THE PACKET

SPRING

APRIL 2021

IN THIS ISSUE

ART BY @ GEORGE BECKER

THE UNIVERSITY OF ARIZONA

THE INAUGURAL

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

THE FUTURE OF INTELLIGENCE

Wednesday - Friday, April 7-9, 2021

8:30AM - 5:00PM

University of Arizona

VIRTUAL EVENT

- Explore careers in the intelligence community
- Learn about the future of national intelligence
- Meet with national, state and industry intelligence leaders

Learn more and register online at

>> https://intelligence-studies.azcast.arizona.edu/content/summit

University of Arizona and Community College students are FREE

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

AGENDA | APRIL 7-9, 2021 | 8:00AM – 5:00PM MST (DAILY)

Wednesday April 7, 2021

Opening Session **8:30AM – 9:15AM** **Patrick Kerr**	• **Welcome & Introductions** • Mr. Jon Dudas Senior Vice President and Chief of Staff for the University of Arizona The opening speaker, Mr. Jon Dudas discusses the 4th Industrial Revolution (4IR), the requirements and measurements for success in the 4IR, and the University of Arizona's (UA) role in the 4IR. Dudas, will deep-dive on the cyber and intel interplay into the 4IR and tells how UA is responding through research, education, and other ventures to the cyber and intel convergence.
9:15 10:15AM **Linda Denno**	• **Keynote Speaker: 'The Future of Intelligence**' Major General Anthony Hale, Commanding General Ft. Huachuca & USAICOE MG Hale discusses the future of US Intelligence Community inclusive of the 18 agencies. He addresses future intelligence challenges and opportunities from shaping operations to driving combat operations. MG Hale also provides clarity on how intelligence will drive cyber operations, kinetic operations, and information warfare.
Lunch Session **11:30PM – 12:30PM** **Chet Hosmer**	• **Guest Speaker: Open-Source Intelligence Collection & Analysis** Ms. Cynthia Hetherington, MLS, MSM, CFE, CII President & Founder, Hetherington Group Ms. Hetherington exposes open-source intelligence (OSINT) and its use by civilian and industry entities. Ms. Hetherington offers insight into the collection of intelligence through publicly available information, the value of OSINT, and the application of OSINT in corporate business operations. Cynthia concludes her session by forecasting the future of OSINT operations in the private industry sector.
12:30PM - 1:30PM **Patrick Kerr**	• **Guest Panel: Law Enforcement Intelligence & Intelligence Driven Policing** Panel Chaired By: Federal Bureau of Investigation Participants: ACTIC, HIDTA, Tohono O'odham Nation Police Department, Cochise County Sheriff The FBI explains the collection, use, and sharing of intelligence to drive law enforcement operations across sectors starting at the federal to the individual. The FBI further discusses the use of Infragard and the information sharing process. The ACTIC, HIDTA, Tohono O'Odham Tribal Police Department, and Cochise County Sheriff's Office will each discuss their mission, area of focus, use of intel in driving criminal justice and policing activities, their interplay and intelligence/information sharing across all levels starting from the individual to the federal government. Additionally, each organization will discuss career path options for those interested in law enforcement and intelligence.
Afternoon Session **3:00PM – 3:30PM** **Linda Denno**	• **Guest Speaker: Intelligence Community – Center for Academic Excellence** Mr. Michael Bennett, ICCAE Program Director Office of the Director of National Intelligence Mr. Bennet provides an overview of the US Intelligence Community agencies (IC) and the Intelligence Community Center for Academic Excellence (ICCAE) Program. Mr. Bennet discusses the goals and objectives of the IC for the future collaboration from the Office of the Director of National Intelligence Perspective. Lastly, he qualifies how the ICCAE program will aid in achieving the IC's strategic plans and the benefits of the ICCAE program.
3:30PM -5:00PM **Patrick Kerr**	• **Guest Panel: Workforce Development – Next Generation of Intel Professionals** Panel Chaired By: Office of the Director of National Intelligence Participants: Department of State, Department of Energy, Federal Bureau of Investigations, National Geospatial-Intelligence Agency The Workforce Panel provides an opportunity for multiple IC agencies to discuss their current and future workforce requirements. Attendees will get gain a basic overview of the agency's mission, their role in support of the IC, and opportunities for employment. The panel consists of five IC agencies and allow for Q&A from the attendees; each agency will have approximately 10-15 min to present information.

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

AGENDA | APRIL 7-9, 2021 | 8:00AM – 5:00PM MST (DAILY)

Thursday
April 8, 2021

Morning Session **8:30AM – 9:15AM** **Linda Denno**	• **Welcome Back & Introductions** • Title Sponsor Address Mr. Austin Yamada, President & CEO University of Arizona Applied Research Corporation Our Title Sponsor, the University of Arizona- Applied Research Corporation (UA-ARC) led by Mr. Austin Yamada, provides the welcome back message for day two of the event and discusses the UA-ARC's role at the University of Arizona. Mr. Yamada, provides and overview of the UA-ARC and their collaborations efforts with University in classified research across different sectors including intel, space, and cyber, and how they support future solutions for the US Intelligence Community.
9:15AM – 10:15AM **Patrick Kerr**	• **Keynote Speaker: 'The Future of Information Warfare'** Lieutenant General Stephen G. Fogarty, Commanding General U.S. Army Cyber Command LTG Fogarty delivers his vision for the future of cyberspace and the new Information environment. His speech highlights how signal, information operations, Information warfare, cyber, and intel come together to shape capabilities for the US. Further, he discusses how the increased capabilities will help support national security decision makers by providing them with information advantage over our adversaries.
Lunch Session **11:30PM –** **12:30PM** **Chet Hosmer**	• **Guest Speaker: Social Engineering** • Chris Hadnagy, Chief Human Hacker, Social-Engineer, LLC Mr. Chris Hadnagy, Chief Human Hacker explores the great depth of which social engineering is employed in data breaches. Chris will deep-dive into what social engineering is, the types of social engineering techniques employed, by who and how.
12:30PM – 1:30PM **Patrick Kerr**	• **Guest Speaker: Cyber Threat Intelligence Sharing** Mr. Tim Roemer, Chief Information Security Officer, State of Arizona Mr. Tim Roemer discusses his role and responsibility as the state of Arizona CISO, the challenges and opportunities he encounters in cyber threat intelligence sharing across the government, corporate entities, and private citizens, and how he overcomes obstacles to ensure the protection of Arizona.
Afternoon Session **3:00PM – 3:30PM** **Chet Hosmer**	• **Student Presentation: Computational Propaganda** Jacob Denno, Cybersecurity Graduate, University of Arizona & Dan Carroll, Principal Data Scientist, CVS Health Jacob and Dan, present on automated propaganda techniques used to sway information in cyberspace and the information environment, by creating fake news, influence trending, changing the narrative using technological advancements through machine learning and artificial intelligence.
3:30PM -5:00PM **Patrick Kerr**	• **Guest Panel: Workforce Development – Next Generation of Cybersecurity Professionals** Panel Chaired By: **(Pending)** Participants: The Washington Center, National Security Agency, USA NETCOM **(Pending other participants)** The Workforce Panel provides an opportunity for multiple IC agencies and private organizations to discuss their current and future workforce requirements. Attendees will get gain a basic overview of the agency's mission, their role in support of the IC, and opportunities for employment. The panel consists of five IC agencies and allow for Q&A from the attendees; each agency will have approximately 10-15 min to present information.

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

AGENDA | APRIL 7-9, 2021 | 8:00AM – 5:00PM MST (DAILY)

Friday April 9, 2021

Morning Session: **8:30AM – 9:15AM** **Patrick Kerr**	- **Welcome Back & Introductions** - Opening Remarks Dr. Gary Packard, Dean College of Applied Science & Technology The founding Dean of the College of Applied Science & Technology provides the opening remarks for the event's last day and an overview of CAST's alignment with University of Arizona's 4IR strategy. Additionally, he offers details on how CAST degree programs will offer the opportunity to every student to understand the cybersecurity environment.
9:15AM-10:15AM **Linda Denno**	- **Keynote Speaker: 'Intelligence & Cyber Support - A Commander's Perspective'** General Joseph L. Votel, USA (Ret.) President & CEO, Business Executives for National Security (BENS) GEN Votel, a national leader provides the future leaders perspective of requirements that will be needed to make national security decisions across the operational environment. He discusses the current and future complex environment challenges that will need to be addressed by intelligence, cybersecurity, and information operations professionals in order for the next COCOM Commander or US President to make sound decisions on a global scale.
Lunch Session **11:30AM-12:30PM** **Patrick Kerr**	- **Guest Speaker: The Cyber-Intelligence Convergence in Private Industry** Jeff Frazier, Chief Operating Officer, Pryon Inc. Mr. Jeff Frazier provides the perspective from the "Office of the CEO" as to why intelligence and cybersecurity cells are imperative in the private industry business environment. Mr. Frazier identifies the future requirements for cyber, intel, and information operations for corporations to counter business threats and challenges presented to multinational corporations.
12:30PM – 1:15PM **Chet Hosmer**	- **Student Panel:** 1LT Sean Michael Mohoroski, Cybersecurity,U.S. Airforce, Ms. Sylvia Vadney, IIO Student, Ms. Sara-Robinson Camarena Cyber Ops Student Wildcat alumni and current students provide renditions of their academic and career achievements. Each participants discusses their personal story on how they became a CAST student, their degree program, achievements they've had while at CAST, and what their future holds.
Afternoon Session **3:00PM-4:30PM** **Pat Kerr**	- **Guest Panel -Workforce Development** - Panel Chaired By: ACA/SFAZ Participants: General Dynamics, The Washington Center, Jacobs **(Pending other participants)** The Workforce Panel provides an opportunity for multiple private industry organizations to discuss their current and future workforce requirements. Attendees will get gain a basic overview of the organization's mission, their role in support of the 4IR, and opportunities for employment. The panel consists of five organizations and allow for Q&A from the attendees; each agency will have approximately 10-15 min to present information.
4:30PM– 5:00PM **Pat Kerr**	- **Closing Remarks & Adjourn** Dr. Linda L. Denno, Civilian Aide to the Secretary of the Army, Arizona Dr. Linda Denno, Civilian Aide to the Secretary of Army for Arizona closes the event with an overview of opportunities available through the US Army and provides the closing remarks.

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- **BEGIN MESSAGE** ---

Welcome to the **APRIL** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and this marks the one-year anniversary that I have spent writing and producing this publication. There have been many design changes over the past 12 months, and I am happy with how this is looking so far. In this edition I am introducing a basic assembly project that will allow anyone to code a bootloader that can be used to make it appear a system has been compromised. I was trying to find something to celebrate April Fool's Day and teach everyone about bootloaders. The code can be modified to display your own ASCII graphics to make it your own. You are limited by size however so make sure not to get too crazy with your designs. If nothing else, I hope to get some of you interested in assembly language and to display some of the powers you have working directly with the system. This month the University of Arizona will also host the Southern Arizona Intelligence Summit which I encourage everyone to attend as many of the speakers represent many of the thought leaders in protecting cyber infrastructure. The Spring semester is almost over, and Summer is just right around the corner. The Fall Semester will soon have classes open, and they will fill up fast so make sure to discuss your plans with your advisor. The month of March reminded the cybersecurity community the dangers 0-days pose to your infrastructure and how security solutions need to overlap with each other. The environment you will be entering once you graduate will never leave you bored for long as the threat environment is always changing and adapting.

--- END MESSAGE ---

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

NOW IT HAS GONE TOO FAR, HACKERS ARE ATTACKING BEER NOW

The Molson Coors Beverage Company has suffered a cyberattack that is causing significant disruption to business operations. Multiple sources in the cybersecurity industry have told Bleeping Computer that Molson Coors suffered a ransomware attack but could not share what malware gang was involved. It is unknown if the attack is localized to the Molson Coors corporate network or if it has spread to the networks of their brands.

CHINA BELIEVED TO BE BEHIND NEW LINUX MALWARE REDXOR

Security researchers at Intezer have discovered a previously undocumented backdoor dubbed RedXOR, with links to a Chinese-sponsored hacking group and used in ongoing attacks targeting Linux systems. Nation-state hackers ARE FOCUSING more on targeting Linux systems, as highlighted by a 2020 Intezer report summarizing the last ten years of Linux APT attacks which said, “nation-state actors are incorporating offensive Linux capabilities into their arsenal and it's expected such attacks will increase over time."

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

K-12 SCHOOLS REPORT 18% INCREASE IN CYBER INCIDENTS

The K-12 Cybersecurity Resource Center recorded 408 publicly disclosed security incidents last year, an increase of 18% from 2019 and the highest number since it began tracking incidents in 2016. These include student and staff data breaches, ransomware and other malware attacks, phishing campaigns and social engineering scams, and denial-of-service (DoS) attacks. This equated to a rate of at least two incidents per school, per day, over the course of last year.

HACKING THE HACKING FORUMS IS THE NEW THING TO DO NOW

The longest running and most venerated Russian-language online forums serving thousands of experienced cybercriminals have been hacked. Members of all three forums are worried the incidents could serve as a virtual Rosetta Stone for connecting the real-life identities of the same users across multiple crime forums. The compromise of Maza and Verified and possibly a third major forum has many community members concerned that their real-life identities could be exposed.

NETFLIX KNOWS YOU SHARE YOUR PASSWORD. IT'S TESTING A WAY TO STOP YOU

Netflix is testing a new pop-up message that warns people who are sharing a password and don't live with the password holder that they need to pony up and pay for their own account. Password sharing is incredibly popular on Netflix and other streaming sites, where people might piece together a portfolio of streaming subscriptions by sharing passwords with their parent, ex-partner, friend or college roommate's dad's cousin. Restricting people from sharing passwords could force some to pay for their own accounts but it also might drive others to simply give up on Netflix and turn to one of the other myriad streaming options. Netflix's Terms of Service state that accounts are for personal use and "may not be shared with individuals beyond your household." The streaming giant has tiered price options that allow customers to stream on one, two or four screens at once. The current test appears to ask users to verify that they are the account holder (or a member using the same password) by asking them to enter a verification code that can be texted or emailed to them. But there also seems to be a way to "verify later," or ignore the prompt.

HOUSE, SENATE DEMOCRATS UNVEIL $94 BILLION BILL TO IMPROVE INTERNET ACCESS

Thirty House and Senate Democrats unveiled a new $94 billion proposal to make broadband Internet access more accessible and affordable nationwide, aiming to remedy some of the digital inequalities that have kept millions of Americans offline during the coronavirus pandemic. Even before the pandemic, the U.S. government had struggled to close the digital divide: At least 18 million Americans lacked reliable connectivity, federal regulators found in a report last year, cautioning at the time that the number might be higher. Some of the money is tucked into the new stimulus that lawmakers adopted, known as the American Rescue Plan, which sets aside $7 billion to help schools furnish the devices that students need to complete their classwork.

MALWARE OPERATOR EMPLOYS NEW TRICK TO UPLOAD ITS DROPPER INTO GOOGLE PLAY

Researchers at Check Point recently discovered that the operator of a malware tool that breaks into mobile users' financial accounts was employing a novel new method to sneak its malware into Google's official Android Play mobile app store. The method involved using Google's own Firebase platform for command-and-control (C2) communications and using GitHub as a third-party hosting platform for downloading the main malware. It allowed the attacker to fool and pass the security checks that Google conducts on all applications before they can be uploaded to its app store or downloaded on a device. When a user downloaded any of the weaponized apps, the app would perform as expected, even as it executed malicious activity in the background. The researchers found that the dropper, called Clast82, was designed specifically to evade detection by Google's Play Protect scanning mechanisms during the app evaluation period. Once the evaluation was complete, the malware author essentially turned on the malicious behavior and got the dropper to install the AlienBot Banker and MRAT, two mobile malware families.

NATIONAL GUARD SUPPORTS CITY OF KINGMAN FOLLOWING RANSOMWARE ATTACK

The Arizona National Guard’s Cyber Joint Task Force is investigating a ransomware attack on the city of Kingman’s infrastructure technology. A spokesperson for the city says that they are having to do things manually from timecards, to helping residents pay bills. A spokesperson for the Arizona National Guard tells ABC15 that they had a five-person team that spent 325 total man hours on site with the City of Kingman. The Cyber Joint Task Force (CJTF) can respond to state and local agencies that are experiencing attacks. The City of Kingman said that they still cannot access some functions, including specialized software, files, and more which are still not accessible to most departments.

SIGN UP FOR CLASSES SOON

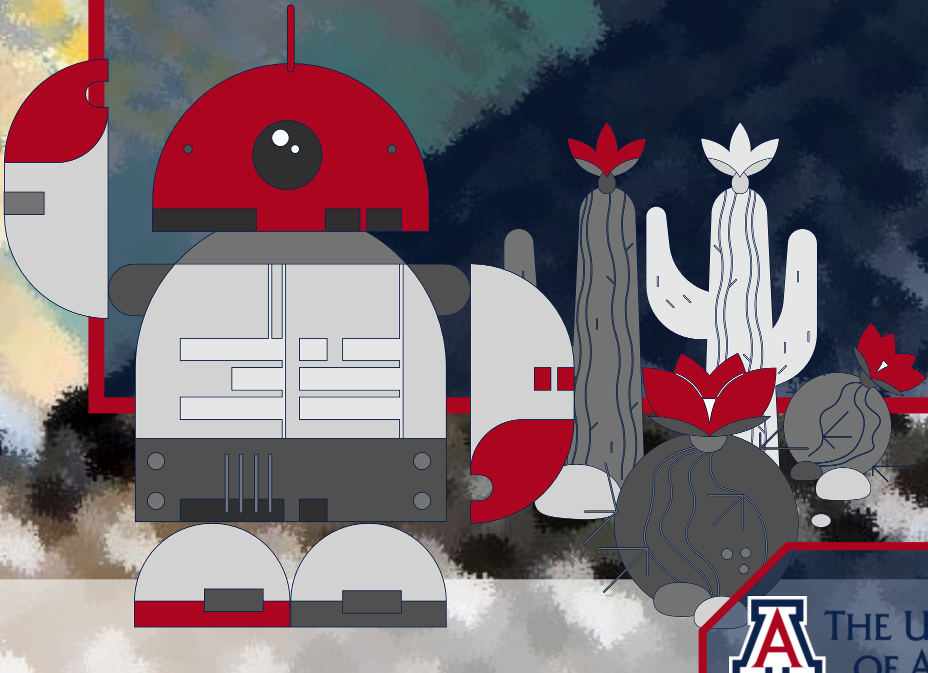
NOTE FROM YOUR ADVISORS

SUMMER AND FALL 2021 ENROLLMENT OPENS ON APRIL 5TH! COURSES OFTEN FILL QUICKLY, SO ENROLL EARLY TO GET THE BEST SELECTION! PLEASE TOUCH BASE WITH YOUR ACADEMIC ADVISOR TO VERIFY THE COURSES YOU PLAN ON TAKING ARE IN LINE WITH YOUR DEGREE PLAN. YOU CAN ALSO SCHEDULE AN APPOINTMENT WITH THEM IF YOU NEED ADDITIONAL SUPPORT WITH YOUR SUMMER AND/OR FALL ENROLLMENT. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE: HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

SUMMER SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 310	INTRO SECURITY PROGRAMMING I	BOOK
CYBV 311	INTRO SECURITY PROGRAMMING II	BOOK
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 385	INTRO TO CYBER OPERATIONS	BOOK
CYBV 400	ACTIVE CYBER DEFENSE	BOOK 1, BOOK 2
CYBV 435	CYBER THREAT INTELLIGENCE	BOOK 1, BOOK 2, BOOK 3
CYBV 436	COUNTER CYBER THREAT INTEL	BOOK



SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 303	WINDOWS SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	BOOK
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	BOOK
CYBV 382	NETWORK FORENSICS	BOOK
CYBV 385	INTRODUCTION TO CYBER OPERATIONS	BOOK
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	BOOK 1, BOOK 2
CYBV 400	ACTIVE CYBER DEFENSE	BOOK 1, BOOK 2
CYBV 435	CYBER THREAT INTELLIGENCE	BOOK 1, BOOK 2, BOOK 3
CYBV 436	COUNTER CYBER THREAT INTEL	BOOK

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 437	DECEPTION & COUNTER-DECEPTION	BOOK
CYBV 450	INFORMATION WARFARE	BOOK 1
CYBV 454	MALWARE THREATS & ANALYSIS	BOOK
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	PENDING BOOK SELECTION
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	BOOK
CYBV 473	VIOLENT PYTHON	BOOK 1, BOOK 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	BOOK 1, BOOK 2
CYBV 475	CYBER DECEPTION DETECTION	PENDING BOOK SELECTION
CYBV 477	ADVANCED COMPUTER FORENSICS	PENDING BOOK SELECTION
CYBV 479	WIRELESS NETWORKING AND SECURITY	PENDING BOOK SELECTION
CYBV 480	CYBER WARFARE	BOOK 1, BOOK 2
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION

BEFORE YOU KNOW WHERE YOU GO, YOU NEED TO KNOW WHERE YOU CAME FROM

CYBER SECURITY HISTORY

SUCH A SIMPLE VIRUS, THE VIENNA VIRUS

The Vienna virus was an extremely simple virus and became a template for more complex and innovative viruses like Ghostballs, Chameleon and (possibly) Zerobug as the source code was published in many places. Damage done by this virus was probably minimal regardless of how widespread it became. Vienna was the first virus to be neutralized by an antivirus program written by German hacker Bernd Fix, this event marks the first documented antivirus software ever written.

APRIL 1, 1988

HEARTBLEED VULNERABILITY PUBLICLY DISCLOSED

Heartbleed was a security bug in the OpenSSL cryptography library, which was a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed could be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It resulted from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. The Canada Revenue Agency reported a theft of Social Insurance Numbers belonging to 900 taxpayers and said that they were accessed through an exploit of the bug during a 6-hour period on 8 April 2014. The UK parenting site Mumsnet had several user accounts hijacked, and its CEO was impersonated. The site later published an explanation of the incident saying it was due to Heartbleed and the technical staff patched it promptly. Anti-malware researchers also exploited Heartbleed to their own advantage in order to access secret forums used by cybercriminals. The problem can be fixed by ignoring Heartbeat Request messages that ask for more data than their payload need.

APRIL 1, 2014

CHERNOBYL VIRUS DESTROYS BIOS AS A STUDENT CHALLENGE

CIH, also known as Chernobyl or Spacefiller, is a Microsoft Windows 9x computer virus which first emerged in 1998. Its payload was highly destructive to vulnerable systems, overwriting critical information on infected system drives, and in some cases destroying the system BIOS. The malware filled the first 1024 KB of the host's boot drive with zeros and then attacked certain types of BIOS, This payload served to render the host computer inoperable, and for most ordinary users the virus essentially destroyed the PC. The payload tries to write to the Flash BIOS. machines that can be successfully written to by the virus have critical boot-time code replaced with junk. This routine only works on some machines. The virus made another comeback in 2001 when a variant of the LoveLetter Worm in a VBS file that contained a dropper routine for the CIH virus was circulated around the internet, under the guise of a picture of Jennifer Lopez. On December 31, 1999, Yamaha released a software update for their CD-R400 drives that was infected with the virus and in July 1998, a demo version of the first-person shooter game SiN was infected by one of its mirror sites.

APRIL 26, 1999

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

1/7

HACK A BOOTLOADER FOR PRANKS AND FUN

In this article we are going to create a very basic bootloader which will display some scarry looking ASCII graphics and make a victim believe they have just been hacked by a malicious USB. I hope you see this before April Fool's Day but if you read this later then feel free to deploy this at any moment you feel like having a laugh. So, in this project we are going to make use of the Assembly programming language. If you have never written in Assembly before, then this would be a nice and quick introduction but don't get intimidated. To start we can use either Windows or Linux. We will cover a OSX version in a later issue. So, let's discuss a few fundamental items, when you first start your computer, it does a series of self tests to make sure everything connected can be seen and accessed by the system. This is when the system POSTS or does a Power-On Self test. The bootloader is then loaded into the systems random access memory or RAM and the function of the bootloader is to help the system find and load the systems operating system. Your computer has a Basic Input / Output System or BIOS which searches the hard drives, CD drives or USB sticks for bootloaders to load the operating system and become a useable computer. To do this it searches for two things, first it looks for the bootloader in the first 512 bytes of information in the system's boot sector and that this is addressed to the memory location of 0x7c00 and second it looks to see that the last 2 bytes contain the magic number of 0xaa55 which indicates to the BIOS that this is a bootloader and is bootable. Windows loads a second bootloader called NTLDR which is responsible for loading the Windows kernel image but for this project we are going to abuse the BIOS and point it to our bootloader.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. THIS SERIES IS INTENDED FOR ACADEMIC PURPOSES ONLY AND IS MEANT TO PROVIDE EDUCATION TO CYBER SECURITY PROFESSIONALS… IF YOU WANT TO DO THIS STUFF FOR REAL, DO GOOD IN SCHOOL AND GET A JOB THAT PAYS YOU TO DO IT - LEGALLY!!

HACK A BOOTLOADER FOR PRANKS AND FUN

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

We will need to install a compiler to translate our assembly messages into a binary format and to do this we will use NASM. For Windows you will install this executable and for Linux you could use your package manager and load NASM directly from that. Next, we want to virtualize the computer start up environment so we will install software called QEMU which can be found here. Both programs work within the command line which will make this project much easier to test and adjust as needed. We then need a text editor that we can work with, I personally like Atom which has been developed by GitHub, but you can use any text editor that you feel comfortable with and won't add any additional formatting into the text file. Finally, we need something to write the code into the boot sector of our USB, on Linux we are going to use the program DD and on Windows you can use the program HxD. Now we are going to write some assembly commands for our compiler to translate into machine code. Create a blank document in your text editor like Atom and save the file as bootloader.asm. The very first line is where we will tell NASM what mode we will be running our code. For this project we will be running at 16 bits and NASM will now know how to translate the document knowing this instruction set. We will write:

```
bits 16
```

Next, we want to tell NASM where we want our program to be loaded into memory. The memory address following this command should be offset by this address and NASM will make those changes for you, we will write:

```
org 0x7c00
```

Origin or “org” is an assembly directive and not a part of the program or instruction. This simply tells the compiler where this should be loaded. Now that we have these parts, we then need to define what this program is going to be doing. We are not worried about loading a operating system so we just need to make use of the video driver and move some text onto the screen.

3/7

HACK A BOOTLOADER FOR PRANKS AND FUN

Next, we need to define the visual environment that will display out text. To do this, we are going to write information directly to the CPU registers. The first register we will write information to is called an accumulator and can be called by the identifier ah or al. This is a very simplified overview, but these registers will allow us to store 8-bits of data on the CPU for our program to make use of later. So first we are going to instruct the program to “move” or copy data from one location to another. Next, we will define the screen size we will be working with using the 16-bit registers CX and DX. CX is called a counter register and DX is a data register. Finally, we will send this data to the BIOS by calling the interrupt 0x10 and the BIOS will interrupt the information we are sending to it. We will write this as the following:

```
mov ah, 0x06
xor al, al
xor cx, cx
mov dx, 0x184f
mov bh, 0x4e
int 0x10
```

By setting the register ah to 0x06 we are telling the BIOS we want to scroll up the display, we set the value to zero which is an easy way for the BIOS to know we want to clear the screen display. We set the value to zero by XOR the al register with itself. Next, we want to define our screen so we are telling the BIOS that the upper left will be at the value zero and lower right will be defined as 0x184f. The upper right is defined by the cx register and to ensure a zero value we XOR it with itself and the lower right value we define as 0x184f and put this value into the dx register. Next, we tell the BIOS what colors we want to use as the background color and the text color. In an 8-bit register these need to be defined by each being only 4 bits. So, the 8-bit value of 0x4e as saying that the background color is going to be the value 4 and the text color will be E. Using this guide, this translates into a red background and yellow text. Sending this over to the BIOS is done by int 0x10.

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

4/7

HACK A BOOTLOADER FOR PRANKS AND FUN

Have I lost you yet? What we just did was tell the BIOS how to display our message on to the screen, next we are going to write our data. We are going to do this by writing 0x0e into the ah register and this is going to tell the BIOS to write on the screen using TTY mode or TeleTYpewriter. So, to do this we are going to write our hacker message into the 16-bit register SI which is the source register.

```
mov si, bootloaderBanner
```

We have not defined what bootloaderBanner is yet, but this will move those contents into the SI register. Next, we will write these characters on screen by the following command:

```
mov ah, 0x0e
loop:
    lodsb
    test al, al
    jz end
   int 0x10
   jmp loop
end:
    hlt
```

So, we are creating a loop and moving each character into the screen from our hacker message. We are taking the data from the source register and printing the information to the screen that is being handled by the BIOS. Now let's write our hacker message, the one I have chosen is below:

```
bootloaderBanner: db "      @@@@@@@@@@@@@@@@@@",13,10,"
@@@@@@@GALDE@@@@@@@@@@@",13,10,"
@@@@@@ARIZONA@@@@@@@@@@@@@@",13,10,"
@@@@@@AZCAST@@@@@@@@@@@@@@@@@@",13,10,"
@@@@@@@@@@@@@@@@/  @  \@@@/  @",13,10,"@@@@@@@@@@@@@@@@@\
@@  @__@",13,10,"@SIERRA VISTA@ @@@@@@@@@  |
\@@@@@",13,10,"@@@@@@@@@@@@@
@@@@@@@@@@\__@_/@@@@@",13,10,"
@@@@@@@@@@@@@@@@/,/,/./'/_|.\'\,\",13,10,"   @@@@@@@@@@@@@|  | | |
| | | | |",13,10,"             \_|_|_|_|_|_|_|_|",13,10,13,10,"  Hacked by Professor
Galde at The Packet", 0
```

HACK A BOOTLOADER FOR PRANKS AND FUN

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

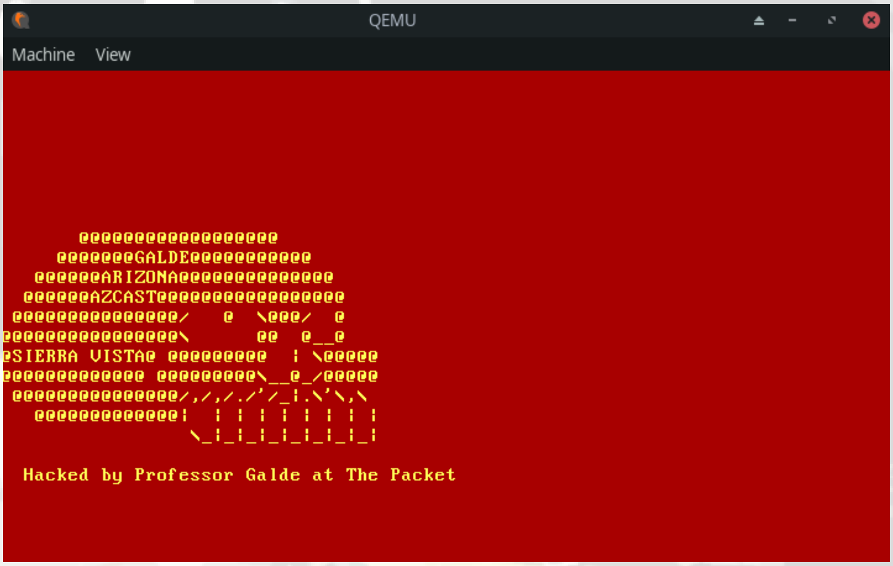
The information under bootloadBanner just looks like a bunch of junk data, what does it all mean? First, db is an assembly directive, this defines bytes, so it takes the ASCII text and translates it into hexadecimal. I then have my string written like @@@@@@@ and then I have a 13 and a 10-value following. The 13 value tells the screen I want a new line, this is the "carriage return" and the 10 indicates I want to start a new line or the "line feed". Basically, it's saying go to the next line. At the end of my string is a 0, and this indicates that my sting will end here and to continue with the program. Next, I want to fill up my bootloader so that I will be a total of 512 bytes, so I write the following command:

```
times 510 - ($-$$) db 0
```

This will take any remaining room and fill it up with 00 bytes and finally we need to enter our magic number of 0xaa55 with the following command:

```
dw 0xaa55
```

When everything is put together and the system loads the instructions you should be presented with the following display.



```
       @@@@@@@@@@@@@@@@@@
     @@@@@@@GALDE@@@@@@@@@@@
   @@@@@@ARIZONA@@@@@@@@@@@@@@
  @@@@@@AZCAST@@@@@@@@@@@@@@@@@
 @@@@@@@@@@@@@@@/   @  \@@@/  @
@@@@@@@@@@@@@@@@\      @@  @__@
@SIERRA VISTA@ @@@@@@@@@  ¦ \@@@@@
@@@@@@@@@@@@@ @@@@@@@@@\__@_/@@@@@
 @@@@@@@@@@@@@@@/,/,/./'/_¦.\'\,\
   @@@@@@@@@@@@@¦  ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦
                 \_¦_¦_¦_¦_¦_¦_¦_¦

  Hacked by Professor Galde at The Packet
```

I found the ASCII skull on the internet and just added a few items that would make it more unique to me. If you were to boot up your computer and you were presented with this screen you may freak out thinking you have just been hacked and may need to call everyone in for the weekend to salvage all your data. So, lets look at deploying and testing this out.

6/7

HACK A BOOTLOADER FOR PRANKS AND FUN

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

RAW SOURCE CODE

```
; Instruct NASM to generate code that is to be run on CPU that is running in 16 bit mode
bits 16

; Tell NASM that we expect our bootloader to be laoded at this address, hence offsets should be
calculated in relation to this address
org 0x7c00

; Set background and foreground colour
mov ah, 0x06    ; Clear / scroll screen up function
xor al, al      ; Number of lines by which to scroll up (00h = clear entire window)
xor cx, cx      ; Row,column of window's upper left corner
mov dx, 0x184f  ; Row,column of window's lower right corner
mov bh, 0x4e    ; Background/foreground colour. In our case - red background / yellow
foreground (https://en.wikipedia.org/wiki/BIOS_color_attributes)
int 0x10        ; Issue BIOS video services interrupt with function 0x06

; Move label's bootloaderBanner memory address to si
mov si, bootloaderBanner
; Put 0x0e to ah, which stands for "Write Character in TTY mode" when issuing a BIOS Video
Services interrupt 0x10
mov ah, 0x0e
loop:
   ; Load byte at address si to al
   lodsb
   ; Check if al==0 / a NULL byte, meaning end of a C string
   test al, al
   ; If al==0, jump to end, where the bootloader will be halted
   jz end
   ; Issue a BIOS interrupt 0x10 for video services
   int 0x10
   ; Repeat
   jmp loop
end:
   ; Halt the program until the next interrupt
   hlt
bootloaderBanner: db "      @@@@@@@@@@@@@@@@@@",13,10,"
@@@@@@@GALDE@@@@@@@@@@@",13,10,"
@@@@@@ARIZONA@@@@@@@@@@@@@@",13,10,"
@@@@@@AZCAST@@@@@@@@@@@@@@@@@",13,10," @@@@@@@@@@@@@@@@/   @  \@@@/
@",13,10,"@@@@@@@@@@@@@@@@@\     @@  @__@",13,10,"@SIERRA VISTA@ @@@@@@@@@  |
\@@@@@",13,10,"@@@@@@@@@@@@@@ @@@@@@@@@\__@_/@@@@@",13,10,"
@@@@@@@@@@@@@@@/,/,/./'/_|.\'\,\",13,10,"   @@@@@@@@@@@@@|  | | | | | | | |",13,10,"
\_|_|_|_|_|_|_|_|",13,10,13,10,"  Hacked by Professor Galde at The Packet", 0

; Fill remaining space of the 512 bytes minus our instrunctions, with 00 bytes
; $ - address of the current instruction
; $$ - address of the start of the image .text section we're executing this code in
times 510 - ($-$$) db 0
; Bootloader magic number
dw 0xaa55
```

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

7/7

HACK A BOOTLOADER FOR PRANKS AND FUN

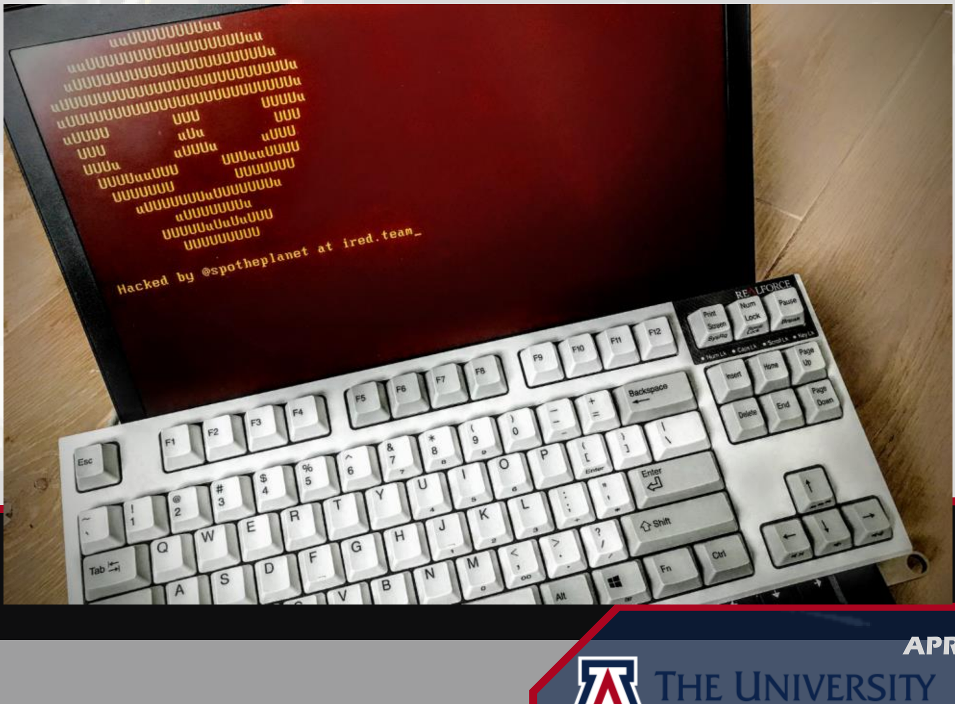
Now that we have written our code in the assembly programing language, we now need to compile it so that the BIOS can read out bootloader. To do this we will run the following command:

```
nasm –f bin ./bootloader.asm –o bootloader.bin (Linux)
nasm  -f bin bootloader.asm –o bootloader.bin (Windows)
```

We are telling nasm to read the file bootloader.asm and output the file bootloader.bin once compiled. This is what will be read by the BIOS. We can simulate this with QEMU.   QEMU stands for Quick EMUlator. To run this, we simply type the following:

```
qemu-system-x86_64 bootloader.bin
```

We are then able to see the output after our bootloader runs. Now we want to move this over to our USB so that when the BIOS looks for a bootloader to run, it will run ours. On Linux you will simply use DD to copy the bootloader.bin to the drive your USB is associated with. With Windows you can open the drive up in HxD in one tab and open bootloader.bin in another tab and copy all the contents. Then move over to your drive and copy the contents over replacing the contents that were in the drive before. Now we simply need to find a victim and make our USB drive the first to load on the victim's system. Now go out and enjoy April Fools Day and learn more Assembly language and make even more awesome and amazing things. I would also like to give a big thank you to Red Teaming Experiments for providing the inspiration for this posting.



Hacked by @spotheplanet at ired.team_

SOMETIMES YOU JUST NEED SOMEONE TO POINT YOU IN THE RIGHT DIRECTION

TIPS & TRICKS OF THE TRADE

Windows 10, after update 1809, includes a built-in packet sniffer, this is useful if you need to do some network diagnosis but are unable to load Wireshark for some reason. This program is like tcpdump and allows you to get all packets going through the computers network interface card. The program is called pktmon and can be called using the windows command prompt or PowerShell window.

So, lets look at some of the basic commands you can do within a pktmon environment

COMMAND	ACTION
pktmon filter add -p 20 21	Capture traffic on port 20 and 21 for FTP
pktmon filter add HTTPFilter –p 80 443	Capture HTTP traffic on port 80 and 443 for HTTP and HTTPS traffic
pktmon filter list	Display list of current filters
pktmon start	Start capture process
pktmon stop	Stop capture process
pktmon start --etw	Capture all interfaces in real time
pktmon start --etw -p 0	Capture all interfaces in real time with all packet information
pktmon comp list	Display all interfaces
pktmon start --etw -p 0 -c 4	Capture from interface 4 in real time with all packet information

One limitation compared to Wireshark is that you can not capture a wireless interface while in monitoring mode but for a quick diagnostic tool this can be a very handy trick to collect network data on a machine that does not allow the installation of Wireshark.

1/2

THE BUSINESS OF HAFNIUM AND THE 0-DAY

The Hafnium group is believed to be attributed to the Chinese government and falls under the advanced persistent threat category. Organizations are unlikely to defend themselves from advanced persistent threat's and if you have an Exchange server it is likely the recent patches you have been deploying have been in response to a recent campaign attributed to this group. The group targeted infectious disease research, law firms, higher education, defense contractors, policy think tanks and non-governmental organocations. Microsoft was the one who coined the term Hafnium. The Hafnium group abused 4 undisclosed vulnerabilities or 0-days to gain access to on-site Microsoft Exchange servers and then deploy a web shell against the compromised servers. The web shell that was used is called China Chopper which was first seen in 2013. China Chopper is an Active Server Page Extended (ASPX) web shell that is typically planted on an Internet Information Services (IIS) server through an exploit. China Chopper is used for post-exploitation by allowing attackers the access needed to execute any code they want on the server. The China Chopper server-side ASPX web shell is extremely small and typically, is just one line of code. There are multiple versions of this web shell for executing code in different languages such as ASP, ASPX, PHP, Jakarta Server Pages (JSP), and ColdFusion Markup Language (CFM). On the attacker side, the attacker can perform many nefarious tasks such as downloading and uploading files, running a virtual terminal to execute anything you normally could using cmd.exe, modifying files, executing custom JScript, file browsing, and more. All this is made available just from the one line of code running on the server. China Chopper is a simple backdoor in terms of components. It has two key components: the Web shell command-and-control (C2) client binary and a text-based Web shell payload (server component). The text-based payload is so simple and short that an attacker could type it by hand right on the target server with no file transfer needed.

2/2 THE BUSINESS OF HAFNIUM AND THE 0-DAY

Looking at Hafnium as an advanced persistent threat, the governments behind APT's generally do not want to be associated with the attack and will publicly deny the attack. In this instance the Chinese government has claimed no knowledge or responsibility. The goal is to pick your targets carefully to avoid increased pressure when you are finally discovered. There is a demand for a response from an affected industry, organization or government.

The Hafnium approach followed this plan initially but once the group discovered that cybersecurity research was focused on their attacks the group went into a free-for-all and scanned the internet for every server that could be infected. Around February 27, 2021 the group exploited multiple networks and left web shells that allowed any group or individual to infiltrate the compromised machines. The initial attack was missed by most security checks: it was only spotted when the company Volexity noticed strange and specific internet traffic requests to the company's customers who were running their own Microsoft Exchange email servers and at this point there were only a few victims. At the end of February, multiple groups started to use this exploit which is uncommon before a public announcement is made. All except one of the active hacking groups are known government-backed hacking teams focused on espionage. Microsoft took a rare step in March, releasing security patches for unsupported versions of Exchange that would normally be too old to secure which is a sign of how severe the company believes the attack is. So now the question is, what is the response of the United States going to be. The response will likely be silent for quite some time and will likely invite multiple hacking groups into China's networks, but this attack was very irresponsible from a historical standpoint. I can only think that the group tried to make it appear as if it was somehow out of control or out of their hands, but the attack profile does not match that approach. Cyber espionage is strategically a silent affair, but this may open the possibility for more blatant attacks in the future to disrupt the trust and security of a nation's infrastructure. Even more reasons to learn about cybersecurity.

BUILD YOUR OWN NETWORK PRESENCE DETECTOR

The moment that you walk into a location that you trust like your home or maybe your work environment you may have your phone set up to automatically connect to the local Wi-Fi. For your home network your family members, room mates and frequent guests may also automatically connect to the local network. So, this project will look at a project that will determine if someone is "home" or not by looking for these connections on your home network. The simple idea in this project is that if this software sees your device on the network, the software will declare that you are "home". This of course will require that the device connects automatically when the Wi-Fi is in range to provide this service. With this software running we can set up alerts when a device enters or leaves the Wi-Fi. The first thing we need is a Raspberry Pi with the latest upgraded software.

The Pi needs to be connected to the same network your device will connect to. If you have 2.4Ghz and 5Ghz options on your router, the Pi can only connect to the 2.4Ghz option but will still be able to see devices on the 5Ghz band.

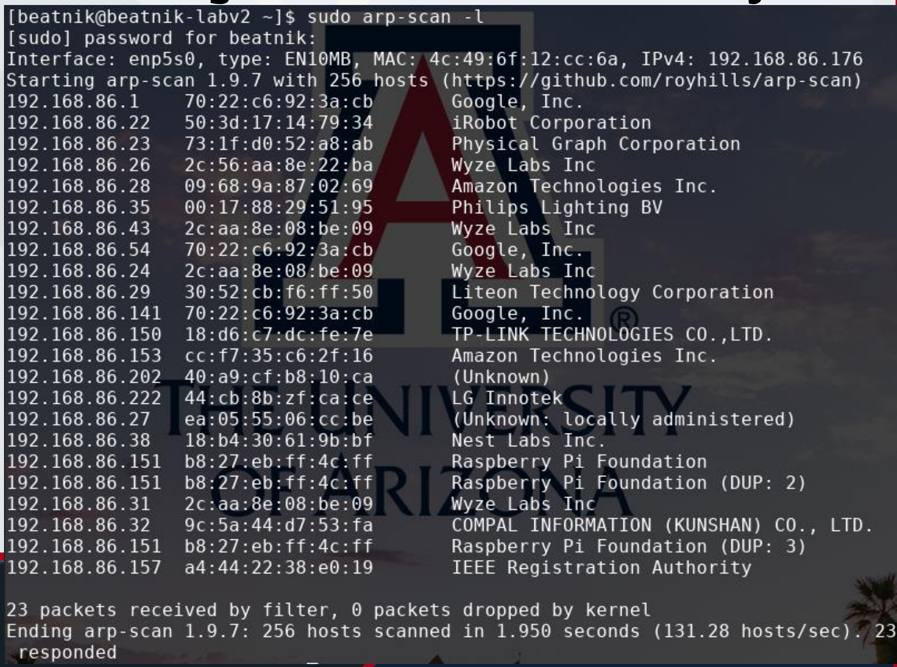
The first piece of software we will install is arp-scan and we can do this with the following command:

sudo apt-get install arp-scan

Once that has completed installing, we can test the software by running

sudo arp-scan -l

I should now get a list of devices that responded to our ARP request. ARP will return the devices physical address or MAC address that is associated with each IP address that was searched for.



```
[beatnik@beatnik-labv2 ~]$ sudo arp-scan -l
[sudo] password for beatnik:
Interface: enp5s0, type: EN10MB, MAC: 4c:49:6f:12:cc:6a, IPv4: 192.168.86.176
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.86.1    70:22:c6:92:3a:cb       Google, Inc.
192.168.86.22   50:3d:17:14:79:34       iRobot Corporation
192.168.86.23   73:1f:d0:52:a8:ab       Physical Graph Corporation
192.168.86.26   2c:56:aa:8e:22:ba       Wyze Labs Inc
192.168.86.28   09:68:9a:87:02:69       Amazon Technologies Inc.
192.168.86.35   00:17:88:29:51:95       Philips Lighting BV
192.168.86.43   2c:aa:8e:08:be:09       Wyze Labs Inc
192.168.86.54   70:22:c6:92:3a:cb       Google, Inc.
192.168.86.24   2c:aa:8e:08:be:09       Wyze Labs Inc
192.168.86.29   30:52:cb:f6:ff:50       Liteon Technology Corporation
192.168.86.141  70:22:c6:92:3a:cb       Google, Inc.
192.168.86.150  18:d6:c7:dc:fe:7e       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.86.153  cc:f7:35:c6:2f:16       Amazon Technologies Inc.
192.168.86.202  40:a9:cf:b8:10:ca       (Unknown)
192.168.86.222  44:cb:8b:zf:ca:ce       LG Innotek
192.168.86.27   ea:05:55:06:cc:be       (Unknown: locally administered)
192.168.86.38   18:b4:30:61:9b:bf       Nest Labs Inc.
192.168.86.151  b8:27:eb:ff:4c:ff       Raspberry Pi Foundation
192.168.86.151  b8:27:eb:ff:4c:ff       Raspberry Pi Foundation (DUP: 2)
192.168.86.31   2c:aa:8e:08:be:09       Wyze Labs Inc
192.168.86.32   9c:5a:44:d7:53:fa       COMPAL INFORMATION (KUNSHAN) CO., LTD.
192.168.86.151  b8:27:eb:ff:4c:ff       Raspberry Pi Foundation (DUP: 3)
192.168.86.157  a4:44:22:38:e0:19       IEEE Registration Authority

23 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.950 seconds (131.28 hosts/sec). 23
 responded
```

GET UP AND RUNNING TODAY TO START SOMETHING NEW

2/3

BUILD YOUR OWN NETWORK PRESENCE DETECTOR

Now that we know the devices on your network, we can write a very simple python program to check if a device is on the network or not. Using python, we can do a simple check and give a read out. This can be expanded on and more logic can be included to do much more.

```
import time
import os

while 1:
    if os.system("ping -c 1 -W 1 192.168.86.27 > /dev/null"):
        print ("Device Not Home")
    else:
        print ("Device Is Home")
    time.sleep(10)
```

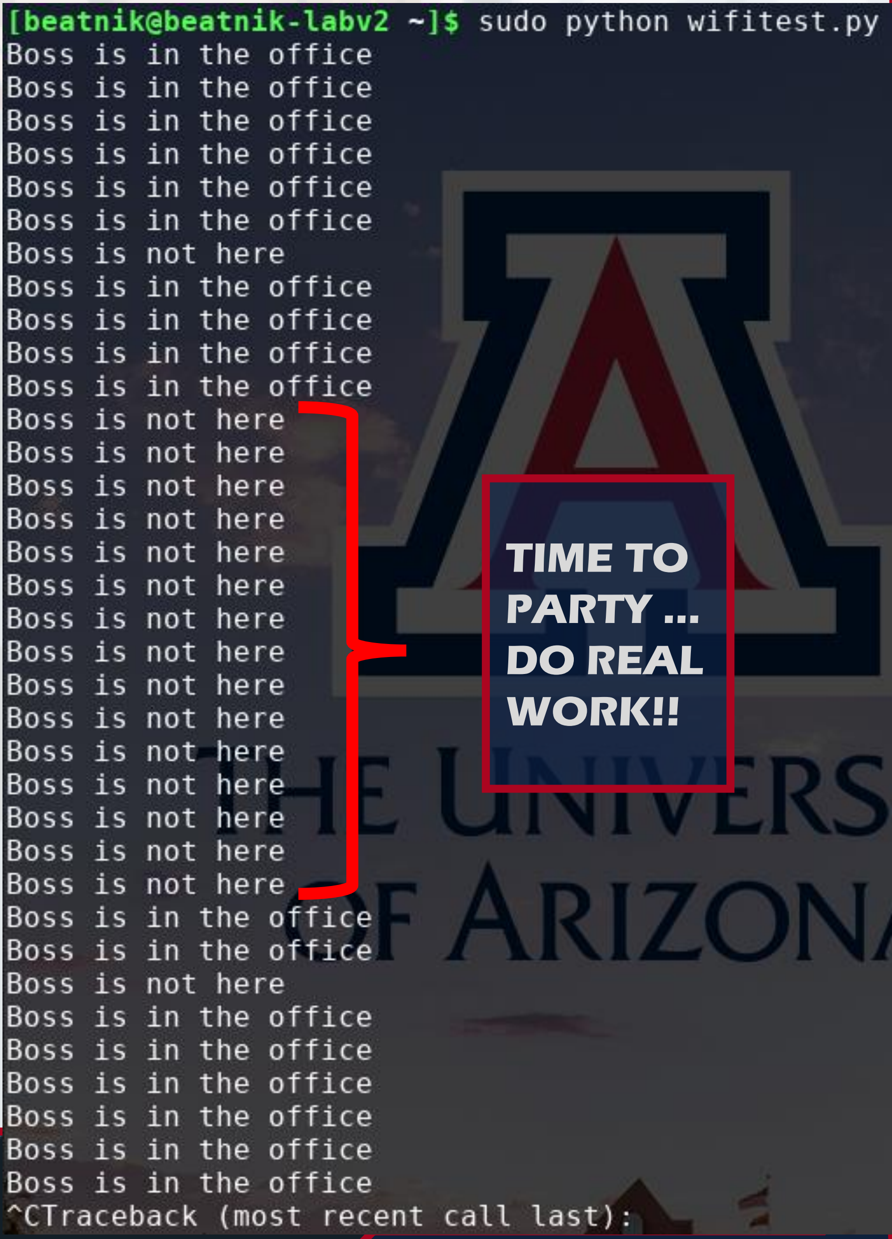
I was able to identify my device as 192.168.86.27. So, I am using python to run the ping command with the flags c and W. The c flag designates how many pings to send out and for this program I only need 1 to be sent. The W flag designates how much wait time to issue, and I set this to 1 second as to not wait. If the device is online and responds to a ping, the program will print that the Device is Home but if the ping fails because the device is not on the network or fails to respond to the ping the program will print the message Device Not Home. Now this method is just checking for the device's IP address so what we want is to check for the devices physical address or MAC address. To do this we will change the code slightly.

```
import time
import os
while 1:
    if os.system("arp-scan -l | grep -o ea:05:55:06:cc:be > /dev/null"):
        print ("Device Not Home")
    else:
        print ("Device Is Home")
    time.sleep(10)
```

3/3

BUILD YOUR OWN NETWORK PRESENCE DETECTOR

So, the only change was to what command we ran on the system. We are running the arp-scan command and are looking to see if your device's physical address is listed. So, if a device took our previous IP address, it is unlikely we would have a device also use our device's physical address. This python program will also need to be ran with administrator privileges so that it can use the arp-scan command. Now this is a very simple python script but there is more logic that can be added. When a device enters or leaves the network, the monitor can email a user alerting that this has taken place. If you are utilizing this at work and you were able to identify your coworkers or supervisor's device address you can be alerted when they enter or leave the office. At the very least you will know when their mobile device disconnects and connects to the local network. You can maybe even change this program completely to identify all known devices and alert you when an unknown device is seen on the network.



```
[beatnik@beatnik-labv2 ~]$ sudo python wifitest.py
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is not here
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is in the office
Boss is in the office
Boss is not here
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
^CTraceback (most recent call last):
```

TIME TO PARTY ... DO REAL WORK!!

```
>.  ---CONNECTION ESTABLISHED---
>.  FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>.  HAVE A HAPPY EARTH DAY
>.  ---END TRANSMISSION---
```

THANK YOU

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

https://cyber-operations.azcast.arizona.edu/

ART BY @ PATRICK BOYER