Cyber@UC Meeting 38

Becoming a Certified Ethical Hacker

If You’re New!

- Join our Slack **ucyber.slack.com**
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- **Ongoing Projects:**
  - Malware Sandboxing Lab
  - Cyber Range
  - RAPIDS Cyber Op Center

Announcements

- **P&G visit set for Jan 22nd 2-3pm**
- We’re planning **school visits,** reach out!
- Logo designs welcome!

Public Affairs

- Please fill out Google form for **GroupMe** Numbers! https://goo.gl/forms/94i9kMJgtpDGXsC22
- Our brand new **YouTube** channel has just been made. We will be live streaming meetings, events, etc and posting relevant videos to the channel. Please subscribe! youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us on our social media:

Facebook:	facebook.com/CyberAtUC/
Twitter:	twitter.com/UCyb3r
Instagram:	instagram.com/cyberatuc/
Website:	gauss.ececs.uc.edu/UC.yber/

Weekly Content

Botnets targets ARC Processors

- What is an ARC Processor?
  - ARC stands for Argonaut RISC Core
  - 32-bit CPUs popularly used for SoC devices
  - World’s second most popular CPU core
  - In more than 2 billion products every year
- A new variant of the Mirai botnet has been found that hijacks insecure devices using ARC processors, known as Mirai Okiru
- Discovered by the MalwareMustDie team, a malware research group
- ARC processor malware is apparently very uncommon
- This malware is similar to another version of Mirai that targeted MIPS and ARM processors

Mirai Okiru (continued)

- The malware used is known as Linux/Mirai ELF
- ELF malware is very difficult to detect because it waits a while after being installed before taking action, and can only be tracked through the memory of the device

https://en.wikipedia.org/wiki/ARC_(processor)

http://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html

https://thehackernews.com/2018/01/mirai-okiru-arc-botnet.html

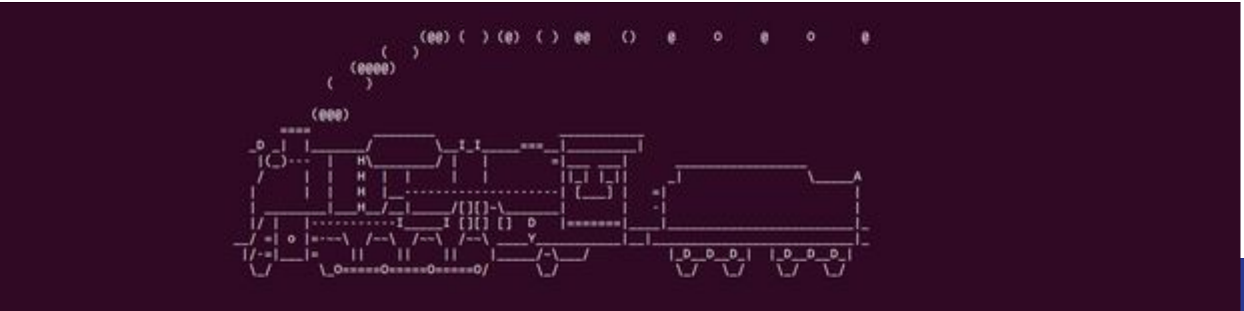
Intel AMT Vulnerability

- Intel AMT (Active Management Technology) is a feature that could allow an attacker to gain complete remote control of a device
- Intel AMT is a feature meant to enable IT admins and the like to easily manage and repair their fleet of workstations
- This feature can also be used to grant remote access, change passwords, etc.
- The attacker just needs to reboot the machine and use CTRL-P during boot-up, allowing them to log into Intel Management Engine BIOS Extension (MEBx), where the attacker can most likely log in with the default password

https://thehackernews.com/2018/01/intel-amt-vulnerability.html

Watch what you Download!!

- We generally follow safe browsing tips and updating anti-virus softwares to prevent downloading viruses.
- But for programming, do we check the packages as we add them?
- Traditionally repository softwares employ a check for known and similar signatures taking direct embedding of malicious code out of the picture.
- But custom made code may often go unnoticed and therefore is a possible delivery mode for malware.
- PPA for Ubuntu and npm (JavaScript) are commonly hit by this.



PIC - https://www.tecmint.com/20-funny-commands-of-linux-or-linux-is-fun-in-terminal/

Watch what you Download!! (contd.)

- Someone created a npm package (shout out to JS people) that implemented some functionality and also hide malware in it.
- On first look this package just enables colorful output to console but the backend gathers all data when submit button is clicked and sends it out.
- https://developers.slashdot.org/story/16/03/27/1258220/new-attack-discovered-on-nodejs-package-manager-npm
- https://hackernoon.com/im-harvesting-credit-card-numbers-and-passwords-from-your-site-here-s-how-9a8cb347c5b5

you can't just use javascript for everything
that's where you're wrong kiddo

PIC - https://devrant.com/rants/682381/rant

Part 1: Introduction to Ethical Hacking

I tilted one of the slides in the regular presentation template 1.6* and nobody noticed yet

Brief Overview of Topics In No Particular Order

- Analysis / Assessment
  - Risk Assessments
  - Technical Assessment Methods
- Security
  - Privacy/Confidentiality (with regard to engagements)
- Procedures/Methodology
  - Security Testing Methodology
- Ethics
  - Professional Code of Conduct
  - Appropriateness of Hacking Activities

Why are We Here

- We, as a chapter of OWASP are here to prevent cyber security failure

The New Terror

- We are here to stop people like him
- How could someone be so evil

The word *HACKER*

- Hollywood and the news made this sound evil, we all know the truth

Pre-1990’s Semantics	
Hacker	**Engineer with free time**
Cracker	**Hacker who causes mischief**

Modern Semantics	
White Hat	**Us, the people trying to make the world more secure**
Gray Hat	**White Hats doing things without permission**
Black Hat	**The bad guys**

Rise of Attacks

- The more valuable something is, the more likely people will abuse it, the internet matures and malicious hacking matures with it
- (Distributed) Denial of Service (DoS)
- Identity Theft
- Internet Vandalism
- Ransomware
- Spyware
- Cross Site Scripting
- Phishing

Motivation for Digital Crime

- Money, money, money
  - Ransomware profits reached at least $2 Billion in 2017
- Everyone and their mother carries the perfect spying toolset in their pockets 24/7
- These devices are also connected to every part of the world
- Digital crime is a business

Generic CyberCrime Examples

- Stealing Data (Passwords, Usernames, Credit Cards)
- Network Intrusion
- Social Engineering (Spam, Phishing)
- Sharing Illegal Material
- Fraud
- Malware
- DoS
- Ransomware

Code of Ethics

CEH holders are expected to follow a strict set of ethics and rules as the information they hold can be used maliciously.

https://www.eccouncil.org/code-of-ethics/

CEH and Penetration Testing

- Penetration Testing may involve handling sensitive client data
- Proper handling of client data is always necessary
- Make sure you and the client have a written agreement that details what you are and aren’t allowed to do on the engagement
- Verbal agreements don’t count
- Always keep the CIA triad in mind

Hacking Methodologies

Finally, the fun stuff

Stage	Action	Description
Information Gathering	Footprinting	Gathering basic system information
	Scanning	Gathering more detailed system & service data
	Enumeration	Looking for exact CVE's and other things to use
Entry	System Hacking	Executing an attack on the system to gain access
	Escalation	Becoming root to have unstoppable force
Persistence	Covering Tracks	Remove evidence of entry in logs
	Backdooring	Being able to go through all of the previous steps, repeatedly and quickly

Things To Keep in Mind

- What information can you use to help the client, because that is your goal?
- Is what I’m doing in scope (allowed by the client) on the test?
- What happens if I take a system down?

Attack Vectors

Consider how you will make your attack approach:

- Malicious Insider
- External Attacker from the outside
- External Attacker from the inside (stolen equipment / network access)
- External Attacker from the inside (social engineering)

Discuss all of these with your client and go with their preference and get it in writing.

The Goal is to Help the Client

- Telling them ‘*your network sucks, pay me*’ isn’t going to cut it
- Fully document all of your findings as well so that you can present and discuss these with your client and help them to understand what they are doing right and what they are doing wrong
- Remember that some fixes may have negative impact on systems and services, be aware of the impact of such fixes

Vulnerability Research and Tools

- https://cve.mitre.org/ The CVE-DB holds just about all system and service exploitations known with well documented effects and you can usually search for proof of concept projects by knowing the CVE number
- Tools like OpenVAS and Nessus can help determine which CVE's effect systems and services you scan.
- Tools appear and disappear every week so you need to keep updated to stay competitive
- Vulnerability research is not the same as Ethical Hacking but the fields do overlap significantly

Pop Quiz

- TODO: or not TODO:

1. Which of the following is an example of a vulnerability

a. Spam email
b. Trojan File
c. Unchecked User Input
d. USB Keylogger

2. How are black-box tests performed?

a. In a lab
b. With no knowledge
c. Maliciously
d. By a black hat

3. Which of the following do you need to evaluate a client's system?

a. Training
b. Permission
c. Planning
d. Nothing

4. The group Anonymous is an example of what?

a. Terrorists
b. Grey Hats
c. Hacktivists

5. Vulnerability research involves which of the following

a. Active Discovery of Vulnerabilities
b. Passive Discovery of Vulnerabilities
c. Applying Security Guidance
d. Designing Secure Networks