Cyber@UC Meeting 71

Networking Part II

If You’re New!

- Join our Slack: cyberatuc.slack.com **(URL changed!)**
- **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 Projects:
  - Research lab!

Public Affairs

Useful videos and weekly livestreams on **YouTube**:
youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** @CyberAtUC
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

NSA Scholarships and Internships

Vicki Baker
Director of Cyber Research Initiatives

University of CINCINNATI

NSA Summer Internships

Cyber Operations:

This internship is NSA's premier outreach program for students enrolled in the Cyber Operations specialization at NSA-designated universities. You will gain knowledge of specific cyber-related topics and apply that knowledge to address various real-world mission-related technical challenges. You will work on a broad range of problems involving applications of computer science and engineering.

https://www.intelligencecareers.gov/icstudents.html

(scroll down to CAE-Cyber Operations Summer Intern Program)

University of CINCINNATI

NSA Summer Internships

The NSA Student Intern Application Window has officially opened (1 September 2018) for the 2019 Summer season. It will close for most NSA Internship programs by 31 October 2018.

In addition to sharing the information with your Cyber Ops students please pass this email and attachments to your Human Resources (or Student Resources) program offices as well as share with your Cyber operations Faculty.

Warmest Regards,
Heather

Notes:
1. There are 30+ NSA Summer Intern Programs - students are permitted to apply for more than one NSA summer internship.
2. Attached is the description for the CAE-CO Summer Intern Program, the one that is specifically tied to our CAE-CO program. This is a copy of information found online at: https://www.intelligencecareers.gov/icstudents.html
3. Attached, is an instruction document from the IC Jobs website that gives some helpful advice on how to complete the application process. https://www.intelligencecareers.gov/NSA/Applying_Online_Doc.pdf
4. For help with the Summer Intern Program, your students SHOULD NOT use the AskCAECyberOps alias – there is intern program contact information in the intern program descriptions.

5.The To Apply instructions in the attached and on-line description for the CAE-Cyber Operations Summer Intern Program is a bit outdated. It should read as follows:

When on the https://www.intelligencecareers.gov/icstudents.html web site:

To submit a resume online during open season:

Press on the "Job Search/Apply" Tab at the top of the page.

Select "~~National Security Agene~~y." Should be "Unified Job Application Portal"

~~To apply, click the arrow next to the words, "Ready to Apply?"~~

In the search box, type keywords "CAE in Cyber Operations Summer Intern Program"

Click on "Search" and select "CAE in Cyber Operations Summer Intern Program"

At the bottom of the description, Click "Apply" and follow the direction as prompted.

NSA Summer Internships

Computer Science:

As a CSIP intern, you will apply your computer science skills to NSA hardware and software systems. Interns are assigned to projects that contribute to NSA's mission and culminate in a short presentation and technical paper. Projects are typically in the areas of:

Ontology/Taxonomy and Graphical Analysis
Information Retrieval
Information Visualization
Computer & Network Security
Information Query and Question Answering
Big Data
Knowledge and Database Crawling
Signal Processing
Software Agent Planning and Control
Architecture & Systems
Machine Learning/Artificial Intelligence
Knowledge and Data Representation, Distillation and Sharing
Human Language Technology/Computational Linguistics

https://www.intelligencecareers.gov/icstudents.html (scroll down to Computer Science Internship Program)

University of CINCINNATI

NSA Summer Internships

Signals Intelligence Collection Program:

Computer competence is required, but students who are majoring in social sciences are also welcome to apply for this internship, where they will apply computer, technical, analytic, communication, problem solving and/or critical thinking skills to NSA's signals intelligence (SIGINT) mission. You will devise strategies, find solutions to complex challenges, design and write computer programs; test hardware and software; build and secure websites; analyze and display data; discern the best methods of collection; develop accesses; analyze and conclude results, and/or develop processing techniques that satisfy foreign intelligence requirements.

https://www.intelligencecareers.gov/icstudents.html

(scroll down to Signals Intelligence Collection Program)

University of CINCINNATI

NSA Summer Internships

Cyber Summer Program:

The Cyber Summer Program (CSP) is NSA's premier program for the best undergraduate and graduate computer science, engineering, mathematics, network security and information assurance students in the country. You will work on a broad range of problems of your own choosing, involving applications of computer science and engineering. You will learn and develop data analysis, network analysis and exploitation techniques and apply that knowledge to obtain real-time solutions for mission-critical cyber-related problems.

https://www.intelligencecareers.gov/icstudents.html

(scroll down to Cyber Summer Program)

University of CINCINNATI

NSA Summer Internships

Data Center Management Intern Program:

Interns will gain experience through a hands-on approach to managing a data center. From deployments of new systems and their associated mechanical, electrical, and IT requirements, you will gain valuable knowledge and insight for a growing demand in the data center marketplace. Past intern projects have focused on how to better manage aspects of a data center, how to optimize data center efficiency and more.

https://www.intelligencecareers.gov/icstudents.html

(scroll down to Data Center Management Intern Program)

University of CINCINNATI

NSA Summer Internships

DUE DATE:

October 31, 2018

University of CINCINNATI

NSA Summer Internships

Cryptanalysis and Signals Analysis:

In this highly competitive program, undergraduate students will solve problems in mathematics, cryptology and communications technology in support of national security. These problems often involve applications of abstract algebra, geometry, number theory, analysis, probability, statistics, combinatorics, graph theory, algorithms and computer science. State-of-the-art computing resources are available to all students, who will be mentored by agency experts, collaborate to solve challenging problems, and present their work in both technical talks and papers, to be published internally at NSA.

https://www.intelligencecareers.gov/icstudents.html

(scroll down to Director's Summer (DSP)/Cryptanalysis and Signal Analysis Summer Program)

University of CINCINNATI

NSA Summer Internships

DUE DATE:

October 15, 2018

University of CINCINNATI

NSA Scholarships

(former IASP Scholarship – being renamed)

The Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) annually announces a Department of Defense Information Assurance Scholarship Program (IASP) grant and scholarship competition. The program is designed to:

- Increase the number of new entrants to DoD who possess key information assurance (IA) and IT skill sets
- Serve as a mechanism to build the nation's IA infrastructure through grants to colleges and universities jointly designated by the National Security Agency (NSA) and Department of Homeland Defense as Centers of Academic Excellence in Information Assurance Education
- Serve as a tool to develop and retain well-educated military and DoD civilian personnel who support the Department's critical IT management and infrastructure protection functions

University of CINCINNATI

NSA Scholarships

Undergraduate Training Assistance Program

A small number of high-achieving and committed secondary school seniors and/or college freshmen and sophomores interested in a career in public service will be offered tuition assistance to accredited colleges or universities, provided challenging summer work, and guaranteed a position in their field of study upon graduation from this highly competitive program. Minorities, women and the disabled needing financial assistance to complete their undergraduate education are strongly encouraged to apply.

University of CINCINNATI

NSA Scholarships

Science, Mathematics and Research for Transformation (SMART)

Students, including current DoD employees seeking advanced degrees, work in a full-time, paid summer internship. Participants must be pursuing degrees in science, technology, engineering and mathematical (STEM) fields of study. Benefits include full tuition and fees, stipend and guaranteed employment upon graduation.

University of CINCINNATI

NSA Scholarships

Louis Stokes Educational Scholarship Program (DIA)

This highly competitive program targets high-achieving, committed secondary school seniors and college freshmen and sophomores interested in a career in public service. The program offers scholarship awardees tuition assistance to accredited colleges and universities, challenging summer work and a guaranteed position in their field of study upon graduation. Students will attend classes full-time during the academic year and work at DIA during the summer in positions related to their course of study. While in school, students must maintain an overall cumulative grade point average (GPA) of 3.0 on a 4.0 scale (or its equivalent) for each semester/quarter.

University of CINCINNATI

Announcements

- **US Bank visit** *THIS PAST FRIDAY*
  - It was a great time!
- **Chipotle fundraiser**
  - Saturday Nov 3rd 4pm-8pm
- **MakeUC Hack-a-thon** this past weekend
  - Hope you checked it out!
- **NSA Codebreaker Challenge** has started codebreaker.ltsnet.net
- Outreach to **Lakota East**
- Think about **Elections**
- **Register to vote!** vote.gov

Weekly Content

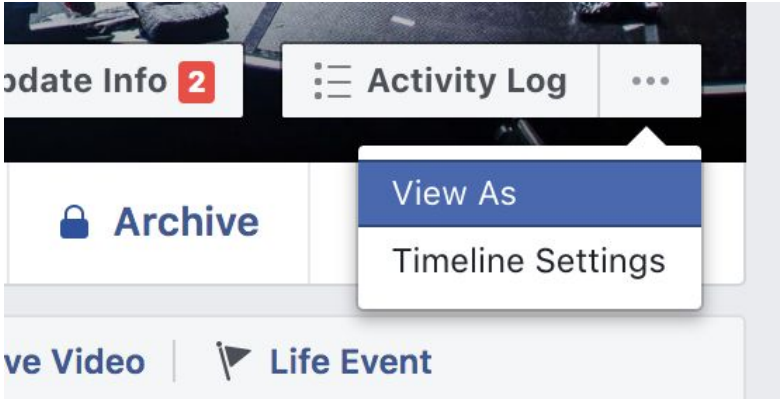
Facebook vulnerability

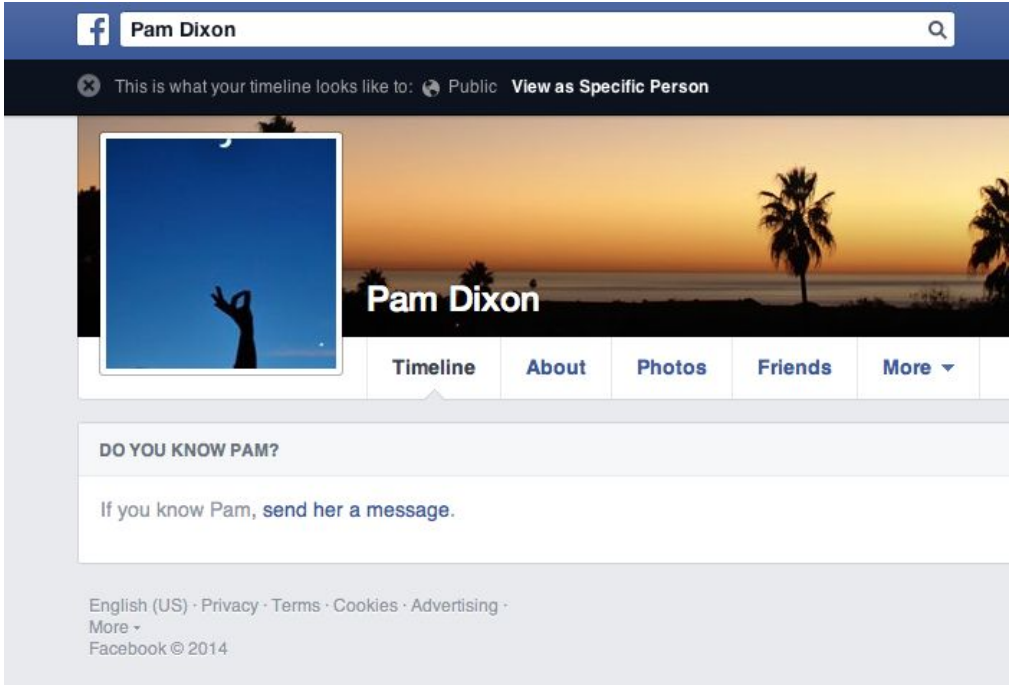
- Attackers took over people's accounts!
- 50 million known affected + 40 million possibly affected
- Still unclear what the attackers did with the access/what their motive was

so.... what the hell happened??

https://newsroom.fb.com/news/2018/09/security-update/

"View As"


odate Info 2
Activity Log
View As
Timeline Settings
Archive
ve Video
Life Event


Pam Dixon
This is what your timeline looks like to: Public View as Specific Person
Pam Dixon
Timeline
About
Photos
Friends
More
DO YOU KNOW PAM?
If you know Pam, send her a message.
English (US) · Privacy · Terms · Cookies · Advertising · More
Facebook © 2014

3 bugs in tandem

1. View As incorrectly allowed opportunity to post videos
2. Video uploader incorrectly had permissions of Facebook mobile app
3. Video uploader generated access tokens for "Viewing As" user, not you

This is a mess!!

Project Zero Finds New Linux Kernel Exploit

- Vulnerability has been in linux kernel between 3.16 and 4.18.8
- Cache invalidation bug in linux memory management
- Use-after-free vulnerability allows attacker to gain root privileges
  - Use-after-free: memory corruption exploit allowing DoS or privilege escalation
- Released PoC takes about an hour to gain root access
- Discovered September 12th, patched and disclosed by 18th
- Debian and Ubuntu still had not released updates by 22nd

https://thehackernews.com/2018/09/linux-kernel-exploit.html

Recommended Reading

https://thehackernews.com/2018/09/apple-server-hack.html

https://krebsonsecurity.com/2018/09/secret-service-warns-of-surge-in-atm-wiretapping-attacks/

https://thehackernews.com/2018/10/ghostdns-botnet-router-hacking.html

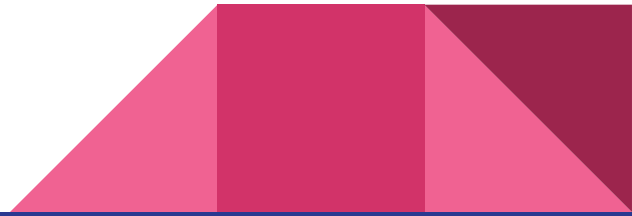
https://securelist.com/roaming-mantis-part-3/88071/

https://www.welivesecurity.com/2018/09/28/whos-behind-ddos-attacks-uk-universities/

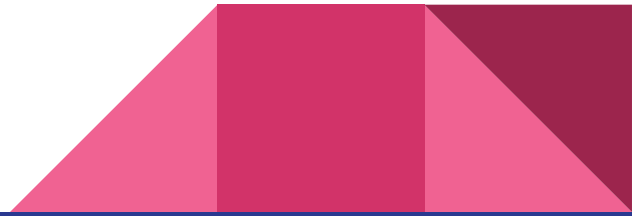
Networking Part 2: Network Analysis

Download Wireshark

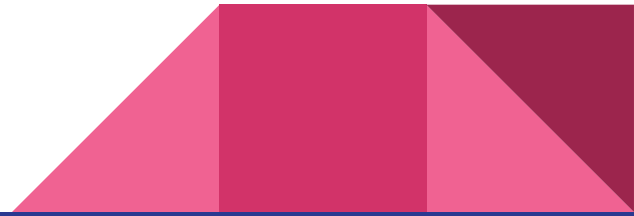
- https://www.wireshark.org/ for Windows and Mac
- Sudo apt get wireshark should work for linux, pre-installed on kali
- Using a sandbox, such as a virtual machine is recommended when performing any sort of malware analysis, including network traffic analysis



TCP vs UDP

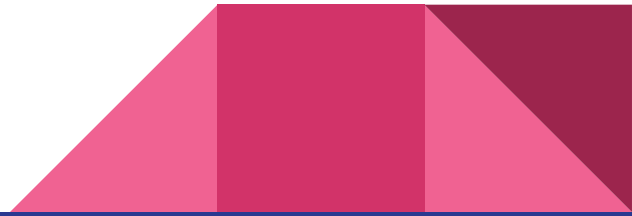


What IP addresses are involved? (2pts)



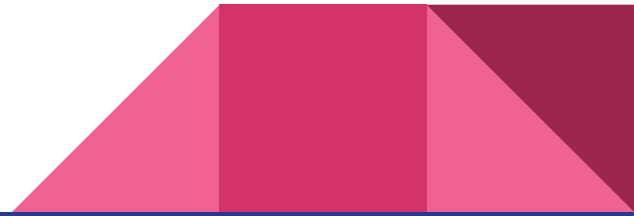
What can we learn about the attacker? (2pts)

We are talking about location here



How many TCP sessions are in the file? (2pts)

How long did the attack take? (2pts)

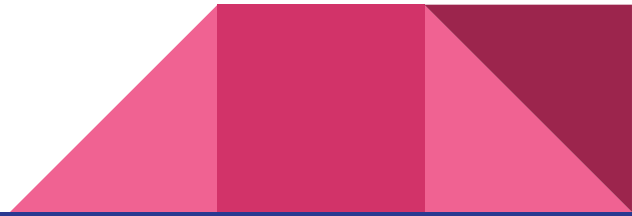


Which OS was targeted by the attack?

Which Service was targeted?

Which Vulnerability was used?

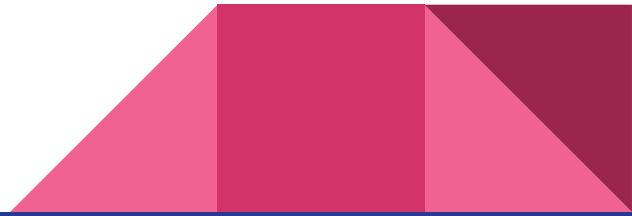
2pts each, 6pts total



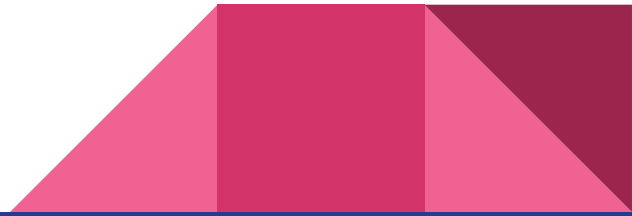
Give general overview of the actions performed?

6pts toal

Hint: try to describe the actions taken in each tcp stream



Was a honeypot used? (4pts)



Was malware involved? 2pts

Hint: think hashing

Was this attack manual or automated? (2pts)