boot) //recommended

“But, do I ***need*** Kali Linux?”

No, you can compete with Mac or Windows just fine.

Kali is a ‘Nix distro based off of the debian system, ***preconfigured*** with ***hundreds*** of hacking tools.

Many of these tools (but not all) are available on other platforms.

If you don’t know any of the tools, get the whole ‘toolkit’ and you’ll have everything you need.

//We can talk about custom systems later this semester!

Jinger Siu

siuj1@unlv.nevada.edu

- computer science senior
- network engineering
- Cisco CENT
- training

UNLV Network Engineering

Student Network Technician (NDE)

Assist Network Development & Engineering (NDE) staff with maintenance, installation, upkeep, inventory control, tracking, replacement of network hardware, and office equipment. To provide excellent service, the employee will: listen to customer and understand their needs; demonstrate an eagerness to help; help customers solve problems; maintain a professional disposition; be approachable, respectful, and team-oriented; take ownership of inquiries and assignments; provide updates for customers; and be familiar with the basic operations of the university in order to serve customers effectively. Preferred freshman/sophomore class standing. Hourly rate starts at $12.00/hr.

https://www.it.unlv.edu/students/it-jobs/oit

Overview

- tcpdump
- wireshark
- netcat

Everything referenced here will be explained in more detail throughout training sessions/Layer Zero’s github

tcpdump

- Transmission Control Protocol (TCP)
  - protocol: *a set of rules governing the exchange or transmission of data between devices*
    - computers need to be speaking the same language in order to understand each other
      - if two computers can both “speak” TCP, they can send data to each other
    - the 1s and 0s need to be sent and interpreted in a specific way, and that’s what the protocol defines
    - can think of it like an *algorithm* of how to interpret and understand various types/forms of data

How TCP/IP Works

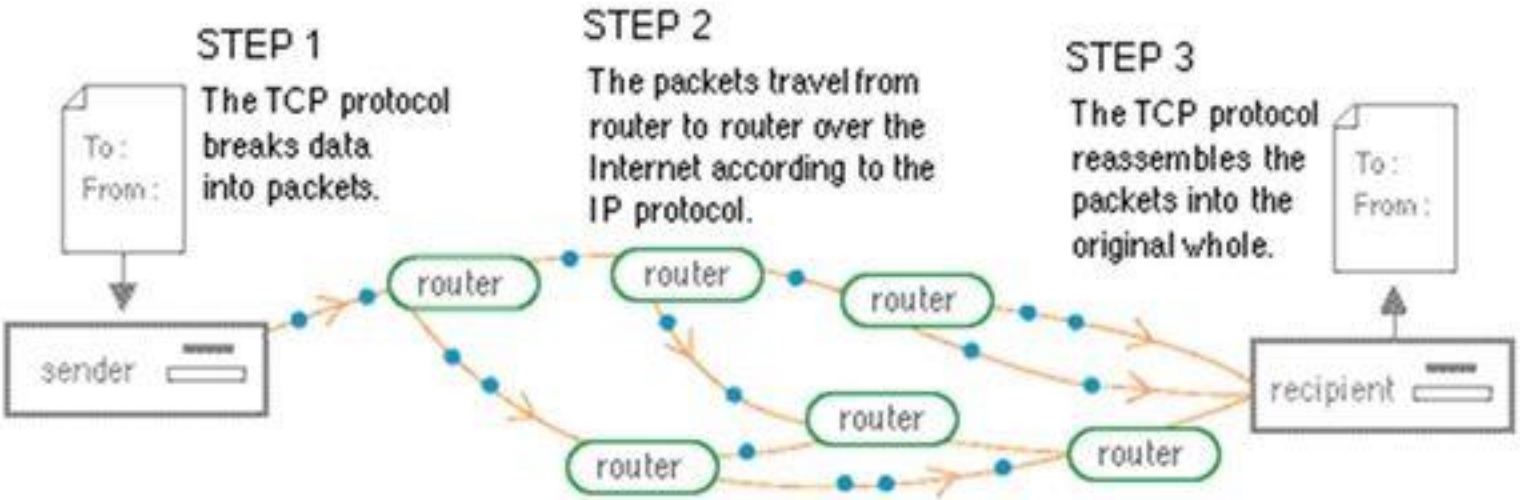


Figure 2. How data travels over the Net.

Dr. Vinton Cerf

MCI

wireshark

- network protocol analyzer
  - GUI or terminal version (tshark)
- log/packet analysis
- https://www.wireshark.org/

tcpdump with wireshark example

useful commands

- *ifconfig*
- *sudo -s*
- *touch* <filename>
- *tcpdump -w* <filename>
- *wireshark* <packet capture>

concepts

- TCP connection
- network interface
- packet captures

TCP ports

- port: *endpoint to a logical connection*
  - client computer has to specify what program it wants to use on the server computer
- standards / protocols have defined mappings between services and port numbers
  - examples
    - HTTP - TCP port 80
    - HTTPS - TCP port 443
    - SSH - TCP port 22

TCP ports cont.

Example scenario: connecting to a UNLV web server (https://unlv.edu)

- I open my web browser and type the URL into the address bar
- my computer will pick a random TCP port number that's greater than 1023
  - my computer isn't running any services, it's just trying to use a server's web service
  - so my port number doesn't matter, as long as it's a number that's not standard for some service
    - ex. my computer might pick my port number to be 3303, but it won't pick port 22 because that's *reserved* for SSH

TCP ports cont.

Example scenario cont.

- my computer will connect to UNLV's web server on TCP port 443
  - port 443 is used because HTTPS services *listen* on that port
- *listening* on a port
  - a listening computer will have software that checks if any other computer is trying to access a specific service (HTTP, SSH, etc)
  - if a client computer is trying to access a service, the listening computer will provide the services as defined by the port number

netcat

- utility for reading/writing from/to network services

TCP ports with netcat example

useful commands

- *lsof -iTCP*
- *netstat -lpnt*
- *touch* <filename>
- *nc -lvp* <port number> */ nc <ip address>*
- *man* <linux program>

concepts

- SSH/shells/reverse shells
- TCP port connections
    - reserved ports vs client ports

netcat example

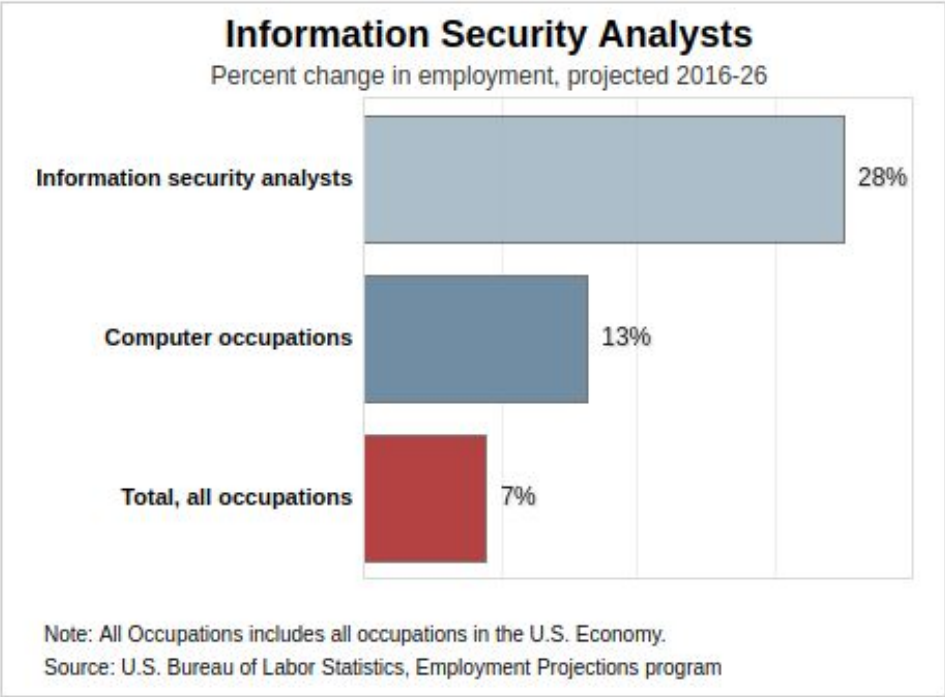
Goal: *gain access to a victim computer's shell via netcat (reverse shell)*

Implementation:

1. set up the *attacker* to listen on a non-reserved port
2. "convince" the *victim* to connect to the attacker's computer on the open port
3. run shell commands on the victim's computer, from the attacker's computer

Thank You

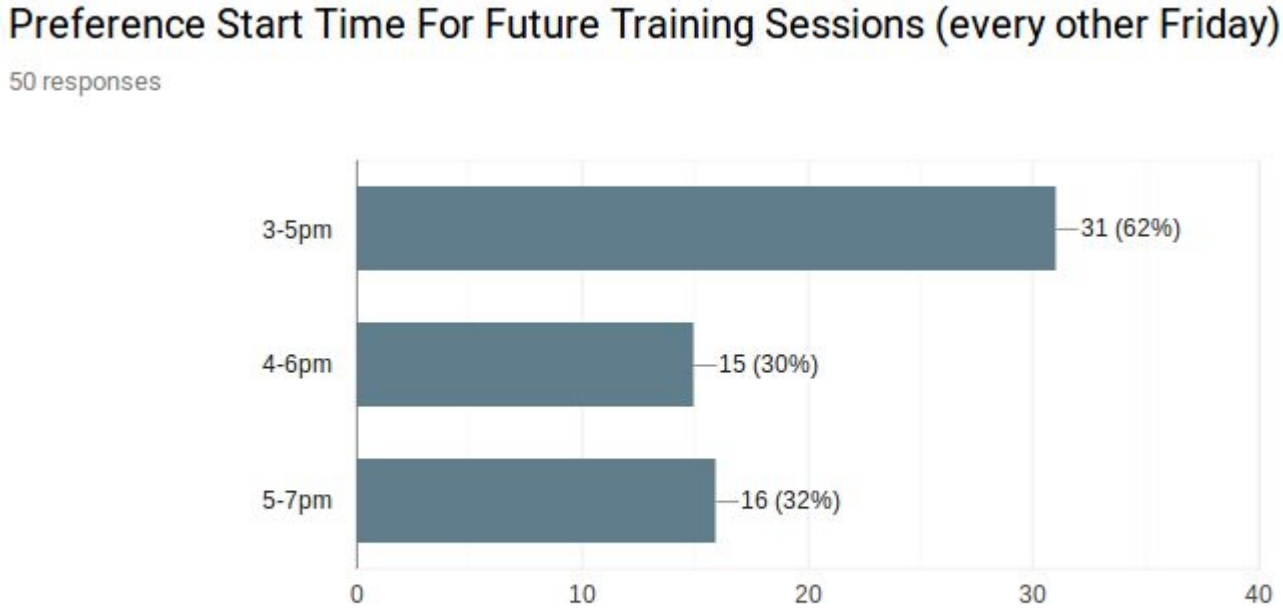
Email us at layer_zero@unlv.edu
Github: https://github.com/layer-zero-unlv


Information Security Analysts
Percent change in employment, projected 2016-26
Information security analysts
28%
Computer occupations
13%
Total, all occupations
7%
Note: All Occupations includes all occupations in the U.S. Economy.
Source: U.S. Bureau of Labor Statistics, Employment Projections program

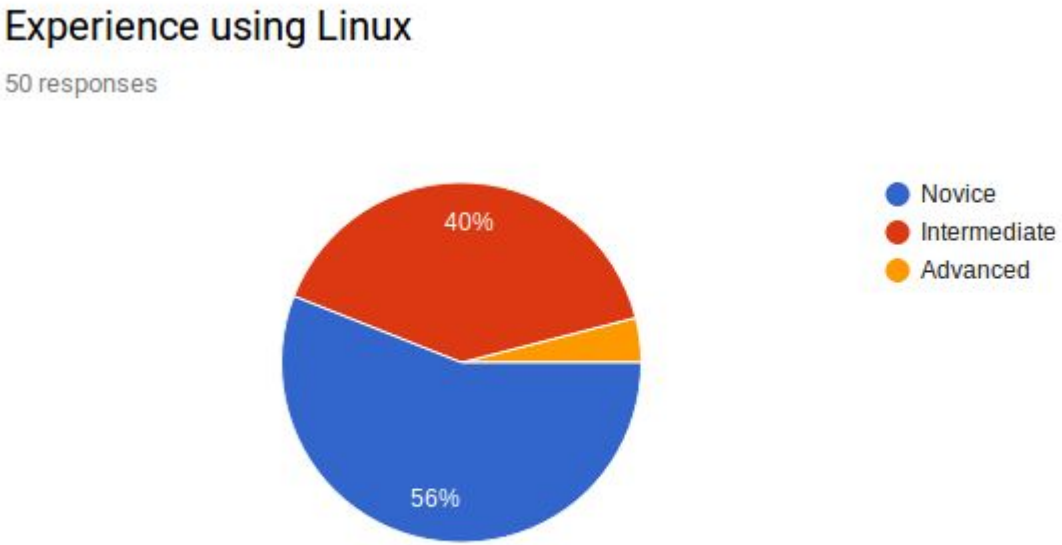

SUPPLY OF CYBERSECURITY WORKERS
Very Low
CYBERSECURITY WORKFORCE
SUPPLY/DEMAND RATIO
National average
2.5

Back

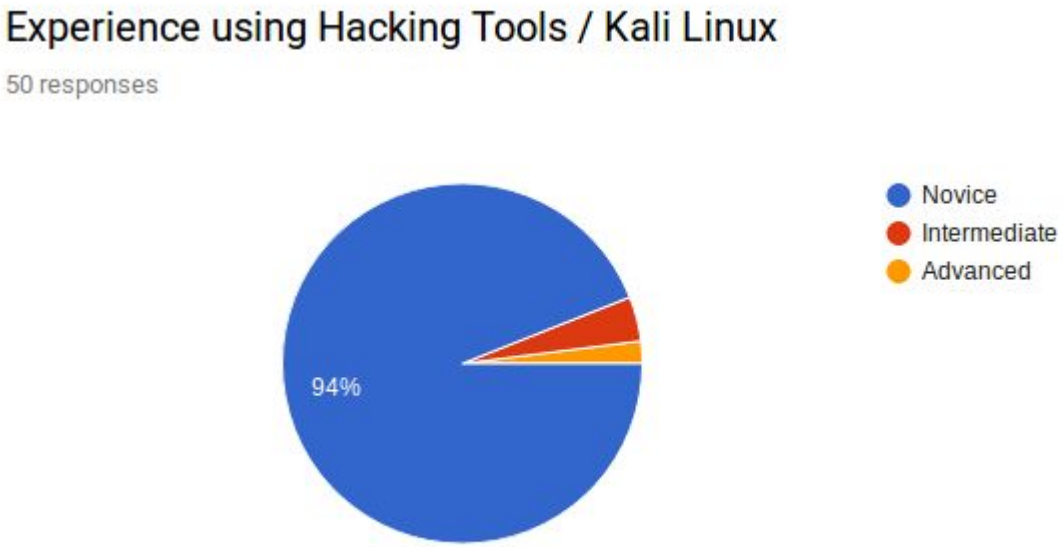
Feedback 1


Preference Start Time For Future Training Sessions (every other Friday)
50 responses
3-5pm
31 (62%)
4-6pm
15 (30%)
5-7pm
16 (32%)
0
10
20
30
40

Feedback 2


Experience using Linux
50 responses
40%
56%
Novice
Intermediate
Advanced

Feedback 3


Experience using Hacking Tools / Kali Linux
50 responses
94%
Novice
Intermediate
Advanced

Feedback 4

Are you interested in competing in National Cyber League's: Capture The Flag (CTF) competition? (don't worry if you have NO experience, that's what the training sessions are for)

50 responses