KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

Overview on Cybersecurity

KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

Context : Data

- **780,000 records of sensitive data** were lost **per day in 2017** because of lack of security. (According to McAfee)
- **58%** of companies have over 100,000 folders **open to the public** (21% of the folders are **non protected**) (According to Varonis).
- French president **Emmanuel Macron emails hacked in 2017.**
- Companies take over 6 months to notice a data breach (According to ZDNet)
- **95%** of cybersecurity breaches are due to human error.(Cybint)

[Cyber security Stats]

Data Connectors
Cybersecurity Community | Since 1999

KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

Context : Attacks

- **64%** of companies experienced **web based** attacks. **62%** experienced **phishing and social engineering** attacks. **59%** companies experienced **malicious code** and botnets. **51%** experienced **denied of service**. (Cybint)
- **30% of phishing emails** in the U.S. are **opened** (Verizon).
- Over **24,000 malicious mobile apps** are blocked **daily**. (Symantec)
- In 2016, **Adware** affected 75% of organizations (Cisco).
- 300 billion passwords exposed worldwide (Cyber Security Media).

Context : Attacks

- Most of the attacks happened because of stolen credits (exposed sensitive data or because of human errors).

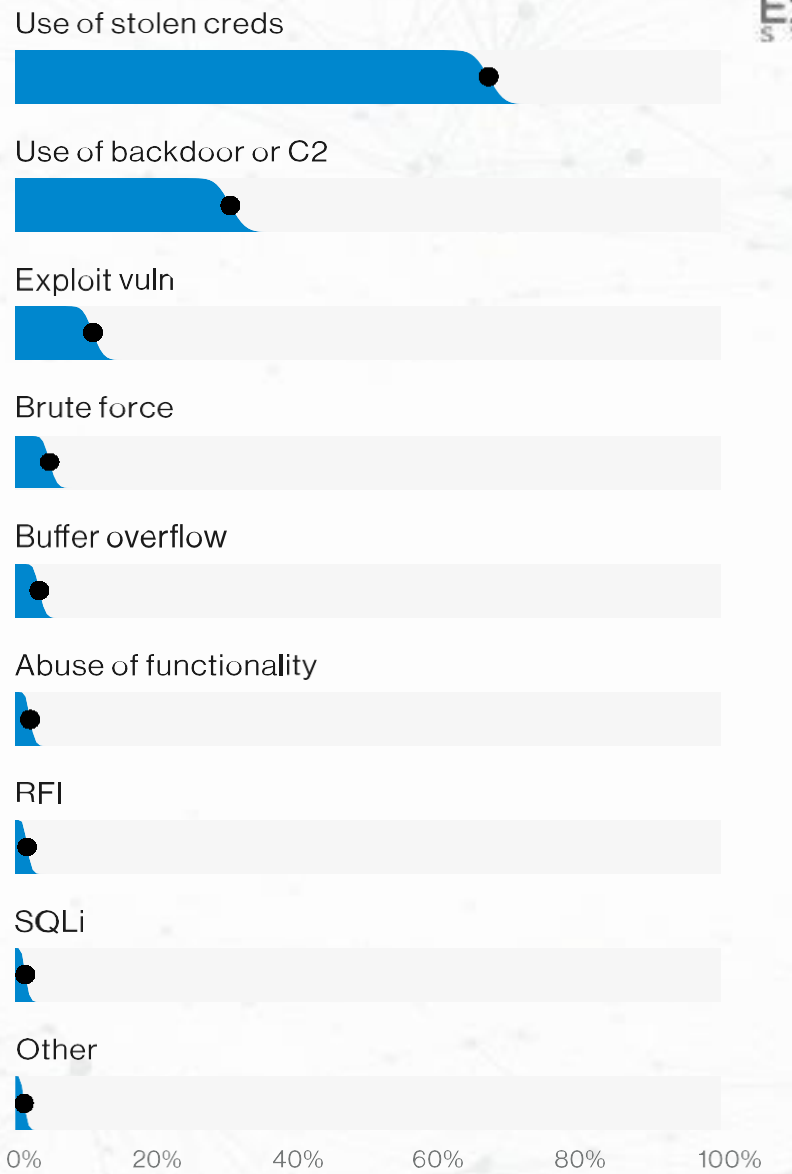


Figure 13. Top hacking action varieties in breaches (n=755)

Context :

- Cyber Crime to cost **$6 trillion** by 2021 (Annual Cybercrime report 2016)
- Cybercrime costs small and medium businesses more than **$2.2 million** a year.

“Cybercrime is the greatest threat to every company in the world.”
Ginni Rometty, IBM’s chairman, president and CEO

History & definitions

What’s do we mean by hacking exactly and when did it start ?

History

- **1960s: The Dawn of Hacking :** The first computer hackers emerge at MIT who “hacked” the electric trains, tracks, and switches to make them perform faster and differently.

- **1970s: Phone Phreaks and Cap'n Crunch :** Phone hackers (phreaks) break into regional and international phone networks to make free calls. **Steve Wozniak and Steve Jobs**, future founders of Apple Computer, later launched a home industry making and selling blue boxes based on the same trick.

- **1986: Use a Computer, Go to Jail** Congress passes the Computer Fraud and Abuse Act, which makes it a crime to break into computer systems.

- **1995: The Mitnick Takedown :** Serial cybertrespasser **Kevin Mitnick** is captured by federal agents and charged with stealing 20,000 credit card numbers.

History

- **2000: Service Denied:** In one of the biggest denial-of-service attacks to date, hackers launch attacks against eBay, Yahoo!, CNN.com., Amazon and others.

- **2001: DNS Attack** Preventing users from visiting Microsoft websites for two days by editing the DNS entries and paths.

[Timeline: A 40-year history of hacking (CNN)]

Definitions

- A **computer hacker** is any skilled computer expert who uses their technical knowledge to overcome a problem, and in a modern context someone who can find bugs and exploits in a computer system and use them to break into it.
- Nowadays it's important to make the difference between three types of hackers :
    - **White hats** : Those who generally work with companies and whose goal is to keep data safe by finding the vulnerabilities and bugs in the company's systems.

Definitions

- **Black hats** :also called the crackers. Those crack and exploit illegally and whose intentions are causing damage and making benefit from selling data and credentials.

- **Grey hats** : Those who hack for fun who exploit bugs and provide fixes later. They are not called “white” because their work is still illegal unless they are authorized to break into systems by their owners for auditing purposes.

Overview on tools

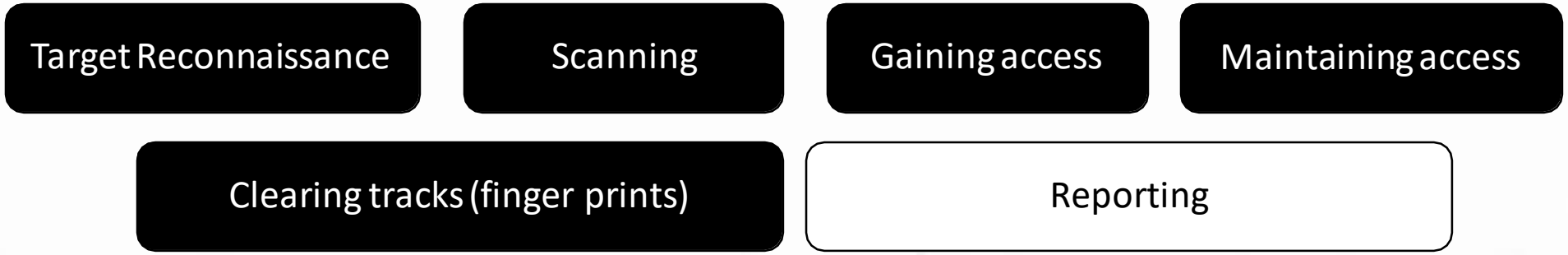
- There are several tools that be helpful sometimes and makes the "hacking" process much more easier and faster.
- These tools keep evolving and changing, for that it's important to stay updated and informed.
- These tools sometimes don't require any deep understanding of the technical aspects of the system, but rather know how it works in general.
- Some tools can serve as an all-in-one and some are very specialized in very specific tasks as we are going to see in details later in this course.

Overview on tools

- Operating systems:
  - There are some Linux distributions that come up with all the necessary tools preinstalled such as **Kali Linux** and **Parrot OS Security, Black Arch Linux,etc .**
  - **Any operating systems can be used depending on how skilled is the hacker and also depending on *"the hack" s.*he is performing.**
- **Kali Linux :** is a Debian based distribution that is especially designed for digital forensics and penetration testing. It comes with more than 300 pre-installed tools for *information gathering*, *networks sniffers and scanners*, *passwords crackers* and exploitation 'programs'.

Overview on process (pipeline)

- There are mainly 5 phases (6 for ethical hacking). Not necessarily a hacker has to follow these steps in a sequential manner. It's a stepwise process and when followed yields a better result.



Overview on process (pipeline)

Target Reconnaissance

- Reconnaissance is the phase where the attacker gathers information about a target using active or passive means.
- Tools used :
  - Google & Social media
  - Maltego
  - Nmap
  - Shodan
  - Etc.

Overview on process (pipeline)

Scanning

- Scanning the target machine.s or network for vulnerabilities than can be exploited.
- Tools used :
  - Nessus
  - Nexpose
  - Nmap
  - DNSenum
  - Etc.

Overview on process (pipeline)

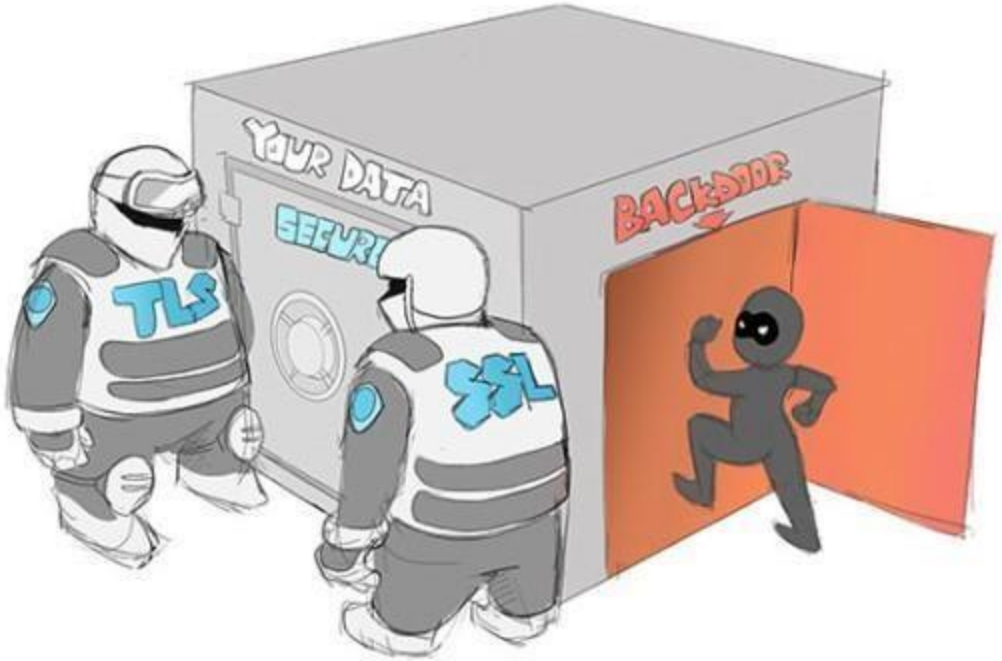
Gaining Access

- Once a vulnerability is found and located, the hacker attempt in this phase to exploit it in order to enter into the system.
- Tools used :
  - Mainly Metasploit.

Overview on process (pipeline)

Maintaining Access

- This happens after gaining access, and in this step the hackers installs some backdoors in order to enter into this system in the future.
- Tools used :
  - Mainly Metasploit.



Overview on process (pipeline)

Clearing tracks

- This process is actually an **unethical** activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.
- Finding logs servers and data bases and delete the records.

Overview on process (pipeline)

Reporting

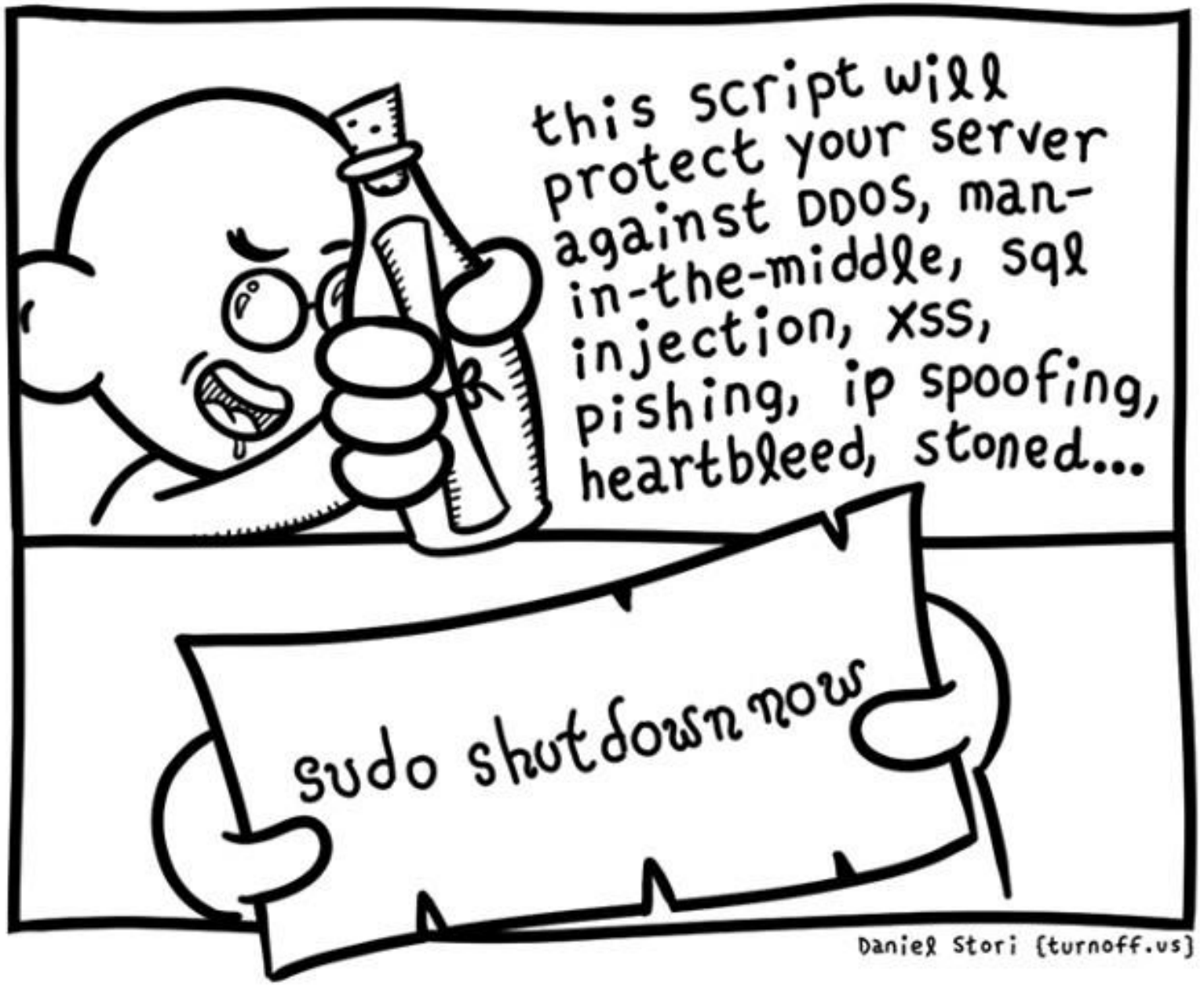
- Reporting is the last step of finishing **the ethical hacking process**. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

Cybersecurity Concepts and projects.

How we can secure our companies ?


this script will protect your server against DDOS, man-in-the-middle, sql injection, xss, pishing, ip spoofing, heartbleed, stoned...
sudo shutdown now
Daniel Stori {turnoff.us}

More Definitions !

- Data/System/Computer security: **detecting** and **preventing** any unauthorized use or access to your system/data.

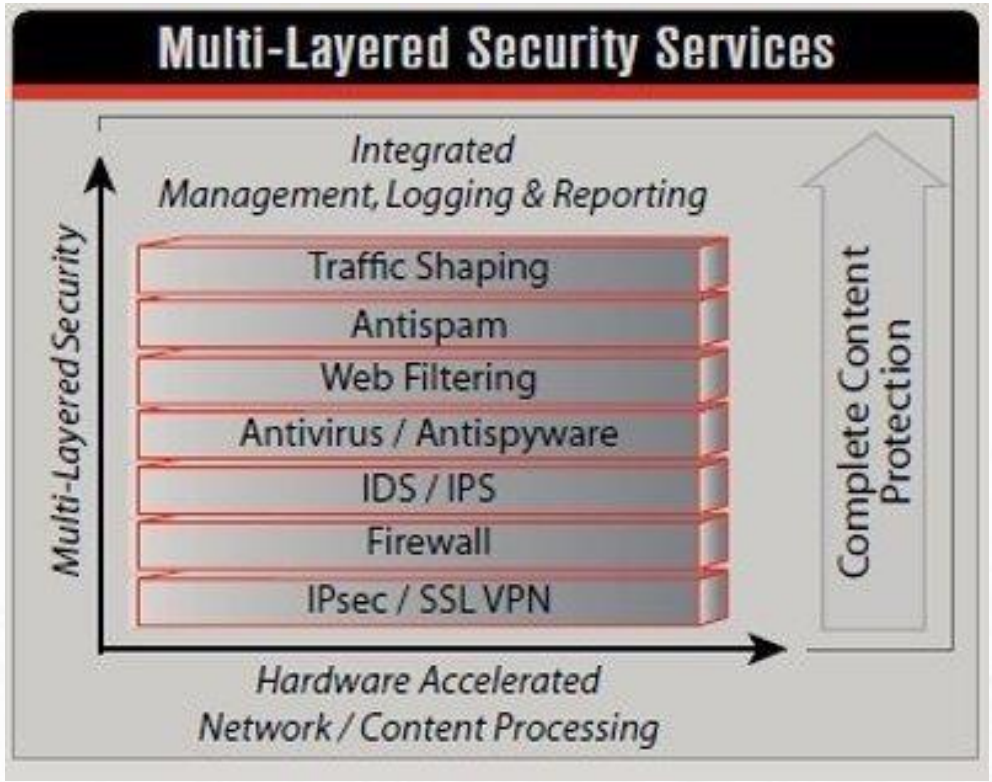
- **In order to do so, we need to be aware of three main concepts:**

Confidentiality | **Integrity** | **Availability**

1.Threat preventing/security.

- Implementing security practices and tools (antivirus, firewalls,etc) to act as the first defender of our system/data.

- Multi-layered security approach by combining multiple tools to secure different levels of our network and system.



1.Threat preventing/security.

2.Threat detection

- Searching for malwares and vulnerabilities in the system (network, apps, data,etc.)

- Tools and Security solutions even with the multi-layer approach **are just the first line of defense**, and are not effective against advanced attacks.

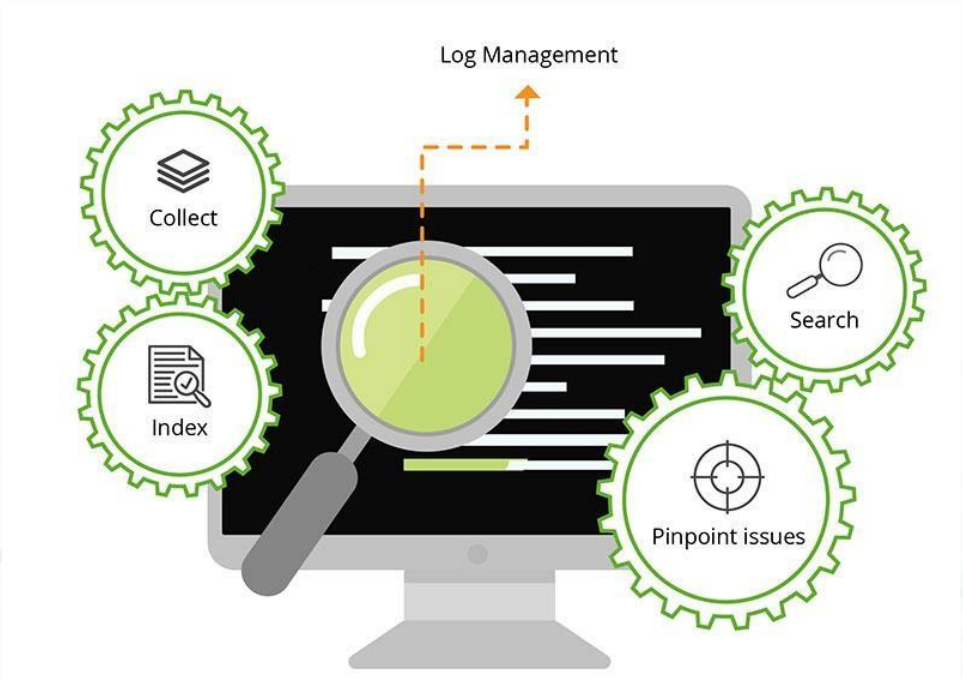
- Threat detection is preventing attacks in their early stages before they happen or cause any damage.

2.Threat detection/ more stats %

- Just figuring out how a cyber attack happened could cost $15,000.
- 40% of small and mid-sized businesses experienced eight or more hours of downtime due to a cyber breach.
- This downtime accounts for an average of $1.56 million in losses.
- Cyber attacks are projected to cause $6 trillion in damages by 2021.

2.Threat detection

- Threat hunting uses a mixture of forensics capabilities and threat intelligence to track down where attackers have established footholds within the network and eliminate their access before any damaging malicious actions can take place.



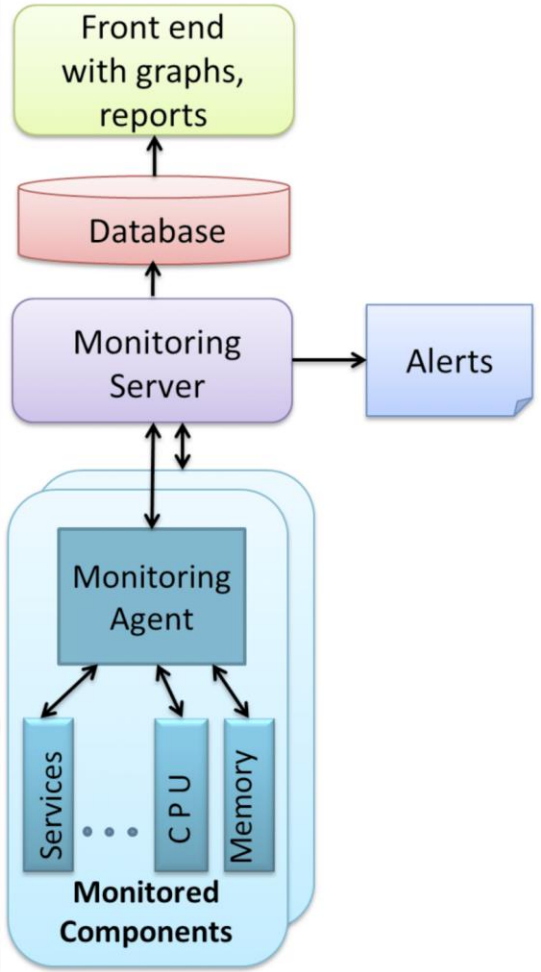
AT&T Cybersecurity

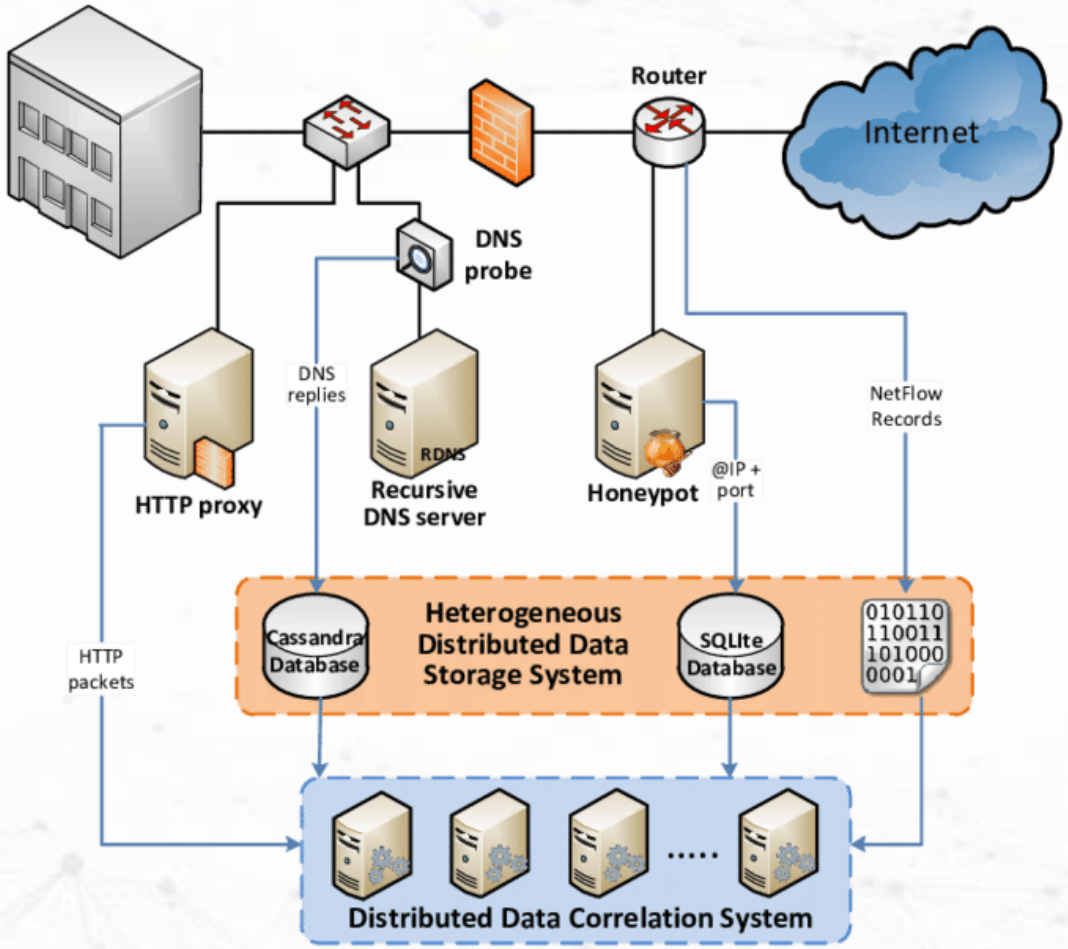
2.Threat detection

- Analyzing and monitoring servers logs, network traffic, configurations, changes in data and much more:
  - Monitoring listening ports of exposed systems (looks for abnormal traffic and unusual exchanges).
  - Monitoring changes in file systems.
  - Monitoring authentication requests (attempts) especially of privileged accounts on endpoints, servers and services.

- Various tools and solutions (software to big data architectures) can be used to collect events and logs for monitoring :
  - Security monitoring tools (logs and events from firewalls,DLPsetc).
  - SIEM solutions.
  - Analytics tools (Statistical analysis and Machine learning models).

2.Threat detection





3.Compliance (Security policies)

3.Compliance (Security policies)

- Establishing risk-based controls (standards and protocols) to protect the integrity, confidentiality, and accessibility (Availability) of information stored, processed, or transferred.
- These rules and standards depends on the industry and the activities the companies does.
  - **Example** : **Healthcare** industry have the **HIPPA** (Health Insurance Portability and Accountability Act) , and if any payment through a point of service is involved in the activity, then the **PCI DSS** (Payment Card Industry Data Security Standards) should be respected as well. In addition to **GDPR** if based * in Europe.

3.Compliance (Security policies)

- **More than 77% of organizations do not have a Cyber Security Incident Response plan !**

KEDGE BUSINESS SCHOOL

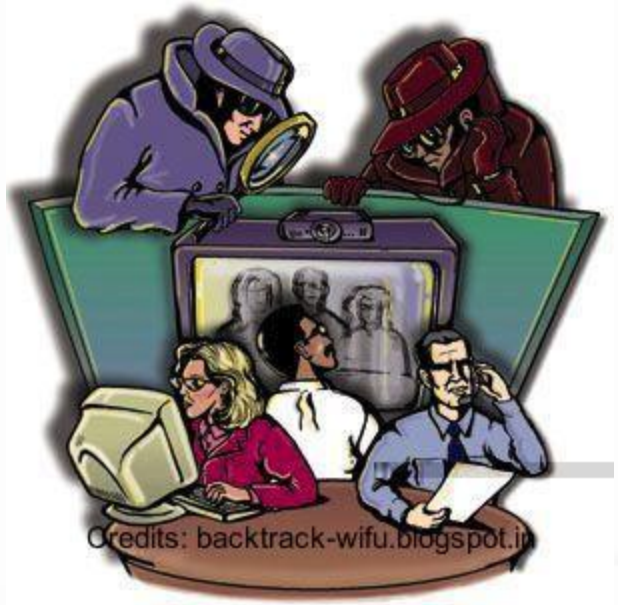
Excelerate SYSTEMS

Ethical hacking 1

Target Reconnaissance (lecture and tools)

1 Target reconnaissance

- Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.
- Gathering as much information as possible about the target system:
  - Initial information (company websites, clients, partners, locals, etc).
  - Network range, active machines and their open ports (misconfigurations), SSL certificats,etc.
  - Fingerprints and OS information (type,etc).



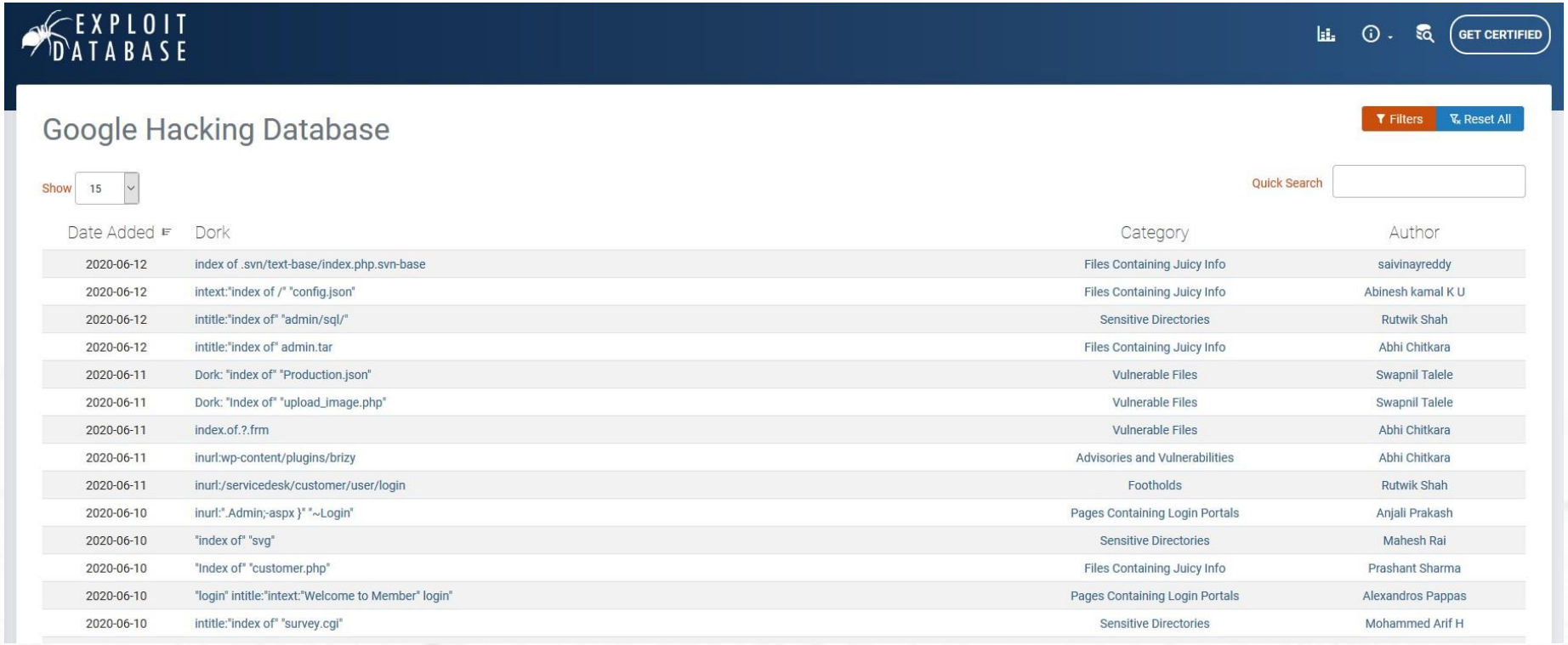
1 Target reconnaissance - footprinting

- Information that a hacker can collect about the target can be :

  - Domain name.s and subdomains.
  - IP addresses
  - Employees information (emails, phone numbers, social media accounts)
  - Clients and partners information (those who interact with the target systems).
  - Data breaches.
  - Exposed servers and databases.
  - Exposed configuration files.
  - Etc.

1 Target reconnaissance - footprinting

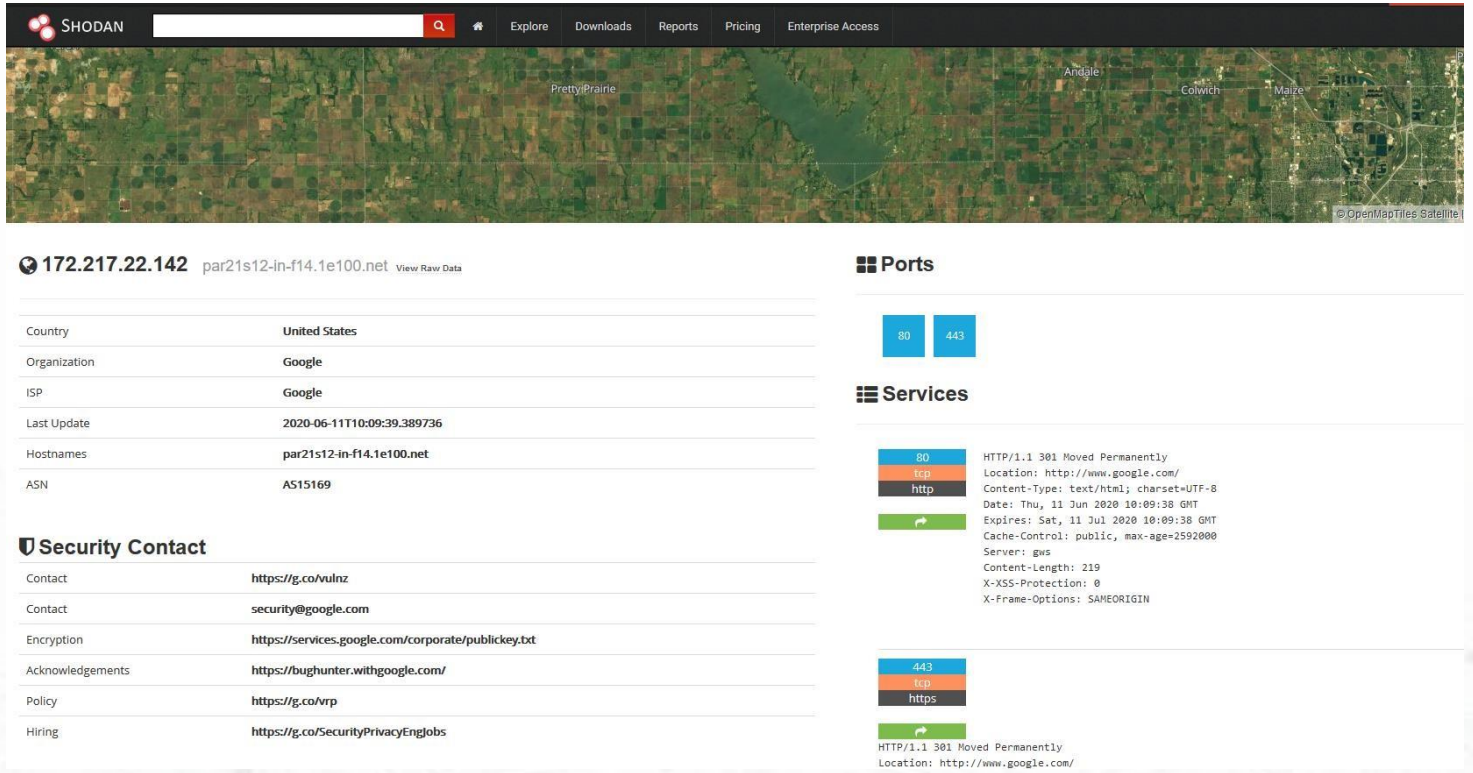
- Many tools can be used during this step :
  - Google Dorks (Hacks) :



Date Added	Dork	Category	Author
2020-06-12	index of .svn/text-base/index.php.svn-base	Files Containing Juicy Info	saivinayreddy
2020-06-12	intext:"index of /" "config.json"	Files Containing Juicy Info	Abinesh kamal K U
2020-06-12	intitle:"index of" "admin/sql/"	Sensitive Directories	Rutwik Shah
2020-06-12	intitle:"index of" admin.tar	Files Containing Juicy Info	Abhi Chitkara
2020-06-11	Dork: "index of" "Production.json"	Vulnerable Files	Swapnil Talele
2020-06-11	Dork: "Index of" "upload_image.php"	Vulnerable Files	Swapnil Talele
2020-06-11	index.of.?.frm	Vulnerable Files	Abhi Chitkara
2020-06-11	inurl:wp-content/plugins/brizy	Advisories and Vulnerabilities	Abhi Chitkara
2020-06-11	inurl:/servicedesk/customer/user/login	Footholds	Rutwik Shah
2020-06-10	inurl:".Admin;-aspx }" "~Login"	Pages Containing Login Portals	Anjali Prakash
2020-06-10	"index of" "svg"	Sensitive Directories	Mahesh Rai
2020-06-10	"Index of" "customer.php"	Files Containing Juicy Info	Prashant Sharma
2020-06-10	"login" intitle:"intext:"Welcome to Member" login"	Pages Containing Login Portals	Alexandros Pappas
2020-06-10	intitle:"index of" "survey.cgi"	Sensitive Directories	Mohammed Arif H

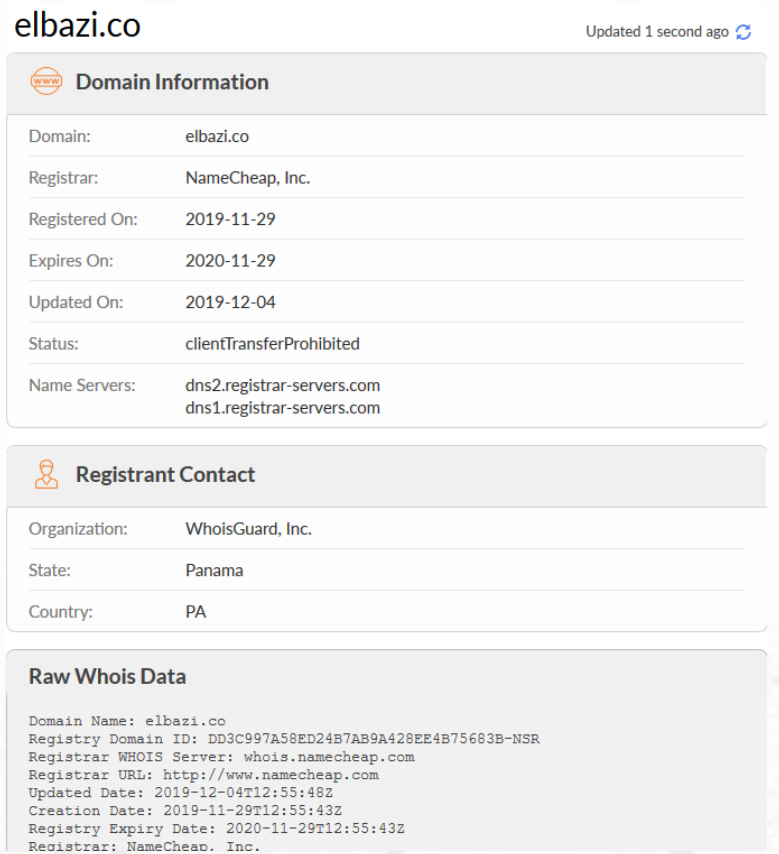
1 Target reconnaissance - footprinting

- Many tools can be used during this step :
  - Shodan(Search engine) :



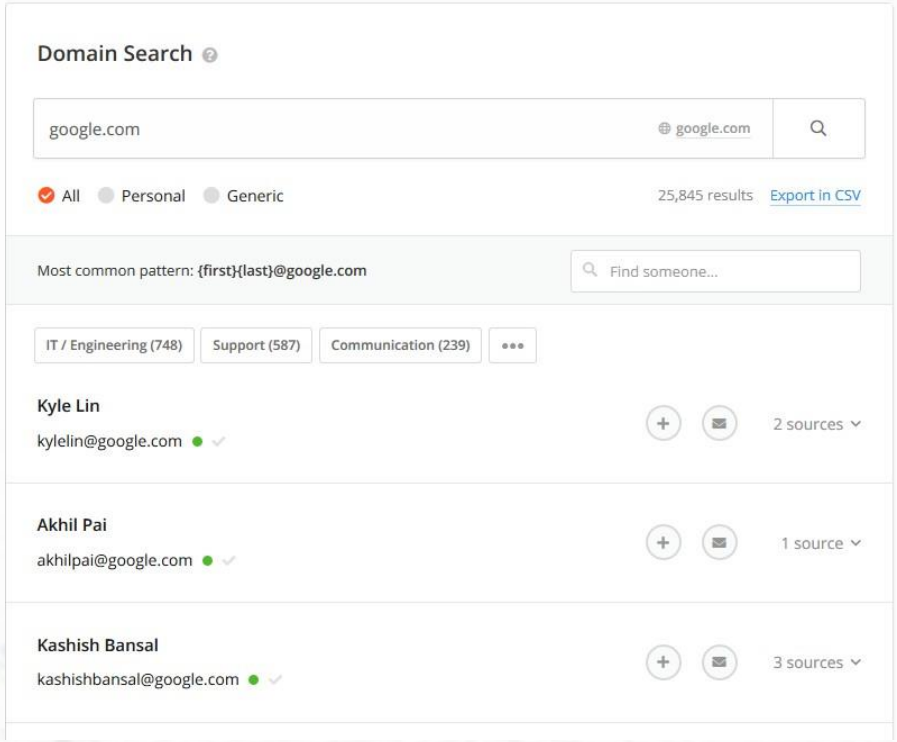
1 Target reconnaissance - footprinting

- Many tools can be used during this step :
  - WHOIS(Search engine) :



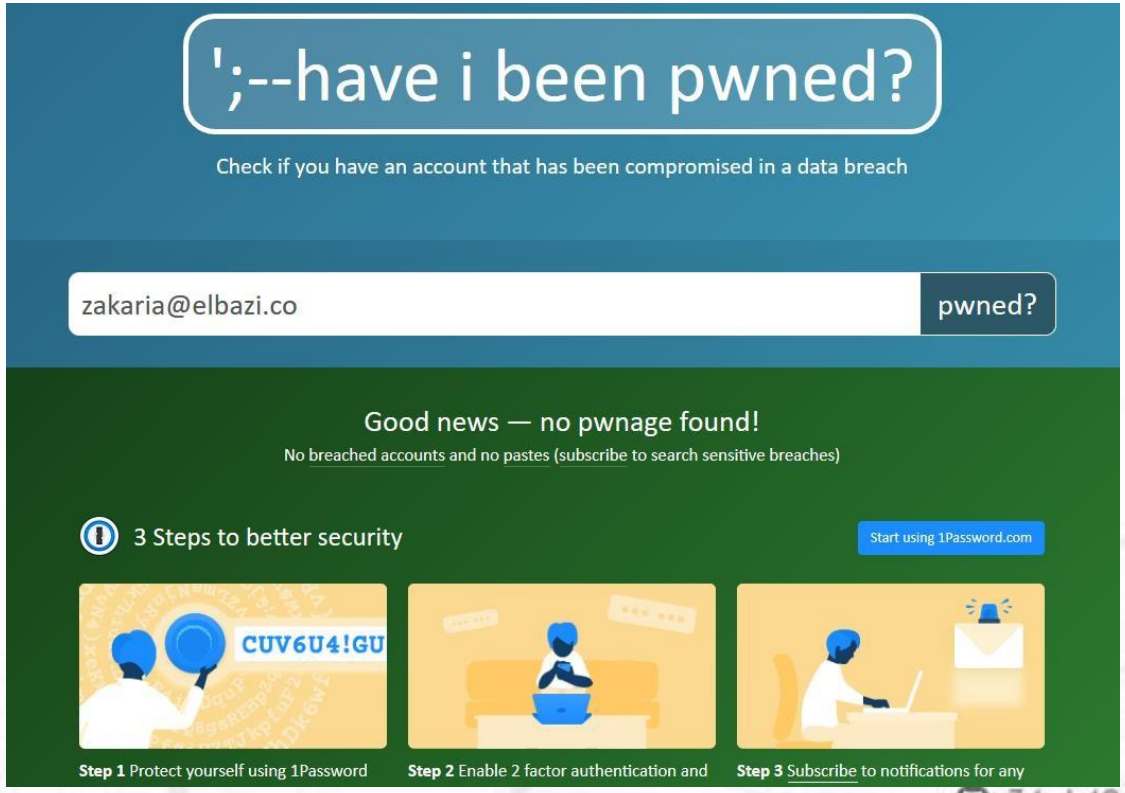
1 Target reconnaissance - footprinting

- Many tools can be used during this step :
  - Hunter.io(Contacts Search engine) :



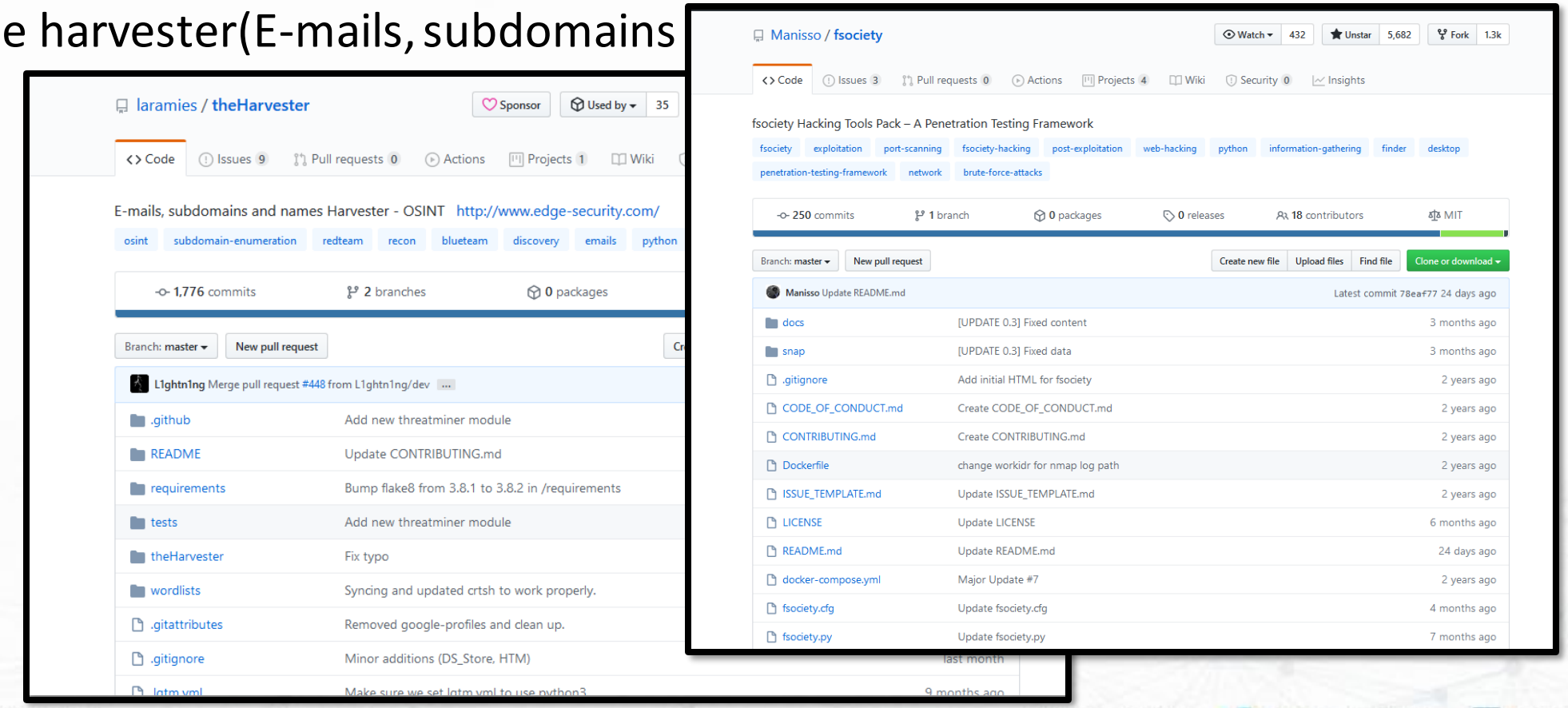
1 Target reconnaissance - footprinting

- Many tools can be used during this step :
  - Data Breaches(Contacts Search)/Dark web:



1 Target reconnaissance - footprinting

- Many tools can be used during this step :
  - The harvester(E-mails, subdomains



1 Target reconnaissance – social media

- Social media are one of the main source of information for hackers, since they provide free and easy to access information about individuals (personal information , interests, chat…) and companies (employees, clients, partners).

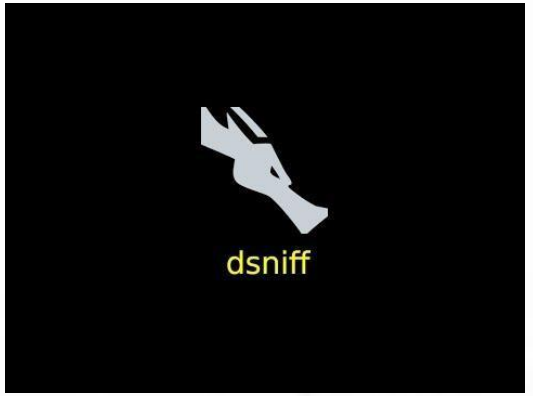
1 Target reconnaissance – social media

- **47% of social media users are seeing more spam in their feeds. Of them, 79% believe the spam includes fake news and cyber crimes. (HubSpot).**
- **30 million Facebook accounts were compromised in a data breach in 2018.**
- **You can purchase a consumer account for $1 on the dark market,** Bank accounts still cost more – **between $3 and $24** a piece.**(RSA)**

2 Target reconnaissance – scanning/sniffing

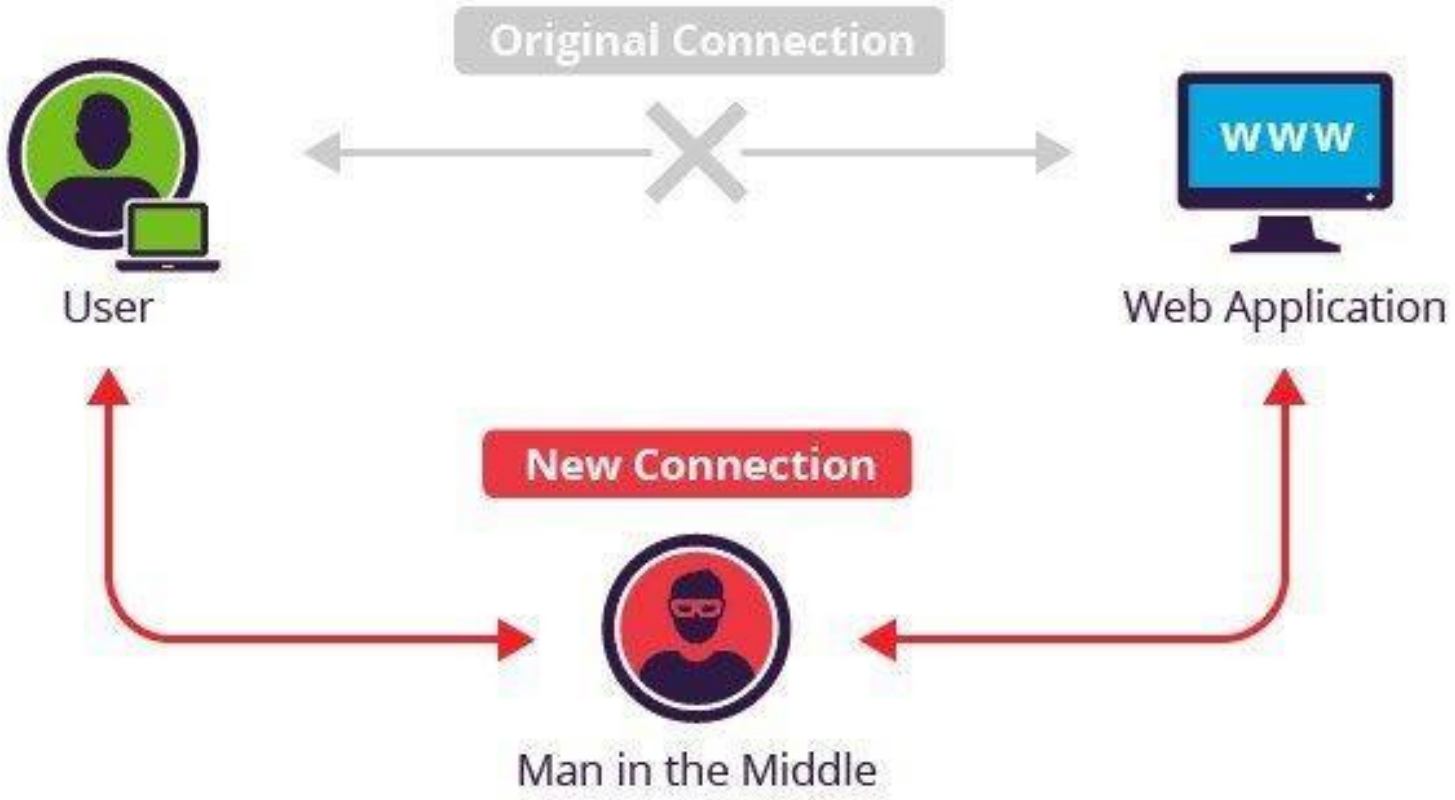
- Sniffing allows you to see all sorts of traffic, both protected and unprotected (Emails, FTP passwords, etc) by intercepting the network traffic using multiple tools and attacks :

Bettercap MITM



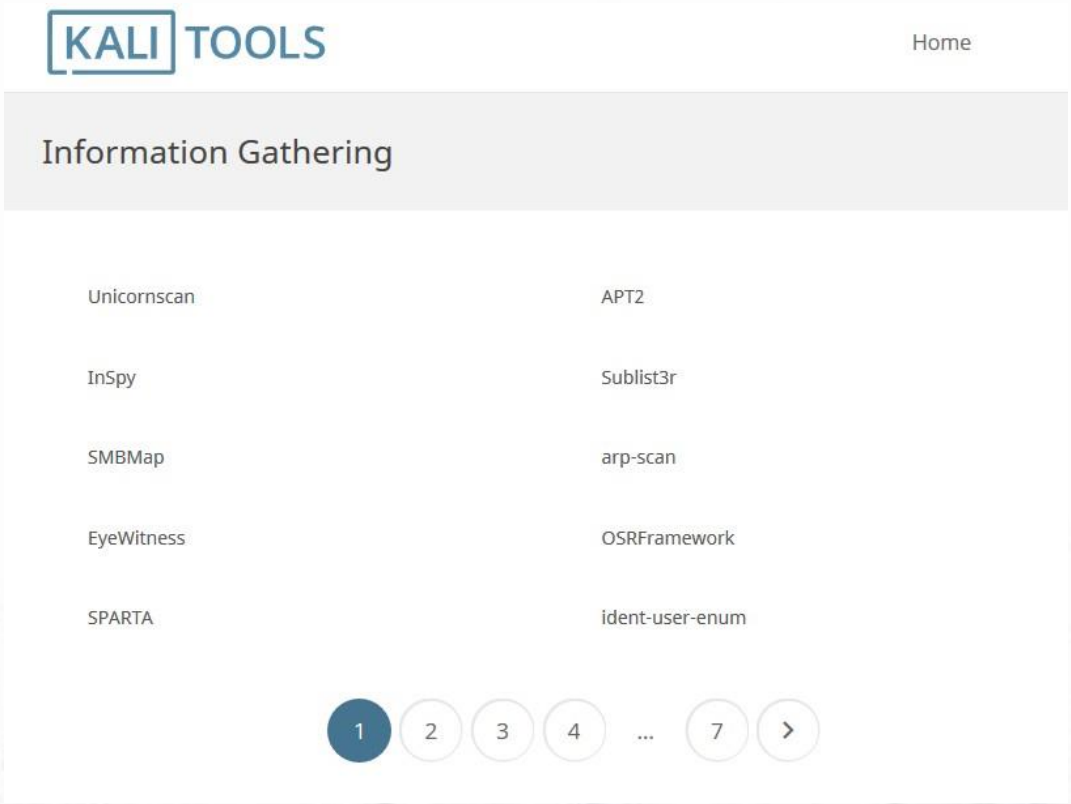
2 Target reconnaissance – scanning/sniffing

2 Target reconnaissance – scanning/sniffing (MITM)



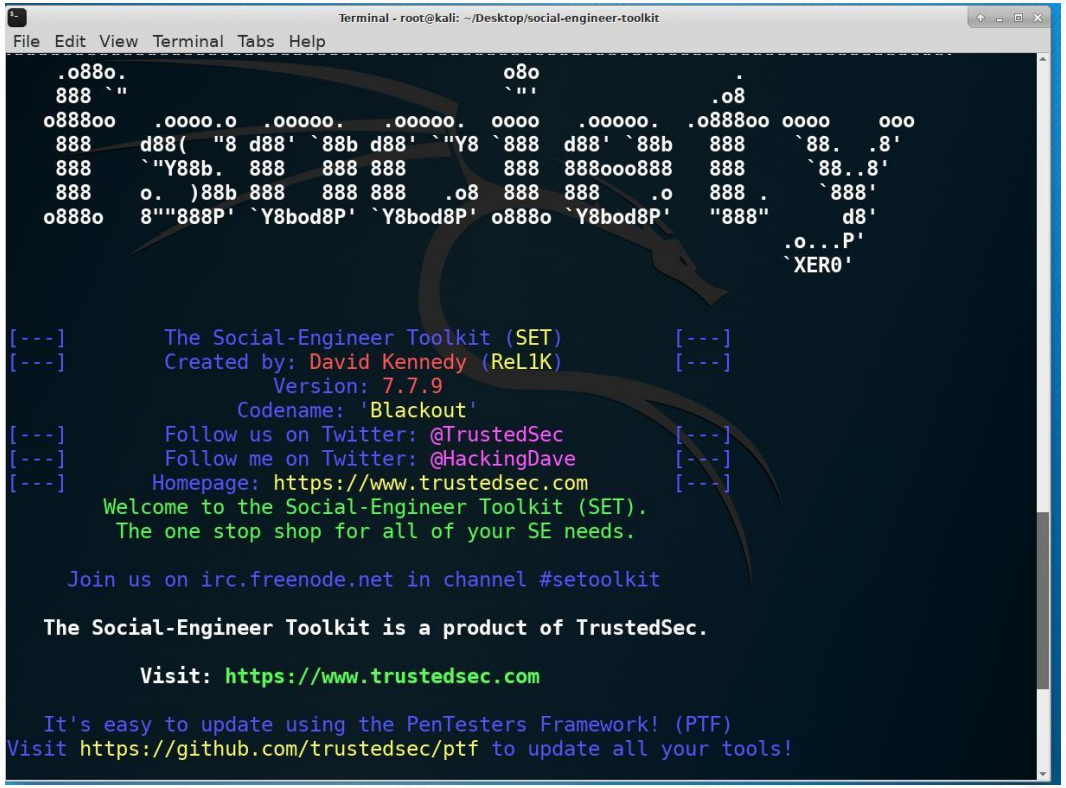
2 Target reconnaissance – Tools kali

- Many tools can be used during this step :



2 Target reconnaissance – social engineering

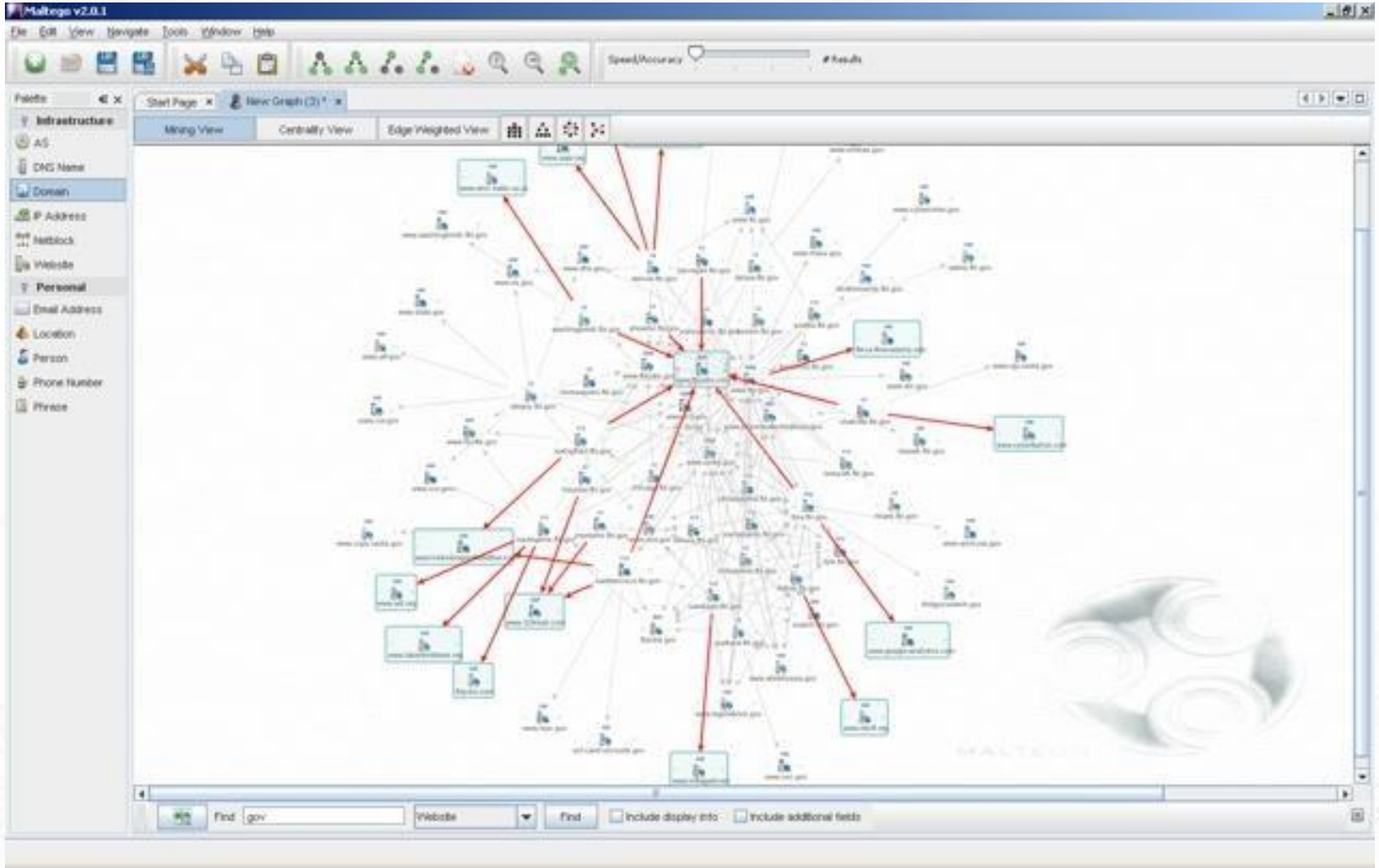
2 Target reconnaissance – social engineering



MALTEGO

2 Target reconnaissance – social engineering/Maltego

"Maltego does a lot of the automated and large data correlation for you, you can save hours of googling looking for information and determining where all that information correlates."



KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

Ethical hacking 2

Gaining & maintaining access

2 Gaining access

- This phase is **where an attacker breaks into the system/network**. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.
- This phases comes after gathering enough information about the target system/network.
- The attackers use various tools and methods:
  - Attacking target's network
  - Targeting an employee and get his credentials (social engineering, phishing,etc).
  - Etc.

2 Gaining access

- The tools or the methods used in this phase depends on the information the hacker could find in the target reconnaissance and scanning phases. (networks attacks in case he found interesting open and public wifi related to the company/partners) or phishing attacks if he could find email addresses and social accounts.
- Main techniques used :
  - Networks attacks (sniffing, man in the middle, evil twin, ARP poisoning, DNS spoofing, session hijacking, TCP/IP hijacking,Ping of death, DDOS, DNS flood,…).
  - **Social engineering.**
  - **Phishing attacks.**
  - **Stolen credentials.**

2 Gaining access / stats%

- **94% of malware was delivered via email** (Verizon DBIR 2019)
- **33% of breaches** included social attacks (Verizon DBIR 2019)
- **65% of attacker groups** used **spear phishing as the primary infection vector (Symantec ISTR 2019).**
- 66% of malware is installed via malicious email attachments (Verizon DBIR 2018)
- 29% of breaches involved use of stolen credentials (Verizon DBIR 2019)
- 48% of malicious email attachments are Office files(Verizon DBIR 2019)

2 Gaining access / stats%

- 32% of breaches involve phishing (Verizon DBIR 2019).
- 64% of organizations have experienced a phishing attack in the past year (Check point report 2018).
- 90% of incidences and breaches included a phishing element (Verizon DBIR 2017).
- **Phishing emails include fake notifications from banks, e-payment systems, email providers, social networks, online games, etc.** (Kaspersky lab report 2016).

2 Gaining access / phishing

2 Gaining access / phishing

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
  It occurs when an attacker, **masquerading as a trusted entity**, dupes a victim into opening an email, instant message, or text message.

- The recipient is then tricked into clicking a **malicious link**, which can lead to the **installation of malware**, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

2 Gaining access

- https://youtu.be/C4Uc-cztsJo

2 Gaining access / phishing

Madame, Mons

Vous devez vou
conditions pou

Avec cette étap
sont pas utilisé

Vous devez acc

Espace Client

Suivez les cons

- 1 Conne
- 1 Accep

Si vous avez de

Cordialement,

L'équipe Crédit

Google play

Nous vous informons que votre compte arrive à expiration dans moins de 48 heures , il est impératif d'effectuer un achat ou une vérification de vos informations dès à présent , sans quoi votre compte sera détruit .
Cliquez simplement sur le lien ci-dessous et ouvrez une session à l'aide de votre Android ID et de votre mot de passe .

Https://play.google.com/login/

Pourquoi ce courrier électronique vous a-t-il été envoyé ?
L'envoi de ce courrier électronique s'applique lorsque la date d'expiration de v
arrive à terme .

Pour plus d'informations , consulter la rubrique *Questions et réponses* .

Merci ,
L'assistance à la clientèle *Google Store* .

Amazon <management@mazoncanada.ca> on behalf of
not an Amazon email address (note the missing A in Amazon)

Suspension

amazon.com

r Client, ← Generic non-personalized greeting

have sent you this e-mail, because we have strong reason to belive, your account has been used by someone
e In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.
've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

confirm your identity with us click the link bellow:

chronopost

Cher(e) Client(e),
Vous avez un colis au bureau de poste.
Vous disposez d'un délai de 96 heures pour récupérer votre colis ,
Sinon il sera retourné à l'expéditeur .
Veuillez confirmer l'envoi du colis à votre domicile en suivant les étapes au dessous:
1: Appeler le Numero de notre service clients: 0903 51 959
2:Recevoir le code de confirmation
3:Envoyer le code de confirmation à l'adresse Mail suivante:
chronopostcodes@post.com

Si vous ne pouvez pas recevoir le code veuillez essayer d'appeler
jusqu'à x3 fois le numero en rouge au-dessus .

RE : [#02221] Amazon: Update your billing information

Traduire le message en : Français | Ne jamais traduire à partir de : Anglais

N no-reply@amzn-updtr.com
Jeu 26/03/2020 18:34
À : Vous

amazon

Update your billing information

Dear zakaria-elbaz[redacted]

We have placed a hold on your Amazon account and all pending orders.

We took this action the billing information you provided did not match the information on file with the card issuer.

To resolve this issue, please verify now with the billing name, address, and telephone number registered to your payment card. If you have recently moved, you may need to update this information with the card issuer.

Simply click on the button below :

Update now

If we are unable to complete the verification process within 3 days, all pending orders will be cancelled. You will not be able to access your account until this process has been completed. We ask that you not open new accounts as any new order you place may be delayed.

We appreciate your patience with our security measures.

Thank you for your concern.

Sincerely,

Amazon.com

RE : [#02221] Amazon: Update your billing information

telephone number registered to your payment card. If you have recently moved, you may need to update this information with the card issuer.

Simply click on the button below :

Update now

If we are unable to complete the verification process within 3 days, all pending orders will be cancelled. You will not be able to access your account until this

bogueur | Réseau | Éditeur de style | Performances | Mémoire | Stockage | Accessibilité | Adblock Plus

```
<table style="width:500px; margin:0 20px" cellspacing="0" cellpadding="0">
  <tbody>
    <tr> ... </tr>
    <tr> ... </tr>
    <tr> ... </tr>
    <tr>
      <td style="padding-left:0; padding-top:9px; padding-bottom:9px">
        <p style="margin:0px; font-size:14px; text-align:justify"> ... </p>
        <p style="margin:0px; font-size:17px; padding-top:18px">
          S
          <span>imp</span>
          ly c
          <span>lic</span>
          k on th
          <span>e bu</span>
          tton b
          <span>elo</span>
          w :
        </p>
        <a href="https://bci-ltd.com/.url/dZVOE" target="_blank" rel="noopener noreferrer" data-auth="NotApplicable" style="text-decoration:none; color:#333"> event
          <div style="border:0px; border-radius:3.5px; padding:10px; margin-top:3%; text-align:center; background-color:#FF9900"> ... </div>
        </a>
      </td>
    </tr>
    <tr>
      <td style="padding-left:0; padding-top:9px; padding-bottom:9px">
        <p style="margin:0px; font-size:14px; text-align:justify; color:#FF9900">
          If w
          <span>e ar</span>
          e un
```

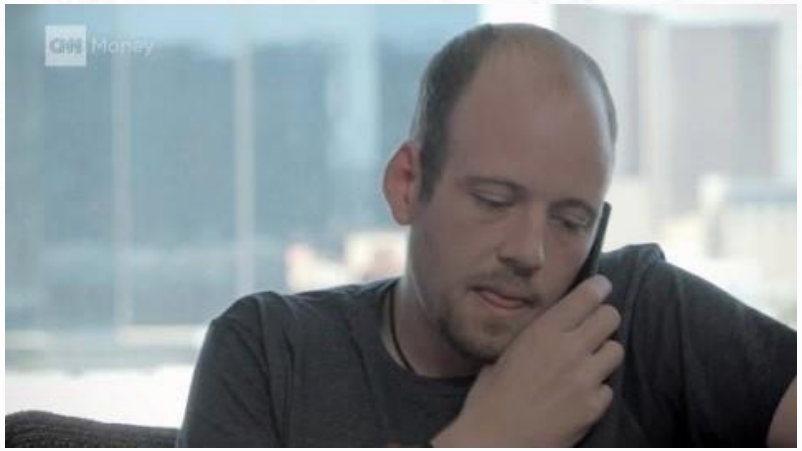
2 Gaining access / social engineering

- **Social engineering is** the term used for a broad range of malicious activities **accomplished through human interactions**. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- After gathering all the necessary information about the target, the attacker moves to gain the target's trust in order to get sensitive information for him or give him access to the system.
  - (pretending to be from the support team of a software the company uses for example)

2 Gaining access / social engineering

2 Gaining access / social engineering

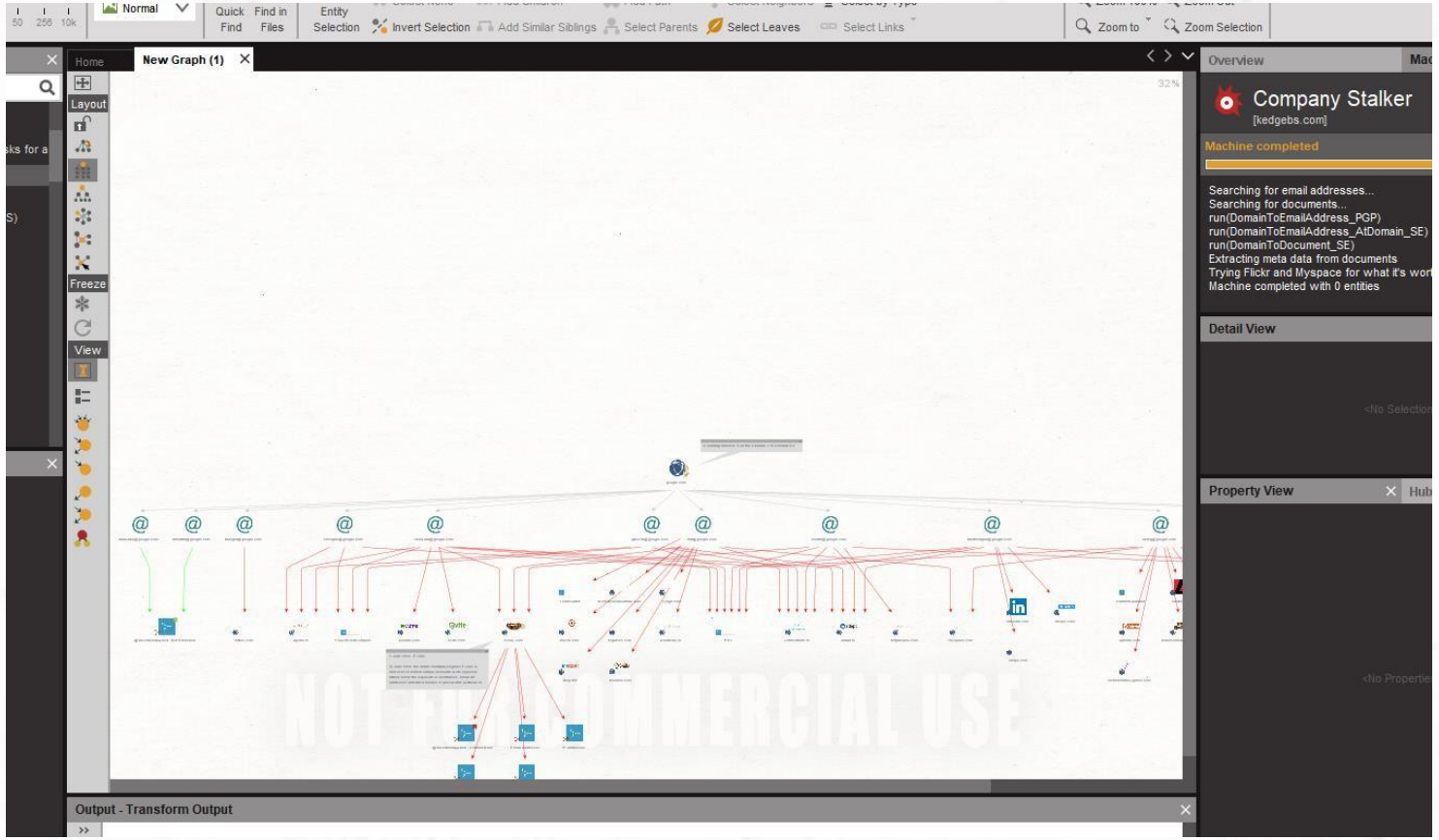
- Social engineering tools :
  - Human interactions.
  - SET (social engineering toolkit), fsociety, etc.
- **Social engineering methods:**
  - Scareware (adwares can be useful for this).
  - Pretexting.
  - **Phishing** (can be general, like an amazon or PayPal spam email)
  - **Spear phishing** (targeted and sophisticated phishing) **:**
    - Replying to job offers from the company.
    - Target specific employees, etc.



https://youtu.be/PWVN3Rq4gzw
A hacker breaking into a company with just a phone call !

https://youtu.be/lc7scxvKQOo
Getting credentials with just a phone call ! (**vishing attack**)

2 Gaining access / stolen credentials



Services providing credentials monitoring : https://alternativeto.net/software/firefox-monitor/

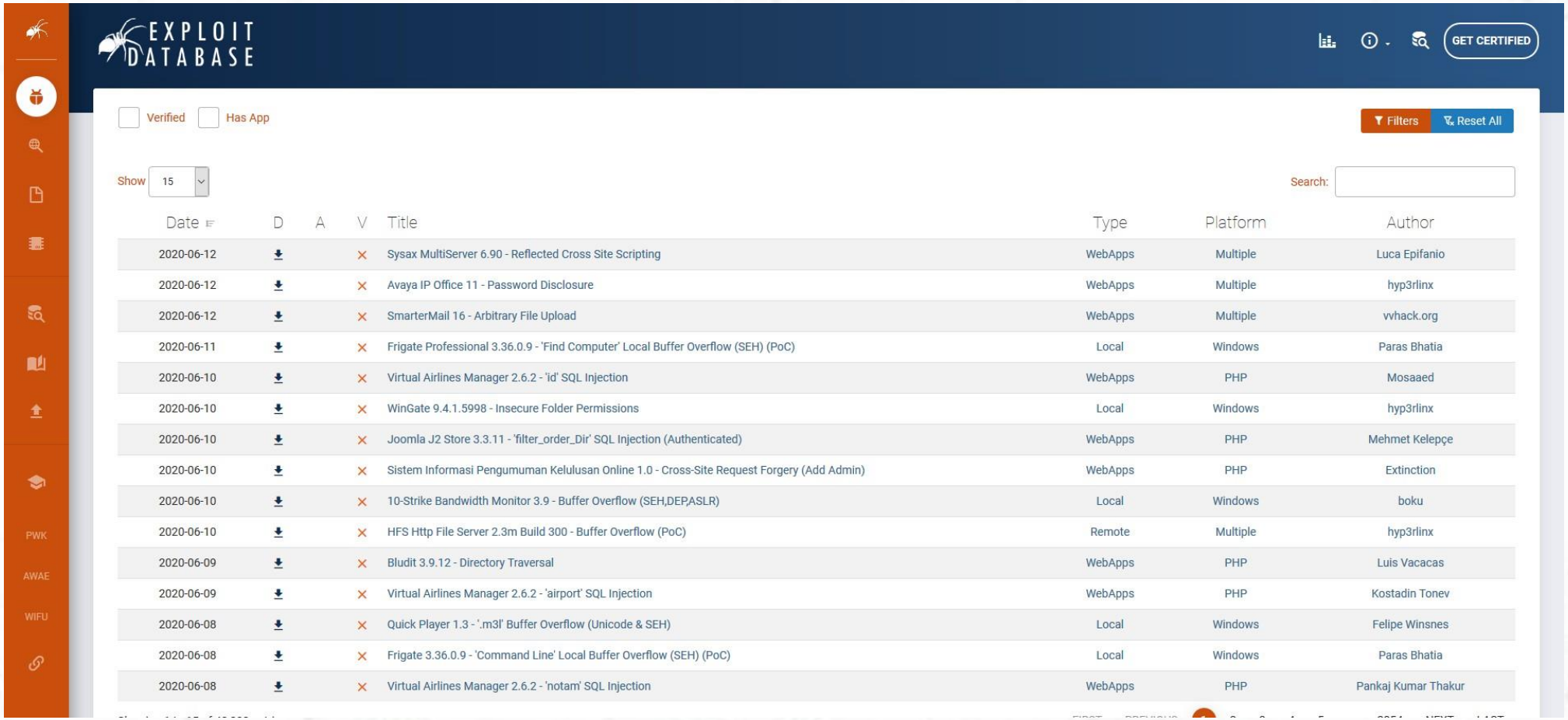
2 Gaining access / Exploitation

- Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities.
- Hackers normally use vulnerability scanners like **Nessus**, **Nexpose**, **OpenVAS**, etc. to find these vulnerabilities or try your systems against known or recent vulnerabilities.
- The main tool for this is as mentioned earlier in this course, **Metasploit**.

2 Gaining access / Exploitation

- Knowing OS target information/ configuration for example (**from the Recon phase**) will let you generate adapted trojans, keyloggers to exploit a specific vulnerability in his system.
- These trojans can be delivered with social engineering and mainly phishing as the statistics shows.

2 Gaining access / Exploitation



Date	D	A	V	Title	Type	Platform	Author
2020-06-12				Sysax MultiServer 6.90 - Reflected Cross Site Scripting	WebApps	Multiple	Luca Epifanio
2020-06-12				Avaya IP Office 11 - Password Disclosure	WebApps	Multiple	hyp3rlinx
2020-06-12				SmarterMail 16 - Arbitrary File Upload	WebApps	Multiple	vvhack.org
2020-06-11				Frigate Professional 3.36.0.9 - 'Find Computer' Local Buffer Overflow (SEH) (PoC)	Local	Windows	Paras Bhatia
2020-06-10				Virtual Airlines Manager 2.6.2 - 'id' SQL Injection	WebApps	PHP	Mosaaed
2020-06-10				WinGate 9.4.1.5998 - Insecure Folder Permissions	Local	Windows	hyp3rlinx
2020-06-10				Joomla J2 Store 3.3.11 - 'filter_order_Dir' SQL Injection (Authenticated)	WebApps	PHP	Mehmet Kelepçe
2020-06-10				Sistem Informasi Pengumuman Kelulusan Online 1.0 - Cross-Site Request Forgery (Add Admin)	WebApps	PHP	Extinction
2020-06-10				10-Strike Bandwidth Monitor 3.9 - Buffer Overflow (SEH,DEP,ASLR)	Local	Windows	boku
2020-06-10				HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)	Remote	Multiple	hyp3rlinx
2020-06-09				Bludit 3.9.12 - Directory Traversal	WebApps	PHP	Luis Vacacas
2020-06-09				Virtual Airlines Manager 2.6.2 - 'airport' SQL Injection	WebApps	PHP	Kostadin Tonev
2020-06-08				Quick Player 1.3 - '.m3l' Buffer Overflow (Unicode & SEH)	Local	Windows	Felipe Winsnes
2020-06-08				Frigate 3.36.0.9 - 'Command Line' Local Buffer Overflow (SEH) (PoC)	Local	Windows	Paras Bhatia
2020-06-08				Virtual Airlines Manager 2.6.2 - 'notam' SQL Injection	WebApps	PHP	Pankaj Kumar Thakur

KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

2 Gaining access / Exploitation

CVE® Common Vulnerabilities and Exposures

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD Go to for: CVSS Scores CPE Info

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 137286

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

Latest CVE News

- CVE Board Charter Updated to Version 3.2
- Xiaomi Added as CVE Numbering Authority (CNA)
- GitLab Added as CVE Numbering Authority (CNA)

More News >>

CVE Blog

CVE Program Report for Calendar Year Q1-2020 Now Available

CY Q1-2020 Milestones - CVE Numbering Authorities (CNAs), CVE Board, CVE Working Groups, and more
CY Q1-2020 Metrics - CVE Entries and requests for CVE IDs from the CVE Program Root CNA

Read More >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Entry is added to the CVE List by a CNA.

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Total CNAs: 128 | Total Countries: 21

Learn How to Become a CNA >>>

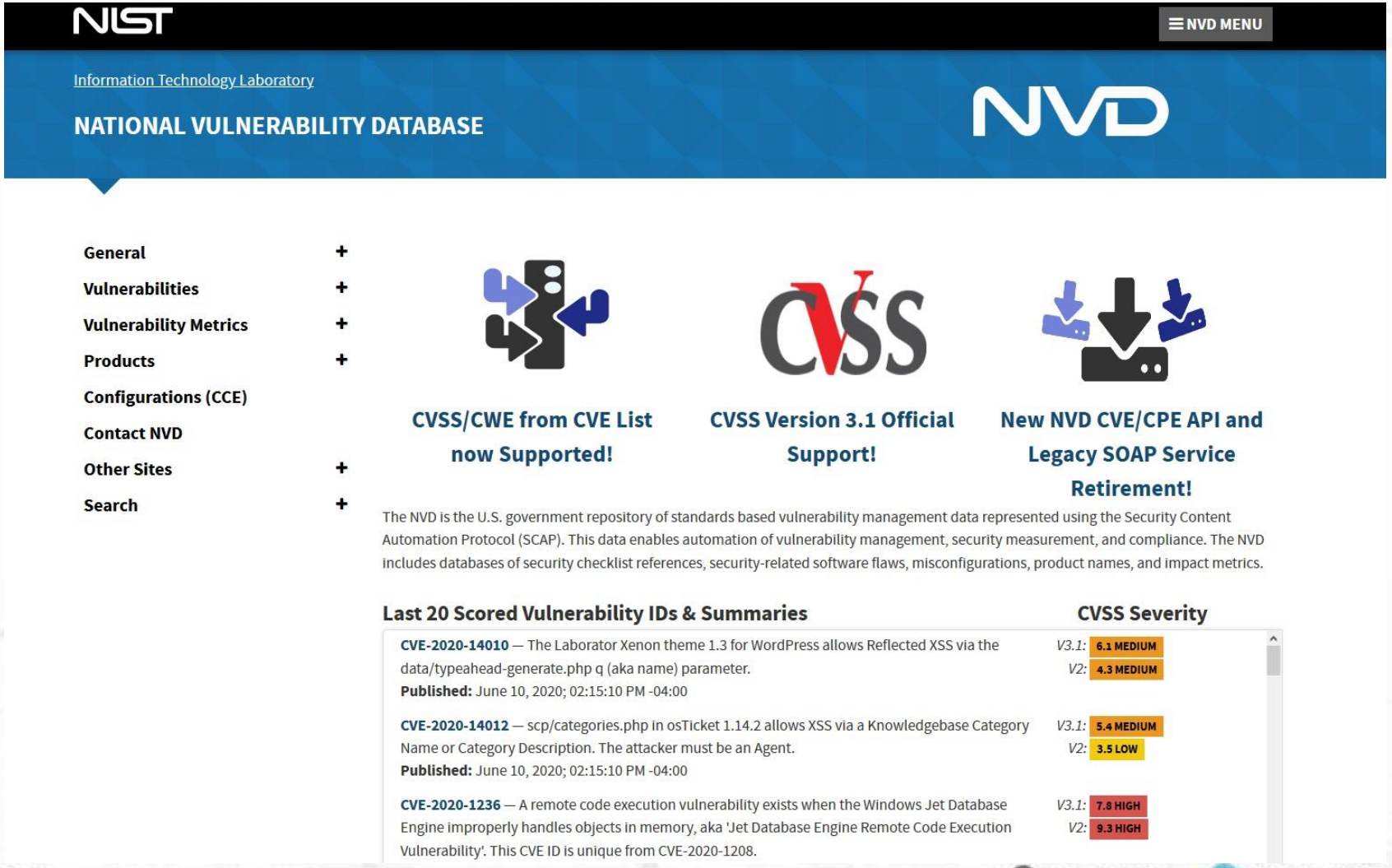
Watch CNA Onboarding Videos >>

Newest CVE Entries

Newest CVE IDs by @CVEnew

Follow @CVEnew >>

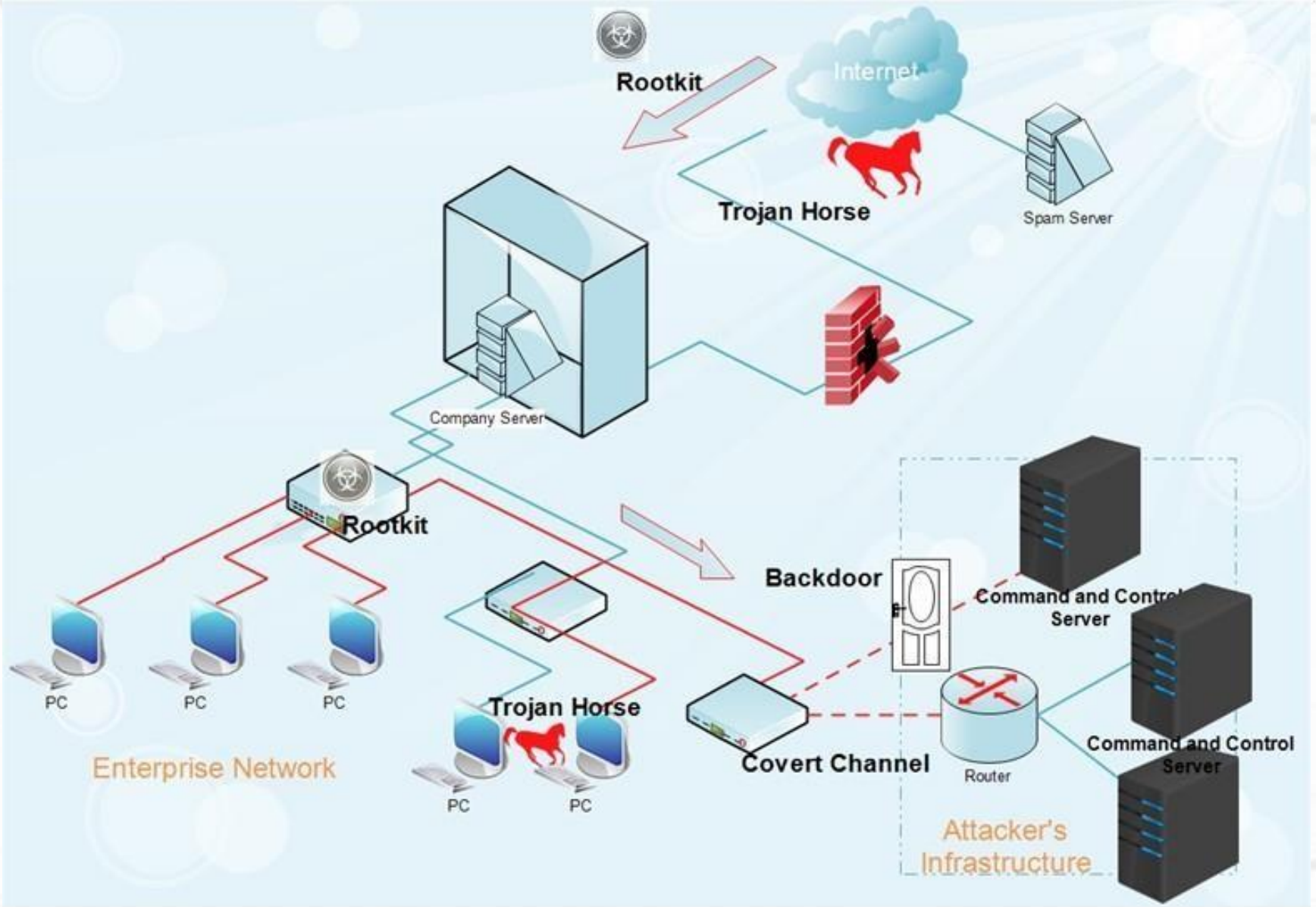
2 Gaining access / Exploitation



3. Maintaining access / Exploitation

3. Maintaining access / Exploitation

- Once a hackers has gained access, they want to keep that access for future exploitation and attacks.
- Once the hacker owns the system (Zombie system), they can use it as a base to launch additional attacks.
- **Methods to maintain access :**
  - **Backdoors :** Trojan is a convenient tool for establishing easy access into the already breached system. A trojan horse provides access at the application level, but to gain it, the user needs to install the piece of malware locally.
  - A **convert channel** (using specific data exchange protocols such us VoIP, HTTP, etc.) to get data from inside the network.
  - **Rootkits** & **Malwares.**


Rootkit
Internet
Trojan Horse
Spam Server
Company Server
Rootkit
Backdoor
Command and Control Server
PC
PC
PC
Trojan Horse
Enterprise Network
PC
PC
Covert Channel
Router
Command and Control Server
Attacker's Infrastructure

4. Clearing tracks

- Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed “noisy”.
- Once access is gained and privileges have been escalated, the hacker seek to cover their tracks by deleting :
  - Sent emails.
  - Server logs.
  - Temp files.
  - Etc.

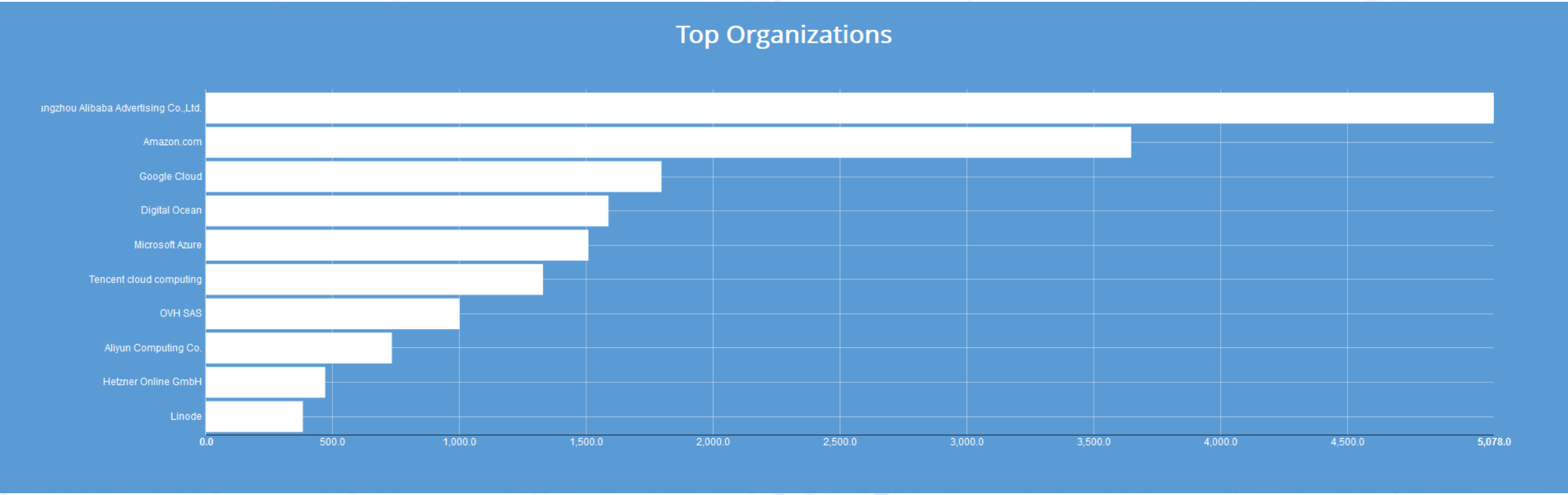
5. Clouds attacks / stats%

- **24%** of organizations have hosts missing high-severity patches in public cloud.
- **49%** of databases are not encrypted.
- **73%** of security professionals who report that their organization has not implemented a privileged account security solution for DevOps.
- An average of **51%** of organizations publicly exposed at least one cloud storage service.
- Only **12%** of global IT organizations understand how GDPR will affect their cloud services.

4. Clouds attacks

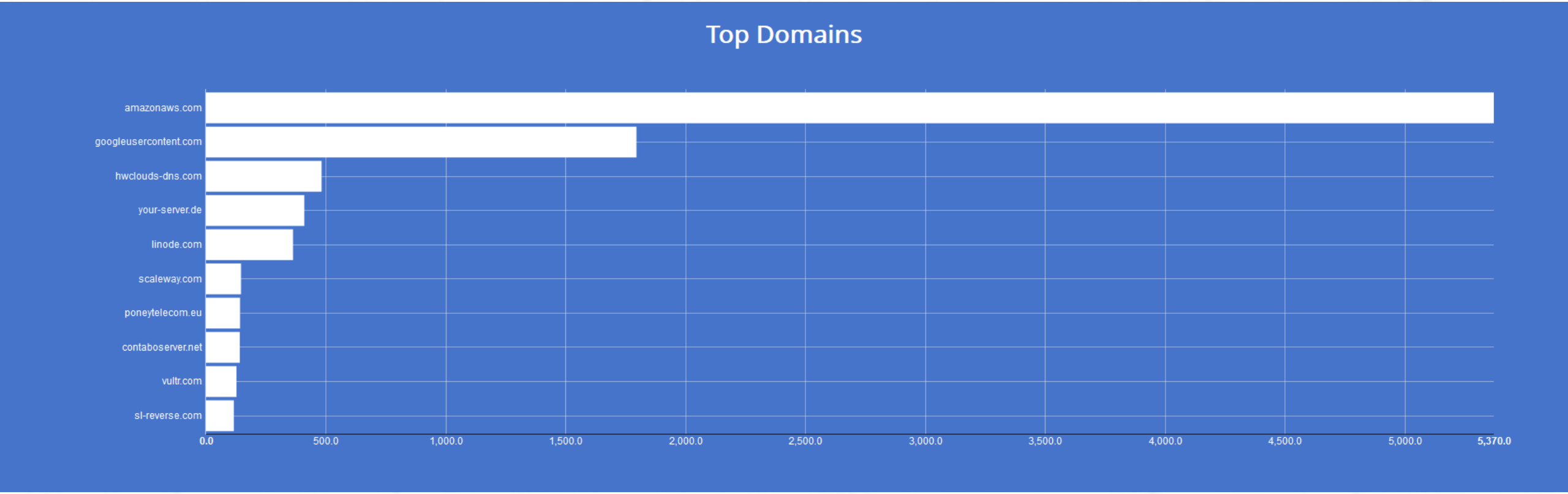
- Performing DDOS attacks against your cloud infrastructure to exhaust server resources.
- Exploiting VM / containers vulnerabilities.
- API security flaws (the main component of SaaS solutions).
- Insufficient out-of-the-box security provided by cloud providers.
- AI-based attacks (attacks than can be adapted to your security stack).

4 Clouds attacks



Exposed elasticsearch clusters, by shodan

4 Clouds attacks



Exposed elasticsearch clusters, by shodan

4 IoT attacks

- **Connected devices has become a primary attack vector for hackers, because of their lack of security:**
  - **Smart cameras**
  - **Connected office tools,**
  - **Etc.**
- **These connected devices can be easily found using mass scan tools (Shodan, Zoomeye,etc.)**
- **Most known attack performed with hacked IoT :**
  - **The Mirai Botnet**

    "Back in October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN."

KEDGE BUSINESS SCHOOL

Excelerate SYSTEMS

4 IoT attacks

Cyberattacks On IOT Devices Surge 300% In 2019

14 688 views | Sep 14, 2019, 02:42am EDT

Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.

[redacted]

Forbes


KEDGE
BUSINESS SCHOOL
Excelerate
SYSTEMS
Cyber security
What we can do to secure our systems/data ?
excelerate systems.com
Z4ck404
Zack_ELBAZI
zakaria-elbazi

1 Cyber security

Being able to **detect** and **prevent** any unauthorized use or access to your system/data by securing each layer in our system.

- **Network security :** securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security :** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect.
- **Information security :** protects the integrity and privacy of data, both in storage and in transit.

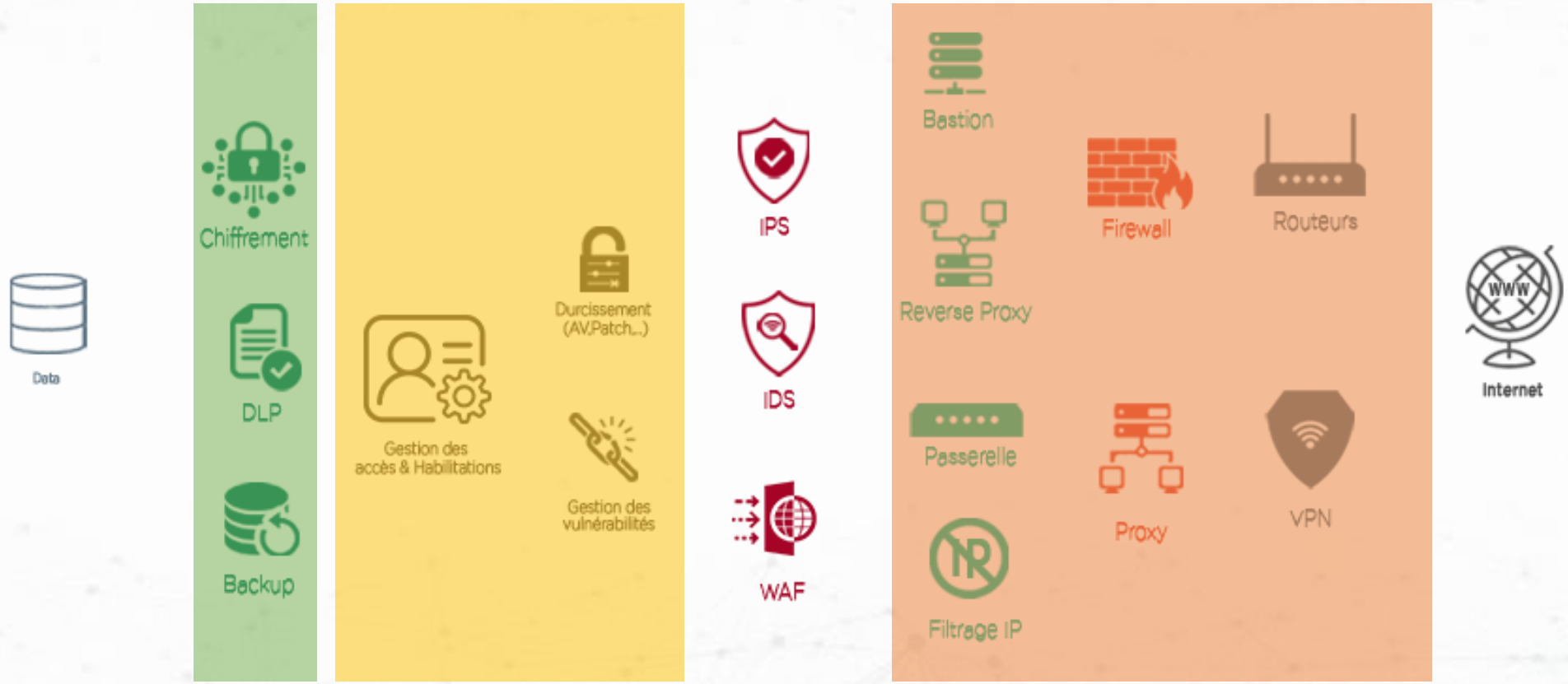
1 Cyber security

- **Operational security :** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella. (roles and permissions).
- **Disaster recovery and business continuity :** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices.

KEDGE BUSINESS SCHOOL

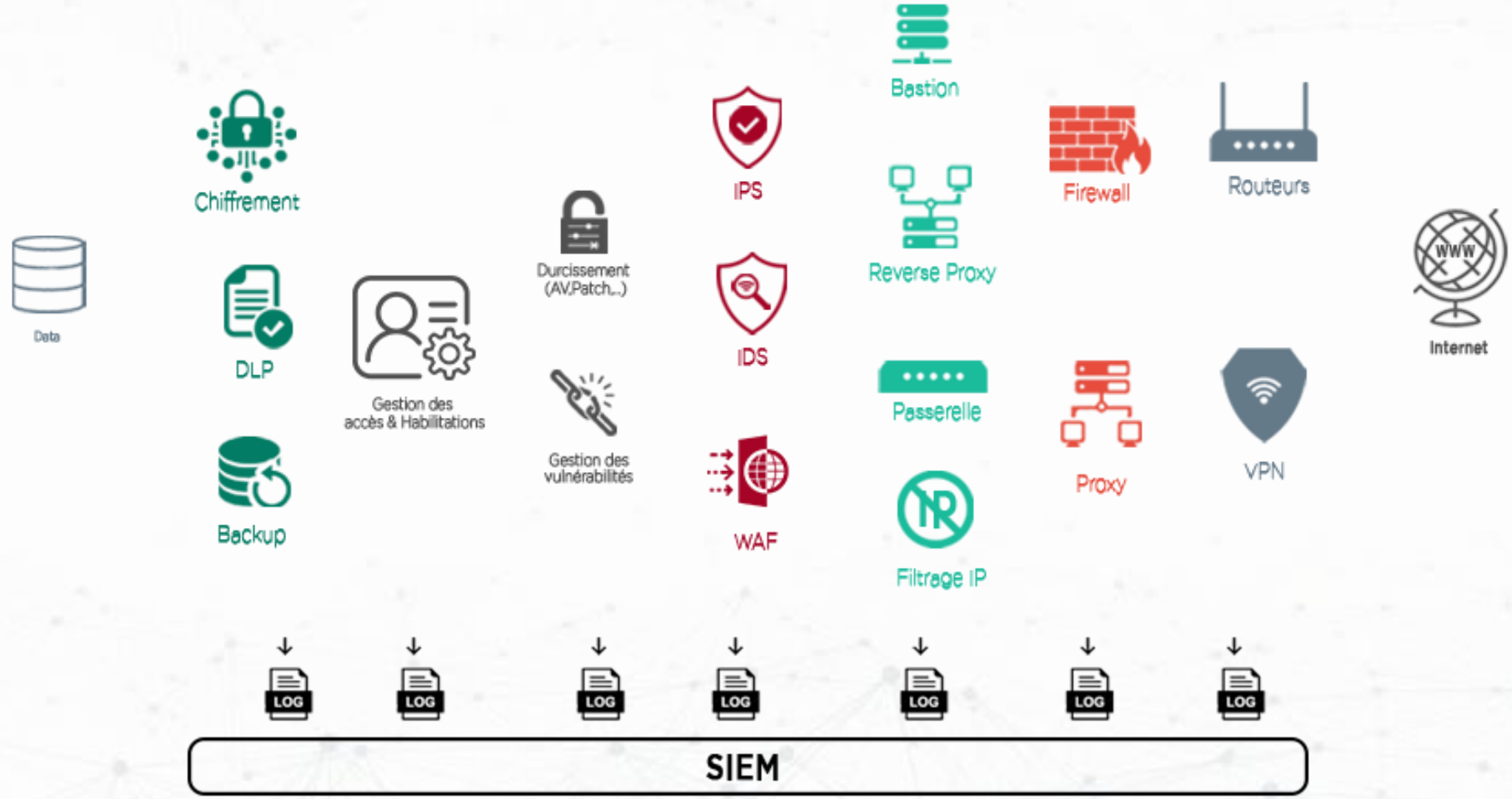
Excelerate SYSTEMS

1 Cyber security



kaspersky

1 Cyber security



2 Compliance

- In cybersecurity, compliance means **creating a program that establishes risk-based controls** to protect the integrity, confidentiality, and accessibility of information stored, processed, or transferred.
- cybersecurity compliance is not based in a stand-alone standard or regulation. It depends on the industry.
  - **HIPPA (Healthcare Insurance Portability and Accountability Act).**
  - **PCI DSS (Payment Card Industry Data Security Standard).**
  - **NERC (electrical power industry)**
  - **ISO/IEC 27001 27002 (Information management security system) – multiple industries can adopt it.**
  - **Etc.**

2 Compliance

- In cybersecurity, compliance means **creating a program that establishes risk-based controls** to protect the integrity, confidentiality, and accessibility of information stored, processed, or transferred.
- cybersecurity compliance is not based in a stand-alone standard or regulation. It depends on the industry.
  - **HIPPA (Healthcare Insurance Portability and Accountability Act).**
  - **PCI DSS (Payment Card Industry Data Security Standard).**
  - **NERC (electrical power industry)**
  - **ISO/IEC 27001 27002 (Information management security system) – multiple industries can adopt it.**
  - **Etc.**

2 Compliance / General guide

1. **Establish a Risk Analysis :**
    1. Identify all information assets and information systems, networks, data.
    2. Review risk level of each data type. Identify high risk information that is stored, transmitted, and collected.
    3. Analyzing the risk : Risk = (Liklihood of Breach x Impact)/Cost
    4. Set Risk Tolerance.

2 Compliance / General guide

2. **Set controls:**
    1. Firewalls
    2. Encryption
    3. Password policies
    4. Employee training.

2 Compliance / General guide

3. Creating internal policies.
   - Password policies.
   - Email policies.
   - Handling sensitive data.
   - Handling an incident.

2 Compliance / General guide

4. Continuously Monitor and Respond: Monitoring and threat detection

2 Cyber security as a service (CSAAS)

- outsourcing information security tasks to maintain a more robust Cybersecurity stance. Traditionally, CSaaS providers offer a security **operations center (SOC)**, **security information and events management (SIEM) system**, or both.

- Recommended for small and mid sized companies.
- Cost effective and easily scalable.