CSE 523S: Systems Security

Computer & Network Systems Security

Spring 2018

Jon Shidal

Plan for Today

- Announcements
  - HW3 assigned today, due 1pm March 21st
- Questions
- Assignment
- Vulnerabilities & Exploits
  - Finding known vulnerabilities
- Today: Mix of lecture and exercises.

Assignment

- HW3 assigned; due 1pm March 21st
  - See hw3 file in handouts

Reviewing our progress

- Module 1 (complete)
  - L01: Introduction
  - L02: Security Principles
  - E03: Getting to know our systems
  - L04: System Design & Security: Why are computers vulnerable?
  - E05: Exploring binaries and processes.
  - L06: System Design & Security: Why are networks vulnerable?
  - E07: Exploring packets
  - L08: Network Security: Revisited
  - E09: Exploring Encryption
  - L10: Understanding Vulnerabilities
  - E11: Exploring Metasploit
- Module 2 (starts today)
  - Finding known vulnerabilities
  - Stack and heap buffer overflows, integer overflows, format string attacks
  - ASLR and NX
    - **A**ddr. **S**pace **L**ayout **R**andomization
    - Stack **N**o-e**X**ecute
  - Fuzzing

Vulnerabilities & Exploits

- Monday, we used ms03_026_dcom to attack our Windows XP instance
- We knew what we were attacking.
- We knew its vulnerabilities.
- We followed a script.
- How might we have done so on our own?

Scanners

- You can actively probe a network to identify machines and services
- Previously, within ***scapy***, we saw how to use ARP to find active IPs on a network
- We can also use a tool called nmap to learn more

Nmap

- Among the most popular open-source network scanners
- Crafts packets to identify OS, open ports, and services listening on ports
- Can be automated and extended via scripts
- Like many tools, integrates well with metasploit

Vulnerability scanners

- Nmap identifies **machines and services**

- Other tools look for known **vulnerabilities**
  - Nessus is the best-known,
    - but it is no longer open-source
  - OpenVAS is a fork of Nessus, and may retake the crown (although it is limited currently)
  - others...

- We can also use tricks within metasploit itself

Organizing information

- When exploring hosts or networks for vulnerabilities, information management can be a problem
  - Have I seen that address before?
  - Has something changed in the past week?
  - What target version is running?
- We can rely on metasploit's database integration to help with managing this information

Let’s get to work!

- See exploring-vulns-notes in Google Docs
  - Important: use your host OS browser, do not use the browser in your VM
- Also use “Tracking Progress 2/28/2018” to indicate when you have reached a gate