LAYER ZERO

UNLV CYBER SECURITY CLUB

General Meeting 9/13/19

WHO WE ARE

Layer_Zero

layer_zero@unlv.edu
github.com/layer-zero-unlv

- UNLV's cyber security org
- UNLV students
- Various certs/vendors
- Various cyber 'domains'

WHAT WE DO

Training

Student lead training

- Network scanning, traffic analysis, log analysis, password cracking, web exploitation and more
- Caters to a variety of academic levels
- Covers material UNLV won’t teach you
- Bring your own device
- Hands on

Challenges

Test yourself against your

- In-session challenges, during hands-on training
- Semester wireless scavenger hunt
- Volunteer to help setup the challenges

Competition

- Open to all college and high school students
- Compete against your peers
- Compete as a team and represent UNLV in national competition
- Validate your skills with hands on exercises
- Receive ‘scout report’ you can add to your resume

Guest Speakers

- Industry professionals
- Represent different domains of cyber
- Hear from experts about their day-to-day work
- Network for employment opportunities

If you’re interested in being an OFFICER, don’t be afraid to step up. We all start somewhere, and we need a variety of skill sets in order to keep the club active.

The general idea->

- For any given core topic/cyber area:
  - Listen to a presentation/lecture
  - Get hands-on practice
  - Validate your training in competition
  - Hear a professional speak on that topic (their job)
  - Evaluate which areas of cyber are best suited to you
- Improve your weaker ares to become more well-rounded, or concentrate on your strengths and begin to specialize
- Just like all other jobs, cyber is ***team based*** - which team to you want to work on, and what are you bringing to the table?

Upcoming Schedule

- Saturdays 1-3pm: Rooms TBD (backup room WHI302)

- Saturday, September 21th - Password Cracking, Cryptography & Steganography (Matt)
- Saturday, September 22 - Network, Traffic & Log Analysis (Jinger)
- Saturday, October 5st - Wireless, Scanning & Web Exploitation (Jinger)
- Saturday, October 12th - Enumerations (Matt)

Members decide by December 3rd

- Monday, October 14th-Monday, October 21st NCL Pre-Season
- Friday, October 25th - Guest Speaker
- Friday, November 1st-3rd - NCL Individual Season
- Friday, November 15th-17th -NCL Team Season

DEMONSTRATION

Jinger Siu

siuj1@unlv.nevada.edu

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

Overview

All slides can be found at *https://github.com/layer-zero-unlv*

- IP addresses, ports
- tcpdump
- wireshark

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

wireshark

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

IP Addresses & Port Numbers

- IP Address
  - Internet Protocol
  - logically identifies a device at the network level
- Port Number
  - identifies a service running on a particular device
  - port numbers are mapped to services (ex. HTTP port 80; SSH port 22)
  - servers *listen* on ports
  - the combination of IP address with a port is called a *socket* (10.10.10.10:80, 10.10.10.10:22)

Important (IPv4) Addresses

- Private addresses
  - not routable over the internet
  - 10.0.0.0/8 **(10.x.y.z)**
  - 172.16.0.0/12 **(172.16-31.x.y)**
  - 192.168.0.0/16 **(192.168.x.y)**
- Localhost
  - 127.0.0.0/8 **(127.x.y.z)**

Some Linux Commands

- ls, cd, mv, man, cat, touch, chmod, pwd, sudo
- alias, ps, top, grep, sed/awk, find, who, crontab, apt-get
- curl, ping, ss, ssh, telnet, ip addr
- |, >>

Example: Capture traffic on a network interface and display it to STDOUT

```
~ $  ip addr # find network interface to use
```

```
~ $  tcpdump -i eth0 # capture and display traffic with tcpdump
```

Example: Show the open (listening) ports on a Linux system

```
~ $  ss -lt
```

Explanation:

socket statistics ss command line utility
options: listening, TCP
man ss

Example: Connect to a telnet server running on 192.168.0.2

WARNING: DO NOT USE TELNET OVER AN INSECURE NETWORK

```
~ $  telnet 192.168.0.2
```

Explanation:

connect over telnet (default TCP port 23) to 192.168.0.2
notice that this is a private address

Web Information

- Github: https://github.com/layer-zero-unlv
- Website:
    - https://layer-zero.org
- Twitter:
    - https://twitter.com/LayerZero1