THE PACKET

THE UNIVERSITY OF ARIZONA

FALL

SEPTEMBER 2020

IN THIS ISSUE

--- BEGIN MESSAGE ---

Welcome to the **SEPTEMBER** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde and I hope everyone is enjoying the start of the fall semester. DEFCON took place last month and was free for anyone to attend virtually and you can see these videos at YOUTUBE. We are starting off the Fall semester strong and if you want to enroll in a class for Seven Week 2 please do so quickly as that window is very closely passing. The world is moving more to online and with that changes to how we interact with our online world. Companies and businesses are struggling to find ways to maintain productivity with work from home and are somewhat surprised at how well the workforce has taken the call. Will this change how employees work? Well, time will only tell but for many organizations the investment in work from home policies is needed and many are realizing that by not having one, the amount of vulnerabilities is increasing and may be taken advantage of by malicious actors. The need for a strong and well-versed cyber workforce is needed and everyone who has an interest in this profession will have to answer this call. Cybersecurity takes no breaks from anyone and who ever has the most tools in their toolbox will be the most effective. As you work to increase what tools and programs you have access to, always keep your eyes pealed for what is needed. It may be that the next best cyber defense tool hasn't been developed yet because you have not made it. Welcome once again to the fall semester, I hope you find opportunity in the COVID-19 world!

--- END MESSAGE ---

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

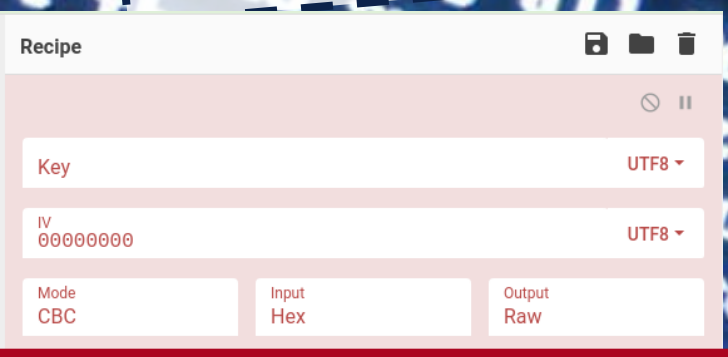
What data encryption standard was first published in 1975?

// INITIATE TRANSMISSION //

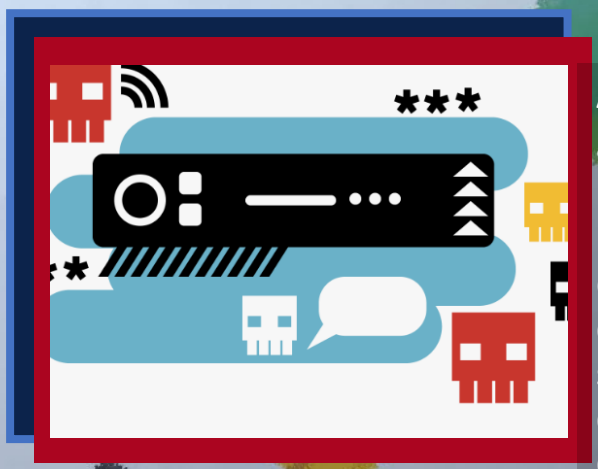
SWITCH TO CIPHER TEXT IN 3… 2… 1…

```
ecc5e83ece0d9eb65fc70a1fa6ad90cdee234a0410df142c0
879b6696bb41c534e29151f869aec7b165f0937905052fb44
8f8f3f597328c8679ee4e19ec8470cf2a681026d40ebae97c
0fb81aaef6a4c1a85c73fe13ca696b50dba2f648fc744c0f6
dcfba081b22bed525ee199f1a9a51d26b90dd6e2f19da0dfa
8a6a7c0bb51b334a9e1a355489348ad3aeb96dcaa374c2619
81a520f276443e1020bb54d1444c30afea303484767a86cdc
acb3ac805edf631be4b44cdcb2f20e5036fa1d3b97d387ced
30d8e75e91ecab37454b2f23452daafc980714baded9e0f1c
6dab4d110ddb585f63247bfb8ee319d7ac46dd44088934280
c5ac1971074f5409898a08fdee8b0fcae251a66505b25caa5
94966001d815621d3bafee9ada686f73d14f572cde2c5f6b2
817f6f35bebbbe392841
```

// TERMINATE TRANSMISSION //



HACKS OF THE MONTH



A secret BOTNET that is not so secret anymore…

FritzFrog which is focused on government, financial institutions, telecom and universities has been discovered trying to hid under the radar with no command and control. The botnet uses proprietary software written from scratch to infect servers and corral them into a peer-to-peer network and no command and control built in.

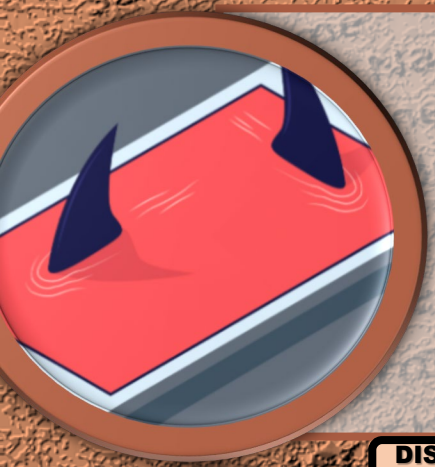
VISHING, its like Phishing but with your voice or another way to say Social Engineering

So as everyone works from home the security engineer tries to discover what new holes have been opened before the hacker does and for some this may be a new type of activity. Now with help from the FBI and CISA system admins have more things to look out for and maybe mitigate them.

The great China Firewall is springing leaks

Three Chinese companies have allegedly been breached and internal documents have been leaked showing what the Chinese government wants blocked internally. After leaking some of the documents, the group was banned by Twitter under its hacked files policy.

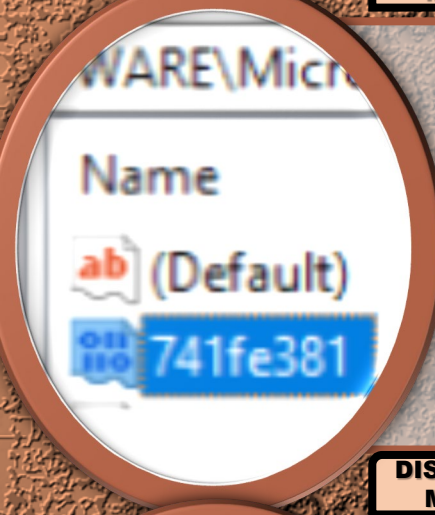
CYBER NEWS UPDATES



VOICE PHISHERS TARGETING CORPORATE VPNs

The COVID-19 epidemic has brought a wave of email phishing attacks that try to trick work-at-home employees into giving away credentials needed to remotely access their employer's networks. But one increasingly brazen group of crooks is taking your standard phishing attack to the next level, marketing a voice phishing service that uses a combination of one-on-one phone calls and custom phishing sites to steal VPN credentials from employees.

DISCOVER MORE | CYBV 480 CYBER WARFARE | CYBV 435 Cyber Threat Intelligence | CYBV 385 INTRODUCTION TO CYBER OPERATIONS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY



RESEARCHERS DISTRIBUTED AN EMOTET VACCINE

Emotet is just a piece of software and as such, Emotet also has bugs. Emotet's "persistence mechanism" which is also known as the part of the code that allows the malware to survive PC reboots has a bug that researchers exploited. Researchers noticed Emotet was creating a Windows registry key and saving an XOR cipher key inside it. By simply changing this value, the malformed registry key triggered a buffer overflow in Emotet's code and crashed the malware, effectively preventing users from getting infected.

DISCOVER MORE | CYBV 454 MALWARE THREATS & ANALYSIS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 388 CYBER INVESTIGATIONS AND FORENSICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

GOOGLE FIXES MAJOR GMAIL BUG SEVEN HOURS AFTER EXPLOIT DETAILS GO PUBLIC

Google has patched on Wednesday a major security bug impacting the Gmail and G Suite email servers. The bug could have allowed a threat actor to send spoofed emails mimicking any Gmail or G Suite customer. The bug also allowed attackers to pass the spoofed emails as compliant with SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting, and Conformance), two of the most advanced email security standards.

DISCOVER MORE | CYBV 436 COUNTER CYBER THREAT INTELLIGENCE | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 329 CYBER ETHICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

CYBER SECURITY DEFENSIVE PROTOCOL

SOCIAL MEDIA HYGIENE, PART 1

Social media has a pervasive reach on the life of the average person, today. The collective platforms expose your daily routine of where you live and the stores you frequent, your dating and family life, what you do at work, your interests, and numerous other details that - when aggregated - can pose a huge security and even personal safety risk. Over the next several issues we will cover defensive protocols to secure your social media presence in an intelligent manner. Our intent is not only to increase your safety and situational awareness, but to augment your perception of the power of OSINT (Open Source Intelligence) and encourage you to think proactively when it comes to security.

The first aspect of social media hygiene we'd like to cover is simple photographs. Whereas your intent in posting a photo of yourself having drinks with friends after work may be to preserve and share the positive memory, you may be unintentionally exposing other details:

Case A: Are the keys to your apartment sitting on the table? The photo can be enhanced, and your front door key replicated.

Case B: Is your access badge for work exposed on its lanyard? This can be recreated in a simple photo editor, your name and photo replaced with those of someone with ill intent.

Case C: Was the photo taken by a device that had location services or GPS enabled? This can be used to develop your pattern of life.

CYBER SECURITY DEFENSIVE PROTOCOL

Case A: The physical nature of our keys convinces us of the mindset that as long as they're in our possession, they - and what they unlock - are secure. However, the clarity of modern photography makes it a simple task to analyze a key and determine its bitings - the specific size cuts the 'teeth'. This is sometimes a numeric sequence on one side of they key's head, or it can be inferred by comparing it to a similar style key. If someone already knows where you live, the implications are obvious. If they don't, we'll show you in Case C how easy it can be to discover that information.

To prevent this, you only need to blur out your keys in your photos. It draws little attention and is sufficient to prevent your keys from being duplicated.

Case B: Similarly to Case A, physical security tokens aren't commonly considered compromised simply by being visible to someone else. However, a work-related identification badge can be easily recreated in a photo editing software, your face and name replaced with the attacker's. Although RFID access cannot be copied with this method, a simple excuse such as "My badge got wet" or slipping behind someone else as they open an RFID access-controlled door are easy tactics, bolstered by the attacker now looking like he or she belongs.

Blurring out your ID badge in pictures is again sufficient to prevent this kind of exploitation. We do, however, recommend tucking it into a pocket. Someone being able to learn your name, position, and place of employment is sufficient to begin developing a social engineering exploit on you.

CYBER SECURITY DEFENSIVE PROTOCOL

Case C: Whenever a photo is taken with a digital device, it contains more information than what's visible. Whereas it may be something as innocuous as time and date or camera settings, with GPS enabled cameras and all smart phones it frequently contains the exact location of the photograph, and even the name of that device owner.

This data is called EXIF data - Exchangeable image file format - also referred to as metadata. A single photo doesn't pose a significant risk, but if multiple photos are analyzed then the metadata can be aggregated. That can be used to develop a pattern of what times you frequent certain locations, and what those locations are; your residence, your favorite cafe, your significant other's apartment.

We recommend a multi-pronged solution to this vulnerability. Your first effort should be to disable location services from connecting to the camera on your phone.

Secondly, understand that when uploading a photo to social media, these photos are frequently compressed and the EXIF data lost in this process. Therefore, it is up to you to disable location tagging on your social media accounts, as well as ensure you don't use hashtags of place or business names. Or, if you have children, the name of their school.

Lastly, if you want to be exceedingly thorough, we recommend a program such as **ExifCleaner**. It is operating system agnostic, open source, and supports numerous filetypes.

JOB BOARD

Information System Security Professional

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!

Cyber Mitigations Engineer/System Vulnerability Analyst

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!

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.

BOOK REVIEW

Effective C, by Robert Seacord

There are a *lot* of books about the C programming language out there. There are *not* a lot of good ones - something this contributor learned while he was learning how to get his own poorly written code to compile.

This book came to the rescue. It goes into greater detail than the average introductory text, and is by far the most up to date and security focused. Getting code to compile is one thing, writing good, 'Effective C' is another.

Seacord covers all of the basics, as is fitting for an introduction to the language, but he doesn't oversimplify . He does, however, succinctly and effectively explain the areas of added detail that other books frequently gloss over, without inundating the reader. His sequence of presentation from chapter to chapter is easier to follow than many books, and is bolstered by occasional end of chapter exercises to bolster your understanding of the material. As with his explanations, the exercises are not overwhelming.

His final three chapters cover the preprocessor, program structure, and debugging, testing and analysis. Three areas that, covered in the initial phases of learning C, truly set you up to be a successful and independent programmer

CYBER OPERATIONS FALL SCHEDULE

CAT #	COURSE
CYBV 301	FUNDAMENTALS OF CYBERSECURITY
CYBV 326	INTRODUCTORY METHODS OF NETWORK ANALYSIS
CYBV 329	CYBER ETHICS
CYBV 354	PRINCIPLES OF OPEN SOURCE INTELLIGENCE (7 WEEK CLASS 2 ONLY)
CYBV 385	INTRODUCTION TO CYBER OPERATIONS
CYBV 388	CYBER INVESTIGATIONS AND FORENSICS
CYBV 400	ACTIVE CYBER DEFENSE
CYBV 435	CYBER THREAT INTELLIGENCE
CYBV 436	COUNTER CYBER THREAT INTELLIGENCE (7 WEEK CLASS 2 ONLY)
CYBV 440	DIGITAL ESPIONAGE (7 WEEK CLASS 1 ONLY)
CYBV 441	CYBER WAR, TERROR AND CRIME (7 WEEK CLASS 2 ONLY)
CYBV 454	MALWARE THREATS & ANALYSIS
CYBV 471	ASSEMBLY LANGUAGE PROGRAMMING FOR SECURITY PROFESSIONALS
CYBV 473	VIOLENT PYTHON
CYBV 480	CYBER WARFARE
CYBV 496	INTRODUCTION TO SECURITY SCRIPTING (7 WEEK CLASS 1 ONLY)
CYBV 498	CAPSTONE IN CYBER OPERATIONS

HACKING

POC

Part 1/6

Cracking a Windows Machine in Minutes

There's Hash Crack, John the Ripper, and numerous other great password cracking tools out there… And then, for a locked Windows machine sitting unguarded, there's easy mode.

After the initial investment of time (maybe 30 minutes if you've got fast internet), this method will grant you access to almost any Windows NT, 2000, 7, 8, or 8.1 machine in just a few minutes.

This method leverages inherently insecure hard drive partitions and the ubiquitous flexibility of Linux Live USBs. Although you could use Ubuntu, or even Kali, for this Proof of Concept we wanted to resurrect Blackbuntu from the graveyard of the Internet. Go grab a blank USB Drive and let's get started.

Firstly, we'll need to install this distro of Blackbuntu. On the following page, we'll walk you through how to etch it and turn it into a Live USB.

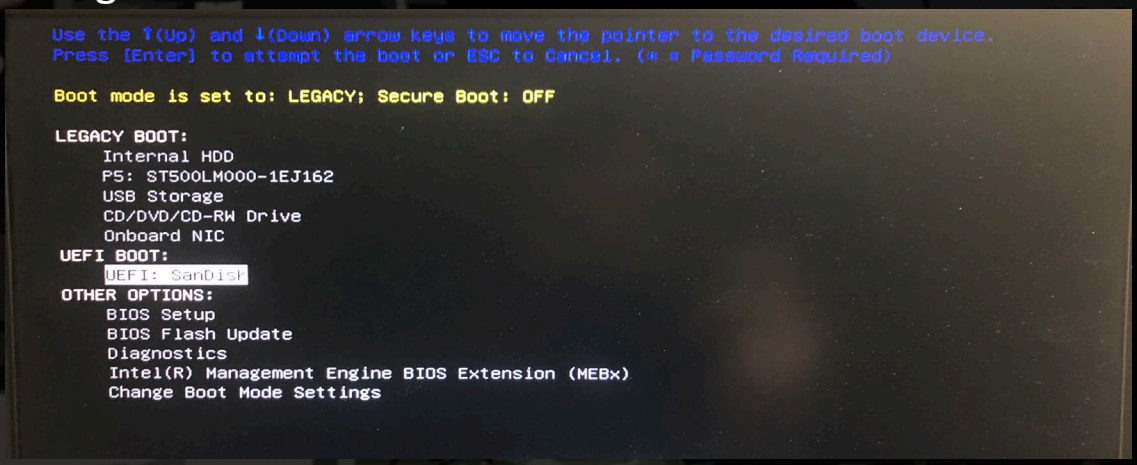
CAUTION — This article shows you how to perform potentially illegal activities. This series is intended for academic purposes only and is meant to provide education to cyber security professionals… If you want to do this stuff for real, do good in school and go get a job that pays you to do it - legally

HACKING POC

Part 2/6

If you weren't with us for last month's edition, download and install Balena Etcher, then we're going to flash the Blackbuntu .iso to the USB drive. Select the .iso file from the directory you downloaded it to, your USB drive as the target, then click Flash! and give it a few minutes.

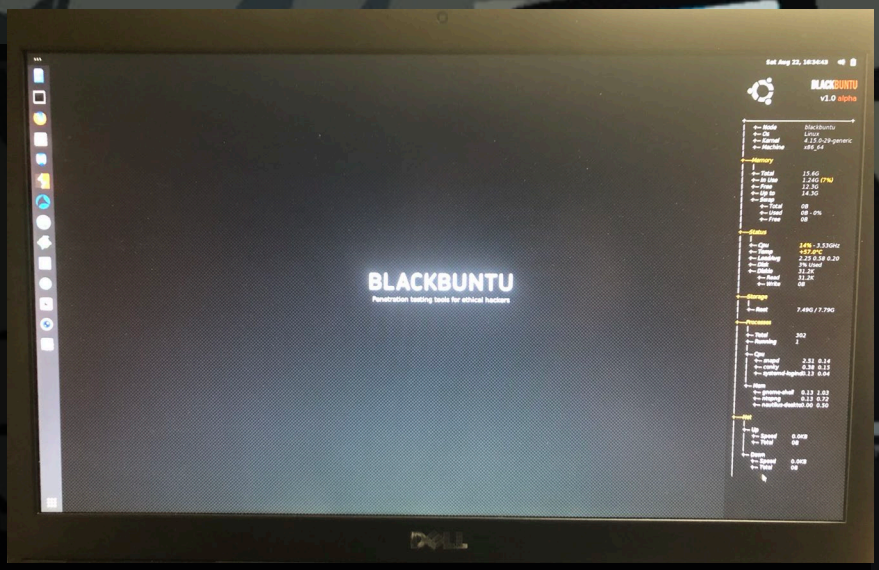
Note that upon completion, your device may give you a message saying it does not recognize the device. Ignore this, remove your fresh little USB stick of doom, and go find a locked Windows machine (*one that you own, or have permission to do this on…*) Plug it in while the machine is powered off, turn it on and repeatedly press the F12 key until you see the following menu:



Select the USB drive under UEFI BOOT. On the following page, select "Try Blackbuntu without installing". It will quickly load and display the Blackbuntu desktop.

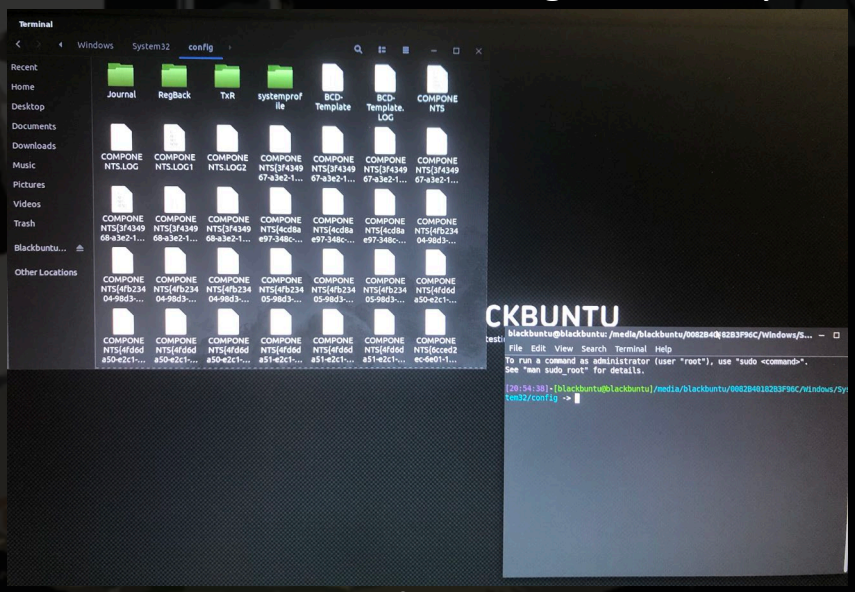
HACKING POC

Part 3/6



First step is to correct a quirk in this distro: It has a native French keyboard layout. Go into Settings > Region & Language > Input Sources and add English (US). Now the fun stuff!

Click on the filing cabinet icon, and navigate to Other Locations > (native hard drive) > Windows > System32 > config. Now right click and select 'Open in Terminal'. This will open the terminal already CDed to the directory we just found - it's easier to navigate visually.



(The native hard drive name may vary from one machine to another. For us, it was '1.0 TB Volume')

HACKING POC

Part 4/6

First we need to identify exactly where the Windows partition is, then remount the file system in Read-Write mode to allow changes to the SAM (Security Accounts Manager) file. Run the following command:

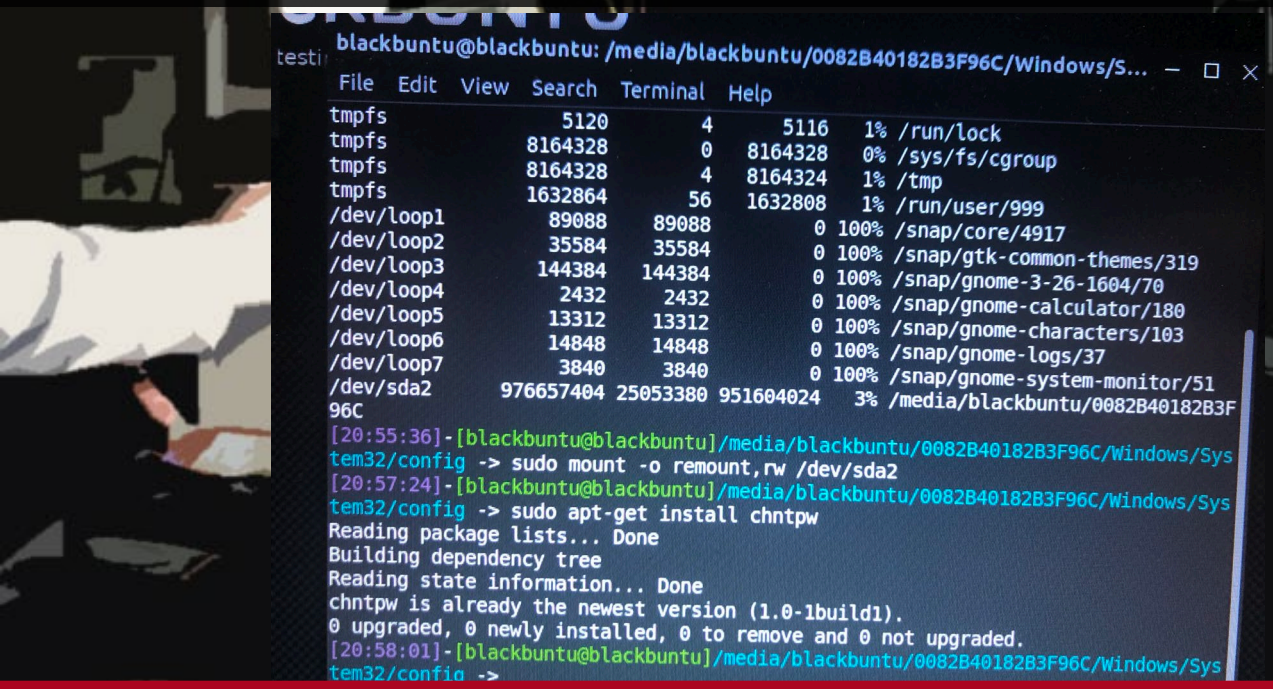
```
df
```

It should be something like /dev/sda2/media/blackbuntu. Now to allow us to read and write, execute this command:

```
sudo mount -o remount,rw (device)
```

Replace (device) with what you found from our previous snooping step

There's no need to run apt-get (as you can see in the photo below). The tool we need - chntpw - comes packaged with Blackbuntu.



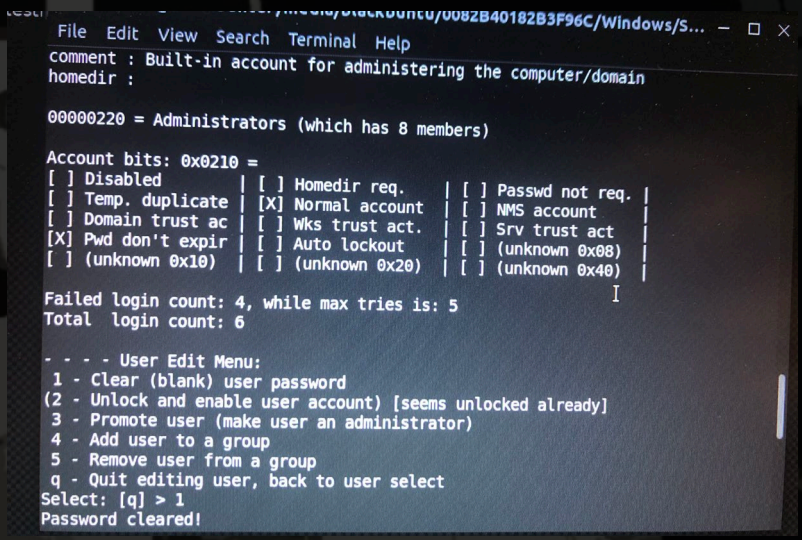
HACKING POC

Part 5/6

Now we are in position to engage in nefarious activity. Let's go straight to the top and get admin level access. The following command will get you there:

chntpw SAM

If you were targeting a specific username, you could specify that with the flag "-u (username) SAM". Now you'll see a list of numbered commands. Option 1 will allow us to clear out the password to grant easy access to the machine with just username (in this case, "Administrator"). Just type 1 and hit enter!



Lastly it will ask you if you want to write hive files. Yes, we do - that will write these changes to the SAM file. Now reboot in Windows and log in as Administrator! No password required.

Understanding what's going on

What did we just do? Let's back track from the end and explain as we go. The SAM - Security Accounts Manager - is a database file that authenticates local user logons. Simply put, it stores password hashes - which, as we know, are one way cryptographic functions. That's why we chose to simply clear out the password: Creating a new password would've required us to generate a corresponding hash for it. This adds complexity to our exploit but without any corresponding value, and we would risk the hash not matching the systems authentication protocol, potentially rendering our password useless.

The hashes in the SAM are either LM (LAN Manager) or NTLM (New Technology LAN Manager). Had we grabbed the hashes instead of clearing them out, we could've used something like Hashcat to crack them, but in this case it's simply unnecessary. It's worth noting, however, that NTLM hashes are not salted.

Since this all seems quite easy, it begs the question - why isn't the SAM secured? Well it is - while Windows is running. By using a live USB, we're able to exploit the lack of security innate to Windows (files are unencrypted by default) and make these changes as we please.

Doing is only half the equation - we want you to understand what's going on, and to use these POCs as a means to that end.

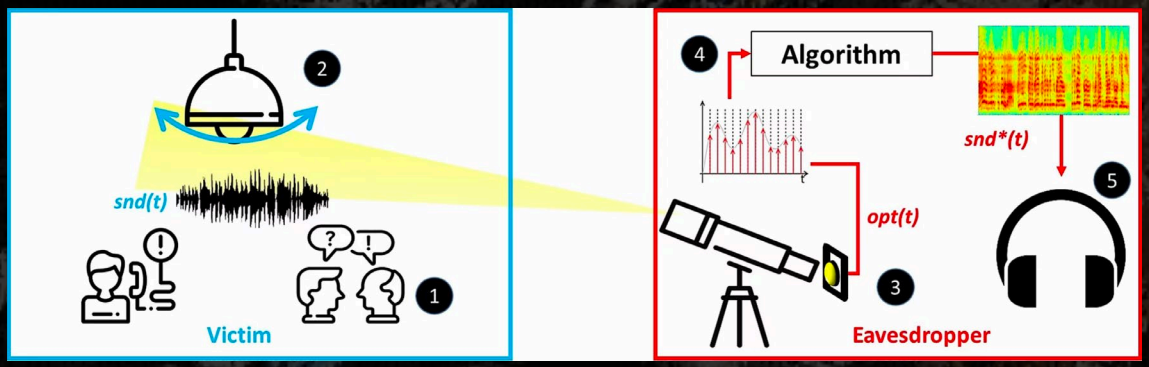
BOLO LIST

Continuing our new section from August, we will be bringing you monthly updates of things to "Be On the Lookout" for from the front lines of the security industry with a cyber focus - but keep in mind, security extends beyond easily defined boundaries. We want to keep you thinking - and looking - outside the box.

LAMPHONE

There are numerous side-channel attacks for eavesdropping, or compromising the confidentiality of digital information. They all, however, require some kind of interaction with the target, or cannot be applied in real time - until now.

Lamphone is a unique method developed by researchers in Israel for eavesdropping sound remotely and passively by using an electro-optical sensor (transducer) to analyze a hanging light bulb's frequency response to sound. Sound causes fluctuations in air pressure, which cause a hanging bulb to vibrate slightly. This can be accomplished at varying degrees of distance (25 meters, in the test they documented), and with complete isolation from the source of the sound: The micro-vibrations are picked up by the transducer, then analyzed by an algorithm which outputs them to sound.



The quality of sound they were able to derive allowed a song they picked up to be identified by the popular app Shazam, and the speech to be successfully identified by Google Cloud Speech API.

QUICK PROJECT

YUNO HOST

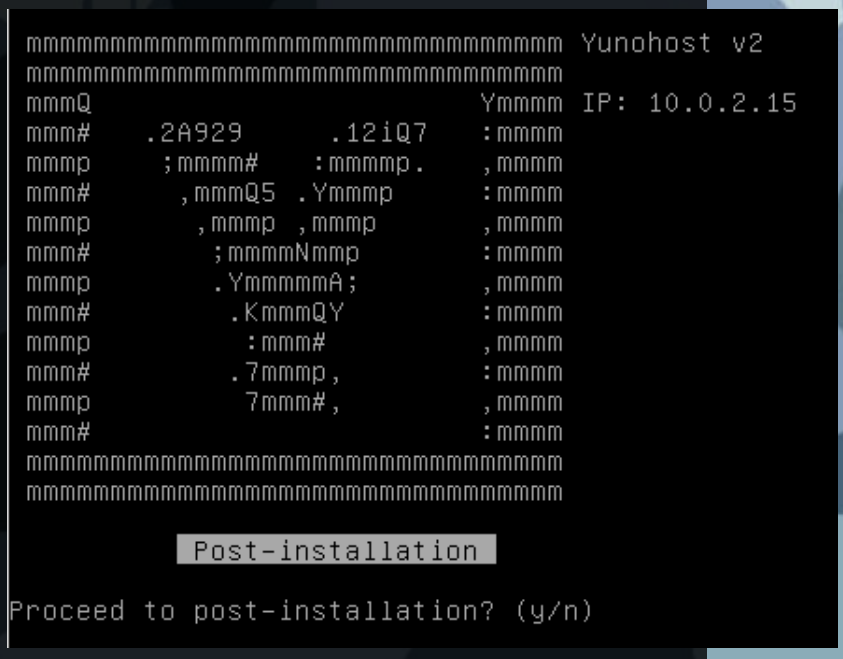
SET UP YOUR OWN CLOUD ON A RASPBERRY PI

So this is an easy process of setting up your very own server to host webpages, email and other types of tasks but by using only a Raspberry Pi to run everything.

1. Download the image for a Raspberry Pi and YUNO Host HERE

2. Flash the image you just downloaded onto your Raspberry Pi, if your using Windows use Etcher. Directions are included HERE

3. Power Up your Pi and make note of your IP



Now all you do is SSH into your new cloud device follow the steps HERE

That is it, you now have a server and you can start to install different apps from the web interface. What will you host on your new server. To access your cloud service from outside your network please make sure that port-forwarding is set up correctly by following the examples HERE.

CYBER SECURITY HISTORY

NMAP RELEASED — SEPTEMBER 1, 1997

Fyodor Vaskovich also known as Gordon Lyon released an open-source network scanner which is used to discover host and services on networks by sending packets and analyzing how the packets were responded to. NMAP can discover hosts on the network, identify which ports are open, using data to identify which version is available on the service, identify what type of OS is installed on the host and also uses Lua as a scripting interface for other utility methods.

Gregory J. Touhill, First Federal CISO — SEPTEMBER 8, 2016

The role of the CISO is to guide cybersecurity policy, planning, and implementation in the U.S. Federal Government. Greg was in this position to January 2017. This position falls under the Office of Management and Budget while reporting to the U.S. Chief Information Officer.

MIT granted US Patent for public key crypto — SEPTEMBER 20, 1983

U.S. Patent 4,405,829 which expired September 20, 2000 describes Public-key cryptography, or asymmetric cryptography which uses pairs of keys. These include the use of public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. Robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public key can combine the same message and the supposed digital signature associated with it to verify whether the signature was valid, i.e. made by the owner of the corresponding private key.

DEBRIEF ROOM

MATT DIETRICH

Time of Debrief: 10:53 Zulu 09 AUGUST 2020

Subject:
Matt Dietrich is a Cyber and Strategic Risk Consultant at Deloitte in Washington D.C. Before his time there, he completed a four year degree in Security and Risk Analysis with a cybersecurity and IT focus in just over two years at Penn State University. He is a four year veteran of the US Army's 75th Ranger Regiment, where he deployed twice to Afghanistan.

You can find out more about Matt on his LinkedIn page or on his Instagram under matt.dtrick

As mentioned on the third page of our interview, Splunk offers free training for veterans.

--- CLASSIFIED DEBRIEF FOLLOWS ---

DEBRIEF ROOM

I wanted to talk to you about your education. What specifically were some highs and lows of the program you went through, in terms of where it prepared you well for working at Deloitte and where it left you hanging?

M. Dietrich: I originally started out in the computer science program. I thought that was the way to go, but then I found out about cyber security and thought "roger that" and jumped straight into it. I talked to a professor who made a great point, he said "Computer science is just the tip of the iceberg, it's literally just half of it. You have computer-human interaction and all of those aspects. If you're not looking to be a programmer, you don't have to be." For me that was a big thing. So I asked myself 'How can I get into this field without having to overload myself?' So I went into the cyber program - it aligned with my passions way more. They prepared me great, going into cyber security policy, how we [as cyber security professionals] interact within an organization. What they didn't prepare me for was how to deal with clients, how to interact in and drive meetings. Luckily for me, some of that stuff came from my military background.

I think that's interesting. Any training program is inevitably going to have shortfalls. They can never completely prepare you for reality. It's interesting too how you mention you started out more with the technical side of things, then went with the soft side of cyber security covering more of the human and policy aspects.

M. Dietrich: Yeah absolutely. And I want everyone to know, you're never going to be 100% prepared for that job. But employers aren't necessarily looking for that, either. When I first sat down with Deloitte, they told me "We don't expect you to know everything. We expect you to come with an open mind. What matters most is are you motivated, are you a hard worker, are you teachable." These kind of soft skills are really important when it comes to landing a job.

DEBRIEF ROOM

That's a great point - It's okay to not be prepared. You'd already done a lot in your life and in your career, then you got out, got an education and started a second life after the military, and there were some things you still didn't know - and that was okay. So for anyone else that's transitioning from one phase of their life to another, it's okay to feel unprepared. There's always something you'll have to learn on the fly. Pay attention, apply yourself, outwork your peers every step of the way, and you'll be fine.

M. Dietrich: Yeah, and once you get there, it's okay to not like what you do. Find what does spark your passion and go a different direction. There's so many things you can do in this field, from working on government policy to any of the other areas in cyber security. There's technical and managerial, for example. You know, you have system administrators that don't necessarily understand the processes or even have security in mind. We need both, but we definitely need more of the technically minded people out there.

And to be honest right now in cyber security you need a little bit more of everybody. It's a career field that's hurting for so many people across all these varied expertise. There aren't a lot of fields that are as diverse, or that touch so many different things. Another thing that sets cyber security apart is the emphasis on certifications. Where you're at right now at Deloitte, where do certs fall in terms of priority and relevance?

M. Dietrich: So, actually, in cyber and information security they're the name of the game. They're way more valuable than your average master's degree. Deloitte actually paid for me to get my Security + cert, and there's more opportunities on the horizon for me here. If you go to apply for a job and already have a couple of certifications, that's awesome, but a lot of companies out there will readily invest in their employees.

DEBRIEF ROOM

M. Dietrich: Another thing regarding certifications, is look beyond the security minded stuff. There are things like Splunk for data aggregation and analysis that you can get smart on and increase your marketability, and also bring something to your team to make a positive difference. They even offer free training to veterans.

Do you have any advice for anybody new to the field, or about to take their first job?

M. Dietrich: Yeah - ask questions! It's okay not to know, and your first few weeks you'll probably feel really lost, but don't make it worse on yourself by pretending to know when you could just ask. Be a sponge and enjoy the ride!

And for anybody at the university who's a veteran or current service member, what do you think veterans and service members uniquely bring to the table?

M. Dietrich: The number one thing is attention to detail. It's a phrase that gets tossed around a lot, but it's so true. They pay attention to the little things that matter and it makes such a difference! The other thing is the leadership experience they carry with them. We all have a strong baseline in how to manage tasks, and we all share that mindset of "How can I get the job done?" The attention to detail and having that mentality is a winning combination.

The ONLY thing I could possibly add to that is for the service members past and present out there, share your experience. You have a background and a mentality and skills that are unique, and people will benefit from you sharing that with them.

DEBRIEF ROOM

M. Dietrich: I got one more for you - this is for the people who are around 18-22 years old - Do the stuff that no one else wants to! This is going to separate you from your peers so much. Build the Power Point decks, help your peers by taking meeting and class notes, anything they don't want to do, do it and find a way to add value to it. This mentality, if you foster it not as a college student, will put you miles ahead in the work place.

That's gold. There are a lot of opportunities out there for the people that are willing to work hard for them. There are even a lot of opportunities within the military and law enforcement world that I think a lot of people are unaware of.

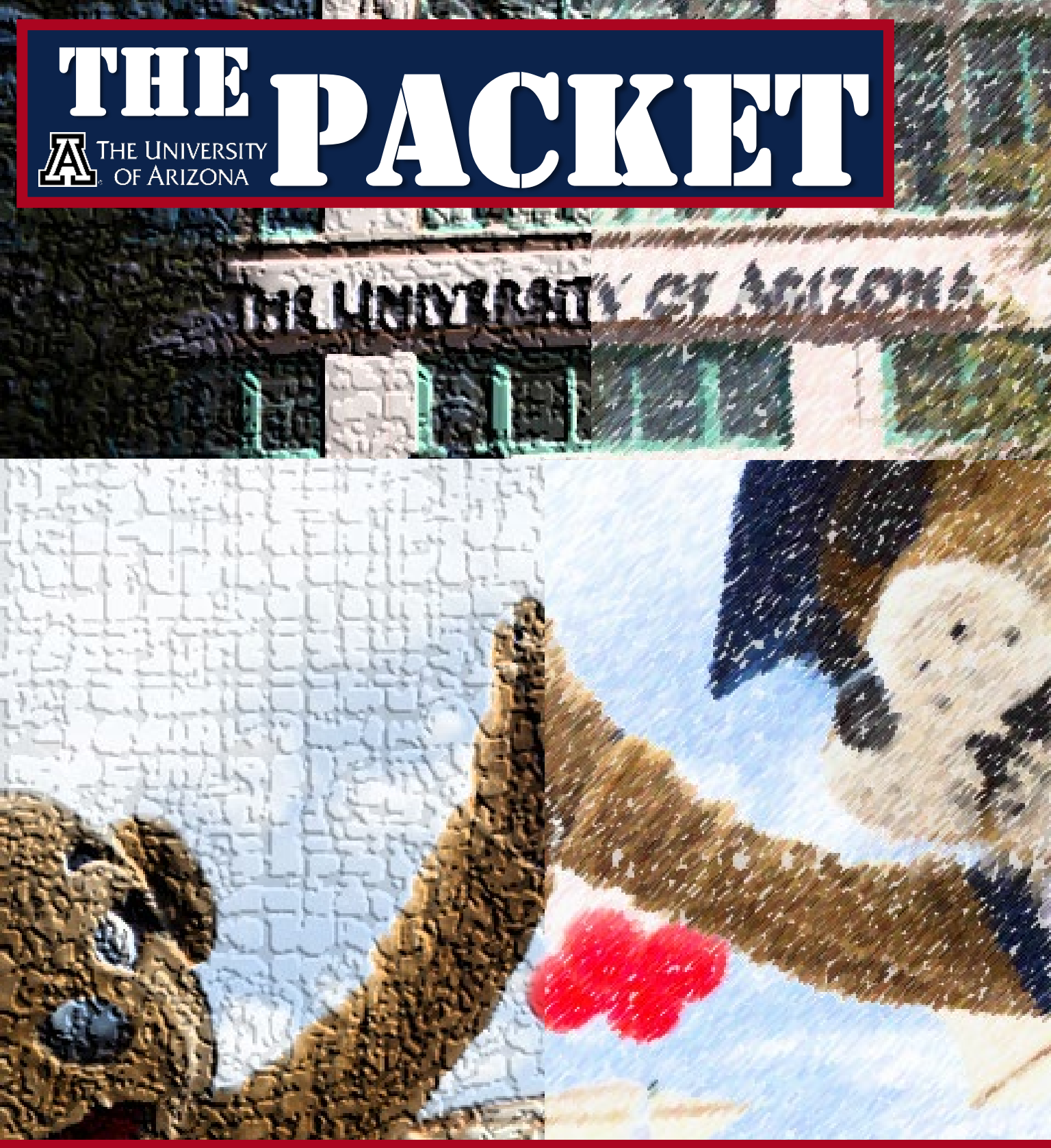
M. Dietrich: It's funny you mention that. Very recently the Ranger Regiment officially stood up its own Military Intelligence Battalion. A big portion of that is cyber and electronic warfare, signals intelligence and things like that. They get to jump out of planes and do all of the cool stuff, too.

The pointy end of the stick of cyber is a cool place to be. Penetration testing is nice, but you're inevitably constrained. Truly having a license to hack and being that well funded sounds like a dream. I've only had a little bit of interaction with those kinds of teams, but they make a huge difference on the battlefield. Man, thanks a lot for talking. We crossed paths because of our work connection and shared interest in cyber, and every time I talk to you it's a good time. Stay safe!

M. Dietrich: It's been a pleasure. See ya!

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