CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Penetration Testing

Chris Samayoa

Week 8 – 1st Lecture
3/8/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Discussion

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Fortinet NSE Associate (Lab 5)
  - Create account: https://training.fortinet.com/login/signup.php
  - Complete NSE 1, NSE 2, and NSE 3
    - https://training.fortinet.com/
- https://arstechnica.com/information-technology/2022/03/linux-has-been-bitten-by-its-most-high-severity-vulnerability-in-years/
- TryHackMe
- https://samsclass.info/
- eLearnSecurity Junior Penetration Tester (eJPT)
  - https://my.ine.com/CyberSecurity/learning-paths/a223968e-3a74-45ed-884d-2d16760b8bbd/penetration-testing-student

Objectives

- Types of Hackers
- Intro to Penetration Testing
- Penetration Testing Stages

Types of Hackers

- White Hat
  - Ethical hacker
  - Trained penetration testers
- Black Hat
  - Malicious attacker
  - “Script Kiddies”?
- Grey Hat
  - Violates laws and ethical standards, but no malicious intent

White Hat

- Permission to engage by organization or customer
  - Always discloses found vulnerabilities
- Techniques
  - Penetration Testing
  - Email Phishing
  - Denial-of-service (DoS) Attack
  - Social Engineering
  - Security Scanning
    - Vulnerability scanners (Nessus)
    - Web Application Vulnerability Scanners (Acunetix / Netsparker)
    - Nikto
    - Metasploit

Black Hat

- Has malicious intent
  - Does not request permission to find vulnerabilities
  - Does not disclose vulnerabilities when found
- Can be skilled hackers or “script kiddies”
  - Title has more to do with intent than ability
  - Traditionally Black Hat hackers referred to skilled malicious actors
- Use same techniques as White Hat hackers
- Often develop specialties
  - Command and control of remote assets
  - (spear)Phishing campains
  - Malicious software development

Black Hat - Organized

- Types of organizations
  - Criminal
  - Nation-state
- Resources
  - Training
  - Sales (partners / resellers / vendors)
  - Call centers
  - International
- Goals:
  - Data exfiltration
  - Extortion
  - Botnets (crypto-mining or DoS for hire)

Grey Hat

- Intent is “typically” not malicious
  - Does not request permission to find vulnerabilities
  - Sometimes discloses vulnerabilities when found
- Can be skilled hackers or “script kiddies”
- Use same techniques as White / Black Hat hackers
- Differences
  - Sometimes violates ethical standards, but without malicious intent
  - Could be attempting to collect a fee for patching vulnerabilities
    - Businesses can decide to seek prosecution
  - Exploitation of vulnerability could be for a “good” cause

Grey Hat - Examples

- MikroTik Routers
  - Russian Grey Hat patched routers
    - Claimed over 100,000 router patches
    - https://www.zdnet.com/article/a-mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers/
  - CVE-2018-14847
    - https://blog.n0p.me/2018/05/2018-05-21-winbox-bug-dissection/
    - Had ability to turn routers into bots (e.g. crypto-mining)
  - Two million MikroTik routers in service during this time
- Ukranian Conflict - Anonymous
  - https://www.youtube.com/watch?v=UpYJ-Mw1trM
  - https://www.youtube.com/watch?v=gkrDIjGP4_w

Penetration Testing

- White Box
  - Internal structure of network environment is known
  - Tester can view source code and have access to applications and systems
  - Test from developer's / administrators point of view
- Black Box
  - Internal structure is unknown for network environment
  - Little to no information provided to testers
  - Can most closely resemble external actors
    - Time restraints are different
- Grey Box
  - Combination of white box and black box
  - Tester can partially "see" inner working of a network environment
    - Allows for more of the network to be tested within a given time frame
    - Tester granted some permissions or internal access on the network
  - Typically where most penetration tests land

Rules of Engagement

- Rules of Engagement (ROE)
  - Written document that specifies the scope and allowable actions during a penetration test
  - Specifies level of communication during engagement
- Type and scope of engagement
  - White box / black box / grey box
  - What attack surfaces can be tested
  - What methods are allowed?
- Client contact details
  - Who knows about the testing?
  - Who should be contacted and in what order?
  - Preferred methods of communication

Rules of Engagement

- IT Team Notifications
  - When should the IT team be engaged?
  - Establish levels of criticality
- Sensitive data
  - Special provisions for regulated data (e.g. HIPAA)
- Meetings and report
  - Pre-determined meeting dates and frequency
  - What types of reports are needed (e.g. technical, executive, sanitized)

Penetration Testing Stages

- Scoping
- Planning and Reconnaissance
- Scanning
- Gaining Access – Lateral Movement
- Maintaining Access
- Analysis Reporting
- Remediation

Tools Overview

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

Scanners

Vulnerability Scanning

Summary