Cyber@UC Meeting 74

Mitre Framework

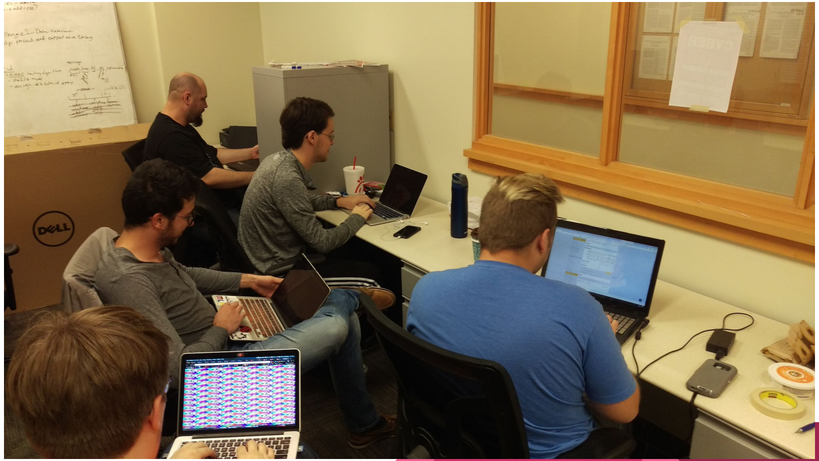
If You’re New!

- Join our Slack: **cyberatuc.slack.com**
- Check out our website: **cyberatuc.org**
- **SIGN IN!** *(Slackbot will post the link in #general every Wed@6:30)*
- Feel free to get involved with one of our committees:

  Content *Finance* *Public Affairs* *Outreach* *Recruitment*
- Ongoing work in our research lab!

Announcements

- **NSA internships** – application window closing **Oct 31st**
- **NSA Codebreaker hack-a-thon** went well
- **UFB DefCon** Funding Approved!
- **Chipotle fundraiser**
  - Saturday Nov 3rd, 4pm–8pm
- Taking **headshots** after this meeting
- **Officer elections** to be held next week
  - Nominees should prepare brief speech
  - Nominations need to be made ASAP!



Election nominees *(incumbents shown in parentheses)*

President *(A.J. Cardarelli)*

- A.J. Cardarelli
- Clif Wolfe
- Ryan Young

Vice President *(Hayden Schiff)*

- Hayden Schiff

Treasurer *(Ryan Baas)*

- Ryan Baas
- Clif Wolfe

Secretary *(Mike Sengleman)*

- Timothy Robert Holstein

Head of Content *(Cory McPhillips)*

- Christopher Morrison

Head of Finance *(Kyle Hardison)*

- Kyle Hardison
- Ryan O'Connor

Head of Public Affairs *(Jai Singh)*

- Jai Singh

Head of Outreach *(Mahathi Venkatesh)*

- Grace Gamstetter
- Mahathi Venkatesh
- Ryan Young

Head of Recruitment *(Greg Barker)*

- Greg Barker

Weekly Content

VestaCP Supply Chain Compromise

- VestaCP is a hosting control platform used to manage multiple websites, emails, databases, DNS records, etc.
- Over the last few months, many users were warned that they were using abnormal amounts of bandwidth
  - Turns out they were being used to make DDoS attacks
- Using malware known as Linux/ChachaDDoS
- The malware was traced to supply chain attack on VestaCP back in May 2018
- Attacker launches the malware from /var/tmp directory via SSH
  - Possible to store the file here due to poor password storage

VestaCP (continued)

- Stage 1 – Persistence: creates a renewal service in the event the malware is stopped or deleted
- Stage 1 – Download: Downloads on port 8852, with IP belonging to 193.201.224.0/24 subnet, Ukraine
  - URL follows a certain pattern `http://{C&C}:8852/{campaign}/{arch}`
  - Available for multiple architectures
- Stage 2 – Running: Downloads and runs stage 3 tasks
- Stage 3 – Tasks: DDoS functions, mainly SYN DDoS attacks

LibSSH Authentication Flaw

- Authentication-bypass introduced in v0.6 in 2014
- Neither OpenSSH nor GitHub are vulnerable
  - GitHub does use libssh, but says it is not vulnerable due to how it uses the library
- Fails to check if a login success message is coming from the server or client
  - A client can just send SSH2_MSG_USERAUTH_SUCCESS message
  - The server then considers authentication to have been successful and allows access without a password
- Shodan search shows about 6,500 servers may be vulnerable
- Versions 0.8.4 and 0.7.6 are patched

iPhone Password Bypass

- Discovered by a Spanish amateur security researcher who also discovered a similar bug in iOS about two weeks ago
- Allows anyone with physical access to your phone access to your photos and sending of them to anyone through Apple Messages
- Works on all current iPhone models and latest iOS
- Current fix until a patch is released is to disable Siri from lockscreen
- Demonstration video in link

Recommended Reading

https://krebsonsecurity.com/2018/10/who-is-agent-tesla/

https://thehackernews.com/2018/10/amazon-freertos-iot-os.html

https://www.darkreading.com/vulnerabilities---threats/us-tops-global-malware-c2-distribution/d/d-id/1333097

https://thehackernews.com/2018/10/tumblr-account-hacking.html

https://www.welivesecurity.com/2018/10/18/tumblr-patches-bug-could-exposed-user-data/

Recommended Reading (continued)

https://www.welivesecurity.com/2018/10/16/phishers-unusual-ploy-targeting-book-publishers/

https://www.darkreading.com/endpoint/privacy/how-to-get-consumers-to-forgive-you-for-a-breach/d/d-id/1333074

https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

https://securelist.com/darkpulsar/88199/

https://securelist.com/darkpulsar-faq/88233/

Recommended Reading (continued)

https://thehackernews.com/2018/10/hacking-tool-luminositylink.html

https://thehackernews.com/2018/10/critical-flaw-found-in-streaming.html

https://thehackernews.com/2018/10/google-android-european-commission.html

https://www.darkreading.com/endpoint/google-patch-to-block-spectre-slowdown-in-windows-10/d/d-id/1333084

https://www.darkreading.com/vulnerabilities---threats/facebook-rumored-to-be-hunting-for-major-cybersecurity-acquisition/d/d-id/1333099

MITRE Framework

The Topics Today Go Something Exactly Like This

- What is Cyber?
- MITRE ATT&CK
- Linux/MAC persistence and privilege escalation

What is Cyber really?

“The internet and its services” - Business People

“The new place to steal” - Black Hats

“The new place to fight” - Governments / Warfare People

“Like phone sex over Omegle?” - Andy from OSU

MITRE ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

- Basically Wikipedia for malware behavior
- Run by the non-profit Mitre near DC
- Includes information about how threat actors and malware behave and how to counter or mitigate such threats

T1156: .bashrc/.bash_profile persistence

Insert code into .bashrc / .bash_profile, similar to AutoRun in Windows

- Allows scripts to run every time bash opens
- Interesting alias entries like sudo can have the user perform priv. Escalation
- Only requires user level access

Red Team Activity

You are an FBI agent with user access to the new Silk Road server. Write your own payload into your .bashrc or .bash_profile that lets you piggy-back off of the system admin using **sudo** without them knowing

- Try something that's hard to notice even when it executes
- Try to keep everything on one line
- Try to make the line delete itself after successful execution so the bad guys suspect nothing

Blue Team Activity

You are an analyst in a Security Operations Center (SOC) for a worldwide software company ~~(You deploy AV and do IT tasks)~~. The logs for the systems are showing an unusually large number of writes to ~/.bashrc and ~./bash_profile

- Write a script that monitors for potential malicious injections into the file
- Make sure to still allow users to modify their files so they can keep working
- Use **syslog** to notify the system of any malicious activity