Cyber@UC Meeting 76

MITRE Framework Continued

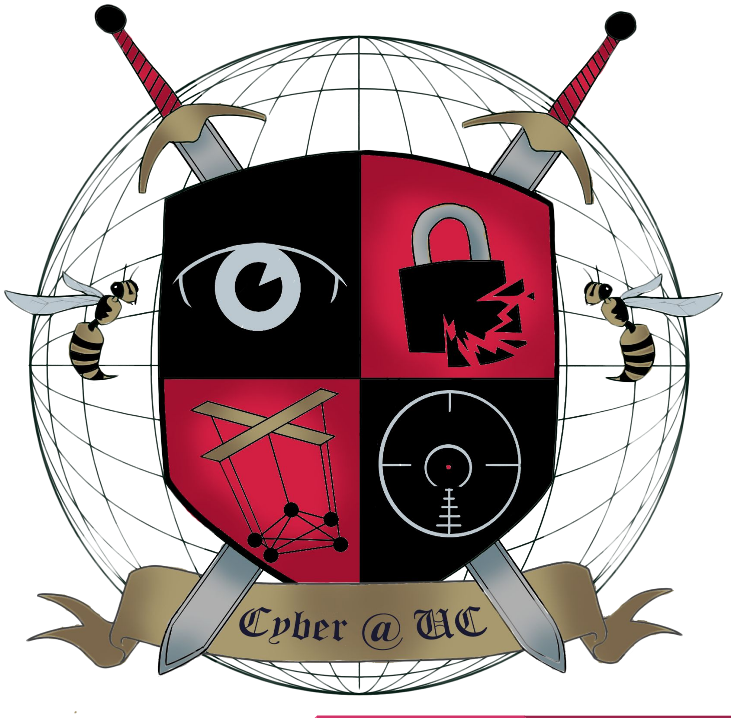
If You're New!

- 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

- **IT'S ELECTION DAY!! Did you vote?**
  - ***You have until 7:30; run to your polling place right now!***
- Emblem Updates!
- **Battelle Visit** Nov. 20th
- NSA internships closed
- US Bank Partnership in the works!
- Chipotle fundraiser
  - $175 raised out of $300 required for donation
  - Learning experience
- Officer elections last week
- AJ Talk thursday
- Lab committee volunteers!



Election Results *(incumbents shown in parentheses)*

President *(A.J. Cardarelli)*
Clif Wolfe

Vice President *(Hayden Schiff)*
Hayden Schiff

Treasurer *(Ryan Baas)*
Ryan Baas

Secretary *(Mike Sengelmann)*
Timothy Robert Holstein

Head of Content *(Cory McPhillips)*
Christopher Morrison

Head of Finance *(Kyle Hardison)*
Kyle Hardison

Head of Public Affairs *(Jai Singh)*
Jai Singh

Head of Outreach *(Mahathi Venkatesh)*
Mahathi Venkatesh

Head of Recruitment *(Greg Barker)*
Greg Barker

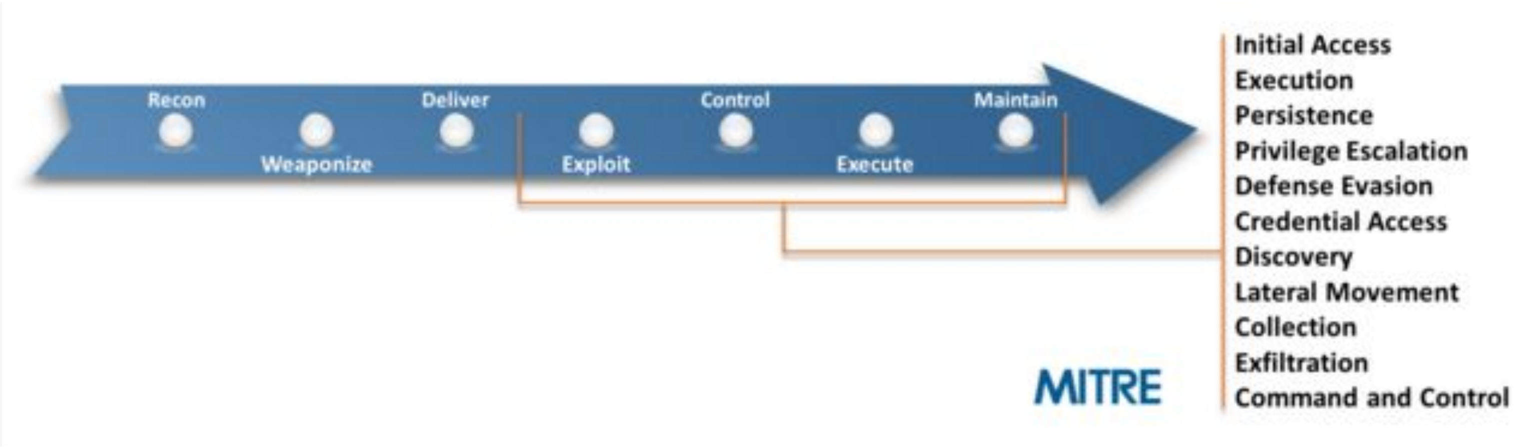
Weekly Content

```
__  __ ___ _____ ____  _____      _  _____ _____ ___     ____ _  __
  \/  |_ _|_   _|  _ \| ____|    / \|_   _|_   _( _ )   / ___| |/ /
 |\/| || |  | | | |_) |  _|     / _ \ | |   | | / _ \/\| |   | ' /
 |  | || |  | | |  _ <| |___   / ___ \| |   | || (_>  <| |___| . \
_|  |_|___| |_| |_| \_\_____| /_/   \_\_|   |_| \___/\/\____|_|\_\

                    Initial Access



hristopher@CRONUS:~$
```

The Topics Today Go Something Exactly Like This

- ATT&CK Techniques and the Cyber Kill Chain
- Initial Access Techniques
- Some Examples
    - Eternal Blue sent via fax (DEF CON 26)
    - SMB Protocol Fuzzing on Nintendo Switch (DEF CON 26)
- Backdoor Factory Exploration

ATT&CK and the Cyber Kill Chain



Initial Access

"The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network." - MITRE

- Boils down to getting code to run on a target via:
  - Technical Exploitation (Remote Code Execution)
  - Social Engineering (Indirect Code Execution)
- For 95% of threats, this means sending out phishing emails and looking for unpatched boxes with exposed services
- 9/10 threats on the OWASP Top Ten 2017 list can manifest as an Initial Access vector that an adversary can exploit

Initial Access Techniques (Technical)

- Drive-by Downloads / Exploits
- Exploits of Public-Facing Services
- Supply Chain Compromise
- Valid Accounts

Initial Access Techniques (Human)

- Malicious USB Devices
- Spear Phishing Attachments (Direct)
- Spear Phishing via Services (Indirect)
- Trusted Relationships (Spys)

Example Technique Implementations

Malicious-USB/USB Rubber Ducky - Emulates a keyboard to abuse trusting USB devices

Hardware-Additions/Poison Tap - Project from Samy Kamkar that routes all of the internet traffic through itself over USB as a MiTM and back door installer.

Public-Services/Eternal Blue - SMB protocol exploit that enabled remote code execution, used by several malware strains from multiple APT’s

Supply Chain/CCBkdr - Malware that was injected into CCleaner’s source code and was distributed with the signed binaries of CCleaner

What the Fax?! (DEF CON 26)

Eternal Blue implemented via custom firmware remotely loaded onto a printer/fax machine via fax:

https://youtu.be/qLCE8spVX9Q?t=2389

Jailbreaking the 3DS (DEF CON 26)

How are exploits like Eternal Blue found? Probably through easy fuzzing like this:

https://youtu.be/WNUsKx2euFw?t=630

Workshop: Backdoor Factory

Backdoor factory is a research utility for injecting backdoors into DLLs/EXE’s

No longer developed, and only for research purposes

Included in Kali, otherwise clone the git repo

Inject a backdoor into an executable then upload it to VirusTotal to see which anti-virus systems would detect it.

```
./backdoor.py -h
```

https://github.com/secretsquirrel/the-backdoor-factory