h4ck1ng 101

a primer to learn hacking and security concepts

r007c0n# disclaimer

hacking is a crime punishable by philippine laws

(cybercrime prevention act of 2012 or RA 10175)

the contents of this course involving security technologies and security software are readily available publicly on the internet. this course is for educational purposes only and conducted on controlled virtual environments. it is aimed to help you improve your company's security posture, but under no circumstances are you allowed to violate any anti- hacking laws with this knowledge. this author and the sponsor of this training will not be held liable if you go to prison for being an idiot.

Punishable by RA 10175

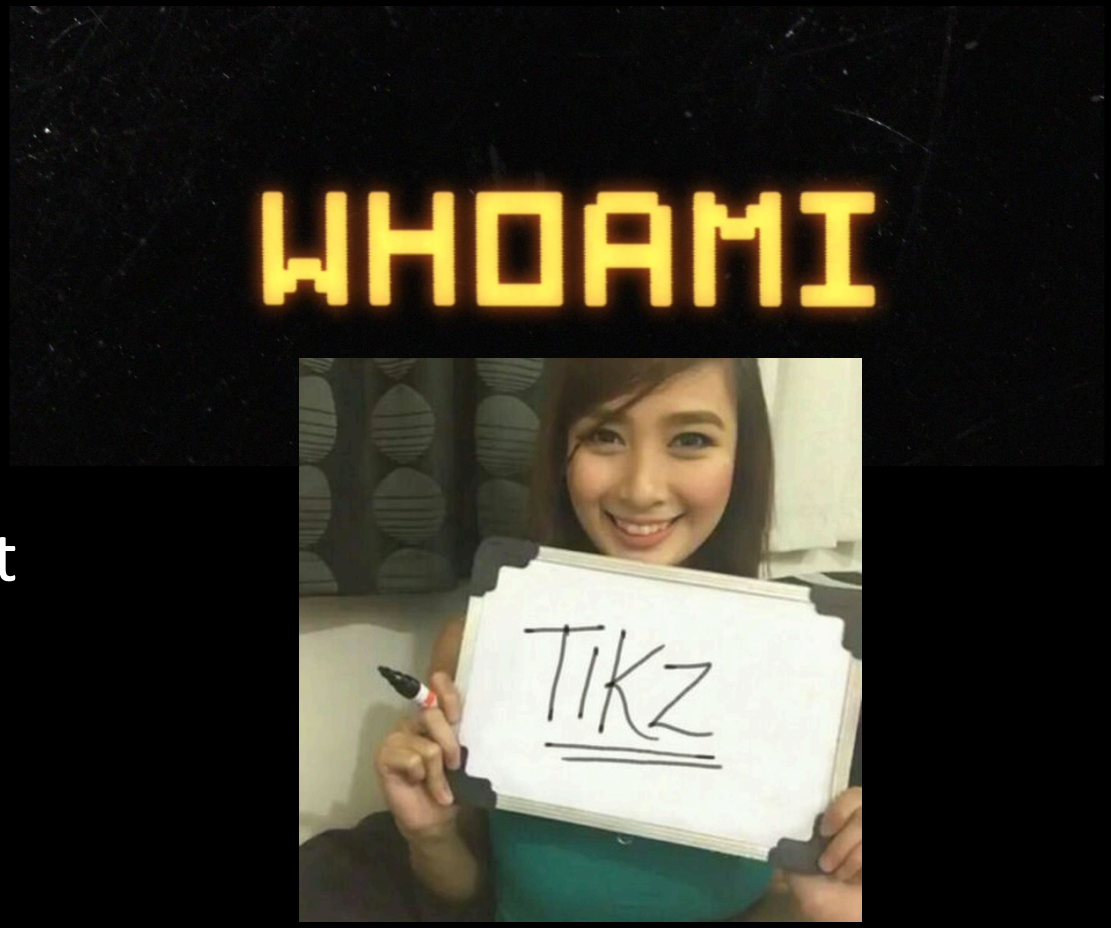
- Illegal access - Unauthorized access (without right) to a computer system or application.
- Illegal interception - Unauthorized interception of any non-public transmission of computer data to, from, or within a computer system.
- Data Interference - Unauthorized alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, and including the introduction or transmission of viruses.
- System Interference - Unauthorized hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data messages, and including the introduction or transmission of viruses.
- Misuse of devices - The unauthorized use, possession, production, sale, procurement, importation, distribution, or otherwise making available, of devices, computer program designed or adapted for the purpose of committing any of the offenses stated in Republic Act 10175.
- Cyber-squatting - Acquisition of domain name over the Internet in bad faith to profit, mislead, destroy reputation, and deprive others from the registering the same.
- Computer-related Forgery - Unauthorized input, alteration, or deletion of computer data resulting to inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.
- Computer-related Fraud - Unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent.
- Computer-related Identity Theft - Unauthorized acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical.
- Aiding or Abetting in the commission of cybercrime – Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.
- Attempt in the commission of cybercrime Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

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

on with the show

tikbalang

- rootcon GOON
- security professional
- into infrastructure management
- into information security management
  - vulnerability assessment
  - penetration testing



your turn

name, background, motto, expectations.

what's in the bag?

* get your feet wet in the hacking culture
* develop the hacker mindset (*without getting into trouble*)
* things you should know to start
* information security
* information security essentials
* practical tips
* hackers arsenal
* some demo

hacking culture

[News] [Paper Feed] [Issues] [Authors] [Archives] [Contact]

.:: Hacker's Manifesto ::.

Issues: [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69]

Current issue : #7 | Release date : 1986-09-25 | Editor : Taran King	Get tar.gz
Intro/Index	Taran King
Phrack Pro-Phile of Scan Man	Taran King
Hacker's Manifesto	The Mentor
Hacking Chilton's Credimatic	Ryche
Hacking RSTS Part 1	The Seker
How to Make TNT	The Radical Rocker
Trojan Horses in Unix	Shooting Shark
Phrack World News VI Part 1	Knight Lightning
Phrack World News VI Part 2	Knight Lightning
Phrack World News VI Part 3	Knight Lightning

Title : Hacker's Manifesto

Author : The Mentor

==Phrack Inc.==

Volume One, Issue 7, Phile 3 of 10

The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

Written on January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my world...
Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...
Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...
Or feels threatened by me...
Or thinks I'm a smart ass...
Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

--===** ArViX **==--

Without Malice, Without Fear

Wednesday, December 21, 2005

Third to the Last Post

What defines me is what hurts me...

This is a true story; One day I was thinking to myself "These fools I work with doesn't have a clue on what I can really do, what networks I've gotten into, stuff that I'd done online. They don't know how good a hacker I've become. They just sit there waiting for their monthly salary, only imagining where they'll go drinking next. They don't understand that there's a world outside their own lives." Then it hit me. I too was living in my own little world. A world of networks, computers and technology. So again I decided I will try to explore beyond the box that this time I had inadvertently put myself into.

I've decided to stop hacking when the new year comes around. **This time it's real**.

Posted by rebarz99 at 12/21/2005 11:25:00 PM 8 comments:

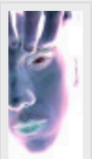
Sunday, July 24, 2005

As time passes by...

Haven't been caught. Not yet anyway... :)

I think it's fitting that I post the following article here. A bit cheesy to the veteran hackers but definitely a must read to someone who visits here with no hacking experience but curious about hacking.

About Me



rebarz99

View my complete profile

Links

- My Whatever
- Zone-h Me
- My email

Blog Archive

December (1)
July (2)
May (1)
April (12)
March (23)
February (15)

Info Security News

- Newly Fired CEO Of Norse Fires Back At Critics

definition

Hacking

is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose.

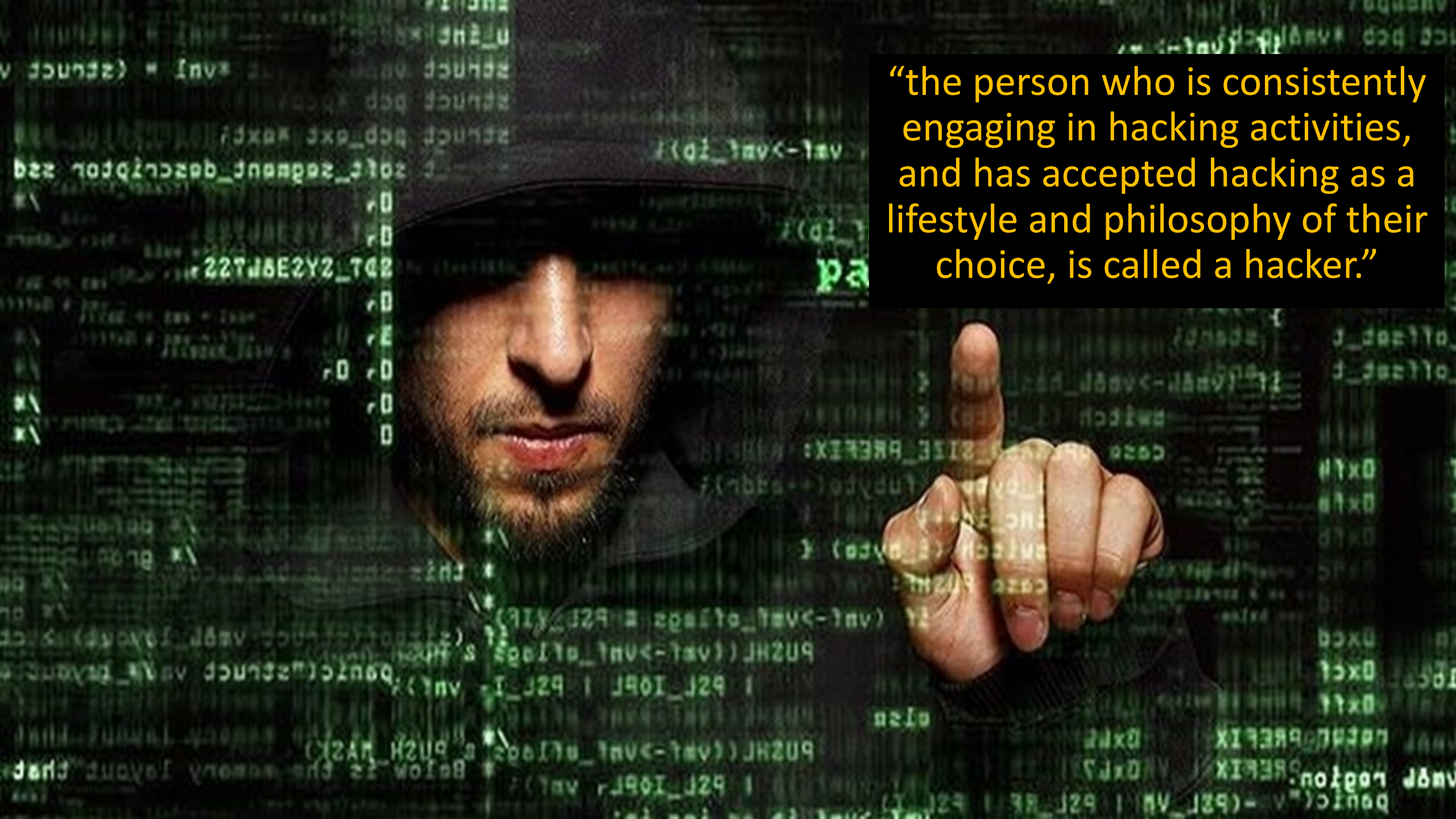
Load required : P171

Procedures:
Text GOTSCOMBOGAF136 to 8080 (P136)
Text GOCOMBOIKEA35 to 8080 (P35)
Redo step 2 for additional 1GB
Redo step 1 to extend validity (prior expiry)

Text GOSAKTO STATUS to 8080 to check status

Valid for 30days

THERE IS NO PATCH FOR HUMAN STUPIDITY.

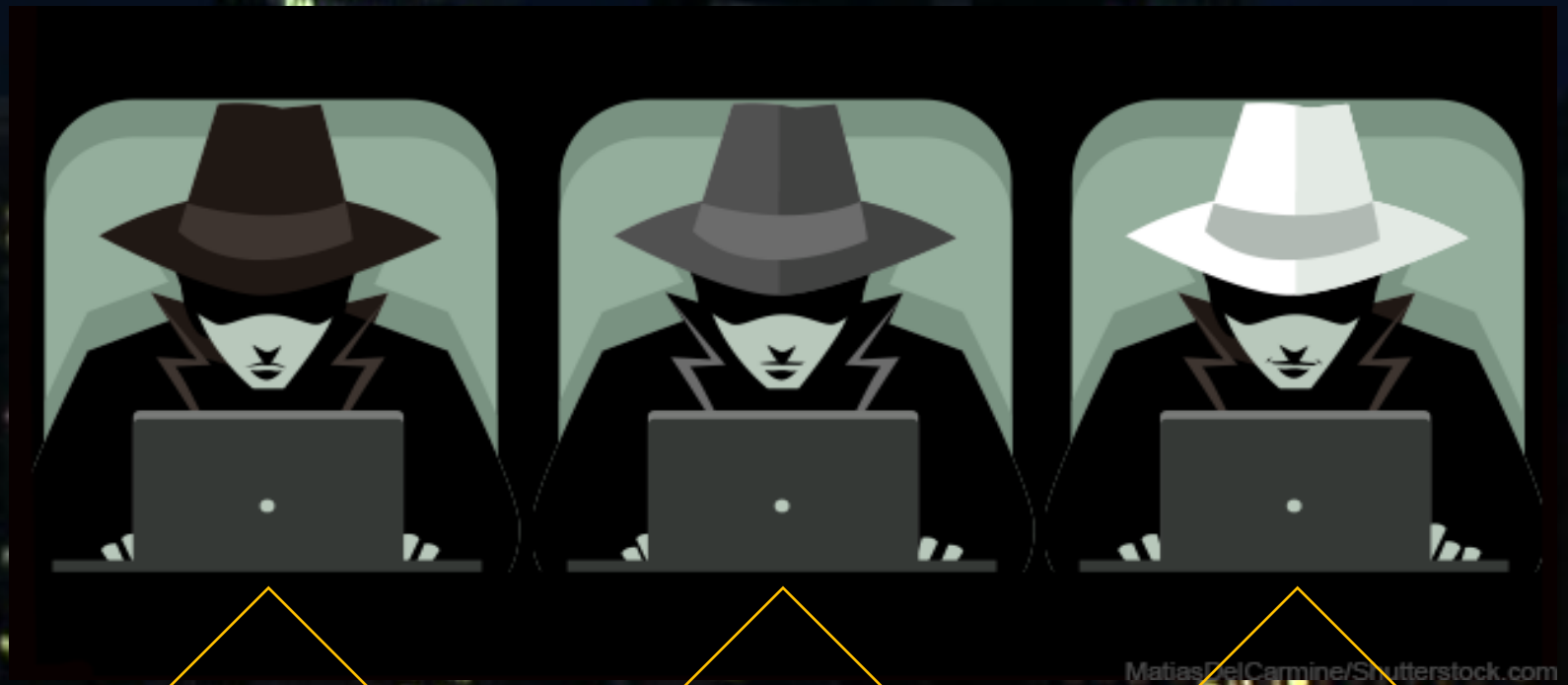

“the person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a hacker.”

quiz: who’s the hacker?

Kristina Svechinskaya is a former Russian money mule hacker

Dubbed "the world's sexiest computer hacker"

hacker mindset



Black-hat hackers violate computer security for personal gain (such as stealing credit card numbers or harvesting personal data for sale to identity thieves) or for pure maliciousness (such as creating a botnet and using that botnet to perform DDOS attacks against websites they don't like.)

A gray-hat hacker falls somewhere between a black hat and a white hat. A gray hat doesn't break into computer security systems to gain personal gain or to cause carnage, but they may illegally compromise other computers and do arguably unethical things.

They're ethical hackers, experts in compromising computer security systems to use their abilities for good, rather than bad, unethical, and criminal purposes.

Arrest shines light on shadowy community of good, bad hackers

By AFP
PUBLISHED: 17:08 BST, 4 August 2017 | **UPDATED:** 20:53 B

Share

The arrest of a security researcher by the FBI after the De delivered a shock to the computer security community

Two months ago, Marcus Hutchins was an "accidental hero," a young computer whiz living with his parents in Britain who found the "kill switch" to the devastating WannaCry ransomware.

Today, the 23-year-old is in a US federal prison, charged with creating and distributing malicious software designed to attack the banking system.

His arrest this week stunned the computer security community and shines a light on the shadowy world of those who sometimes straddle the line between legal and illegal activities.

Hackers are generally classified as "white hats" if they stay within the law and "black hats" if they cross the line.

"But there are people who do security research... who understand that sometimes in order to improve security, you have to stick your nose in areas that may break the law. They don't want to hurt anyone but they are doing it for research."

SOURCE: hxxp://www.dailymail.co.uk/wires/afp/article-4761628/Arrest-shines-light-shadowy-community-good-bad-hackers.html

http://fouroclockproject.iwarp

fouroclockproject.iwarp.com/mirror/inq7.html

Search

'Wake-up call'

"So my fellow haxor keech of FDN [Filipino developers network] organized a Project called 4'Oclock, where we will be defacing all ph sites, to give this administrators a wake up call.

"Well I can't explain much right now, but if you read all the messages on the selected defacements, it might give you an idea on what we are fighting for," dcoder added.

In the mirror of the defaced Brainshare Online website, Asian Pride explained:

"The 4 o Clock project is a system composed of Filipino freelance security enthusiasts that aims to disseminate the importance of Information security here in the Philippines. This team has conducted a survey, scanning random (website) hosts and informing the people (Internet service provider administrators) about (problems). (We then) encourage them to fix their servers. We have no intention, however, of destroying, and/or hijacking information, ... We are not paid to do this."

Liao somewhat agreed. He observed that while the hackers were able to "penetrate" MosCom's servers, they did not delete or destroy any files.

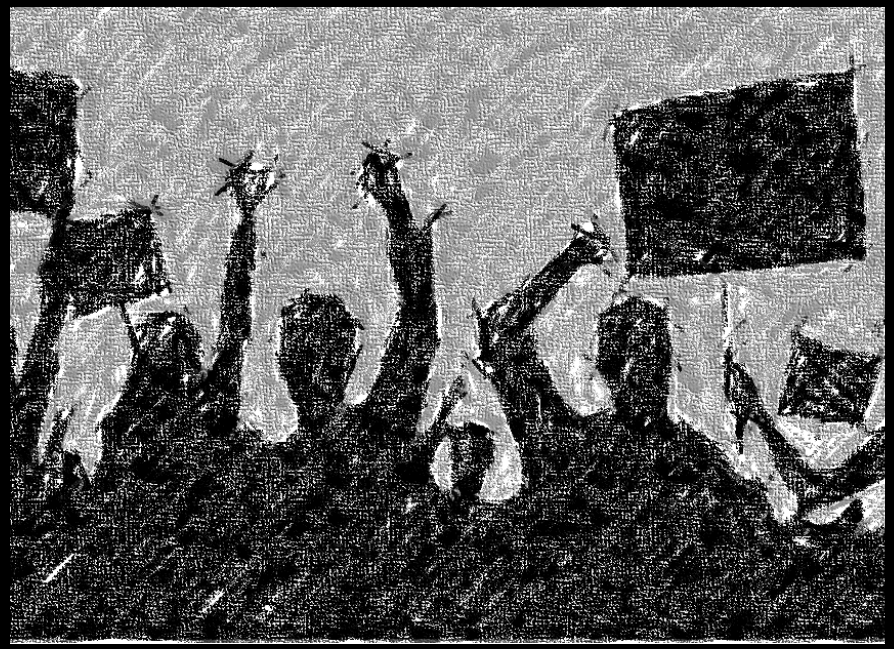
The hackers uploaded programs (executable files) that will only run when a website administrator begins uploading the new main page (index) into the server. The program blocks anyone from uploading into the server, but prompts the user to download a new file, which includes a message explaining the purpose of the defacement.

Liao, however, said that the hackers also offered the option not to accept the new file. "It sort of gives you permission to delete the files," he added.

Asian Pride claimed that "more than 90 percent of (MosCom's) servers can be exploited through common vulnerabilities, therefore jeopardizing the security of their clients as well as their office."

The group said that they have warned administrators of MosCom of vulnerabilities, "but were just subjected to insult, despite their professional approach."

"They scorned us with their witty remarks, bragging about their degrees, and that we knew less. So what did they accomplish? Absolutely nothing productive," the group added.



Hacktivist

hacking for fun or profit

for fun

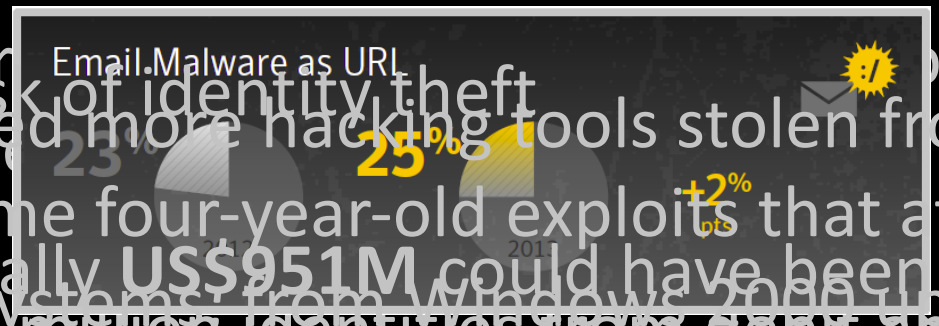
[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

26-Year-Old Hacker Sentenced to Record 334 Years in Prison

Monday, January 11, 2016 Wang Wei

A 26-year-old hacker has been sentenced to 334 years in prison for identity theft as well as mass bank fraud in Turkey, or in simple words, he has been sentenced to **life in prison**.



REPUBLIC ACT NO. 10175

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

for profit

"It's Impossible." said Pride.
"It's Risky." said Experience.
"It's Pointless." said Reason.

If you really are Hacker !
then Give it a Try!

./ PCbots Lab's

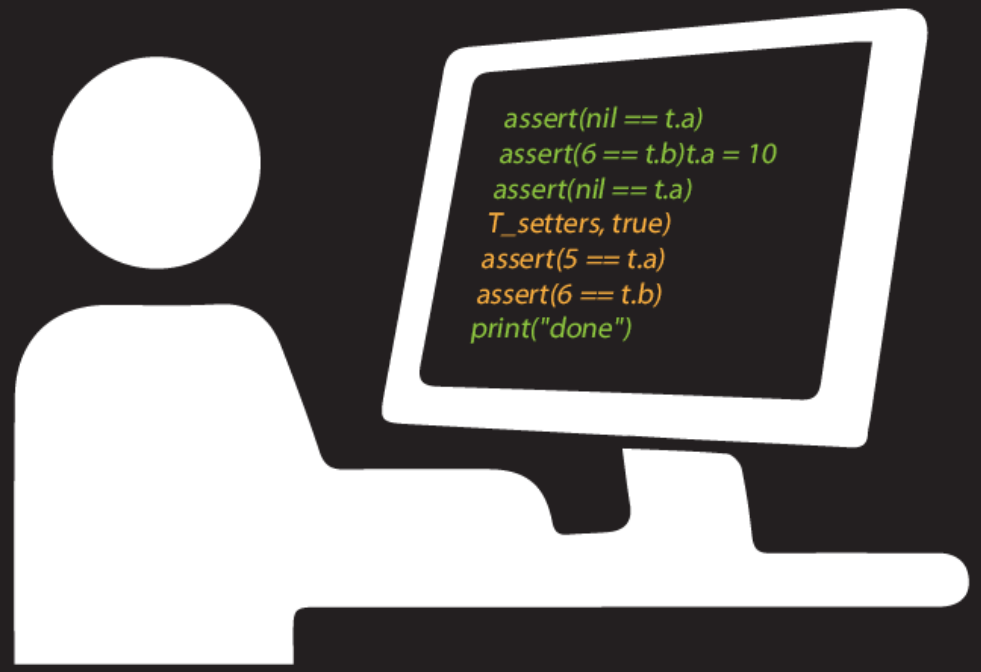
~~CAN~~ YOU MAKE A CAREER OUT OF BEING AN ETHICAL HACKER?


PINOY STOP COMICS
2016 © www.pinoystop.org
THIEF, OH!
$
RB '16

Penetration Testing

VS.

Vulnerability Scanning



what it takes

Layer		
Application (7)	Servic end u	
Presentation (6)	Forma can be Encryp	
Session (5)	Establ betwe	
Transport (4)	Respo protoc	
Network (3)	Reads the pa	
Data Link (2)	Reads the da	
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

ng Cracker is an
ucator from
0-5000 yuan per
ss for helping
other people crack
software.

what it takes

what it takes

nmap – network mapper

- free open source
- use
  - network security audit
  - network discovery
  - host discovery
    - Port scanning
    - Version detection
    - OS detection
    - Device type
    - MAC address

https://nmap.org/

nmap – network mapper

- demo
- scanning
  - single target
  - multiple targets
  - random targets
  - excluding targets
- options
  - aggressive

https://nmap.org/

nmap – network mapper

- demo (cont.)
- more discovery options
  - don’t ping/simple ping
  - SYN/ACK
  - alternative options
- some advance options
  - xmas scan
  - scanflags

https://nmap.org/

nmap – network mapper

- demo (cont.)
- port scan
  - os detection
  - service detection
  - timing option
  - fw evasion
- output to file

https://nmap.org/

nmap – network mapper

- demo (cont.)
- troubleshooting scan
- GUI interface

https://nmap.org/


ROOTCON