Cyber@UC Meeting 42

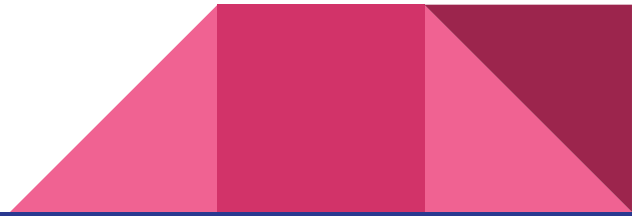
CEH Cryptography

If You’re New!

- Join our Slack **ucyber.slack.com**
- **SIGN IN!**
- 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

- We will be **running a CTF** at the **RevUC Hackathon**!
- **Sport Team Updates?**
- **Planning to visit DEFCON 2018**
- Presenting to **SAB** tomorrow to become official
- HAPPY VALENTINES DAY



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/

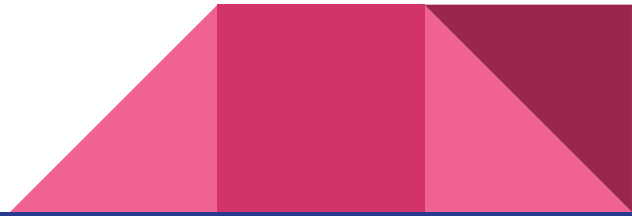
Weekly Content

Nintendo Switch Hacked

- The hack was created by the group Fail0verflow
- Claimed that it can’t be patched or blocked by firmware updates by currently existing switches
- It is a bootrom bug (The code that is similar to a Bootloader for a PC)
- The hack can be performed without a modchip (Similar to a JTAG for an Xbox), which is a external device that is attached to perform the hack
- This allows the device to run other operating systems (currently only Linux)
- Opens the pathway for Homebrew games and other projects

iBoot Leaked

- The IOS 9 bootrom known as iBoot was publicly leaked to Github
- Was leaked by an intern in the company to five of his friends
- The main purpose of leaking was to help them with their efforts of improving the jailbreak software
- While it isn't the latest version of IOS, there are still parts that are in use today, and could be a potential issue if weaponized
- https://github.com/m57/iBoot, However the page has a DMCA takedown notice at the moment



Winter Olympics Opening Ceremony Attacked

- Attack began during the opening ceremony last Friday
- Attack caused 12 hours of downtime
- Cause of disruption was a wiper malware spread using stolen credentials
- Malware has now been dubbed Olympic Destroyer by Cisco Talos
- built -in tools of Olympic Destroyer have also been see in Bad Rabbit ransomeware and Not Petya wiper malware
- Not attributed to any group at this time

https://thehackernews.com/2018/02/pyeongchang-2018-winter-olympics.html

Hacking Government Sites for Cryptocurrency

- Over 4000 government websites have been found to be infected with cryptocurrency mining scripts
- Users who visited these infected websites were immediately cryptojacked
- Infection was made possible through a popular vulnerable third-party plugin called Browsealoud, used by all the infected sites
- Browsealoud is meant to assist visually impaired users

https://thehackernews.com/2018/02/cryptojacking-malware.html

Part 3: Cryptography

You’re here because you don’t have Valentine’s day plans

The Topics Today Go Something Exactly Like This

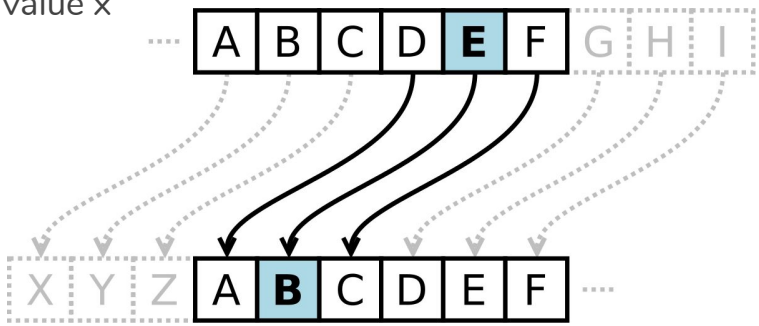
- Types of Cryptography
  - Shift Ciphers
  - Hashing
  - Public-Private Key Pairs
- Tool Overviews
  - HASHNAMEsum
  - John the Ripper (JTR)
- 127.0.0.1 on the range
  - Find & crack the real document

Put on your ~~3D glasses~~ Linux Distro now

KALI

Cryptographic Method: ROTx Cipher

- Good in ancient times when only important people could read
- You change all the letters based on a chosen shift value x
- Sometimes also called caesar cipher when x = 3
- Biggest Weakness: widespread literacy



‘DEF’ becomes ‘ABC’ in ROT3

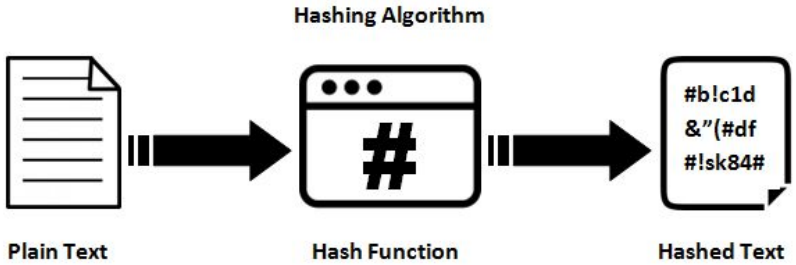
Cryptographic Method: Polyalphabetic Cipher

- Take the previous method and give it more than one shift value
- The new shift value set, or key breaks up our message
- Shorter keys are weak because we can use the use frequency of letters in any given alphabet to try to guess what the encrypted value is
- Longer keys are better because you use a short message and keep each key value unique to prevent decryption
- Weakness: both the encryptor and decryptor must have the same key

‘DEF’ becomes ‘ABC’ with key 555
‘DEF’ becomes ‘AAA’ with key 567

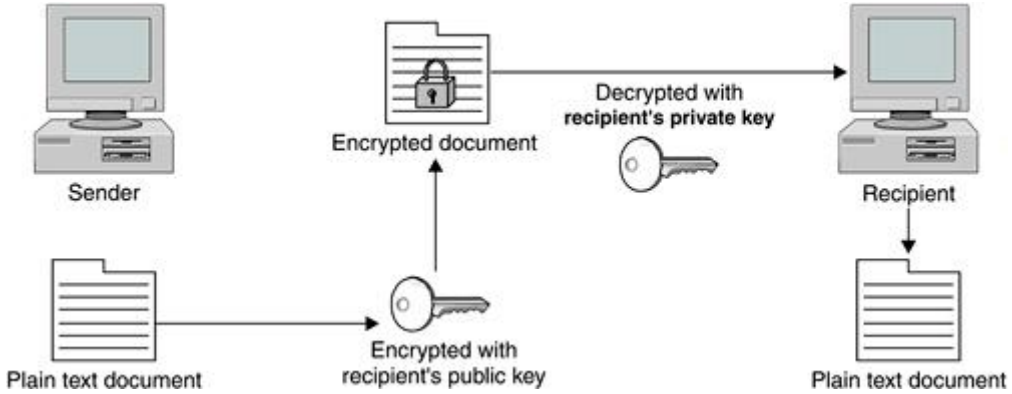
Cryptographic Method: Hashing

- Hashes are **one way** cryptographic functions
- The output is not meant to be decoded ever
- Used to verify data integrity in things such as radio signals
- Also used to store passwords in databases so that they aren't in plaintext but can still be used for authentication
- Ideally f(**x**) = **y** such that g(**y**) = **x** so that no two inputs have the same hash
  - However because hash functions have set size outputs, there will be 'collisions'
- Weakness: hash functions with small length outputs will have multiple **x**'s for any **y**



Cryptographic Method: Key Pairs

- With key pairs two keys are used
- **Public key - encrypts data**
- **Private key - decrypts data**
- This method is very slow but can be used to share a large key for a faster crypto method in a secure way. This is how SSL works.



Tool Overview: HASHNAMEsum

- Installed already on most Linux systems, especially Kali

Hash Function	Hash Length (bigger = better)	Command
MD5	128	md5sum
SHA-1	160	sha1sum
SHA-224	224	sha224sum
SHA-256	256	sha256sum
SHA-384	384	sha384sum
SHA-512	512	sha512sum

Tool Overview: John the Ripper (JTR)

- Installed already on Kali, otherwise: **cd /opt; git clone https://github.com/magnumripper/JohnTheRipper**
- Fast password cracking tool
- Auto-detects hash types
- Can use both dictionary (known password) attacks and brute force attacks
- Can extract password hashes from various local files
- Can crack password hashes stored in databases

Hashing and Cracking!

- To hash a file: **md5sum <file>**

Lets try hashing a “password” with md5 sum!

- **echo -n “Password1” | md5sum | tr -d “ -” >> hashes**

And let’s crack it:

- **john --format=raw-md5 ~/hashes --show**
- **john --format=raw-md5 ~/hashes --wordlist=/opt/SecLists/Passwords/rockyou.txt**

127.0.0.1 on the Range

- It’s Valentine's day and I can’t login to the CYBER@UC email account to see all our love letters.
- I did happen to accidentally download all of my emails as password protected PDF’s that I don’t have the passwords to open them.
- Your challenge is to:
  - Find the email with a **hash containing 1ade10273096e321cb0322fb989164**
  - Find the password to that email using **JTR**
  - **Don’t open that email just yet!** Come up to the front to show everyone how you did it then open the email for all of us to see.

127.0.0.1 on the Range (extra)

- Crack all the PDF's!