Computer Security in the Real World

What we do and why you care

Who’s this guy?

Chris Newman, BS from Cal Poly in CSc in ’02

- 11 years with US Government Defense Contractor
  - 4 years coding defense
  - 4 years coding offense
  - 3 years “security research” pentesting
- 5 years with VMware
  - 2 years pentesting
  - 3 years managing pentesters “Security Engineering Manager”
  - newmanc@vmware.com

Penetration Testing

Incident Response

Bug Bounty

Coding Offense Tools

Coding Defense Tools

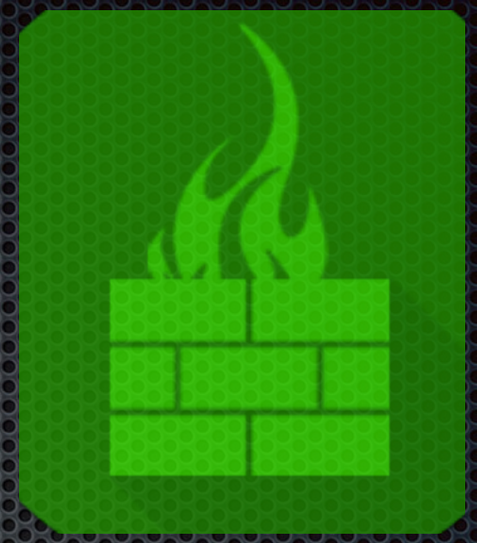
Defensive Coding

Internal Security

Defensive Coding

- Free isn't Free
  - Open Source should be treated like a puppy, not a toilet
- Assume You're Owned
  - Contain compromises by lowered privileges and defending in depth
- All Input is Evil
  - Use Abuse Cases to test your code with bad input
- If You Don't, They Won't
  - Don't expect customers to harden systems
- Use the right framework that removes whole classes of attack
- Don't assume good behavior (Hardware, OS, Users)

Coding Defense Tools



Where

- Symantec
- McAfee
- VMware
- Microsoft
- FireEye
- Top 500 cyber security companies

What

- Antivirus
- Firewalls
- Network tunnels
- Hypervisors
- Phishing detection
- ...

Incident Response

Where

- Every organization with a network
- Consultancy

What

- Forensics
- Mitigations / Fixes
- Short or Long term engagement

Penetration Testing

Where

- NCC Group
- IOActive
- Rapid7
- Dozens more....

What

- Zero Days
- Travel
- Super short engagements

Bug Bounty

Where

- Your House
- Bugcrowd
- HackerOne
- Direct Bug Bounties
  - MS
  - Google
- More…

What

- Zero Days
- “Free time”
- Read the contract!
- How do you get the target?
  - IoT device?
  - Car?
  - Expensive software?
  - Test servers?

Coding Offense Tools

Where

- Governments
  - NSA, CIA, NRO, FBI Military, etc
- Government contractors
- Police/Law Enforcement

What

- Zero Days
- Remote Access Tools
- Medium-term engagements

Internal Security Testing

Where

- Every company who ships software
- Every company who runs an online service

What

- Zero Days
- Mitigations / Fixes
- Long term engagement

Resume Fodder

- Capture The Flag (CTF)
- Internships
- Common Vulnerabilities and Exposures (CVEs)
- OSS submissions
- Conferences (Student scholarships available to most)
- Rewarding your use of free time is inherently classist and sexist but sadly common
- Senior Projects/Master's Thesis
- Independent research with a professor
- The right classes: Security, Compilers, OSes, Networking

Interview Prep

- Reverse Engineering: challenges.re
- Code challenges: leetcode.com
- Code review: be able to find bugs in any language on your resume
- Python
- Books
  - Hacking: the Art of Exploitation
  - Web Application Hacker's Handbook 2
  - Practical Malware Analysis
  - The Art of Software Security Assessment

- OSINT
  - Down the Rabbit Hole An OSINT Journey: Open Source Intelligence Gathering for Penetration Testing by Chris Kubecka
    - https://www.amazon.com/Down-Rabbit-Hole-OSINT-Journey/dp/0995687544
  - Open Source Intelligence Techniques - 6th Edition (2018) by Michael Bazzell
    - https://www.amazon.com/dp/1984201573
- Tools
  - https://www.kali.org/
  - https://www.hex-rays.com/products/ida/
- Bug Bounty programs
  - bugcrowd.com
  - hackerone.com
- Cons
  - BlackHat
  - DEFCon
- Other
  - CVE - cve.mitre.org or cvedetails.com
  - Find devices online shodan.io

Penetration Testing

Incident Response

Bug Bounty

Coding Offense Tools

2057693

Coding Defense Tools

Defensive Coding

Internal Security