THE PACKET

The University of Arizona

MAY 2020

THE UNIVERSITY OF ARIZONA
THE PACKET
MAY 2020

IN THIS ISSUE

--- BEGIN MESSAGE ---

Welcome to the **MAY** issue of **"The PACKET"** produced under the University of Arizona Cyber Operations program. My name is Professor Galde and it is my pleasure to produce this second issue. April and March brought an explosion of work from home as businesses respond to the COVID-19 pandemic. The University has responded with a focus on every student's safety as our top concern. Any student who has difficulty affording basic necessities, groceries, or accessing sufficient food to eat every day, or who lacks a safe and stable place to live and believes this may affect their performance in the course is urged to contact your professors, program director, department head or the Dean of Students for support. In addition, the University of Arizona Campus Pantry is open for students to receive supplemental groceries at no cost. Please see their website at campuspantry.arizona.edu for operating hours. For up-to-date information and guidance on COVID-19 please visit https://www.arizona.edu/coronavirus-covid-19-information.

Cybersecurity professionals are under increased stress as enterprise users are moving to online operations to provide remote support. Defensive network operations need skilled operators to identify malicious activity. The fall schedule is now available and anyone who wants to take part in defending the digital landscape can look at page 11 for what is offered this year.

--- END MESSAGE ---

CYBER CLASSIFIED BY: PROFESSOR GALDE
REASON: CYBER OPERATION PROGRAM
DECYBER ON: JANUARY 2060

HACKS OF THE MONTH

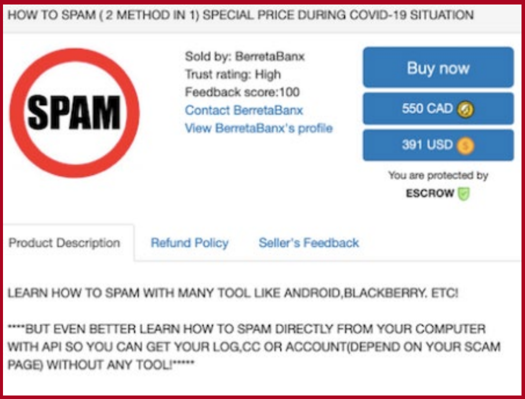
BlackBerry.
Intelligent Security. Everywhere.
Decade of the RATs
Cross-Platform APT Espionage Attacks Targeting Linux, Windows and Android

GAPS IN SECURITY USUALLY STAY THAT WAY BECAUSE NO ONE KNOWS THEY EXIST…

Blackberry, who I just realized is still in business, has put together an excellent threat report on recent security trends. "This research paints a picture of an espionage effort targeting the very backbone of large organizations' network infrastructure that is more systemic than has been previously acknowledged."

IS CASH KING IN A CASHLESS WORLD?

Well it turns out digital skimming techniques are becoming more successful as more companies are focused on getting their work force into remote operations. Threat research RiskIQ, says the company has detected a 20 percent increase in online skimming activity in March compared to February.



HOW TO SPAM (2 METHOD IN 1) SPECIAL PRICE DURING COVID-19 SITUATION

SPAM

Sold by: BerretaBanx
Trust rating: High
Feedback score:100
Contact BerretaBanx
View BerretaBanx's profile

Buy now
550 CAD
391 USD
You are protected by ESCROW

Product Description | Refund Policy | Seller's Feedback

LEARN HOW TO SPAM WITH MANY TOOL LIKE ANDROID,BLACKBERRY. ETC!

****BUT EVEN BETTER LEARN HOW TO SPAM DIRECTLY FROM YOUR COMPUTER WITH API SO YOU CAN GET YOUR LOG,CC OR ACCOUNT(DEPEND ON YOUR SCAM PAGE) WITHOUT ANY TOOL!*****

THE COVID-19 MALICIOUS PANDEMIC SALE

For everyone saving up their pennies for distributed denial of service (DDoS) attack tools, spamming, and other services, now may be your lucky day as multiple hacker forums are reporting discounts as deep as 20% to even 40% off services. "I don't think most people realize how much cybercriminal services have become professionalized," … "But unlike other professions, most of us would be happy to see them go out of business because of COVID-19."

CYBER NEWS UPDATES

BURNING CELL TOWERS OUT OF BASELESS FEAR THEY SPREAD THE VIRUS

Ignoring the fact that every country that has COVID-19 does not have 5G coverage, a very popular conspiracy theory is leading followers to believe that cellphone towers will make you sick. It is important to note that people accept misinformation not because they are ignorant or unintelligent but because they are desperate or frightened.

DISCOVER MORE

CYBV 480 CYBER WARFARE

CYBV 441 CYBER WAR, TERROR, CRIME

CYBV 385 INTRODUCTION TO CYBER OPERATIONS

CYBV 354 PRINCIPLES OF OPEN SOURCE INTELLIGENCE

DUTCH POLICE SHUT DOWN 15 DDOS-FOR-HIRE SERVICES

Dutch police have confirmed the takedown of 15 DDoS-for-hire services and the arrest of one individual suspected of launching a distributed denial-of-service attack against websites that send government updates to citizens. The websites held information about the coronavirus and personal data.

DISCOVER MORE

CYBV 441 CYBER WAR, TERROR, CRIME

CYBV 435 CYBER THREAT INTELLIGENCE

CYBV 388 CYBER INVESTIGATIONS AND FORENSICS

CYBV 354 PRINCIPLES OF OPEN SOURCE INTELLIGENCE

THE WORK-AT-HOME ADVICE CYBERSECURITY FIRMS ARE GIVING THEIR EMPLOYEES

Protocol.com asked more than a dozen cybersecurity companies to share the memos, emails and other guidance that they have sent to their own employees in the past few weeks to protect their systems. Almost every cybersecurity company contacted has been regularly warning employees about sophisticated phishing attacks that leverage COVID-19 information to get victims to click on malicious files.

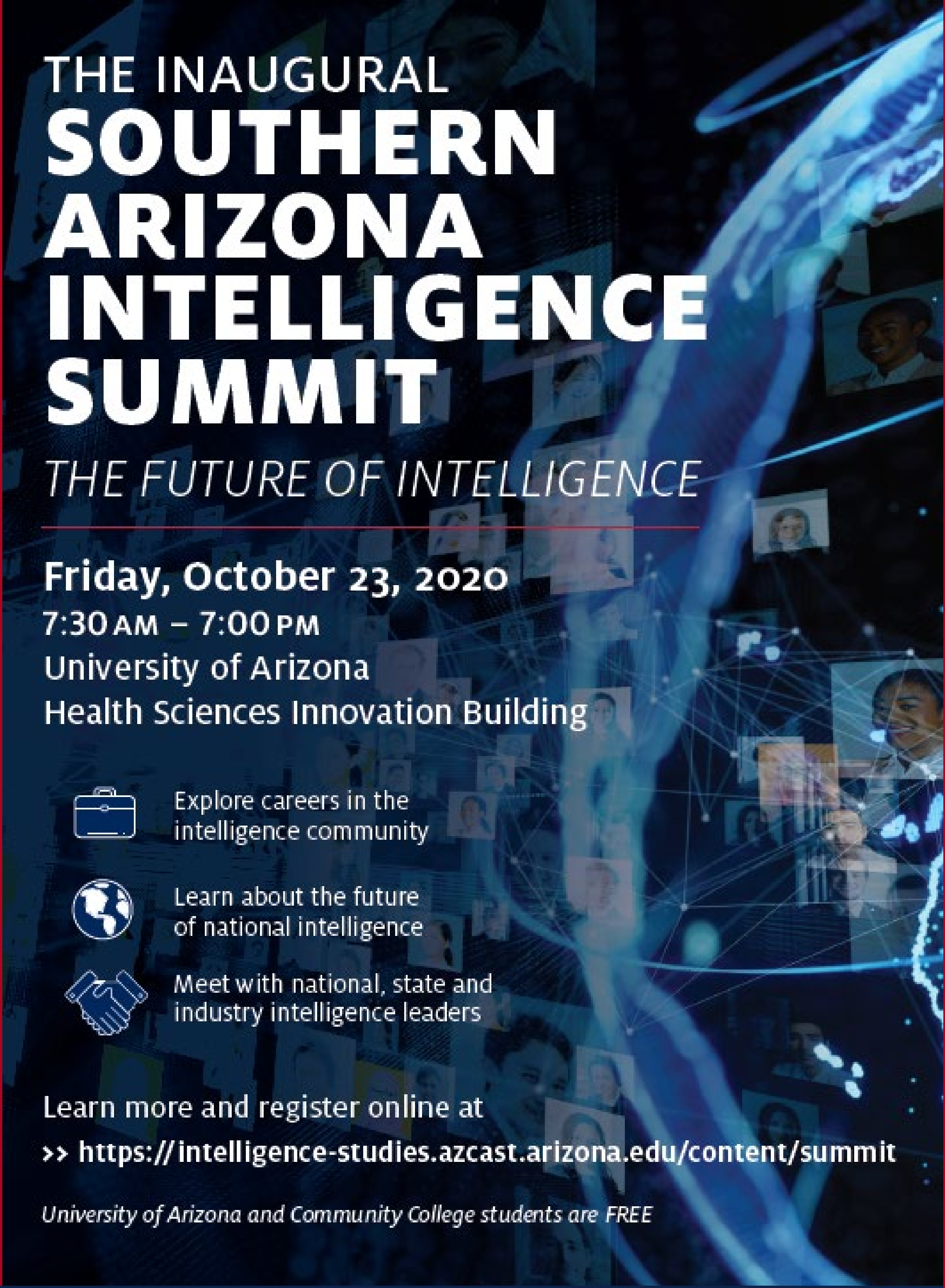
DISCOVER MORE

CYBV 474 ADVANCED ANALYTICS FOR SECURITY OPERATIONS

CYBV 435 CYBER THREAT INTELLIGENCE

CYBV 329 CYBER ETHICS

CYBV 301 FUNDAMENTALS OF CYBERSECURITY



THE INAUGURAL

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

THE FUTURE OF INTELLIGENCE

Friday, October 23, 2020

7:30 AM – 7:00 PM

University of Arizona
Health Sciences Innovation Building

- 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

JOB BOARD

Network / Capabilities Manager

NSA is in search of top-notch cyber professionals with technical expertise and driving desire at the forefront of their field. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satelli...

Cybersecurity Principal Specialist - Awareness #402

This is advanced professional work assessing effectiveness and efficiency of instruction according to usefulness of the instructional technology used and student learning, knowledge transfer, and satisfaction outcomes. The incumbent will coordinate with internal and external subject matter experts to ensure existing qualification ...

Cybersecurity Senior Specialist #5360

This is professional work coordinating, implementing and maintaining technologies and processes to protect the confidentiality, integrity, and availability of Senate information systems. Work includes translating functional requirements into technical solutions, building, installing, configuring, and testing dedicated cyber defense hardware and checking system hardware availability, functionality, integrity, and efficiency.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD

COPY EDITOR / GRAPHIC DESIGNER / TECHNICAL WRITING/PUBLICATION EDITOR

COPY EDITOR – Someone with experience putting together articles, magazine like publications, editing, proof reading, etc. NEEDS A SECRET CLEARANCE

GRAPHIC DESIGNER – Somebody who knows how to create digital graphics, pictures, etc. for publications. Must be creative and know how to use a variety of modern graphic design software and tools. NEEDS A SECRET CLEARANCE

TECHNICAL WRITING/PUBLICATION EDITOR – same as the copy editor, but instead of the focusing on magazine side they are worried about the actual Army Pubs, FMs, ARs, etc. NEEDS A TOP SECRET

Associate- Help Desk Technician - Illinois

As a Help Desk Technician, you provide phone and in-person technical support for end users in an enterprise level environment. This is a full-time position to support and maintain in-house computer systems, desktops, and peripherals. This includes installing, diagnosing, repairing, maintaining, and upgrading all hardware and equipment while ensuring optimal workstation performance. Troubleshoot problem areas in a timely and accurate fashion and provide end user training and assistance where required.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD

Intermediate Virtualization/Storage Administrator - Arizona

The ideal candidate will be responsible for virtualization/storage administration. The ideal candidate will operate and maintain storage and VMware virtualized environments. Troubleshooting, work with remote customers, diagnostic tools, plan/coordinate/document the use of revised/updated procedures, processes, and methods for the operations and maintenance of the Data Services infrastructure.

Arizona Senior Network Administrator (SME)

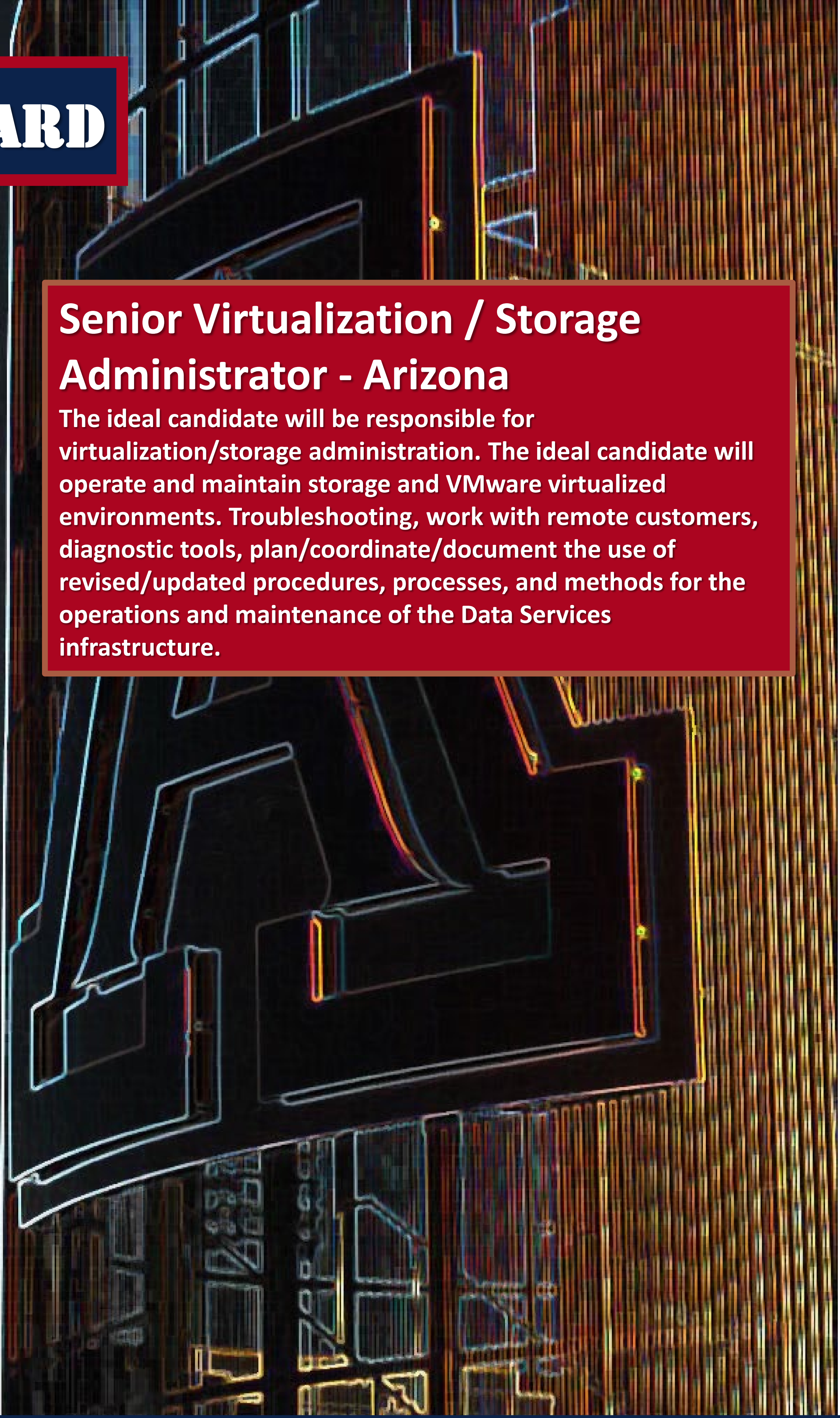
The selected candidate will assist with daily leadership and technical guidance for a team of network analysts while performing daily management network assets from various vendors to include firewalls, routers, switches, load balancers and VPNs on behalf of the United States Army. Writing documentation to include SOPs and TTPs. Utilizing a diverse suite of network monitoring technology, troubleshoot a dynamic and complex environment while assisting third parties to solve various network connectivity problems.

Network Administrator - Illinois

The ideal candidate will be responsible for administration and day-to-day operation of organization's local area network (LAN). The Network Administrator will provide integrated team support and maintenance of LAN hardware and software. The ideal candidate will have experience with protocol analysis, knowledge of common network protocols, satellite networks, and Cisco ASA and Palo Alto firewalls.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD



Senior Virtualization / Storage Administrator - Arizona

The ideal candidate will be responsible for virtualization/storage administration. The ideal candidate will operate and maintain storage and VMware virtualized environments. Troubleshooting, work with remote customers, diagnostic tools, plan/coordinate/document the use of revised/updated procedures, processes, and methods for the operations and maintenance of the Data Services infrastructure.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 301	Fundamentals of Cybersecurity (7 Week class 1 & 2)	Paul Wagner
CYBV 326	Introductory Methods of Network Analysis Section 101 - 106	Jordan Vanhoy
CYBV 326	Introductory Methods of Network Analysis Section 107 - 110	Michael Galde
CYBV 329	Cyber Ethics (7 Week Class 1 & 2)	Heidi Calhoun-Lopez
CYBV 354	Principles of Open Source Intelligence (7 Week Class 2 only)	John Mccary
CYBV 385	Introduction to Cyber Operations (7 Week Class1 & 2)	Michael Galde
CYBV 388	Cyber Investigations and Forensics Section 101 - 104	Troy Ward
CYBV 388	Cyber Investigations and Forensics Section 105 - 106	Steven Wood
CYBV 393	Internship in Cyber Operations	Jason Denno

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 399 CYBV 499	Independent Study	Jason Denno
CYBV 400	Active Cyber Defense Section 101 - 104	Thomas Jewkes
CYBV 400	Active Cyber Defense Section 105 - 106	Colin Brooks
CYBV 435	Cyber Threat Intelligence (7 Week Class) Section 101 - 104	Thomas Jewkes
CYBV 435	Cyber Threat Intelligence (7 Week Class) Section 102 & 104	Harry Cooper
CYBV 436	Counter Cyber Threat Intelligence (7 Week Class 2 only)	Harry Cooper
CYBV 440	Digital Espionage (7 Week Class 1 only)	Kate Mabbett
CYBV 441	Cyber War, Terror and Crime (7 Week Class 2 only)	Kate Mabbett
CYBV 454	Malware Threats & Analysis	Luis Mendieta

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 470	C Programming for Security Professionals	Keith Rezendes
CYBV 471	Assembly Language Programming for Security Professionals	Mohamed Meky
CYBV 473	Violent Python	Chester Hosmer
CYBV 474	Advanced Analytics for Security Operations	Chester Hosmer
CYBV 479	Wireless Networking and Security	Jordan Vanhoy
CYBV 480	Cyber Warfare Section 101 - 102	Rock Stevens
CYBV 480	Cyber Warfare Section 103 - 104	Roy Luongo
CYBV 496	Special Topics in Cyber Security - Introduction to Security Programming I & II (7 Week Class 1 & 2)	Keith Rezendes
CYBV 498	Capstone in Cyber Operations	Jordan Vanhoy Heidi Calhoun-Lopez

THE UNIVERSITY
OF ARIZONA

The Intelligence & Information Operations (IIO) Program *Presents:*

ICCAE *SPEAKER SERIES* 2020

The Intelligence Community Center of Academic Excellence (ICCAE)

2020 Student, Staff & Faculty Professional Development Speaker Series (April – June 2020)

A designated Intelligence Community Center of Academic Excellence, The College of Applied Science & Technology's Intelligence & Information Operations program affords its students, staff, and faculty exclusive professional development opportunities. Event attendees learn from and engage with the leaders and practitioners of the United States IC and private sector.

The IIO program culminates the 2020 academic calendar year with a professional development speaker series that will deep dive into issues such as cybersecurity, military intelligence analysis, politics, topics of national security and more.

All sessions will be streamed live via Zoom **(Meeting ID: 605 128 853):** **https://arizona.zoom.us/j/605128853.** Topics and speakers will be announced as they are confirmed; upcoming speaker segments will be posted on the *CAST IIO's ICCAE Academic and Professional Development webpage*. We encourage you to join us for live interactive events, as not all session will be available for a later viewing.

For questions or concerns, please contact: Professor Craig Nazareth at cnazareth@arizona.edu or 520-458-8278 ext. 2185

HACKING POC

Part 1/3

LETS CREATE MALWARE FOR FUN!!

May is the month in which both the ILOVEYOU virus and the WANNACRY ransomware emerged as two very important and defining moments in cybersecurity. So in “Celebration” of these events and the current COVID-19 viral pandemic, I want to take a few editions to go over what goes into developing malware from start to finish.

In this edition, we will illustrate how easy it is to make something that is similar to malware. I will be creating this in Python and borrowing very heavily from the Oncogene project.

Step one is to determine: what kind of malware behavior do I want?

I want to:

- Get a shell
- Get system Info
- Take a screenshot
- Download files from victim
- Run a keylogger
- Copy user clipboard

I was lucky to find a GitHub project that touched on a lot of these principles and we will utilize that framework for this project.

CAUTION — This article shows you how to create a piece of software some may misuse and/or misunderstand. This malware series is intended for academic purposes only and is intended to provide education to cyber security professionals… Plus you will likely be caught if you don’t make major changes. You assume any risk of using the information in this article.

HACKING POC

Part 2/3

CREATE CONTROL PROGRAM

So First we need to create a program that the malware will call back to. To do this we first download a few files from Github:

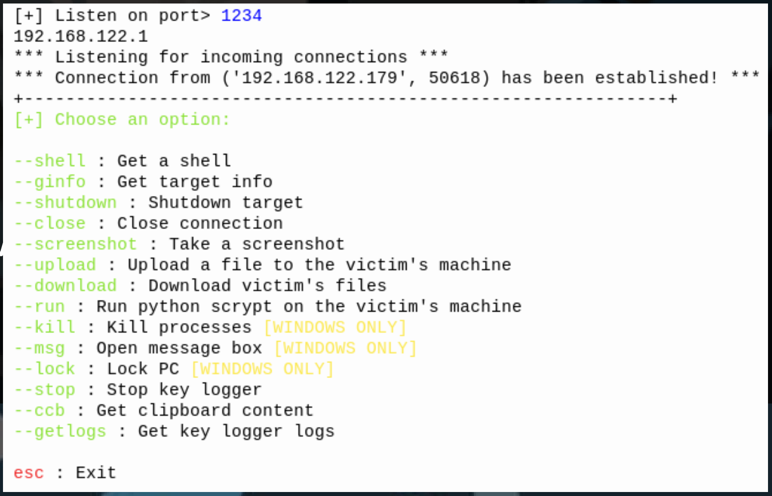
- Malwarecontrol.py
- mainMenu.py

So mainMenu.py is set up to give you a nice interface to work with and Malwarecontrol.py is the main piece we will be working with. This controller is designed to be run under Linux but you may be able to make it work under Windows.

You will place the IP address for your listener under Line #9.

Now you can run your program and select the port you want to wait on. We will select *1234*

Once the client connects, you are now able to make a few selections of what to do!



```
[+] Listen on port> 1234
192.168.122.1
*** Listening for incoming connections ***
*** Connection from ('192.168.122.179', 50618) has been established! ***
+--------------------------------------------------------------+
[+] Choose an option:

--shell : Get a shell
--ginfo : Get target info
--shutdown : Shutdown target
--close : Close connection
--screenshot : Take a screenshot
--upload : Upload a file to the victim's machine
--download : Download victim's files
--run : Run python scrypt on the victim's machine
--kill : Kill processes [WINDOWS ONLY]
--msg : Open message box [WINDOWS ONLY]
--lock : Lock PC [WINDOWS ONLY]
--stop : Stop key logger
--ccb : Get clipboard content
--getlogs : Get key logger logs

esc : Exit
```

HACKING POC

Part 3/3

CREATE MALWARE CLIENT

Next, we need malware to run on our victim or um…. test machine. We will copy files over once again to create this environment.

- Malwareclient.py

You can change the IP for your control server on line 18 and if you wish you can change line 19 to the port of your choice. We are going to use port *1234* in this example.

For my example I needed to install pyperclip and mss using pip.
So I would run the command
Pip install pyperclip mss
Everything else should be standard in Python 3.5

Once you input the IP address and the port you can run the server and allow the client to connect.

Feel free to play with this and explore, you now have a “secret” backdoor into a Windows machine that allows you a large amount of control. Play with it and see what you can do and feel free to play around with the code to do even more fun and malicious things. Fork the project on GitHub or add to my repo.

Next month we will discuss how to “pack” the malicious Python file into a regular normal program to trick a user into running it.

QUICK PROJECT

PIJUKEBOX
PART 1/2

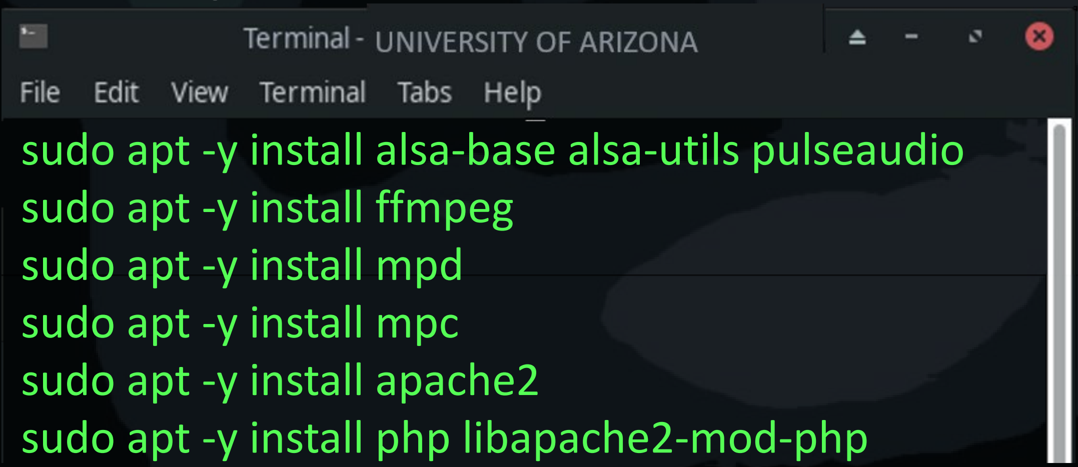
USE A RASPBERRY PI TO CREATE A MUSIC JUKEBOX

So we are stuck inside for a while, maybe you want a quick project to do. Maybe you like music and want something fun to play with… well give this project a quick try.

WHAT WE NEED:

- RASPBERRY PI
- SD CARD
- SPEAKERS

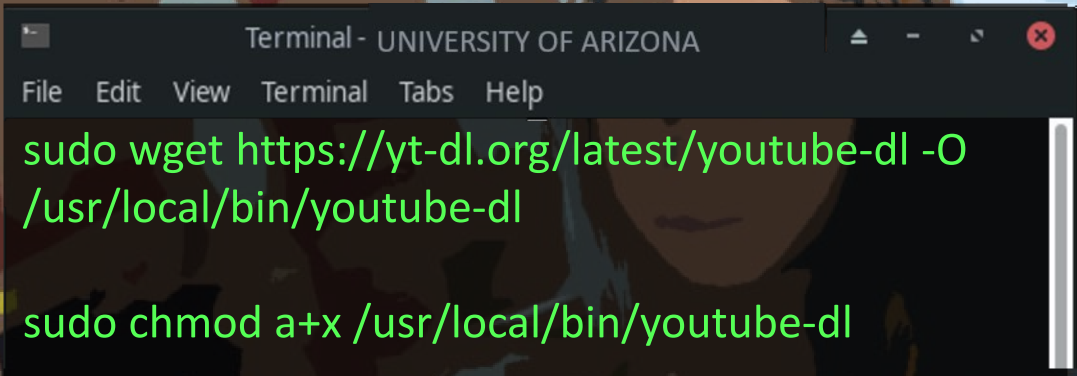
So hook it up to a monitor, mouse and keyboard and install the latest version of Raspian. Go ahead and install all updates and then install the following:



```
sudo apt -y install alsa-base alsa-utils pulseaudio
sudo apt -y install ffmpeg
sudo apt -y install mpd
sudo apt -y install mpc
sudo apt -y install apache2
sudo apt -y install php libapache2-mod-php
```

QUICK PROJECT

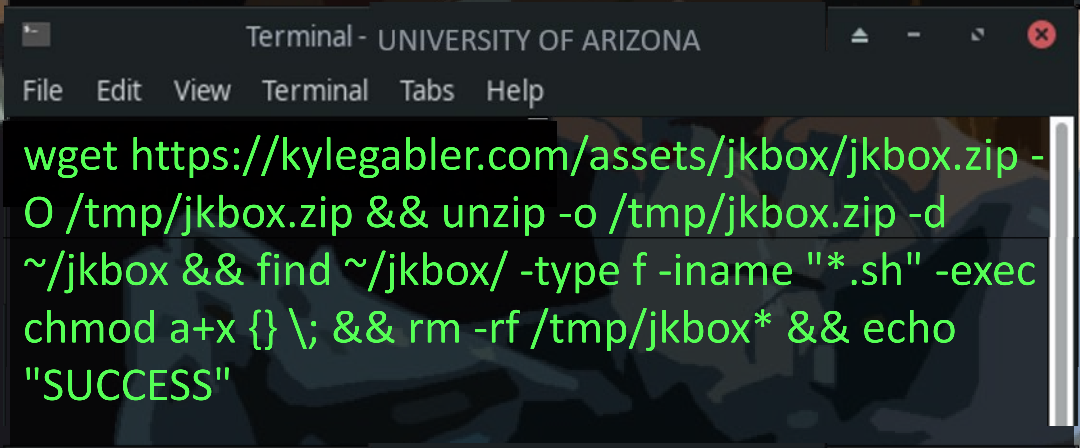
PIJUKEBOX PART 2/2


Terminal - UNIVERSITY OF ARIZONA
File Edit View Terminal Tabs Help

```
sudo wget https://yt-dl.org/latest/youtube-dl -O /usr/local/bin/youtube-dl

sudo chmod a+x /usr/local/bin/youtube-dl
```

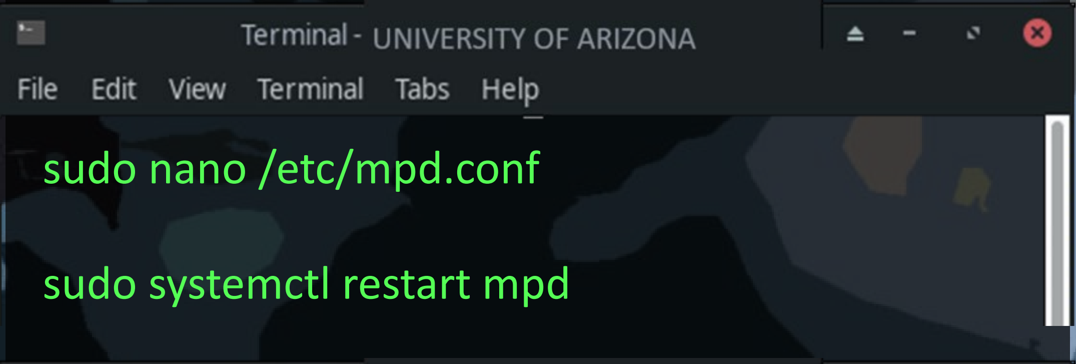
Now lets install Youtube-dl project


Terminal - UNIVERSITY OF ARIZONA
File Edit View Terminal Tabs Help

```
wget https://kylegabler.com/assets/jkbox/jkbox.zip -O /tmp/jkbox.zip && unzip -o /tmp/jkbox.zip -d ~/jkbox && find ~/jkbox/ -type f -iname "*.sh" -exec chmod a+x {} \; && rm -rf /tmp/jkbox* && echo "SUCCESS"
```

Install the JKBox script that will run the host PHP page

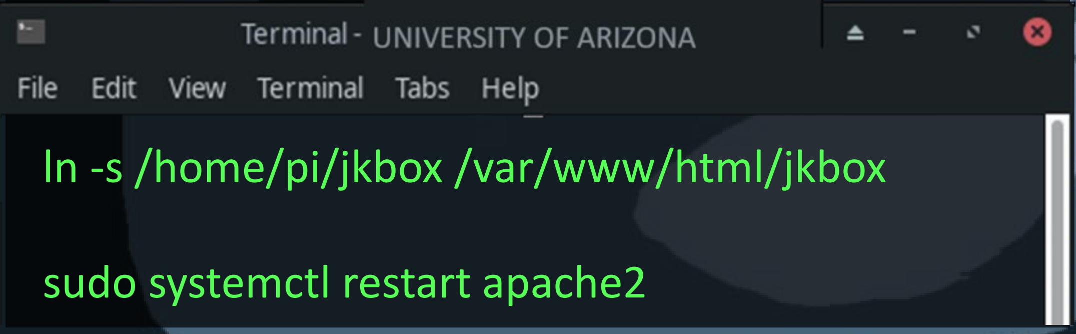
Set your Pi at a static IP address


Terminal - UNIVERSITY OF ARIZONA
File Edit View Terminal Tabs Help

```
sudo nano /etc/mpd.conf

sudo systemctl restart mpd
```

Edit the mpd music service to monitor music input and Set music_directory to /home/pi/jkbox/tracks


Terminal - UNIVERSITY OF ARIZONA
File Edit View Terminal Tabs Help

```
ln -s /home/pi/jkbox /var/www/html/jkbox

sudo systemctl restart apache2
```

Set up network service for the php webpage we downloaded

VISIT YOUR NEW JUKEBOX AT **HTTP://PI-IP-ADDRESS-HERE/JKBOX/**

CYBER SECURITY HISTORY

DISCOVERY OF ILOVEYOU VIRUS MAY 5, 2000

The very first virus that I remember growing up making the news was the ILOVEYOU computer worm that infected over ten million Windows personal computers on and after May 5th, 2000. The ILOVEYOU virus sends a user an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". The latter file extension was most often hidden by default on Windows computers of the time (as it is an extension for a file type that is known by Windows), leading unwitting users to think it was a normal text file. Opening the attachment activates the Visual Basic script. The worm inflicts damage on the local machine, overwriting random types of files (including Office files, image files, and audio files; however after overwriting MP3 files the virus hides the file), and sends a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook. This made it spread much faster than any other previous email worm. The worm searches connected drives and replaces files with common extensions like JPG, JPEG, DOCS and more with copies of itself making the user's computer unbootable. Since there were no laws in the Philippines against writing malware at the time, Filipino programmers named Reonel Ramones and Onel de Guzman were released with all charges dropped by state prosecutors. To address this legislative deficiency, the Philippine Congress enacted the E-Commerce Law in July 2000, just two months after the worm outbreak. As of 2012, the ILOVEYOU virus was regarded as the tenth-most virulent computer virus.

RELEASE OF WANNACRY MAY 12, 2017

WannaCry is a ransomware crypto worm that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments. It is considered a network worm because it also includes a "transport" mechanism to automatically spread itself. The attack began on Friday, May 12, 2017 with evidence pointing to an initial infection in Asia at 07:44 UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. Researcher Marcus Hutchins discovered the kill switch domain hardcoded in the malware. Registering a domain name for a DNS sinkhole stopped the attack from spreading as a worm because the ransomware only encrypted the computer's files if it was unable to connect to that domain, which all computers infected with WannaCry before the website's registration had been unable to do.

THE PACKET

THE UNIVERSITY OF ARIZONA

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

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

Phone: 520-458-8278 ext 2155

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

THE UNIVERSITY OF ARIZONA