ch4p73r 1

1n7r0duc710n 70 h4ck1n6 4nd pr3v3n710n

m0hd 24k1

Which one is secure ?

A

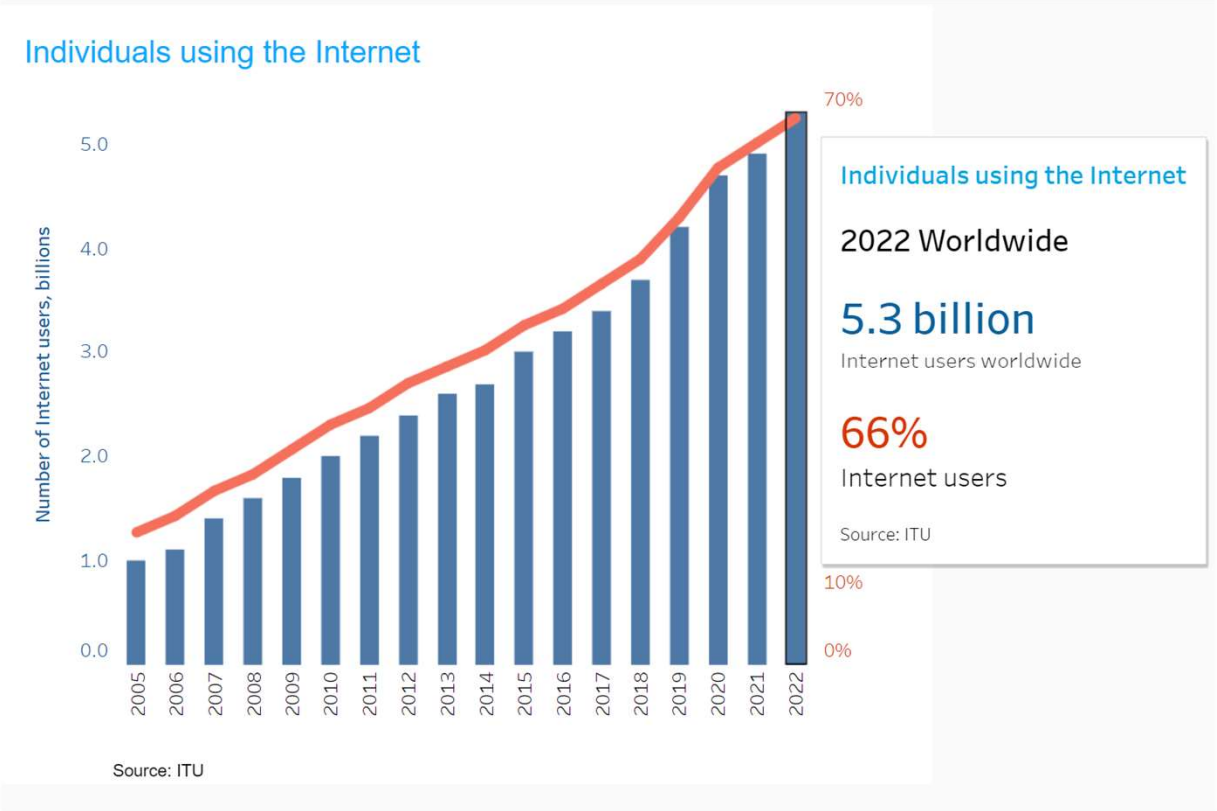
B

https://tinyurl.com/whichonesecure


THERE ARE NO SECURITY,
THERE ARE ONLY OPPURTUNITY

Cybersecurity, Why ?

- **International Telecommunication Union** (ITU) estimates that approximately **5.3 billion people** – or 66 per cent of the world's population – are using the Internet in 2022
- The Internet has been used as a source of personal fulfilment, professional development and value creation.
- Throughout the COVID-19 pandemic, Internet Connection is vital for working, learning, accessing basic services and keeping in touch.

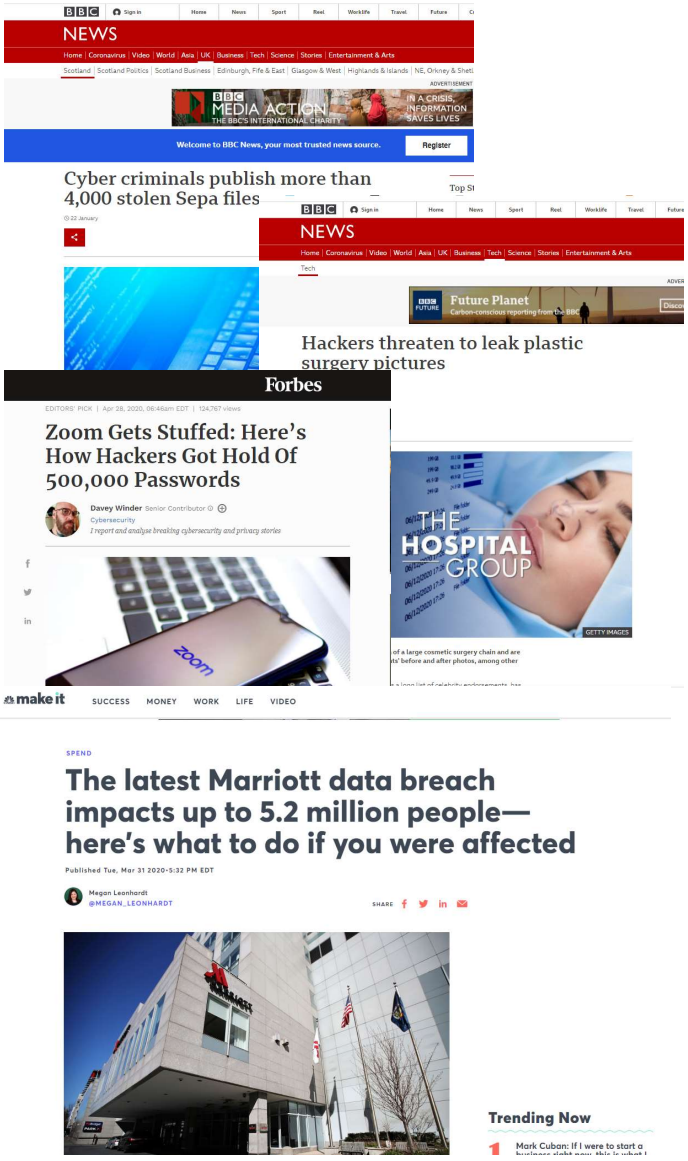


What is Security

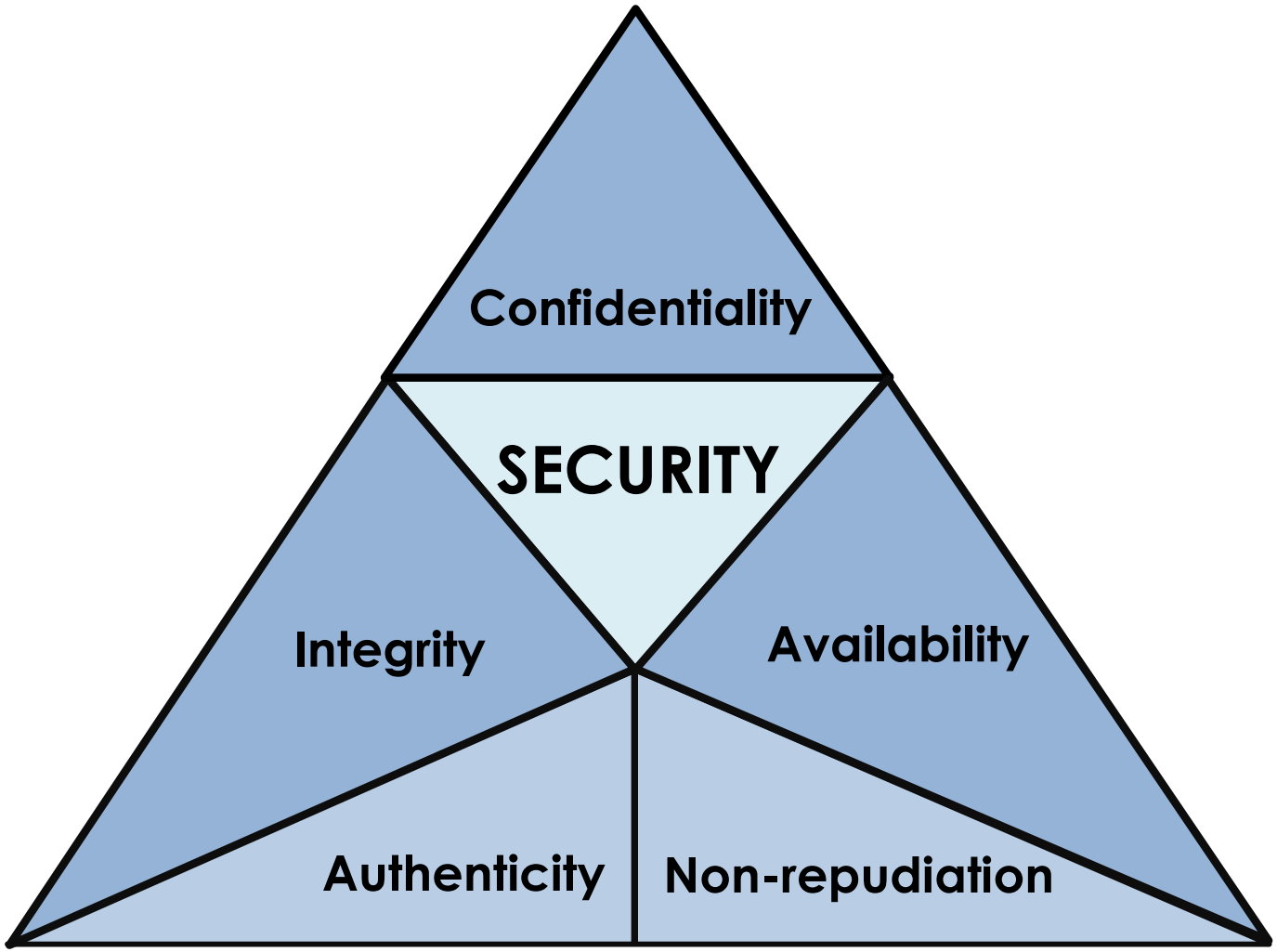
- Dictionary.com says:
  - 1. Freedom from risk or danger; safety.
  - 2. Freedom from doubt, anxiety, or fear; confidence.
  - 3. Something that gives or assures safety, as:
    - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
    - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.
- Etc…

Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: AFS
- Guarantee availability of resources
  - Ex: 5 9's (99.999% reliability)



ELEMENT OF INFO. SEC.



Element of Info Sec

Confidentiality	Assurance that the information is accessible only to those authorized to have access
Integrity	The trustworthiness of data or resources in terms of preventing improper or unauthorized changes
Availibility	Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine
Non-Repudiation	A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Topic

- Describe the role of an ethical hacker
- List the type of hackers
- The Attacker processes
- Types of attack
- Describe what you can do legally as an ethical hacker
- Describe what you cannot do as an ethical hacker

INTRODUCTION TO ETHICAL HACKING

WHAT IS ETHICAL HACKING

HACKER

What my friends think I do

What my Mom thinks I do

What society thinks I do

What the government thinks I do

What I think I do

```
hello:~# nmap -A -T4 scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2004-03-26 12:51 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp open  smtp    Sendmail 8.12.8
53/tcp open  domain  ISC Bind 9.2.1
80/tcp open  http    Apache httpd 2.0.49 ((Unix) mod_gzip/1.3.19.1a PHP/4.3.4 mod_ssl/2.0.49 OpenSSL/0.9.7a)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.21 - 2.4.24 (X86), Linux 2.4.18 - 2.4.20 (X86)
Uptime 188.655 days (since Thu Sep 11 23:10:57 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 37.388 seconds
hello:~#
```

What I actually do

What Is Hacker ?

- individual who uses computer, networking or other skills to overcome a technical problem.
- The term hacker may refer to anyone with technical skills.
- often refers to a person who uses own abilities to gain unauthorized access to systems or networks in order to commit crimes.
- A hacker may, for example, steal information to hurt people via identity theft, damage or bring down systems and, often, hold those systems hostage to collect ransom.

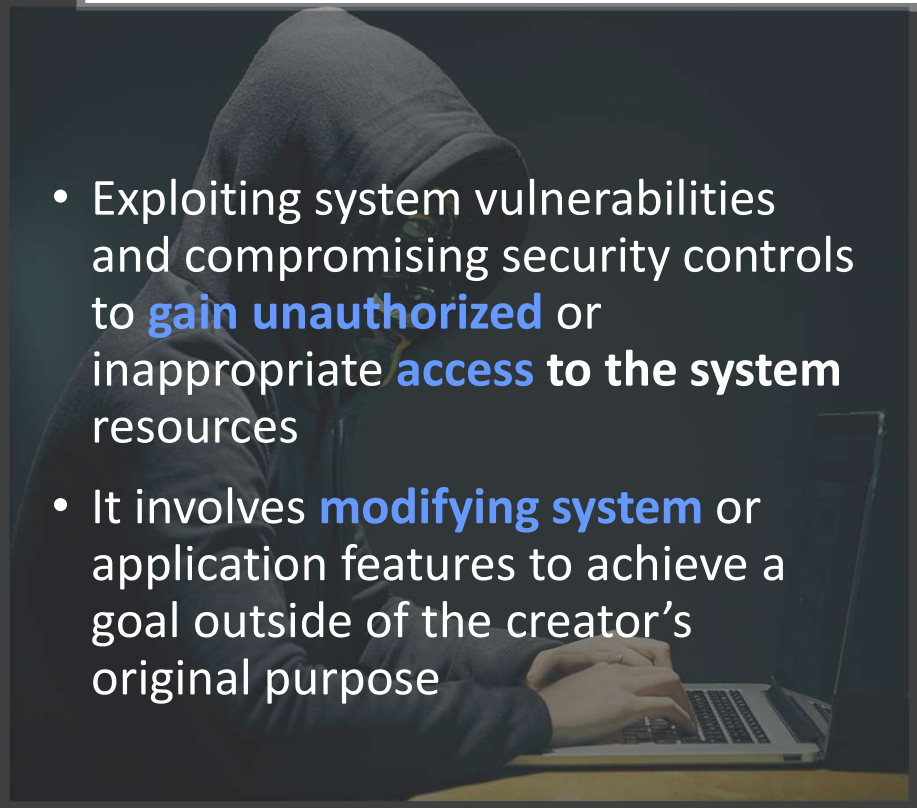
A Hacker is

- a computer expert who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means

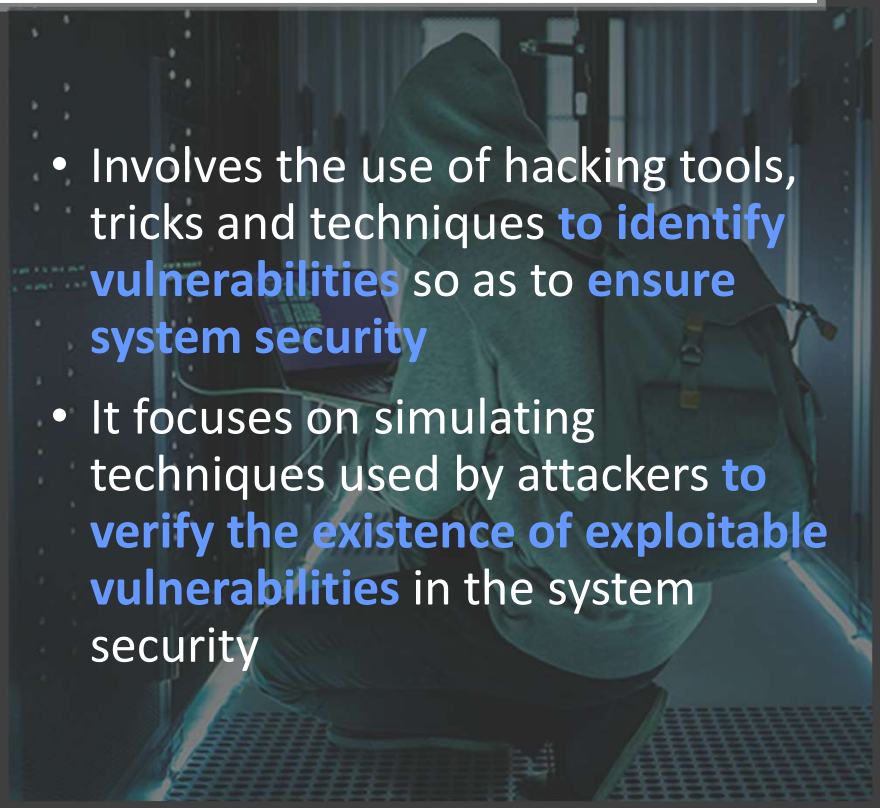
Introduction to Ethical Hacking

- Ethical hackers
  - Employed by companies to perform penetration tests
- Penetration test
  - Legal attempt to break into a company's network to find its weakest link
  - Tester only reports findings, does not solve problems
- Security test
  - More than an attempt to break in; also includes analyzing company's security policy and procedures
  - Tester offers solutions to secure or protect the network

Hacker VS Ethical Hacker



- Exploiting system vulnerabilities and compromising security controls to **gain unauthorized** or inappropriate **access** **to the system** resources
- It involves **modifying system** or application features to achieve a goal outside of the creator's original purpose



- Involves the use of hacking tools, tricks and techniques **to identify vulnerabilities** so as to **ensure system security**
- It focuses on simulating techniques used by attackers **to verify the existence of exploitable vulnerabilities** in the system security

BlackHat
hacker who violates computer security for their personal profit or malice

WhiteHat
ethical computer hacker, or a computer security expert

GrayHat
in the middle between "good" and "bad."

Spy Hacker
Employed by Organization to steal info.

The Type of HACKERS

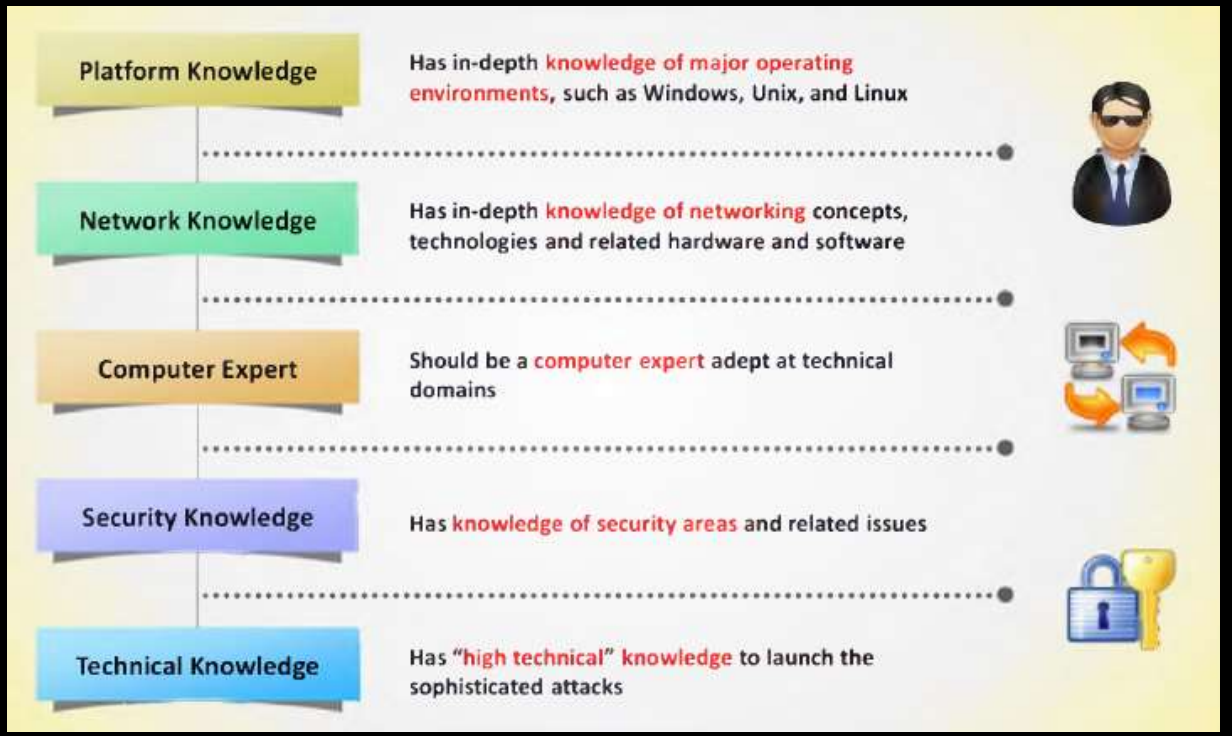
You might come across online

Script Kiddies
Young inexperienced hackers, just used tools

Suicidal Hackers
ready and willing to perform an attack for a "cause"

Cyber Terrorist
hacker who violates computer security for their personal profit or malice

Skill Required For Ethical hacking



How the hackers think ?

Motives , Goals , and Objectives

Goals

- Attackers have motives or goals such as disrupting business continuity , information theft, data manipu lations , or taking revenge

Motives

- A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system

Objectives

- Attackers try various tools , attack methods , and techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

Attacks = Motive (Goal) + Method + Vulnerability

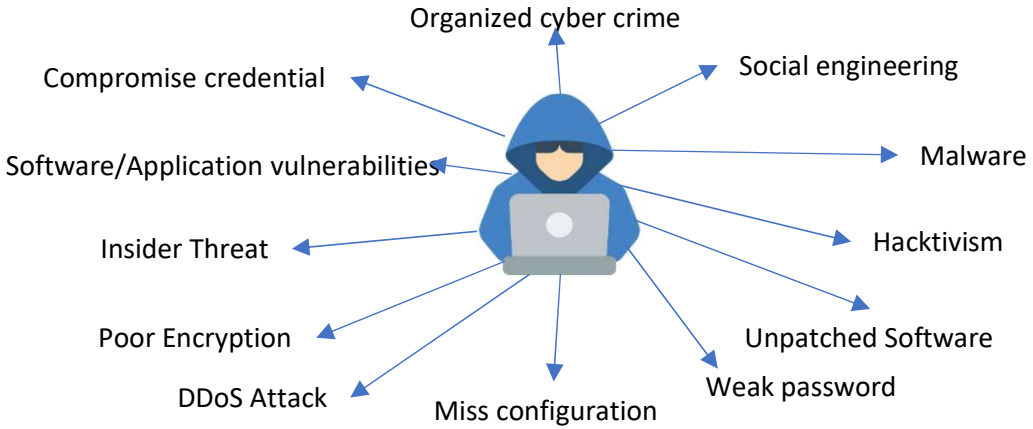
Motives behind information security attacks

- Disrupting business continuity
- Stealing information and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Causing financial loss to the target
- Propagating religious or political beliefs
- Achieving a state’s military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom

ATTACK METHODOLOGY

Information Security Attack Vector

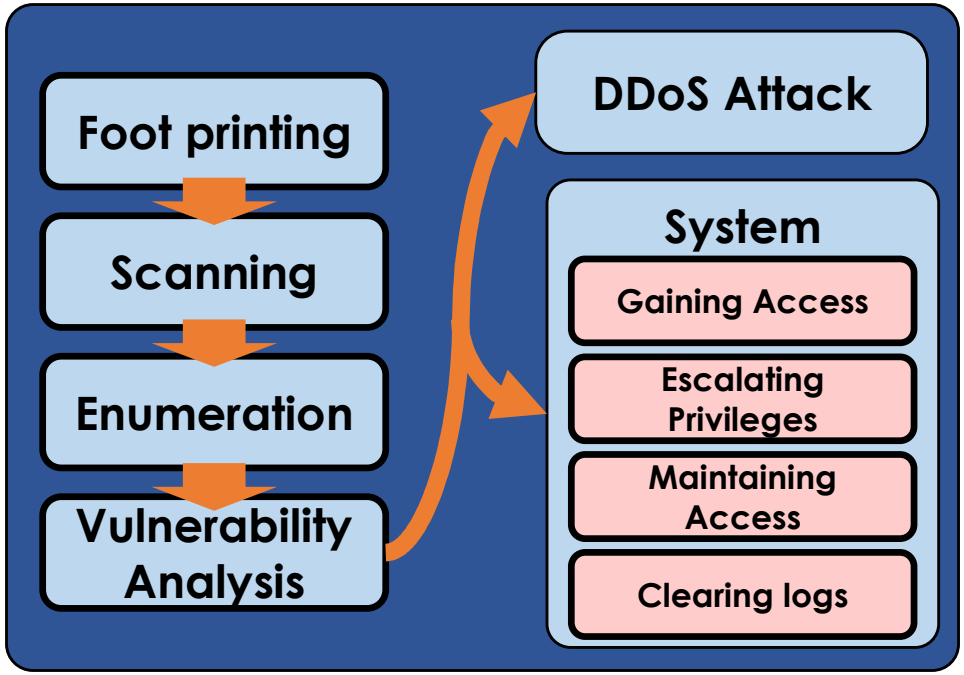
- The method or way by an adversary can breach or infiltrate an entire network/system. Attack vectors (or threat vectors) enable hackers to exploit system vulnerabilities, including the human element.



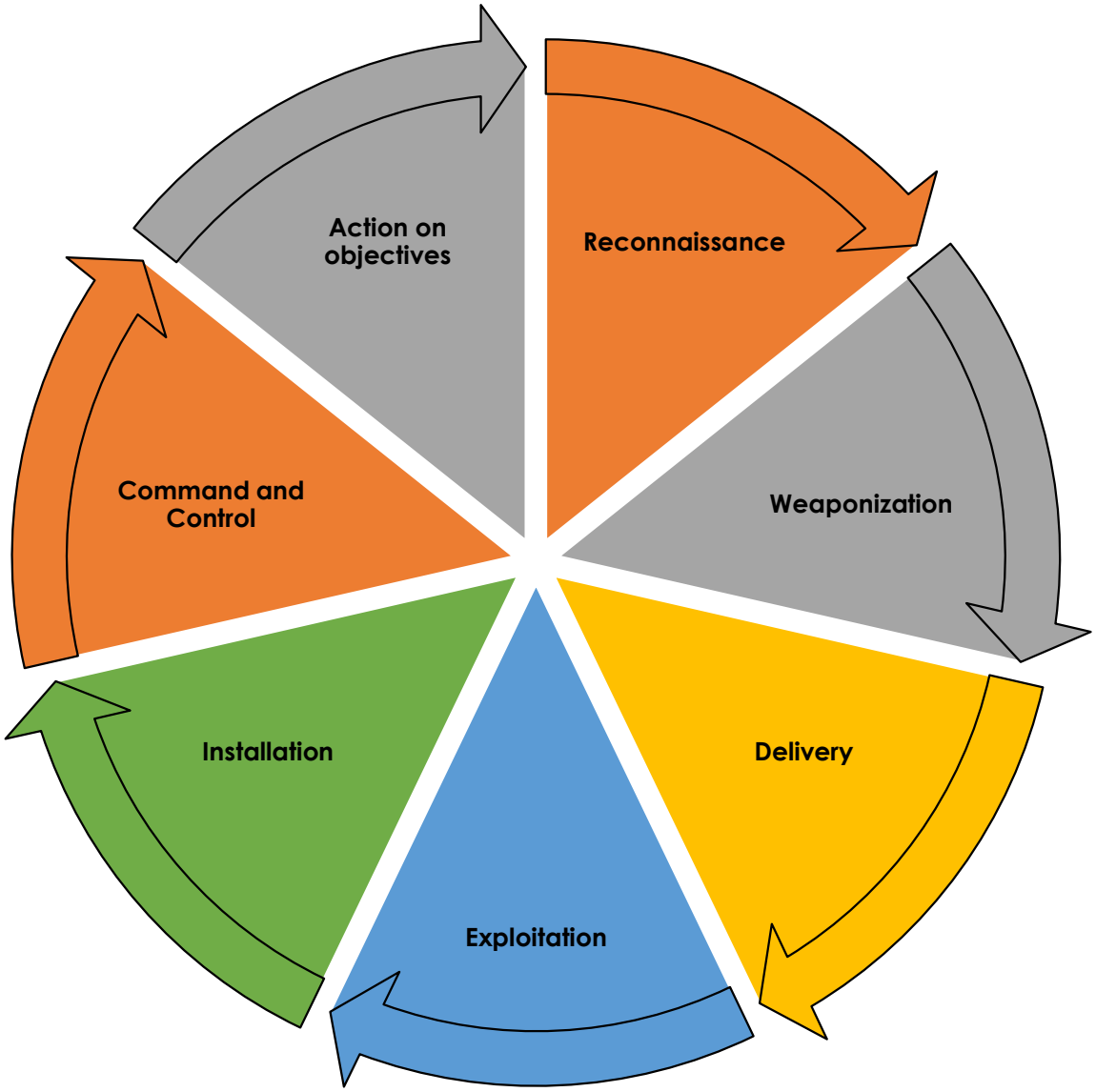
Classification of Attack

Passive Attack	• Passive attacks do not tamper with the data and involve intercepting and monitoring network traffic and data flow on the target network • Examples include sniffing and eavesdropping
Active Attacks	• Active attacks tamper with the data in transit or disrupt the communication or services between the systems to bypass or break into secured systems • Examples include DoS, Man in the Middle, session hijacking, and SQL injection
Close-in Attacks	• Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or disrupt access to information • Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attack	• Insider attacks involve using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems • Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attack	• Distribution attacks occur when attackers tamper with hardware or software prior to installation • Attackers tamper with the hardware or software at its source or in trans

Hacking Methodology



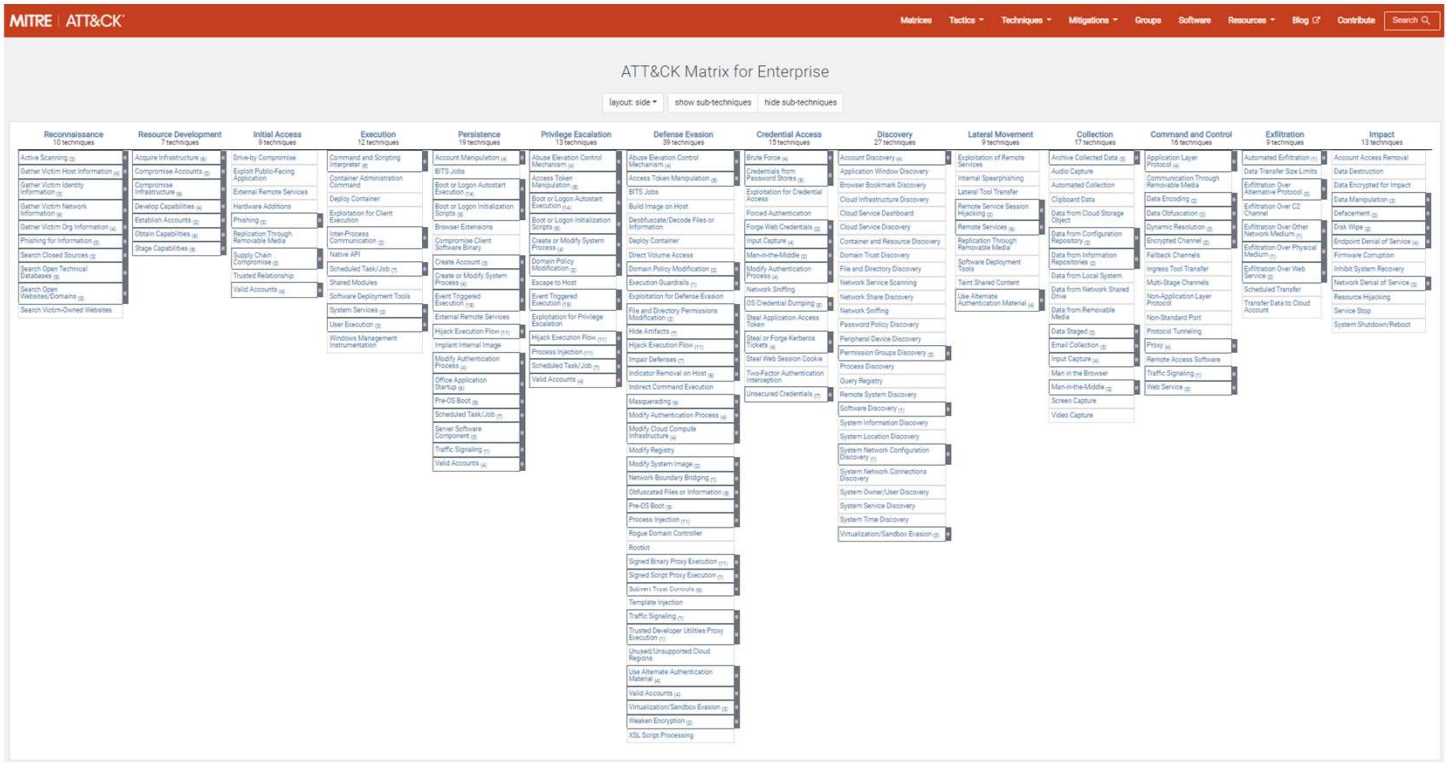
Cyber Kill Chain Methodology



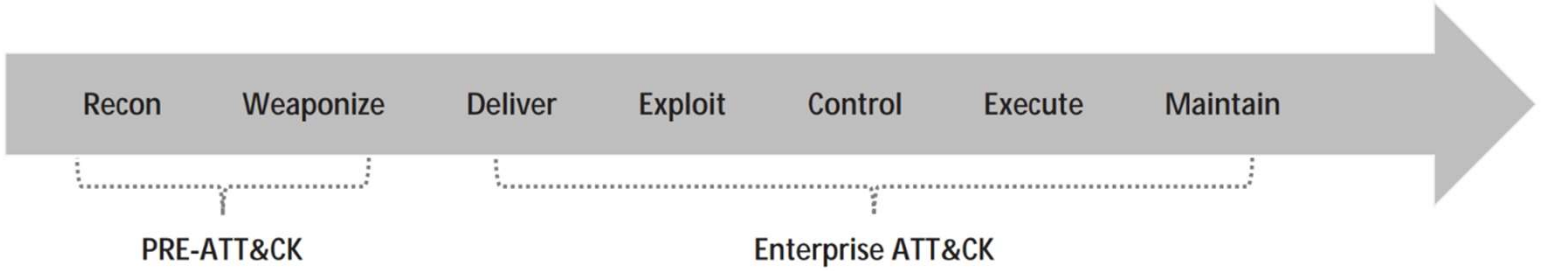
- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities
- It provides greater insight into attack phases, which helps security professionals to understand the adversary's tactics, techniques, and procedures beforehand

MITRE ATT & CK

https://attack.mitre.org/



Adversarial Tactics, Techniques, and Common Knowledge, is a knowledge base of adversary tactics and techniques. These techniques are indexed and break down into detail the exact steps and methods that hackers use, making it easy for teams to understand the actions that may be used against a particular platform.




Cybersecurity Case

MALAYSIA

Digital Ministry says looking in latest 'Padu' hack by R00TK1T

Digital Minister Gobind Singh Deo says his ministry wants to look at the issue in depth before making a announcement. — Picture by Sayuti Zainudin

Join us on our WhatsApp Channel, follow us on Instagram, and receive browser aler latest news you need to know.

By R. Loheswar
Tuesday, 20 Feb 2024 1:47 PM MYT

CYBERJAYA Feb 20 — The Digital Ministry said today it will make a statement soon on this latest cyber attack on a Malaysian company.

Its minister Gobind Singh said they wanted to look at the issue in depth before making any

The Star Maxis says its system is unaffected after R00tk1t hacker group threatens to expose 'treasure trove of customer

Maxis says its system is unaffected after R00tk1t hacker group threatens to expose 'treasure trove of customer data'

By CHRISTOPHER FAM

CYBERSECURITY

Monday, 05 Feb 2024
2:15 PM MYT

Related News

PHILIPPINES 12 Mar 2024
Microsoft to train Philippine women in AI, cybersecurity

TECHNOLOGY 14 Mar 2024
Microsoft expands availability of its AI-powered cybersecurity...

TECHNOLOGY 12 Mar 2024
Italy's Leonardo to boost cybersecurity, space and AI in 5-year plan

Maxis discovered a suspected incident of unauthorised access to a system belonging to one of its third-party vendors. — Maxis

PETALING JAYA: Maxis released a statement saying that it did not find any issues with its systems after the notorious hacker group R00tk1t claimed to have breached its infrastructure and threatened to expose a "treasure trove of customer data".

However, it discovered a suspected incident of unauthorised access to a system belonging to one of its third-party vendors.

"Earlier today, Maxis received a report alleging a cybersecurity breach. We immediately launched an investigation to determine the validity.

"While we did not identify anything related to our own systems, we identified a suspected incident involving unauthorised access to one of our third-party vendor systems that resides outside of Maxis' internal network environment," it said.

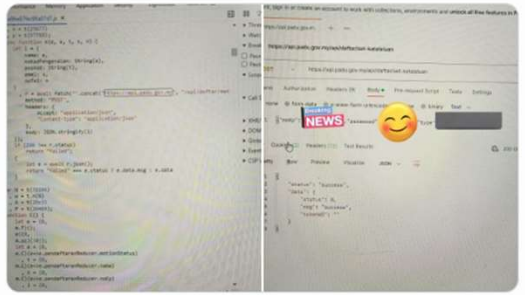
useState('drmsr')
@drmsr_dev · **Follow**

Guess what.

I only need your IC number to override and change your PADU login password.

@farhanhelmycode

@rafiziramli @Dr_Uzir @lamkanahraf



7:14 PM · Jan 2, 2024

6.3K Reply Share

Read 152 replies

thestar.com.my/news/nation/2023/12/11/hacking-issue-human-resource-ministry-taking-appropriate-action-to-avoid-recurrence-says-sivakumar

awareness | [Tutorial] Reversing... | 10 Idea Hidangan P... | 15 Best Websites to... | 4DigitalBooks - DL-... | 5 Free PDF Passwor... | About Us - Infe

Majoriti StarProperty StarCherish StarCarsifu StarSearch myStarjob Kuali Kuntum SuriaFM 988FM

The Star

StarPlus | News | Asean+ | Business | Sport | Metro | Lifestyle | Food | Tech | Education | Opinion | Videos

TOPICS : StarExtra | Flood Alert | StarESG | Urban Biodiversity | True or Not | SOBA 2023 | Covid-19 Watch

Socso hacking: Human Resources Ministry taking appropriate action to avoid recurrence

NATION

Monday, 11 Dec 2023

6:36 PM MYT

KUALA LUMPUR: The Human Resources Ministry has taken appropriate action to ensure that cyberattacks on Social Security Organisation (Socso) systems will not recur.

Its minister V. Sivakumar, said follow-up action would also be taken as soon as the mastermind responsible for hacking Socso's IT systems, database and website is identified.

He said the problem is under control and Socso's daily operations are running smoothly as usual, including the process of paying compensation and benefits to eligible recipients as well as processing of new contributor applications.

"All appropriate action needed has been executed by Socso. There is nothing (no problem) in the Socso operations for now," he said after a Socso media event here on Monday (Dec 11).

Socso chief executive officer Datuk Seri Dr Mohammed Azman Aziz Mohammed previously said that forensic investigations are underway on the alleged involvement of certain parties behind the cyberattack.

Meanwhile, Sivakumar said his ministry, together with the Economy Ministry and several other ministries, is studying in detail the implementation of the progressive

Related News

STARPICKS 14 Dec 2023
TOWARDS A PROGRESSIVE WAGE POLICY

NATION 02 Dec 2023
Progressive Wage Policy: Human Resources

nst.com.my/news/nation/2023/12/988005/perkeso-confirms-cybersecurity-breach-saturday

awareness | [Tutorial] Reversing... | 10 Idea Hidangan P... | 15 Best Websites to... | 4DigitalBooks - DL-... | 5 Free PDF Passwor... | About Us

-cyberattack-claims-leaked-data-is-questionable-and-incomplete/106563

15 Best Websites to... | 4DigitalBooks - DL-... | 5 Free PDF Passwor... | About Us - Infentc

HOME | MALAYSIA | SINGAPORE | MONEY | WORLD | LIFE | EAT/DRINK | SHOWBIZ | OPINION | SPORTS | TECH/GADGE

MALAYSIA

Socso confirms cyberattack, claims leaked data is questionable and incomplete

The organisation admitted that this isn't the first time it had a cyberattack as they faced a series of breaches previously. — SoyaCincau pic

*Join us on our **WhatsApp Channel**, follow us on **Instagram**, and receive **browser alerts** for the latest news you need to know.*

By Alexander Wong
Friday, 08 Dec 2023 6:29 PM MYT

KUALA LUMPUR, Dec 8 — Perkeso, Malaysia's social security organisation (Socso) has issued a

NEWS | BUSINESS TIMES | LIFE & TIMES | SPORTS | WORLD | NST TV | OPINION

NST VIRAL | CRIME & COURTS | NATION | GOVERNMENT / PUBLIC POLICY | POLITICS

Perkeso confirms cybersecurity breach since Saturday

By Amalina Kamal - December 8, 2023 @ 5:11pm

Social Security Organisation (Perkeso) today confirmed that its system, information base and website was hacked since last Saturday STR / FAIZ ANJAR

news@nst.com.my

KUALA LUMPUR: The Social Security Organisation (Perkeso) today confirmed that its system, information base and website was hacked since last Saturday (Dec 2).

In a statement, Socso said a crisis management plan was activated on the same day with its information technology and communication technology (ICT) unit mobilising a system recovery.

"The initial modus operandi of the cyber attack was identified as an effort to cripple the entire infrastructure used by Perkeso for daily operations.

-line-ransomware/

dea Hidangan P... 15 Best Websites to... 4DigitalBooks - DL-... 5 Free PDF Passwor... About Us - Infento Android Malware D... Architecture measur...

NEWS FORUMS GAMING MOBILE $ PRICELISTS MORE

RapidKL Says MRT Putrajaya Line Was Affected By Ransomware In Now-Deleted Tweet

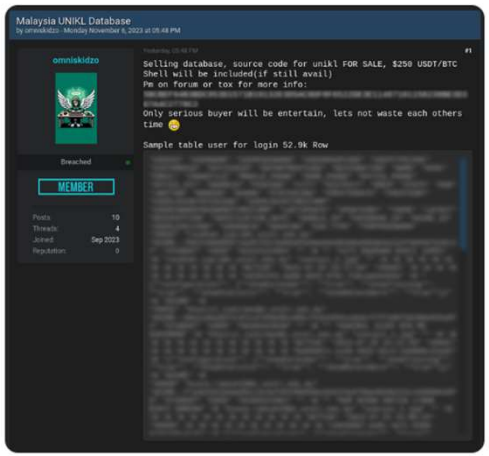
In response to a user asking why they couldn't reload their Touch 'n Go cards.

BY IAN CHEE JUNE 7, 2023

FalconFeeds.io
@FalconFeedsio

A forum user is offering to sell a breached database from the Malaysian University UNIKL (unikl.edu.my), which includes source code. The claimed data includes sensitive information like user IDs, usernames, passwords, and personal details of students, staff, and admissions records.

#Malaysia #databreach #dataleak #cti #darkweb



3:20 PM · Nov 7, 2023 · **9,359** Views

Search...

l-portal-was-hacked-last-saturday-jakim-confirms/107422

P... 15 Best Websites to... 4DigitalBooks - DL-... 5 Free PDF Passwor... About Us - Infento

HOME MALAYSIA SINGAPORE MONEY WORLD LIFE EAT/DRINK SHOWBIZ OPINION SPORTS TECH/GADGE

MAHANS Primary School

MALAYSIA

Malaysia's Halal Portal was hacked last Saturday, Jakim confirms

On Saturday night, Jakim's Halal Facebook page announced that the official Halal portal was inaccessible due to technical issues. — File picture by Firdaus Latif

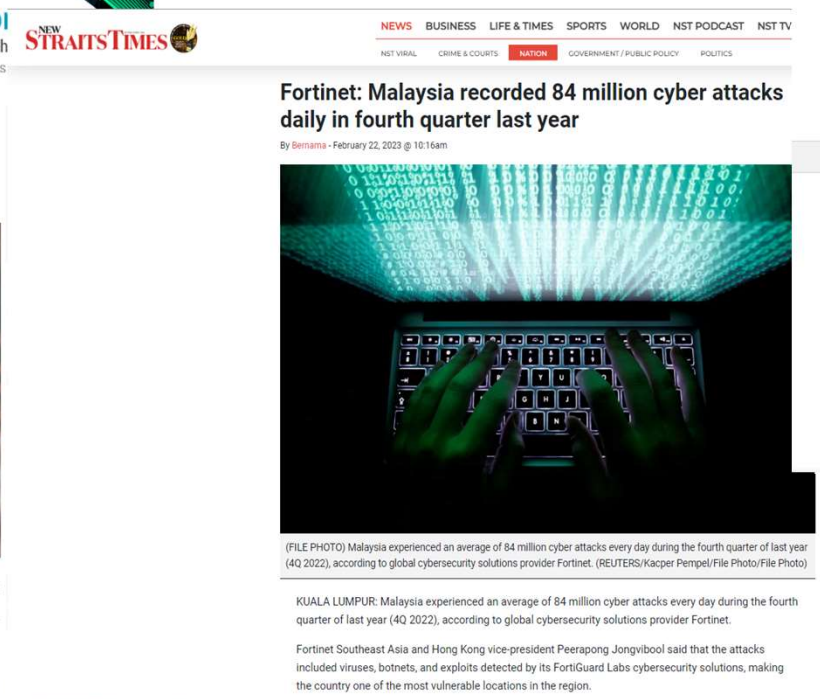
*Join us on our **WhatsApp Channel**, follow us on **Instagram**, and receive **browser alerts** for the latest news you need to know.*

By Alexander Wong
Thursday, 14 Dec 2023 8:30 AM MYT

KUALA LUMPUR, Dec 14 — The official Halal Portal of Malaysia was hacked last weekend and it was taken down temporarily. The incident which took place on December 9, 2023 was confirmed by Jakim's Halal Facebook page.

to conduct an investigation and prepare a comprehensive report on the matter.

https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722



https://www.nst.com.my/news/nation/2023/02/882387/fortinet-malaysia-recorded-84-million-cyber-attacks-daily-fourth-quarter

https://www.thestar.com.my/news/nation/2023/04/05/hackers-steal-rm19mil-from-batu-pahat-company039s-account

https://cybersecurityasean.com/daily-news/recurring-data-breaches-malaysia-plain-ignorance-or-just-weak-enforcement

HOME | NEWS | MALAYSIAN NEWS

Malaysian Military Network Targeted in Cyberattack

Noah Lee
Kuala Lumpur
2020-12-29

Tweet | Share 12 | Email | Comment | Share | Print

INESS | LIFE & TIMES | SPORTS | WORLD | NST TV | OPINION | VOUCHERS | GALLERY | COVID-19 VACCI

CRIME & COURTS | NATION | GOVERNMENT / PUBLIC POLICY | POLITICS

'Anonymous Malaysia' hacker group issues 2nd cyber attack threat

By Bernama - January 30, 2021 @ 10:15am

+ 15

ZDNet

VIDEOS | EXECUTIVE GUIDES | SECURITY | WORKING FROM HOME | CLOUD | INNOVATION | CXO | MORE | NEWSLET

Malaysia Airlines suffers data security 'incident' affecting frequent flyer members

Security breach compromises personal data of the airline's frequent flyer programme Enrich, including members' contact details and date of birth registered between March 2010 and June 2019, and reportedly involved a third-party IT service provider.

Ad closed by Google

By Eileen Yu for By The Way | March 2, 2021 -- 15:19 GMT (23:19 SGT) | Topic: Security

[Editor's note: SITA, the third-party IT service provider involved in this breach, has since clarified

AND FUTURE-

REUTERS

World | Business | Markets | Breakingviews | Video | More

MEDIA AND TELECOMS NOVEMBER 2, 2017 / 3:58 AM / UPDATED 3 YEARS AGO

Malaysia investigating reported leak of 46 million mobile users' data

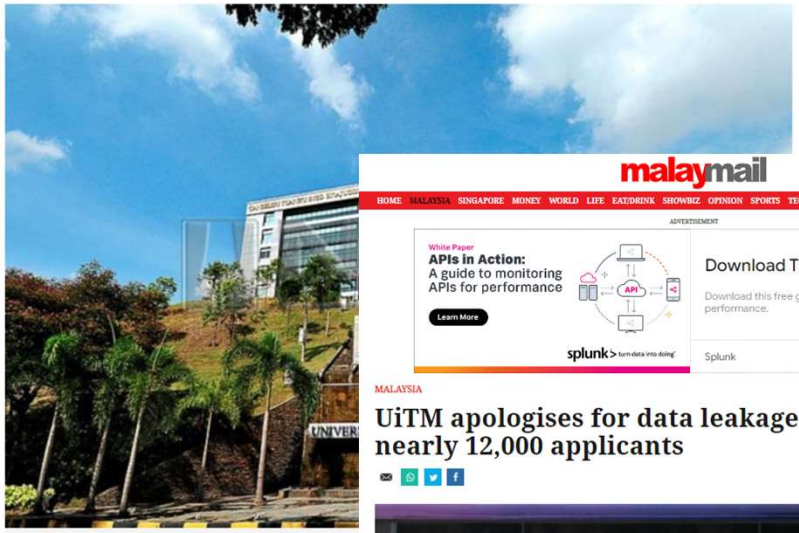
By Rozanna Latiff, Jeremy Wagstaff

4 MIN READ

KUALA LUMPUR/SINGAPORE (Reuters) - Malaysia is investigating an alleged attempt to sell the data of more than 46 million mobile phone subscribers online, in what appears to be one of the largest leaks of customer data in Asia.

UiTM to probe claims of data breach

By Veena Babulal, Beatrice Nita Jay - January 25, 2019 @ 6:50pm



(Stock image for illustration purposes) Vice-chancellor be conducting the investigation to ensure no one from

KUALA LUMPUR: A probe will be carried out by more than a million of its students' personal da

malaymail

HOME MALAYSIA SINGAPORE MONEY WORLD LIFE EAT/DRINK SHOWBIZ OPINION SPORTS TECH/GADGE

ADVERTISEMENT

White Paper
APIs in Action:
A guide to monitoring APIs for performance

Learn More

splunk> turn data into doing

Download The Fr

Download this free guide to r performance.

Splunk

MALAYSIA

UiTM apologises for data leakage of nearly 12,000 applicants

Yesterday, a Twitter user claimed that UiTM had published the MyKad numbers and emails of nearly 12,000 applicants on an unsecured link. — Picture by Yusof Mat Isa

Follow us on Instagram, subscribe to our Telegram channel and browser alerts for the latest news you need to know.

Wednesday, 10 May 2023 11:21 AM MYT

Universiti Malaya, JPDP looking into report of massive data breach affecting the university

By QISHIN TARIQ

TECH Premium

Saturday, 19 Oct 2019
1:34 PM MYT

Related News

Trending in Tech

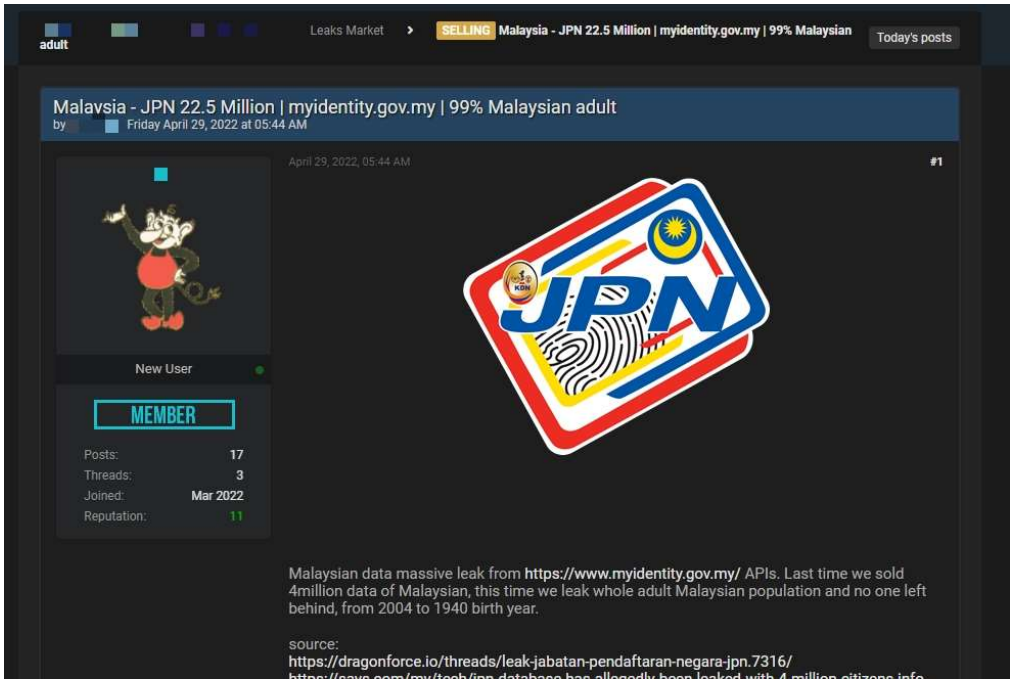
1 NATION 4h ago
Siti Bainun shouted angrily, asking who had given water to...

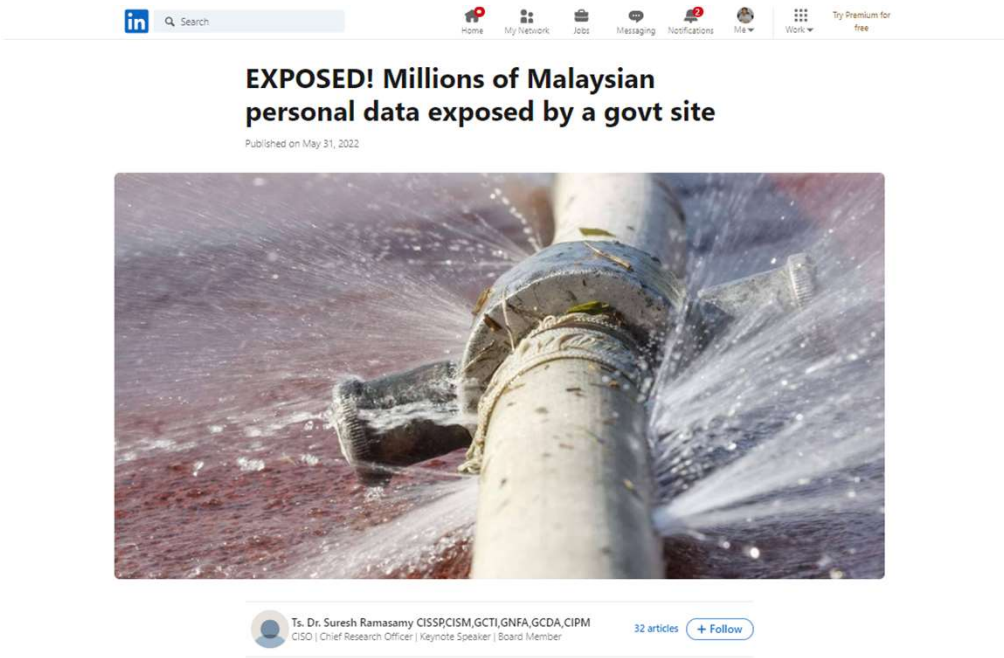
Malaysian data breach sees 46 million phone numbers leaked

31 October 2017

Malaysia's communication watchdog is investigating a huge data breach affecting 46 million mobile subscribers

A massive data breach has seen the customer data of more than 46 million mobile subscribers in Malaysia leaked on to the dark web





https://soyacincau.com/2022/05/17/personal-data-breach-ekyc-photos-of-malaysians-obtained-from-jpn-and-spr-sold-online/

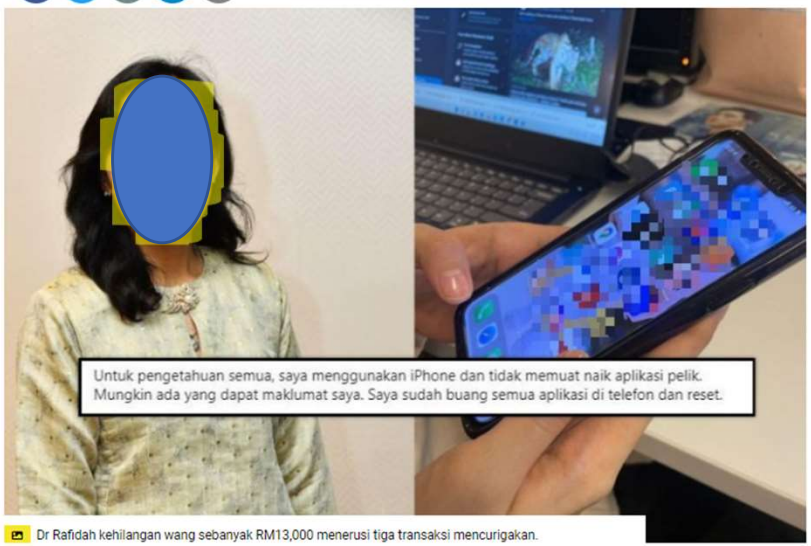
Duit RM13,000 lesap pukul 2 pagi! Dr Rafidah pelik 3 transaksi berlaku tanpa TAC... Bakal tutup akaun bank sele tahun

VIRAL

Duit RM13,000 lesap pukul 2 pagi! Dr Rafidah pelik 3 transaksi berlaku tanpa TAC... Bakal tutup akaun bank selepas 30 tahun

Sabtu, 20 Ogos 2022 2:00 PM

Oleh: MSTAR



Dr Rafidah kehilangan wang sebanyak RM13,000 menerusi tiga transaksi mencurigakan.

MEDIA sosial kecoh apabila pakar perubatan terkenal Dr Rafidah Abdullah mendedahkan wang simpanan sebanyak RM13,000 lesap dalam akaun bank miliknya.

k, pakar buah pinggang itu meluahkan rasa kecewa apabila wang

BORNEO POST online

THE LARGEST ENGLISH NEWS SITE IN BORNEO

HOME | SARAWAK | SABAH | NATION | WORLD | BUSINESS | SPORTS | LITE STORIES | FEATURES | COLUMNS

YOU ARE AT: Home » News » Crime » 4 love scam cases involving losses of RM128,000 reported from Jan 1 to 31, says CCID chief

4 love scam cases involving losses of RM128,000 reported from Jan 1 to 31, says CCID chief

BY JACQUELINE DAVID ON FEBRUARY 14, 2022, MONDAY AT 7:01 AM

CRIME, SARAWAK

Supt Maria Rasid

KUCHING (Feb 14): A total of four love scam cases involving losses of RM128,000 have been reported in the state for the period of Jan 1 until Jan 31 this year.

TRENDING

Sarawak - August 30, 2022

Street protest if Hadi not arrested, prosecuted, says Peter John

Sarawak - August 30, 2022

Sri Aman Interchange open to road users starting tomorrow

Data peribadi rakyat Malaysia dilelong

Data rakyat Malaysia dilelong secara pukal di dark web.

Oleh MASZUREEN MAOZMAN 27 April 2023, 7:33 am

PETALING JAYA: Data rakyat Malaysia daripada pelbagai organisasi kerajaan dan swasta dikesan 'dilelong' secara pukal di laman web gelap atau dark web dengan harga serendah RM4,400 sehingga RM45,000. Kesemua data yang diperoleh daripada pelbagai industri termasuk perbankan, telekomunikasi dan agensi kerajaan dijual kepada penggodam menerusi pasaran gelap seperti forum dan aplikasi telegram bagi mengelak dikesan pihak berkuasa. Data-data yang 'dilelong'...

TERKINI

- Penyeludup ulang alik isi diesel dicekup
  31 Mei 2023, 11:09 am
- Lelaki maut kereta terbabas, langgar tiang lampu
  31 Mei 2023, 11:07 am
- Tawaran senjata nuklear jika sokong kesatuan Belarus-Russia
  31 Mei 2023, 11:00 am
- Gagal memotong, dua individu maut
  31 Mei 2023, 11:00 am
- Peranan besar Akademi Pengajian Melayu kaji kekuatan bangsa
  31 Mei 2023, 10:59 am
- Harimau Malaya lawan Papua New Guinea bukan Yemen
  31 Mei 2023, 10:59 am

Utusan Malaysia

TERKINI NASIONAL EKONOMI RINGGIT LUAR NEGARA GAYA SUKAN RENCANA PANCAINDERA SERI PREMIUM

Data 223 juta rakyat di tangan penggodam

Lebih 223 juta data peribadi rakyat Malaysia berisiko jadi mangsa penipuan dengan adanya sistem pangkalan data yang 'dikawal' dan 'dibangunkan' oleh penggodam untuk 'dilelong' kepada sindiket.

Oleh MASZUREEN MAOZMAN 31 Mei 2023, 7:00 am

PETALING JAYA: Lebih 223 juta data peribadi rakyat Malaysia berisiko jadi mangsa penipuan dengan adanya sistem pangkalan data yang 'dikawal' dan 'dibangunkan' oleh penggodam untuk 'dilelong' kepada sindiket. Ia dipercayai dibangunkan oleh penggodam terdiri daripada pakar-pakar teknologi informasi (IT) berpangkalan di negara ini yang ingin mengaut keuntungan dengan mudah tanpa sebarang jejak. Dengan hanya mendaftar ke dalam sistem berkenaan, pelayar...

TERKINI

- Lelaki maut kereta terbabas, langgar tiang lampu
  31 Mei 2023, 11:07 am
- Tawaran senjata nuklear jika sokong kesatuan Belarus-Russia
  31 Mei 2023, 11:00 am
- Gagal memotong, dua individu maut
  31 Mei 2023, 11:00 am
- Peranan besar Akademi Pengajian Melayu kaji kekuatan bangsa
  31 Mei 2023, 10:59 am
- Harimau Malaya lawan Papua New Guinea bukan Yemen
  31 Mei 2023, 10:59 am
- 1.6 hektar Hutan Simpan Kuala Langat Selatan terbakar
  31 Mei 2023, 10:17 am

MyCERT | CyberSecurity MALAYSIA

ABOUT US | SERVICES | RESOURCES | CONTACT US

Reported Incidents based on General Incident Classification Statistics 2022

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	8	5	6	15	7	27	286	27	27	27	31	12	478
Intrusion	68	54	50	74	59	89	82	45	76	73	44	41	755
Malicious Codes	62	68	174	103	70	75	98	124	86	61	60	42	1,023
Denial of Service	0	2	1	1	4	2	0	1	3	2	0	1	17
Fraud	431	423	388	396	509	486	429	294	566	285	244	290	4,741
Intrusion Attempt	15	12	4	6	15	14	32	21	20	15	13	13	180
Content Related	2	0	0	2	2	7	1	10	7	5	6	8	50
Vulnerabilities Report	6	3	3	4	5	5	3	2	0	5	8	4	48
	592	567	626	601	671	705	931	524	785	473	406	411	7,292

https://www.mycert.org.my/portal/index

Do Your Part.
#BeCyberSmart

Cybersecurity starts with YOU and is everyone's responsibility.


CYBERSECURITY THREAT
average 45%
average 45%
27%
54%

- Natural Threats
  - Natural threat sinclude natural disasters such as earth quakes, hurricanes , floods , or any nature – created disaster that can not be stop.
  - Information damage or lost due to natural threats can not be prevented as no one knows in advance that the setypes of threats will occur.
  - However, you can implement a few safeguards against natural disasters by adopting disaster recovery plans and contingency plans.
- Physical Security Threats
  - Physical threats may include loss or damage of system resources through fire, water, theft and physical impact.
  - Physical impact on resources can be due to a collision or other damage, either intentionally or unintentionally.
  - Some times, power may also damage hardware used to store information.

- Human Threats
  - Human threats include threats of attacks performed by both insiders and outsiders.
  - Insider attacks refer to attacks performed by disgruntled or malicious employees.
  - Outsider attacks refer to attacks performed by malicious people not within the organization.
  - Insider attacker scan be the biggest threat to information system as they may know the security posture of the information system, while outsider attackers apply many tricks such as social engineering to learn the security posture of the information system .

- Network Threats
  - A network is defined as the collection of computers and other hardware connected by communication channels to share resources and information.
  - As the information travels from one computer to the other through the communication channel, a malicious person may break into the communication channel and steal the information traveling over the network .
  - The attacker can impose various threats on a target network :

- Information gathering
- Sniffing and eavesdropping
- Spoofing
- Session hijacking and man-in-the-middle attacks
- SQL injection
- ARP Poisoning
- Password-based attacks
- Denial of service attack
- Compromised-key attack

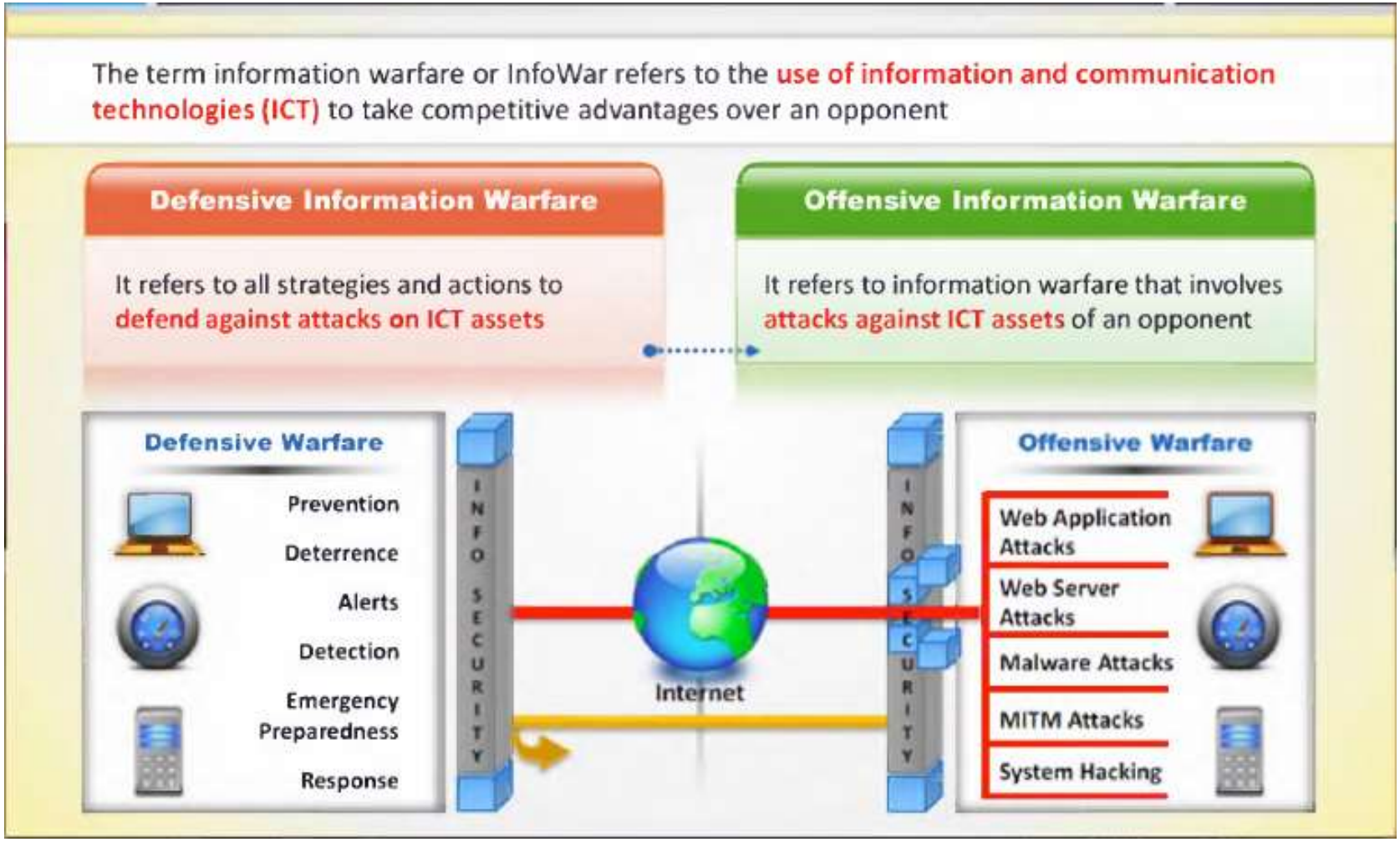
- Host Threats
  - Host threats are directed at a particular system on which valuable in formation resides
  - Attackers try to breach the security of the information system resource. The following are possible threats to the host :

- Malware attacks
- Target Foot printing
- Password attacks
- Denial of service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Backdoor Attacks
- Physical security threats

- Application Threats
  - If the proper security measures are not considered dur ing development of the particular application, the application might be vulnerable to different types of application attacks .
  - Attackers take advantage of vulnerabilities present in the application to steal or damage the information.
  - The following are possible threats to the application :

- Data/Input validation
- Authentication and Authorization attacks
- Configuration management
- Information disclosure
- Session management issues
- Buffer overflow issues
- Cryptography attacks
- Parameter manipulation
- Improper error handling and exception management
- Auditing and logging issues

Information Warfare



Types of attack

- There are several ways an attacker can gain access to a system .
- The attacker must be able to exploit a weakness or vulnerability in a system :

  - **Operating system attacks :**
    - Attackers search for OS vulnerabilities and exploit them to gain access to a network system .

  - **Application-level attacks:**
    - Software applications come with myriad functionalities and features . There is a dearth of tim to perform complete testing before releasing products. Those applications have various vulnerabilities and become a source of attack .

  - **Misconfiguration attacks:**
    - Most administrators don't havem the necessary skills to maintain or fix issues, which may lead to configuration errors. Such configuration errors may become the sources for an attacker to enter into the target's network or system.

  - **Shrink wrap code attacks:**
    - Operating system applications come with numerous sample scripts to make the job of administrator easy, but the same scripts have various vulnerabilities, which can lead to shrink wrap code attacks .


Defense and
CounterMeasures


OUTSIDE THREAT PROTECTION
PERIMETER SECURITY
DMZ
VPN
2FA/MFA
IDS/IPS
WAF
Web Content Filter
Honeypot
NETWORK SECURITY
VoIP Security
Wireless Security
External Vuln Scanning
Firewall
Virtual Patching
Mobile Security
Message Security
Internal IDS/IPS
NAC
ENDPOINT SECURITY
DLP
NGAV/EDR/MDR (malware/ransomware)
File Integrity Monitoring
Internal Vuln Scanning
DDos Prevention
Internal Firewall
Patch Management
Physical Security
Endpoint App White/Blacklist
APPLICATION SECURITY
Network Device Hardening
DLP
Endpoint Disk Encryption
ICAM/ZTA (2FA/MFA)
Endpoint Firewall
Application Vuln Scanning
Dynamic App Testing
Physical Security
Logging
Endpoint Hardening
Database Security
DATA SECURITY
Static App Testing
ICAM/ZTA (2FA/MFA)
WAF
ICAM/ZTA (2FA/MFA)
DLP
Physical Security
ICAM/ZTA (2FA/MFA)
Data Classification
Logging
Logging
Data Integrity Monitoring
CSIRT
Continuous C&A
Data/Drive Encryption
Data Wiping
Focused Ops
SIEM
IT Security Governance
Security Plan
PKI
DLP
Logging
Security Dashboard
Digital Forensics
Vulnerability Assessment
Business Continuity Plan
SOC/NOC Monitoring (24x7)
Escalation Management
Security Awareness Training
IT Disaster Recovery Plan
Continuous Monitoring & Assessement
Security SLA/SLO
Situational Awareness
Reporting
Security Architecture & Design
Risk Management
Penetration Testing
Cyber Threat Intelligence
Security Policies & Compliance
Data Classification
MISSION CRITICAL ASSETS
POLICY MANAGEMENT & PREVENTION
MONITORING & RESPONSE / OPERATIONS
DEFENSE-IN-DEPTH MODEL
COLOHOUSE

Security Policy

- Security policy is a compromise that
- organization decides to adopt between
- absolute security & absolute access
- Who can get in/out
- Where they can go
- When they can get in/out
- What they can bring in/carry out
- **Physical access**
  - Protecting management station

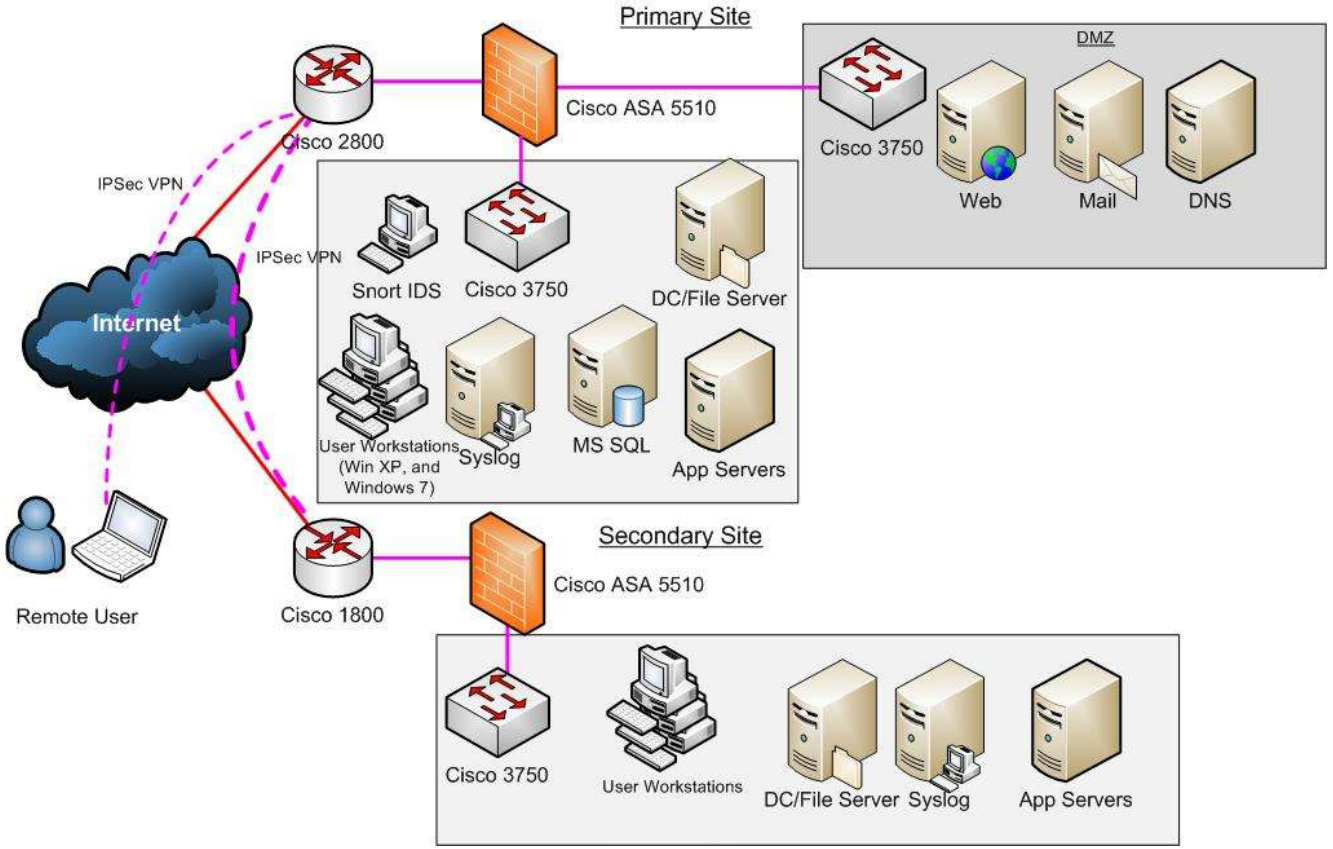
A typical network design.

Logging Sources

- Syslog and SNMP Trap
- Network
  - Cisco IOS
  - Snort IDS/IPS
- Servers/Workstations
  - Enterprise Linux
  - Microsoft Windows
- Applications
  - BIND (DNS)
  - Exchange
  - MS SQL
  - Host Intrustion Detection

Logging Services

- SYSLOG
  - SYSLOGD
  - SYSLOG-NG
  - RSYSLOG
- SNMP TRAP



SIEM

- SIEM - Security Information Event Management
  - Countermeasures to detect attempts to infect internal system
  - Identification of infected systems trying to exfiltrate information
  - Mitigation of the impact of infected systems
  - Detection of outbound sensitive information (DLP)

Continual/ Adaptive Security Strategy

Security Assessment

- **Security Audits**
  - Focus on the people and processes
  - To design, implement, and manage security on a network.
  - There is a baseline involved for processes and policies within an organization.
  - use the specific baseline to audit the organization
- **Vulnerability Assessment**
  - identifying security vulnerabilities.
- **Penetration Testing**
  - act of testing an organization' s security by simulating the actions of an attacker

Vulnerability assessment: Security scanning process

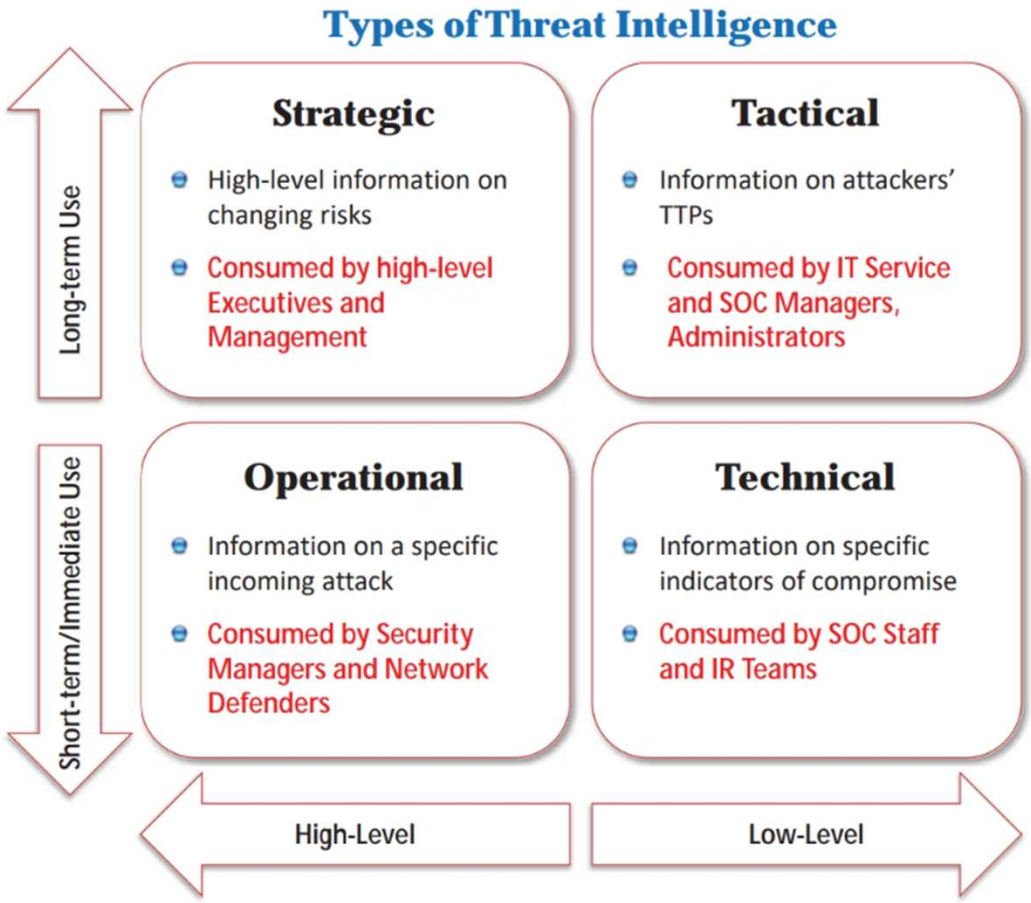
- In general, the security scanning process consists of four steps: testing, analysis, assessment and remediation.

*source: https://www.imperva.com/learn/application-security/vulnerability-assessment/

Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) is defined as the collection and analysis of information about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks

- Cyber threat intelligence helps the organization to identify and mitigate various business risks by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies



Conclusion

What You Can Do Legally

- Laws involving technology change as rapidly as technology itself
- Find what is legal for you locally
  - Laws change from place to place
- Be aware of what is allowed and what is not allowed

Laws of the Land

- Tools on your computer might be illegal to possess
- Contact local law enforcement agencies before installing hacking tools
- Written words are open to interpretation
- Governments are getting more serious about punishment for cybercrimes

Is Port Scanning Legal?

- Some states deem it legal
- Not always the case
- US Federal Government does not see it as a violation
  - Allows each state to address it separately
- Read your ISP's "Acceptable Use Policy"
  - IRC "bots" may be forbidden
    - Program that sends automatic responses to users
    - Gives the appearance of a person being present

What You Cannot Do Legally

- Accessing a computer without permission is illegal
- Other illegal actions
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs

Security Professional Certification

https://certification.comptia.org/certifications/security

CompTIA

Partners Contact Us Help My Account Store

WHY CERTIFY CERTIFICATIONS TRAINING TESTING CONTINUING EDUCATION STAY CONNECTED

ZERTIFIZIERUNG > COMPTIA SECURITY+

CompTIA Security+

EXAM CODES SY0-401 OR SY0-501

OVERVIEW EXAM DETAILS PREPARATION RENEWAL TRY CERTMASTER

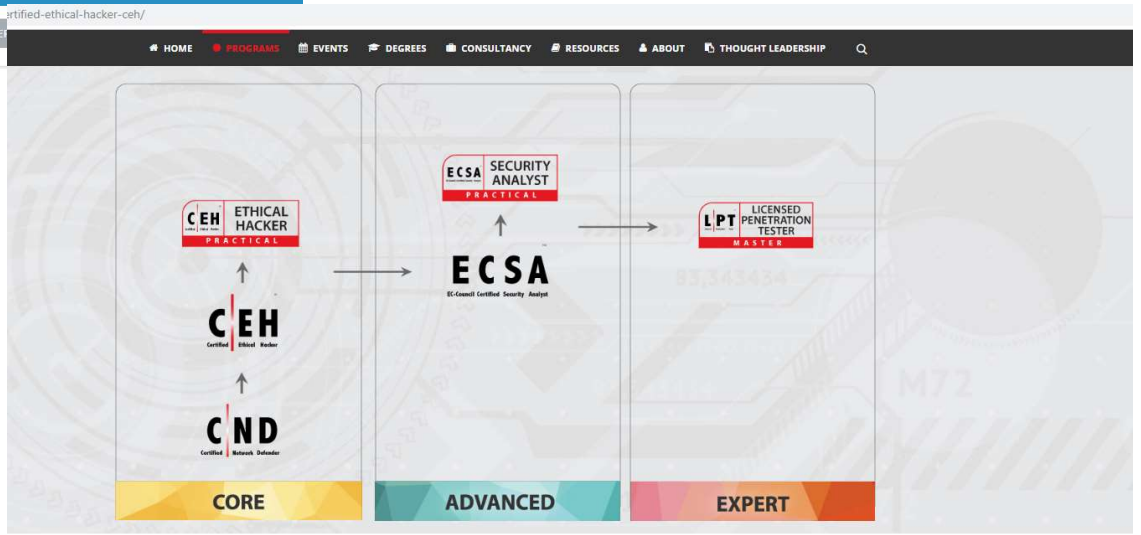
CompTIA Security+

CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career.

Why is it different?

ertified-ethical-hacker-ceh/

HOME PROGRAMS EVENTS DEGREES CONSULTANCY RESOURCES ABOUT THOUGHT LEADERSHIP



Certified Ethical Hacker Certification

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Security Professional Certification

ty.com/information-security-certifications/oscp-offensive-security-certified-professional/

OFFENSIVE® security

Courses | Certifications | Online Labs | Penetration Testing | Projects | Blog | About | ENROLL NOW

Offensive Security Certified Professional (OSCP) Overview

OFFENSIVE® security OSCP MOST POPULAR

GET CERTIFIED

Limited seats available for each course session

- OSCP is the most well-recognized and respected certifica info security professionals
- To become certified, you must complete Offensive Secur Penetration Testing with Kali Linux (PwK) course and pas hour hands-on exam
- An OSCP has mastered a comprehensive and practical understanding of the penetration testing process
- For hands-on experience, each student receives access t penetration testing lab where techniques learned within course can be practiced

Real World Exams

The *OSCP examination* consists of a virtual network containing targets of varying configurations and operating systems. At the start of the exam, the student receives the exam and connectivity instructions for an isolated exam network that they have no prior knowledge or exposure to.

The successful examinee will demonstrate their ability to research the network (information gathering), identify any vulnerabilities and successfully execute attacks. This often includes modifying exploit code with the goal to compromise the systems and gain administrative access.

rtifications/CISSP#

REGISTER FOR EXAM | SIGN IN

(ISC)² ABOUT | CERTIFICATIONS | EDUCATION & TRAINING | MEMBERS | NEWS & EVENTS | ADVOCACY | COMMUNITY

CISSP®

Become a CISSP – Certified Information Systems Security Professional

Accelerate your cybersecurity career with the CISSP certification.

Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program. With a CISSP, you validate your expertise and become an (ISC)² member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

Prove your skills, advance your career, and gain the support of a community of cybersecurity leaders here to support you throughout your career.

Free CISSP Ultimate Guide

Get everything you need to know about preparing for the CISSP exam, including:

- Why you should get certified
- CISSP *Fast Facts*
- What to expect on the exam
- How to prepare for the exam
- Value of (ISC)² certification

DOWNLOAD

Security Professional Certification

Ethical Hacking in a Nutshell

- What it takes to be a security tester
  - Knowledge of network and computer technology
  - Ability to communicate with management and IT personnel
  - Understanding of the laws
  - Ability to use necessary tools