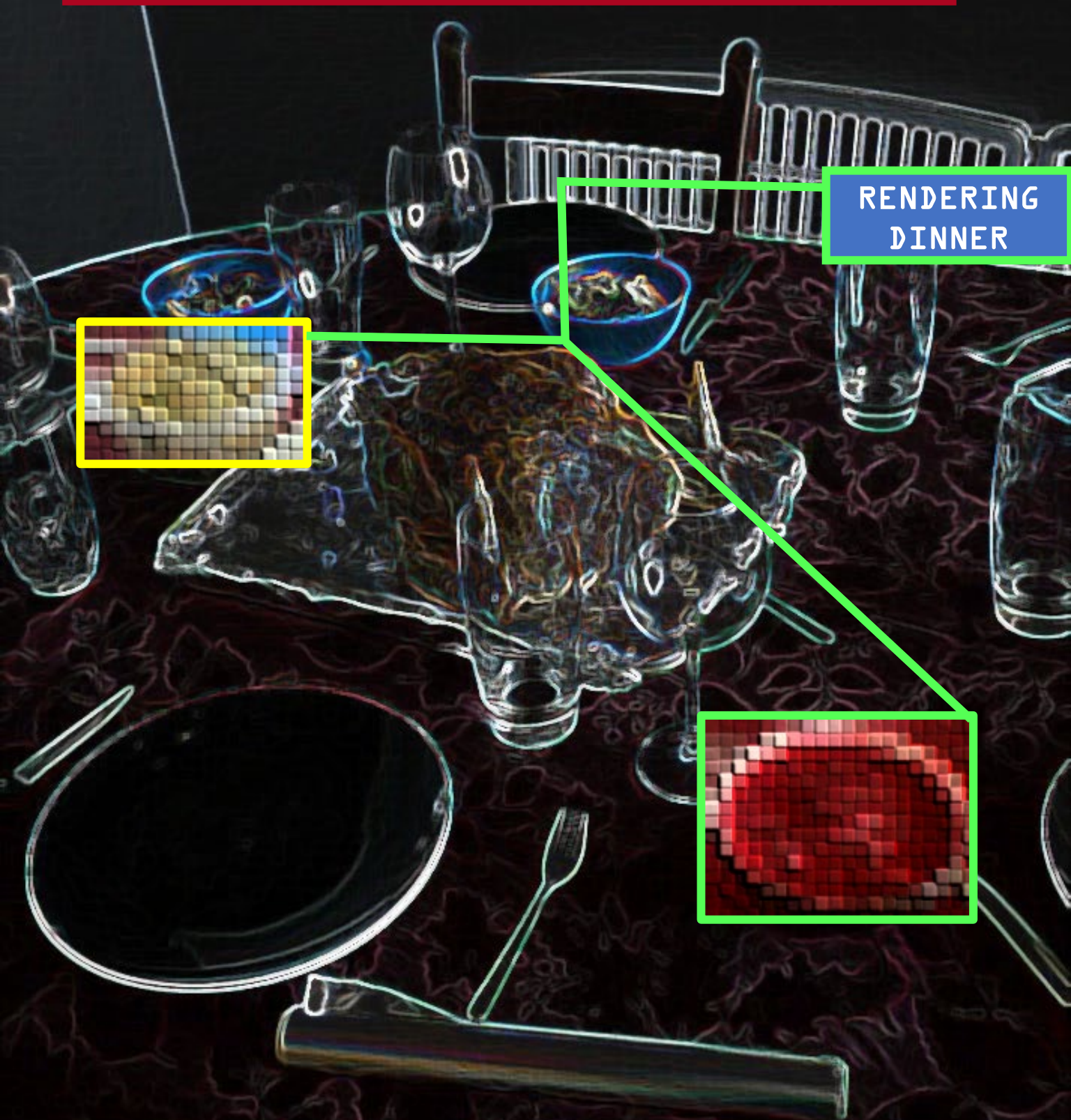


THE PACKET

 THE UNIVERSITY OF ARIZONA



RENDERING
DINNER

FALL

NOVEMBER 2020



IN THIS ISSUE

**HACKS OF THE
MONTH**

4

**CYBER NEWS
UPDATES**

6

HACKING POC

8

QUICK PROJECT

19

**CYBER
SECURITY
HISTORY**

20

--- BEGIN MESSAGE ---

Welcome to the [gobble gobble](#) or **NOVEMBER** issue of "The PACKET" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and we are now done with 7W1 classes and are moving forward in moving 2020 into the history books. 7W1 finals are behind us and Finals for the end of the fall semester is just around the corner. This fall we are all adjusting to COVID-19, Among Us, Cyberpunk 2077 coming out on November 19 (I hope its real this time) and a Presidential Election. These events have been drawing our attention in various directions. Education is important however, and I know everyone is waiting to attend your next lecture or at least waiting for the next round in Among Us to play Imposter. 32 years ago, the Internet witnessed one of the first global computer worms and things have only gotten worse as malicious adversaries improve tactics and techniques. Cyber security professionals have started to pop up and learn so many new mitigation techniques to counter this rising threat and Cyber security professionals still need help and each of you can help provide the much-needed protection. Cybersecurity issues are always advancing as new tactics and techniques are realized. Ransomware being the most recent newcomer and the next threat may be just around the corner. As you learn more about cybersecurity, you start to realize how vulnerable everything is. As hackers, we will inherently trust no one, including each other. This is a request to remain calm, enjoy the month of November and find a nice hacking project to settle into a learn by doing.

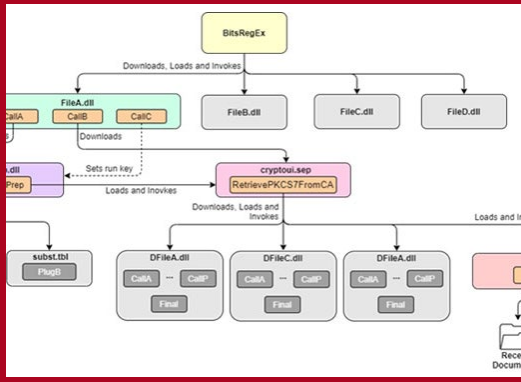
--- END MESSAGE ---

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

HACKS OF THE MONTH

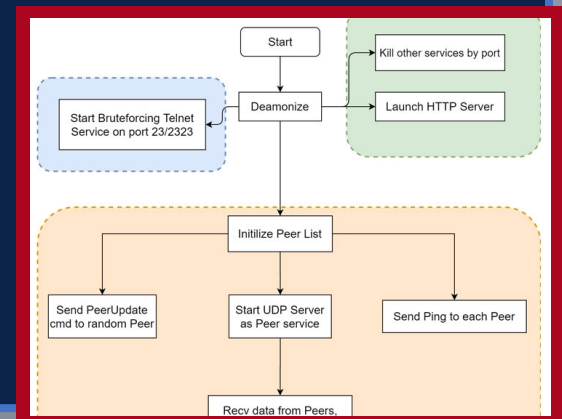
MosaicRegressor, Awesome name but...

MosaicRegressor is a new malware, which takes a clue from the VectorEDK boot kit. This malware targets diplomats and various NGO's in the continent of Africa, Asia and Europe. UEFI or Unified Extensible Firmware Interface is made to protect a computers BIOS, but for the second time UEFI has been the infection point and if you are into conspiracy theories, you would love to read up about badBIOS.



Wait, telnet is still a thing?!

The HEH botnet, written in Go, was named HEH because of how the file is packed. "In case you were wondering". HEH focuses on the IoT devices with telnet running for communication. The botnet sets up a P2P environment and runs on various architectures x86(32/64), ARM(32/64), MIPS(MIPS32/MIPS-III), and PowerPC. if the Telnet service is opened on port 23 or 2323, it attempts a brute-force attack using a password dictionary consisting of 171 usernames and 504 passwords



Incoming call, its malware, do you accept the charges?

Microsoft has warned about a new strain of mobile ransomware that takes advantage of incoming call notifications and Android's Home button to lock the device behind a ransom note. Dubbed "MalLocker.B", which has now resurfaced with new techniques, including a novel means to deliver the ransom demand on infected devices as well as an obfuscation mechanism to evade security solutions.

```
public class RansomActivity extends Activity {
    public static volatile RansomActivity activityObj;

    @Override // android.app.Activity
    public void onBackPressed() {
    }

    @Override // android.app.Activity
    protected void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        RansomActivity.activityObj = this;
        HelperTwo.putActivityObj(this);
        HelperThree.checkPresenceOfVirtualMachines(this);
        this.getWindow().addFlags(RansomActivity.getFlags());
        try {
            Context context = this.getApplicationContext();
            this setContentView(webViewAggregator.getView(context, context.getCacheDir().get
        } catch (Exception exception) {
            exception.printStackTrace();
        }
    }

    @Override // android.app.Activity
    protected void onResume() {
        super.onResume();
        this.startActivity(new Intent(this, RansomActivity.class));
    }

    public static int getFlags() {
        return 0x680480;
    }
}
```

DEPARTMENT OF DEFENSE

CYBER SCHOLARSHIP

INFORMATIONAL MEETING

VIEW THE INFO MEETING AND LEARN HOW YOU CAN APPLY FOR THE PROGRAM BY VISITING [HERE!](#)

- Full cost of tuition and ALL fees provided for 2020-2021 academic year.
- A \$25,000 (undergraduate) or \$30,000 (graduate) stipend for room and board.
- Covering the cost of all required books (up to \$1,250 a year).
- A laptop (up to \$1,500).

BASIC REQUIREMENTS

- Minimum cumulative GPA of 3.2 (undergraduate) or 3.5 (graduate).
- Must be entering junior or senior year or a graduate program in Fall 2020.
- Must be a U.S. Citizen.
- Agree to work for the DoD as a civilian for one year for each year of scholarship received.

CYBER

NEWS UPDATES

BLACKBERRY UNCOVERS MASSIVE HACK-FOR-HIRE GROUP BAHAMUT

BlackBerry released new research highlighting the true reach and sophistication of one of the most elusive, patient, and effective publicly known threat actors – BAHAMUT. BlackBerry researchers link the cyberespionage threat group to a staggering number of ongoing attacks against government officials and industry titans, while also unveiling the group’s vast network of disinformation assets aimed at furthering particular political causes and hampering NGOs



BAHAMUT: Hack-for-Phishing, Fake News,
BlackBerry investigates one of the most effective publicly known

DISCOVER MORE

CYBV 480
CYBER WARFARE

CYBV 435
Cyber Threat Intelligence

CYBV 385
INTRODUCTION TO CYBER OPERATIONS

CYBV 301
FUNDAMENTALS OF CYBERSECURITY

MICROSOFT AND PARTNERS UNITE TO TARGET TRICKBOT INFRASTRUCTURE IN LEGAL TAKEDOWN

Microsoft announced Monday morning that it has obtained a court order to dismantle Trickbot, a notorious botnet composed of millions of devices that U.S. officials worry could be used to sabotage state and local election-related IT systems ahead of the 2020 Presidential election. “We disrupted Trickbot through a court order we obtained as well as technical action we executed in partnership with telecommunications providers around the world,”



Microsoft

DISCOVER MORE

CYBV 454
MALWARE THREATS & ANALYSIS

CYBV 435
CYBER THREAT INTELLIGENCE

CYBV 388
CYBER INVESTIGATIONS AND FORENSICS

CYBV 385
INTRODUCTION TO CYBER OPERATIONS

FIVE HACKERS FOUND 55 BUGS IN APPLE PRODUCTS IN 3 MONTHS AND MADE \$288,500

Five hackers researched and analyzed several Apple online services for three months and found a grand total of 55 vulnerabilities, some of them potentially very dangerous, according to a blog post written by one of the hackers. One of the worst of all the bugs they found would have allowed criminals to create a worm that would automatically steal all the photos, videos, and documents from someone’s iCloud account and then do the same to the victim’s contacts.



DISCOVER MORE

CYBV 436
COUNTER CYBER THREAT INTELLIGENCE

CYBV 435
CYBER THREAT INTELLIGENCE

CYBV 329
CYBER ETHICS

CYBV 385
INTRODUCTION TO CYBER OPERATIONS

CYBER OPERATIONS SPRING 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 326	INTRO METHODS OF NTWK ANALYSIS	Book
CYBV 329	CYBER ETHICS	Book
CYBV 351	SIGINT AND EW	Book 1 , Book 2 , Book 3
CYBV 354	PRINCIPLES OPEN SOURCE INTEL	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	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
CYBV 437	DECEPTION & COUNTER-DECEPTION	Book
CYBV 440	DIGITAL ESPIONAGE	Book 1 , Book 2
CYBV 441	CYBER WAR, TERROR AND CRIME	Book 1 , Book 2
CYBV 450	INFORMATION WARFARE	Book 1
CYBV 454	MALWARE THREATS & ANALYSIS	Book
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 480	CYBER WARFARE	Book 1 , Book 2
CYBV 481	SOC ENG ATTACK & DEFENSE	Book 1 , Book 2
CYBV 496	SPCL TOPICS IN CYBER SECURITY	Book
CYBV 498	CAPSTONE IN CYBER OPERATIONS	

POC

Let's build a Raspberry Pi Tor Access Point

Tor is free and open-source software for enabling anonymous communication. Tor allows you to browse anonymously but please note the risks associated with a Tor Appliance when being used for browsing. You are at risk of being too easily fingerprinting. Tor protects a user's privacy but does not hide the fact that someone is using Tor. Tor makes use of the Onion routing protocol. Onion routing is implemented by encryption in the application layer, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit with a random-selection of Tor relays. With that out of the way, we are going to need a few components:

[Raspberry Pi 4](#) x 1

[USB WiFi Dongle](#) x 1

[USB Power Bank](#) x 1

[SD Card](#) x 1

[Debian Buster Lite Download](#)

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 go get a job that pays you to do it - legally!!

POC

Let's build a Raspberry Pi Tor Access Point

The first thing we need to do is build a headless Raspberry Pi and we will do that with our Debian Buster Image. With this being 'headless' we don't want to use external screen or keyboard; we need to allow an SSH access to the Raspberry Pi OS on the first boot. After we created our bootable SD card, we need to mount it and add a file called "ssh" inside a boot partition.

This will enable and start ssh daemon on pi at boot.

To continue the setup we will need an Ethernet Cable with DHCP and Internet Connection. Insert the SD card and the Ethernet cable and boot your pi by connecting power. At this point the pi should boot the new OS from the SD card and get a DHCP address.

Find the new address your pi just got from your dhcp server.

If you can't find the new address, you can connect it to address, you can connect it to the external screen and keyboard - use the default credentials to login and 'ip addr' command to discover what address it was assigned.

SSH to the Raspberry Pi Default credentials:

User: **pi**

Password: **raspberrypi**

The first thing now is to change the default password using the **passwd** command

POC

Let's build a Raspberry Pi Tor Access Point

Now let's change the host name for the device using the command `sudo raspi-config` and navigate to network options and then the hostname. Change this to whatever you decide to use.

Next, let's add some utilities with the following command `sudo apt install -y net-tools curl wget traceroute htop`

This will install net-tools, curl, wget, traceroute and my favorite htop.

Now we will need to reboot, and we can do this by the command line with the command `sudo reboot` it is as easy as that.

Now let's build a really easy web interface so that we can make changes as needed easily. A project has already been completed for this step and we will borrow from the [RaspAP](#) project.

Run the following command

```
curl -sL https://install.raspap.com | bash
```

You will have a selection of questions you will need to answer and those are available over on the right

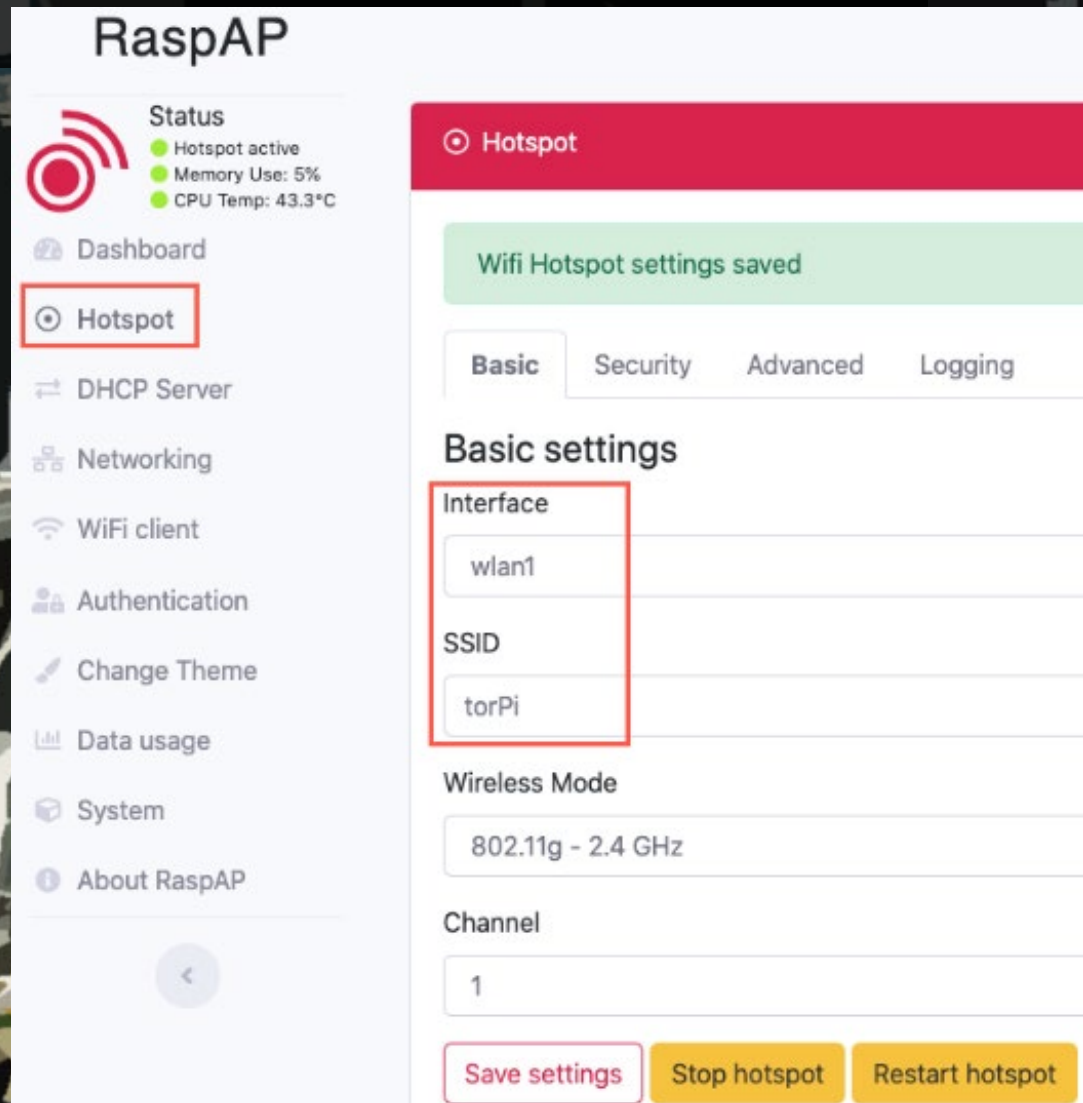
You will then be able to log into your interface after the reboot at the devices IP address. The first thing is to **change the default web-ui Credentials**

Question	Answer
lighttpd root: /var/www/html?	Y
Complete installation with these values?	Y
Enable HttpOnly for session cookies (Recommended)?	Y
Enable RaspAP control service (Recommended)?	Y
Install ad blocking and enable list management?	n
Install OpenVPN and enable client configuration?	n
The system needs to be rebooted as a final step. Reboot now?	y

POC

Let's build a Raspberry Pi Tor Access Point

We selected the Raspberry Pi 4 which has a wireless interface already. By adding our dongle we will set our internal one as a hotspot and the dongle as the client. You will do this in the Hotspot tab on the right.



RaspAP

Status

- Hotspot active
- Memory Use: 5%
- CPU Temp: 43.3°C

Dashboard

Hotspot

DHCP Server

Networking

WiFi client

Authentication

Change Theme

Data usage

System

About RaspAP

Hotspot

Wifi Hotspot settings saved

Basic Security Advanced Logging

Basic settings

Interface

wlan1

SSID

torPi

Wireless Mode

802.11g - 2.4 GHz

Channel

1

Save settings Stop hotspot Restart hotspot

POC

Let's build a Raspberry Pi Tor Access Point

Now we will need to install the Tor Service

```
sudo apt install -y tor
```

Delete the current configuration file

```
sudo rm -rf /etc/tor/torrc
```

Create new torrc and edit it

```
sudo nano /etc/tor/torrc
```

Add the following lines to the configuration file:

```
VirtualAddrNetwork 10.192.0.0/10
```

```
AutomapHostsSuffixes .onion,.exit
```

```
AutomapHostsOnResolve 1
```

```
TransPort 10.3.141.1:9040
```

```
TransListenAddress 10.3.141.1
```

```
DNSPort 10.3.141.1:53
```

```
DNSListenAddress 10.3.141.1
```

You can also add the following as well to rotate the exit node every 10 seconds:

```
CircuitBuildTimeout 10
```

```
LearnCircuitBuildTimeout 0
```

```
MaxCircuitDirtiness 10
```

POC

Let's build a Raspberry Pi Tor Access Point

Let us now set the service to start every time the device reboots by doing to the following commands

```
sudo systemctl start tor.service
```

```
sudo systemctl enable tor.service
```

To ensure this is done correctly we need to make sure that the service is running run the following command and looks for the tor program attached to a pid

```
sudo netstat -plnt
```

```
pi@torPi ~
$ sudo netstat -plnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 10.3.141.1:9040         0.0.0.0:*                LISTEN      2186/tor
tcp        0      0 0.0.0.0:80             0.0.0.0:*                LISTEN      399/lighttpd
tcp        0      0 0.0.0.0:53             0.0.0.0:*                LISTEN      4663/dnsmasq
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      533/sshd
tcp        0      0 127.0.0.1:9050         0.0.0.0:*                LISTEN      2186/tor
tcp6       0      0 :::80                  :::*                    LISTEN      399/lighttpd
tcp6       0      0 :::53                  :::*                    LISTEN      4663/dnsmasq
tcp6       0      0 :::22                  :::*                    LISTEN      533/sshd
```

IF YOU ARE UNABLE TO RUN THE NETSTAT COMMAND, PLEASE ENSURE YOU INSTALLED THE NET-TOOLS PACKAGE FROM EARLIER.

POC

Let's build a Raspberry Pi Tor Access Point

Now it is possible that you are unable to get the Tor service to start, you may need to install monit to mitigate this and you do this by running the following commands:

```
sudo apt install monit
```

You will then need to edit the configuration file and add the following at the bottom:

```
sudo nano /etc/monit/monitrc
```

```
check process gdm with pidfile /var/run/tor/tor.pid  
start program = "/etc/init.d/tor start"  
stop program = "/etc/init.d/tor stop"
```

This will start the service as needed at boot if not already done. To active this we just need to enable the service by doing the following.

```
sudo systemctl restart monit  
sudo systemctl enable monit
```

Now to configure firewall rules you can follow the steps located [here](#). But please enjoy browsing the Onion network like a boss!!

STUDENT

INTERVIEW

Part 1/4

I had the pleasure to meet with the recent University of Arizona recipient of the VetSuccess Immersion Academy under SANS, Devin Glauner.

SANS has a few eligibility requirements for the applicants to include:

- Transitioning service members not more than six months away from separation.
- Veterans with less than ten years out of the service. Veterans cannot be working in the information security field or have prior work experience from the information security field outside of the military
- Active duty spouses not working in the information security field or with prior work experience in the information security field.
- Must be a U.S. citizen or Permanent Legal Resident (Green card holder).

Candidates meeting the Academy requirements may submit an application and proceed to complete an online assessment. Based on the results, applicants may be invited to submit additional documentation to complete their application and may advance to the next step for a personal interview. The Admissions Committee will determine which candidates are accepted and will notify them of next steps.

SO WITH THAT OUT OF THE WAY, DEVIN, WHAT DID YOU WANT TO BE WHEN YOU GREW UP AS A CHILD, AND WHAT MADE YOU WANT TO BE IN CYBERSECURITY?

I want to work in cyber because I enjoy IT and networking, and like the idea that the field is ever-changing and will pose new challenges throughout my entire career.

STUDENT

Part 2/4

INTERVIEW

INTERESTING, WELL WAS YOUR DREAM JOB AS A CHILD?

I wanted to be an astronaut as a child and had an entire astronaut and spaced themed bedroom based around that desire.

I WOULD HAVE LOVED A SPACE BEDROOM, OR AT LEAST THOSE GLOW IN THE DARK STARS YOU PUT ON YOUR CEILING. IF YOU COULD TALK TO YOUR SELF-10-ISH YEARS AGO, WHAT WOULD YOU SAY?

I would have told myself to skip college the first time around because I didn't know what I wanted to do and ended up having six majors in 5 semesters and an abysmal GPA. Coming back to school with a passion for what I'm learning has made this go around fun and successful.

FINDING YOUR PASSION I WOULD SAY IS ONE OF THE HARDEST THINGS TO DO AT A YOUNG AGE. WELL AS YOU STUDY CYBERSECURITY WHAT TOPIC IN IS YOUR FAVORITE VS. WHAT COULD YOU DO WITHOUT?

My Favorite is Hunt team and penetration testing and not sure yet what to do with that yet.

STUDENT

Part 3/4

INTERVIEW

SOUNDS LIKE YOU ARE ENJOYING IT, HOW DID YOU FIND OUT ABOUT THIS SCHOLARSHIP AND OPPORTUNITY, HOW WOULD YOU RECOMMEND ANYONE ELSE WITH YOUR BACKGROUND TO FIND THIS?

Professor Wagner spoke about the SANS certs in the CYBV326 course, which drove me to research opportunities through SANS. I found the Immersion Academy during this research.

NICE, WELL ANY RECOMMENDATIONS YOU WISH TO SHARE IN GENERAL FOR OTHER STUDENTS OR STUDENTS TRANSITIONING FROM MILITARY SERVICE?

I'm still in the process of transitioning, for others in the same process prepare in advance, research everything, and take advantage of the programs available. Also, look into DoD SkillBridge internships. For anyone pursuing certs I have found it helpful to study for a cert that matches the courses I am taking. I took sec+ after 385 and have scheduled my CySA+ to coincide with the end of 400.

WELL THANK YOU VERY MUCH FOR YOUR TIME AND FOR EVERYONE ELSE IF YOU WOULD LIKE TO LEARN MORE ABOUT THIS TYPE OF PROGRAM GO OVER TO <https://www.sans.org/cybertalent/cybersecurity-career/vetsuccess-academy>

STUDENT

INTERVIEW

Part 4/4

SANS OFFERS MULTIPLE OPPORTUNITIES AND ENCOURAGES EVERYONE TO APPLY. SANS OPPORTUNITIES ARE BROKEN DOWN INTO VARIOUS PROGRAMS AND BELOW ARE A FEW THAT YOU MAY BE INTERESTED IN.

- **Vet Success** - <https://www.sans.org/cybertalent/cybersecurity-career/vetsuccess-academy>
- **Women's Academy** - <https://www.sans.org/cybertalent/cybersecurity-career/womens-academy>
- **Cyber Workforce Academy** - <https://www.sans.org/cybertalent/cybersecurity-career/cyber-workforce-academy>
- **Diversity Cyber Academy** - <https://www.sans.org/cybertalent/cybersecurity-career/diversity-cyber-academy>
- **Diversity Cyber Workforce Academy - California** - <https://www.sans.org/cybertalent/cybersecurity-career/diversity-cyber-workforce-academy-ca>

QUICK PROJECT



Raspberry Pi
E-Ink
Dashboard.

LET'S MAKE A E-INK DASHBOARD IN PYTHON

So I love Raspberry Pi's as both a physical device and the edible pastry treat. Now when I come across a good-looking dashboard I want to try and emulate what I see. Well a project put on by zoharsf creates a beautiful dashboard on a Raspberry Pi and can be a fun project for a side table information panel that will tell you the current Date, Weather, COVID-19 info and your current Internet Speed all within a Raspberry Pi device that you could run other things on as you build out other projects.

For this project you will need:

[Raspberry Pi 4](#) x 1

[USB Power Bank](#) x 1

[SD Card](#) x 1

[Waveshare E-reader Screen](#) x1

[Debian Buster Lite Download](#)

Follow the instructions on the GitHub page to configure everything and move the project over. It is a fairly easy copy and paste procedure and hardware is configured very nicely. Then change the dashboard to whatever you want. Show yours off and send me pictures for future updates!!



CYBER SECURITY HISTORY

MORRIS WORM DISCOVERED

NOVEMBER 2, 1988

In an attempt to “Map the Internet” a student created a self-replicating worm that would spread between computers in 1988. The worm was distributed by the internet which was new at the time as malicious files usually had to be spread by other means like floppy disks. The worm was designed to infect a computer and move on if the machine was already infected but the author, Robert Morris believed that users would figure out a way to stop the worm so the worm would infect the computer again in a 1 in 7 chance. This was expected to be a rare occurrence but every machine that was infected tried to infect other computers again and given enough time machines were infected multiple times forcing multiple slowdowns as resources were exhausted. The Morris worm is also called the Great Worm because of the devastation that this worm caused. On January 22nd, 1990, Robert Tappan Morris was prosecuted under the charge of fraud and deception. He was sentenced to three years of probation, plus a fine of \$10,050, and the costs of his supervision and 400 hours of community work. Such sentence was the first one which used the 1986 computer fraud law, and Morris was the first malware writer who was convicted in history.

“COMPUTER VIRUS” TERM FIRST USED

NOVEMBER 10, 1983

Fred Cohen coined the term “Computer Virus” to help explain what was happening during a security seminar. Fred Cohen defined a computer virus as “a program that can infect other programs by modifying them to include a possibly evolved copy of itself”. Cohen didn't invent the virus, but his demonstration made computer scientists aware of the threat they posed.

THE PACKET

 THE UNIVERSITY OF ARIZONA



CONTACT US

CHIO@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

