Internet of Things and Cyber-Physical Systems 3 (2023) 280–308

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

Ethical hacking for IoT: Security issues, challenges, solutions and recommendations

Jean-Paul A. Yaacoub [a], Hassan N. Noura [a], Ola Salman [b,*], Ali Chehab [b]

[a] Univ. Bourgogne Franche-Comté (UBFC), FEMTO-ST Institute, CNRS, Belfort, France
[b] American University of Beirut, Department of Electrical and Computer Engineering, Lebanon

ARTICLE INFO

Keywords:
Internet-of-things (IoT)
IoT ethical hacking
IoT penetration testing
Internet of ethical hacking things (IoEHT)
IoT cyber-security

ABSTRACT

In recent years, attacks against various Internet-of-Things systems, networks, servers, devices, and applications witnessed a sharp increase, especially with the presence of 35.82 billion IoT devices since 2021; a number that could reach up to 75.44 billion by 2025. As a result, security-related attacks against the IoT domain are expected to increase further and their impact risks to seriously affect the underlying IoT systems, networks, devices, and applications. The adoption of standard security (counter) measures is not always effective, especially with the presence of resource-constrained IoT devices. Hence, there is a need to conduct penetration testing at the level of IoT systems. However, the main issue is the fact that IoT consists of a large variety of IoT devices, firmware, hardware, software, application/web-servers, networks, and communication protocols. Therefore, to reduce the effect of these attacks on IoT systems, periodic penetration testing and ethical hacking simulations are highly recommended at different levels (end-devices, infrastructure, and users) for IoT, and can be considered as a suitable solution. Therefore, the focus of this paper is to explain, analyze and assess both technical and non-technical aspects of security vulnerabilities within IoT systems via ethical hacking methods and tools. This would offer practical security solutions that can be adopted based on the assessed risks. This process can be considered as a simulated attack(s) with the goal of identifying any exploitable vulnerability or/and a security gap in any IoT entity (end devices, gateway, or servers) or firmware.

1. Introduction

Due to the pervasive nature of IoT systems in our daily lives and our constant ongoing reliance on them, the protection of IoT, although critical, is not that efficient due to the poor or absence of the right security measures, for such a tremendous number of devices (75.44 billion by 2025, compared to 15.41 in 2015) [1], of which most of them are resource-constrained [2].

Malicious attackers are exploiting the IoT existing vulnerabilities and security gaps [3], especially those caused by third parties [4]), which are due to poorly and hastily configured IoT devices, gateways, servers, networks. Thus, rendering the applications prone to cyber-physical attacks. This paper presents the concepts of ethical hacking, penetration testing and vulnerability assessment in the context of IoT, and discusses the different types of security vulnerabilities and attacks that could be led against IoT components, along with their impact in terms of the essential security services, mainly, confidentiality, integrity, availability, and authentication. Moreover, the lack of training and awareness among employees and IT staff is also problematic, especially with the advanced techniques of social engineering. Thus, a framework is presented, from the users' perspective, based on the main IoT domains.

In general, periodic and effective penetration testing and ethical hacking are mandatory. This can be achieved by evaluating the levels of security/safety against known vulnerabilities and threats and consequently attacks via vulnerability assessment, foot-printing, and risk evaluation. This work also highlights the importance of using machine learning solutions to build automated security measures for IoT systems for early detection of any possible vulnerability, and consequently, to avoid the corresponding attacks.

The main objective of this work is to highlight the importance of ethical hacking in performing and conducting penetration testing on IoT systems against a variety of cyber attacks [5]. This helps with the evaluation of the levels of security and immunity of a given IoT entity against known and unknown threats, through assessment and mitigation, and thus, increases the levels of awareness, safety and security.

* Corresponding author.
E-mail address: oms15@mail.aub.edu (O. Salman).

https://doi.org/10.1016/j.iotcps.2023.04.002
Received 29 December 2022; Received in revised form 1 April 2023; Accepted 7 April 2023
Available online 25 April 2023

1.1. Related work

Our paper expands the already presented work which discusses the importance of ethical hacking [6,7] and penetration testing [8,9] in a both general and generic manner. Moreover, recent studies also analysed the digital forensics and anti-forensics concept for IoT systems and components, which is presented, described, and analysed in Refs. [10,11] but with little or no information concerning the ethical hacking, nor its relation with the IoT. In addition to what is presented, this paper studies and analyses the motivations of ethical hackers after identifying and classifying them to supplement the work done in Refs. [12,13] to identify the main IoT vulnerabilities and consequently attacks [14] that can be detected, avoided and mitigated through simulated ethical hacking attacks as part of penetration testing, and to suggest suitable security solutions and modern countermeasures. Moreover, this paper assesses the main IoT vulnerabilities and specifies IoT-related risks and how to mitigate them, while analyzing different approaches from different authors. Unlike the presented work in Ref. [15], which analyses the current cyber-security certification schemes, our work focuses on the main security threats, attacks, and issues that can affect the IoT domain from an ethical hacking perspective [16]. presented IoT-related security attacks that can be mitigated using Machine Learning (ML) methods. However, this work rather relies on the adoption of the ethical hacking concept where ML is one of the main security solutions. Moreover [17], discussed security-related challenges and threat sources in IoT applications. Additionally, this work includes discussing security-related issues against IoT servers, devices, systems, and applications alike [18]. presented an analysis of IoT security from 2016 to 2018, its trends, and open issues. However, this work rather focuses on current and recent issues that surround the IoT domain instead, especially from a cyber-security viewpoint [19]. presented a study on the state-of-the-art IoT security threats, vulnerabilities, and possible attacks while presenting possible solutions for improving the IoT security architecture. In addition to the presented work, our paper further expands this work, while also discussing real-case attacks and zero-day exploits, as well as the proper security measures and counter-measures that are or should be adopted to avoid similar attack cases. For the best of our knowledge, ethical hacking for IoT systems is partially described with no in-depth discussion nor a close linkage together with the IoT systems. Therefore, there's a need for a work that discusses the possible implementation of Ethical hacking in several IoT key parts. Unlike previous surveys, this paper covers the appliance of ethical hacking in a variety of IoT fields, especially medical [5], cyber-physical [20], long-range [21] and power-lines communications [22], as well as robotics [23,24].

1.2. Contribution

In this paper, a new holistic and analytical viewpoint is presented to offer a better understanding of how ethical hacking and penetration testing can be linked and applied to IoT systems mainly through a vulnerability assessment. In fact, the importance of this work is that it focuses on covering even a broader range of IoT vulnerabilities, challenges, threats, and consequently attacks while analyzing their presented security solutions based on all the targeted IoT components, which are listed in Fig. 6.

Thus, the contributions of this paper can be summarised as follows:

- **Methodical Way:** of classifying and analyzing IoT hackers based on their motives and gains in a more detailed and specific way.
- **Analytical Study:** of how to assess IoT vulnerabilities in terms of IoT-related risks.
- **Analysis:** of most known IoT attacks, their structure, and how to mitigate them.
- **Detailed Understanding:** on how penetration testing is linked to ethical hackers, and how ethical hackers conduct their penetration testing in the IoT domain while presenting different approaches from different authors.
- **Evaluation:** of how penetration testing is used to evaluate the security and protection levels in IoT against different possible potential attacks.
- **Security & Safety Procedures:** are presented in a suitable way that maintains a secure environment pre/post and during an IoT incident.
- **Presentation and Analysis:** of vulnerabilities based on each component of IoT entity.

1.3. Organisation

This paper is divided into ten sections aside the introduction and is presented as follows (see Fig. 1): in section 2, the IoT background and overview are presented including IoT systems, applications, vulnerabilities via penetration testing, in addition to the identification of hackers including their motives and gains. In section 3, cyber-attacks against different IoT fields are presented, including their types and activities. Real-case events, vulnerability exploits and assessment against IoT systems are presented in section 4. In section 5, the ethical hacking domain is presented in terms of IoT, including its life-cycle, tools, challenges and issues. section 6, penetration testing is further expanded in terms of IoT, including its testing tools, knowledge types, testing appliance and existing solutions. IoT security and safety procedures are presented in section 7, especially in terms of IT security policy and incident response. The lessons learnt are presented in section 8, while future research directions, suggestions and recommendations are presented in section 9 and section 10, respectively. In section 11, we conclude our work.

2. IoT: background & overview

The remarkable rise of IoT devices and domains, requires a significant innovation that improves the wireless range, overall performance, easiness of use, efficiency, and interoperability, to solve key issues related to traffic and transportation, energy, and waste management without affecting the resource/power budget. In fact, IoT is based on smart equipped devices with embedded technologies that allow them to either automatically or selectively collect information from IoT servers and databases before aggregating them to connect and communicate with other users' end-devices via device-to-device communications using sensor technology and actuators [25]. As a result, IoT 2.0 may as well become the new replacement for traditional IoT by becoming the "Intelligence of Things" [26].

In this section, the necessary background to further explain IoT systems, in addition to the processes of identification of IoT hackers are introduced. Also, it highlights their motives and gains through their performed cyber-activity in parallel with the adopted cyber-attack structure. Finally, a suitable framework for IoT will be presented. However, before starting, it is important to define two main concepts which are "ethical hacking" and "penetration testing" to explain the difference to avoid confusing them with each other [27]. **Ethical hacking** is more flexible in simulating (cyber-physical) attack methods and approaches (i.e., phishing, brute force, social engineering, etc), while allowing a thorough assessment. Ethical hackers offer recommendations about best-practice security solutions to adopt against security gaps. **Penetration Testing** primarily focuses on the system weaknesses [28], allowing targeted tests to be performed on a specific IoT component (i.e device, mobile, desktop, iPad, etc). Even though limited in its testing range, pen-testing offers a higher accuracy in detecting and exposing these flaws before addressing them [29]. In other words, ethical hacking relies on adopting a variety of simulated attacks in realistic scenarios via hacking techniques to uncover security flaws and vulnerabilities, verify the IoT system's security, and secure any possible gaps. On the other hand, penetration testing, being one aspect of ethical hacking, focuses more on verifying both safety and security of the IoT's defense systems [30,31].

Next, we describe IoT networks, the known IoT attacks, and in Fig. 3,

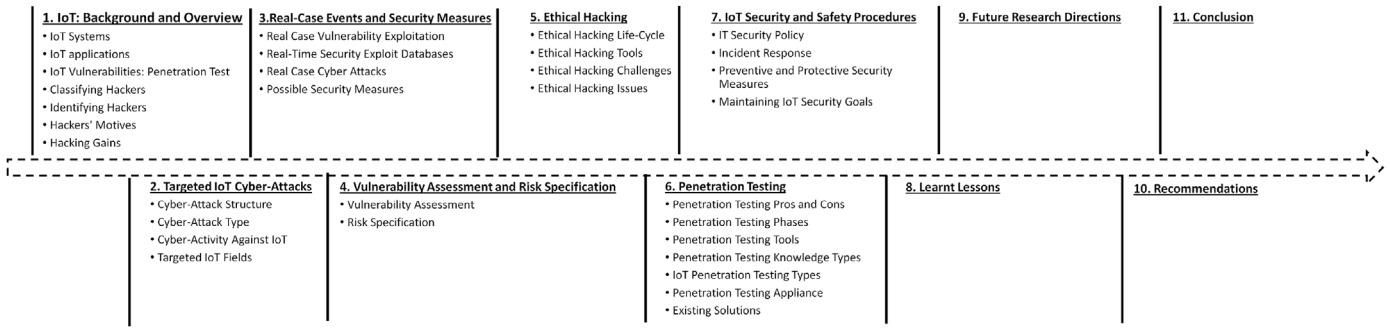

Fig. 1. Visual Structure of this survey paper.

we summarize the concepts of ethical hacking, and how they could be applied within IoT domains.

2.1. IoT systems

As part of its enormous growth, the IoT test architecture is set to become more advanced, standardized, and universally applicable in the near future with multi-technology convergence [32]. As a result, the embedded IoT systems, applications, and devices will become more prone to ongoing persistent challenges, and ethical hackers are in a constant race to capture the ever-growing threats, and to identify the main exploitable vulnerabilities that surround them to present suitable security solutions. Table 1 summarizes the most frequently used IoT tools. As shown in Fig. 2, an IoT network consists of devices that are connected to a data center (or application servers) through a gateway, such as the case of LoRa end-devices [21] that are connected via wireless channels to several gateways.

Currently, the ethical hacking domain is being extensively adopted in IoT systems, applications, devices, mobile devices, servers, and networks to search, scan, detect, and investigate IoT-related vulnerabilities and security gaps. Thus, the introduction of an ethical hacking process to be integrated into IoT would lead to the Internet of Ethical Hacking Things (IoEHT), or Ethical Hacking for IoT (EHIoT).

2.2. IoT applications

The adoption of ethical hacking in IoT systems and applications is increasing to cover all IoT fields including but not limited to Medical IoT [5], Industrial IoT (IIoT), Internet of Cyber-Physical Things (ICPoT), Internet of Powerlines Things (IoPT) [22], Internet of Agricultural Things (IoAT), Internet of Communication Things (IoCT) (i.e LoRaWAN) [21], and Internet of Military Things (IoMT)/Internet of Battlefield Things (IoBT) [33,34]. This also includes Internet of Robotics Things (IoRT) [23,24], especially modular robots and Unmanned/Autonomous Aerial, Ground, Surface, Underwater and Underground vehicles [35,36].

More specifically, ethical hacking for IoT was used to evaluate the levels of safety and security of IoT systems, servers, applications, end-devices, gateways, and application servers to present the best security practices that are not computationally expensive nor energy exhaustive, especially for limited and resource-constrained IoT devices [5].

In IoT-related military, law enforcement and police fields, there are increasing demands to apply ethical hacking to ensure that systems, servers, and devices are protected from any cyber or/and physical attacks, especially attacks linked to (cyber) sabotage [37], espionage [38], spying, cyberwarfare [39], terrorism [40,41], web defacement and (distributed) denial of service.

Fig. 3 shows a set of possible applications that benefit from IoT, as briefly described below:

- **Medical Systems:** healthcare systems have become digitized with the ability to achieve remote monitoring and diagnosis, along with the ability to perform tele-medical operations, and implant smart medical devices. As a result, the IoMT domain became prone to a variety of cyber-attacks (mostly ransomware and phishing) [42] that target the patients' privacy, mostly targeting medical records and interrupting/intercepting operations [43]. Hence, it is very important to adopt the Ethical Hacking for IoT approach to detect security and vulnerability gaps to reduce the likelihood of these events from occurring [44].
- **Industrial Systems:** especially cyber-physical systems such as smart factories, smart grids, power grids, smart enterprises and smart cities, which rely on constant data transmission between these IoT distributed systems, made them prone to a variety of cyber-attacks (i.e worm) mostly linked to sabotage and espionage acts such as the case of targeting the US grids, as well as the ongoing cyber-war between Israel and Iran [45,46], Russia and Ukraine [47,48], including attacks against Ukrainian nuclear facilities, [49,50]. This made the Industrial Control Systems (ICS) and other smart devices, systems, and servers the most vulnerable to these attacks. Hence the reliance on the EHIoT concept is highly recommended to not only detect possible security gaps but also how to enhance them and ensure a higher reactive response by First Incident Responders Team (FIRT).
- **Traffic Control Systems:** especially AI-based Intelligent traffic control Systems with the ability to offer early detection, prediction, and prevention of any network traffic congestion or road closures [51] to prevent accidents and avoid traffic problems via a constant collection of data traffic [52] are also prone to attacks. These attacks can have control of all traffic signs or can even jam, control or redirect traffic, or even intercept and manipulate transmitted data. Hence, the EHIoT should be adopted to discover these vulnerabilities and security gaps to prevent such fatal accidents from possibly occurring.
- **Agriculture Systems:** as agriculture and farming are being fully integrated into IoT, especially Agriculture 4.0 to ensure smart farming, crops monitoring and watering, and other tasks, except that they became more prone and susceptible to cyber-attacks [53]. These attacks are mostly related to security concerns that affect the data that is being transmitted which would reduce its accuracy and hinder agricultural/farming efforts. This is achieved by targeting IoT supply

Table 1
Most prominent IoT pen testing tools.

Name	Type	Description
Binwalk	Firmware Extraction Tool	Analyses IoT Device's Firmware, Retrieves File Systems Contents
Fiddler	Open-Source Web Application	Used to Debug, Manipulates/Reuses HTTP Requests, Allows Users to Track
Firmwalker	Bash Script	Scans Extracted Files from IoT Firmware
Maltego (CE)	Open-Source Intelligence & Forensics	Real-Time Analysis via Information Gathering Using Open-Source Intelligence
SAINT	Static Taint Analysis Program	Protects Cloud-Facing IoT from XSS, CSRF and SQLi, Tracks the Information Flow

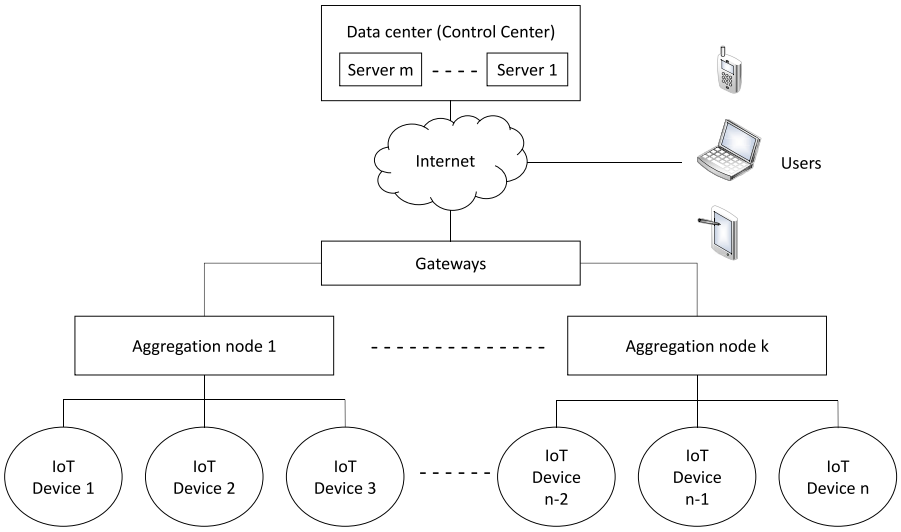

Fig. 2. An Example of Internet-of-Things System with *n* IoT Devices, *k* Aggregation Nodes & *m* Servers. Aggregator nodes might not exit and IoT devices can connect gateways directly.

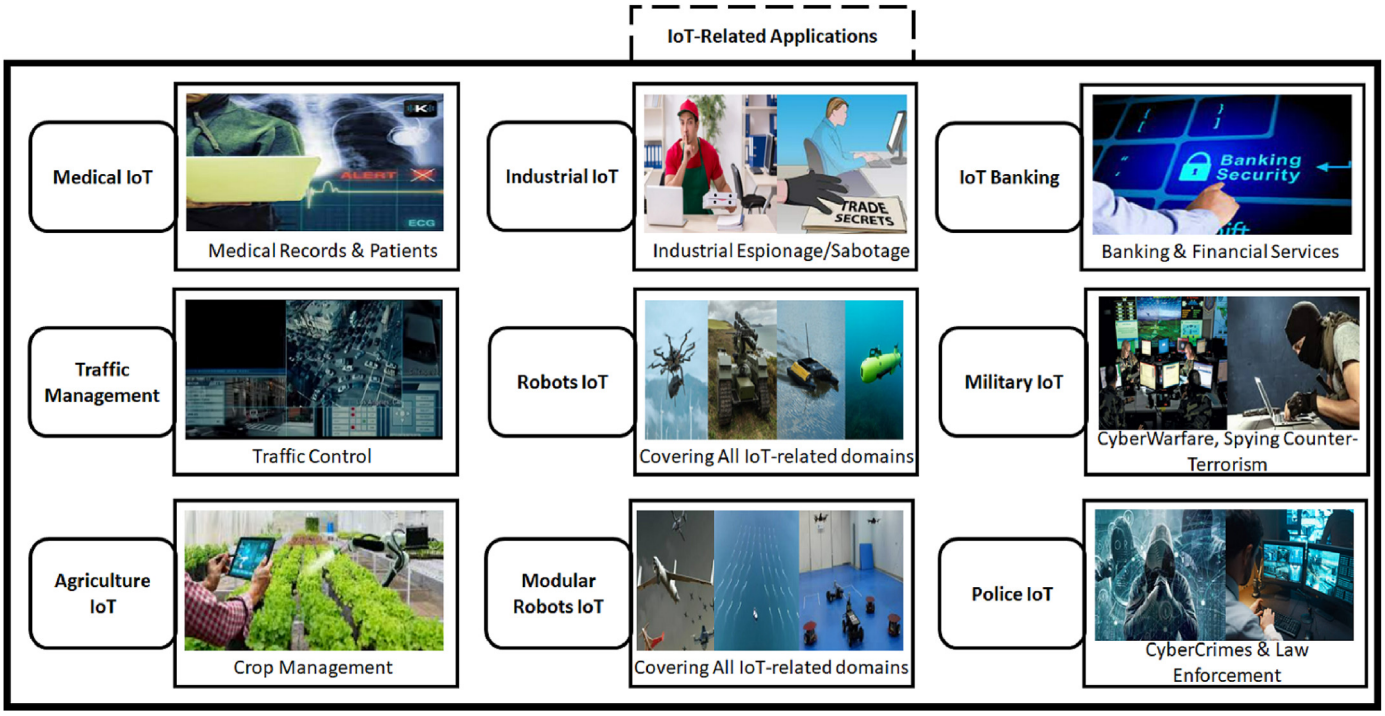

Fig. 3. Ethical Hacking in Different IoT-related domains.

chains, data, networks, and applications [54]. As a result, EHIoT should be adopted and employed to detect any vulnerability or security gap to patch and update it, as such attacks can seriously affect the food chain.

- **Banking and Finance Systems:** most financial institutions are now integrated into the IoT domain with the online transaction being performed on a daily continuous basis, as well as other operations such as e-commerce and e-banking ecosystem, net-banking, Unified Payments Interface (UPI), and cloud computing. As a result, they became prone to several cyber-attacks (i.e DDoS attack against Ukraine including PrivatBank and Oschadbank on February 2022) [55,56], security threats and vulnerability exploit targeting customers, important documents, financial details, classified and sensitive banking information [57]. As a result, ethical hacking should be employed to detect any device, network, or system breaches, while detecting keyloggers on devices and skimmers on ATM booths. This can help protect and safeguard IoT banking sectors, especially devices, systems, servers, and applications, reduce security breaches, as well as detect to act and react against any possible security breach or event (i.e attack).
- **IoT Robotic Systems:** robotics, which are now being integrated into all of the IoT-related domains such as medical, agriculture, industry, banking, search and rescue, military (combat/reconnaissance), law enforcement, etc evolved to include modular robotic types [58], as well as the swarm robotics [59]. This includes Unmanned Ground Vehicles (UGV), Unmanned Underground Vehicles (UUgV),

Unmanned Surface Vehicles (USV), Unmanned Underwater Vehicles (UUwV), and Unmanned Aerial Vehicles (UAVs) [23,24]. This left them prone to a variety of IoT robotic-related attacks especially targeting the network and communication aspects, as well as systems, gateways, and devices. Hence, the EHIoT aspect should also be adopted and applied to detect any vulnerability and security gap to prevent any future security breaches.

- **Military Installation Systems:** as military installations/embassies are being more and more digitized and AI-based, they became targets [60,61] for cyber-attacks by their opponents, especially with the employment of (jamming/signal) Electronic Measures (EM) and Electronic Counter-Measures (ECM). These installations also became a target for cyber-terrorists and hacktivists [62,63]. As a result, cyber-armies were established with cyber-units to perform defense, offense, or/and counter-offense duties. Hence, the concept of ethical hacking is extensively being employed especially under the concept of game theories.
- **Police and Law Enforcement Systems:** as all forms of electronic records became digitized, sensitive police information and records related to criminals, victims, convicts and police officers are also prone to cyber-attacks and can be leaked mostly through exploits and ransomware attacks, such as the case of the Washington, D.C., Metropolitan Police Department ransomware attack on May 2021 [64].

In the following, we explain the background of hackers and ethical hacking and its corresponding classification in detail, along with how it is closely linked to the IoT domain including its devices, systems, servers, applications, etc.

2.3. IoT vulnerabilities: penetration test

In IoT systems including digital systems, robotic systems, cyber-physical systems, power-lines, medical and agricultural system etc, attackers will use existing vulnerability tools (or develop their own) to detect (via searching and scanning) vulnerabilities that can be useful to plan and conduct an internal/external attack. Such vulnerabilities can exploit IoT applications via weak access controls, malicious third parties, cryptographic failures, injection exploits, security gaps, insecure design, data integrity failures, outdated components, identification and authentication failures [65], IoT devices via system misconfigurations, unpatched software, malicious insider threats, zero-day exploits, poor data encryption, old anti-virus, weak vulnerability detection and lack of cyber-security Vulnerability Assessment [66], IoT servers via injection flaws, weak authentication, missing function level Access Control, exposure of sensitive data, security misconfiguration, system configuration and directory exploits [67], and IoT networks (which can be hardware-based, software-based, and human-based) via unauthorised access, denial of service, malicious code/data injections, insider threats and privilege escalation [68,69]. Therefore, the main challenge is to not only identify these vulnerabilities and security gaps but to also fix them. A task that can be very challenging, since it requires defining new specialised countermeasures and security measures to preserve IoT systems, devices, gateways, application/network servers, and architecture. This task's complexity is due to the fact that IoT systems consist of a different set of technologies, software, hardware, middleware, and applications, as well as resource-constrained devices. For this reason, the technical skills for any Internet of Things - Penetration Testing (IoT-PT) should be high and diverse to cover various IoT systems' components including computers, networks, cloud/fog, mobiles, etc, where new majors and domains need to be introduced to fulfill the gap and leave IoT-PTs capable of specializing in one IoT-related domain, rather than cover a wider general aspect.

Unfortunately, all threat types come from the same sources that aim to target IoT systems and compromise devices, gateways, servers, applications, and components, to launch internal/external attacks against other IoT-related systems (indirect attack) or against their internal systems (i.e software or application). This is done by detecting (via reconnaissance and scanning) the vulnerabilities or/and security gaps, followed by exploitation.

Given the fact that 1) IoT systems rely on typical Operating Systems (OS), 2) use the Internet for interconnection and to connect to either application servers at the edge or in the cloud, and 3) mobile devices are used to access IoT systems, IoT penetration testing (PT) involves computer PT, network PT, and mobile PT.

2.4. Identifying hackers

Before proceeding any further, it is important to categories hackers in terms of their aim, objectives and goals, to try and build a bigger picture about each classification and try to understand and figure out what are their main targets against an IoT domain.

- **State/Nation Sponsored:** This type of hacker is employed by a given government with open and even unlimited resources available at their disposal, in addition to the employment and use of very advanced sophisticated tools. This helps them exploit any security gap or vulnerability to gain confidential information about another rival government to stay on the lead [70]. Moreover, this also allows them to achieve further goals based on influencing a government election, like when Russia was accused of interfering in the US elections in 2016 [71].
- **Hacktivists:** Hacktivism usually occurs when a hacktivist mainly hacks for either a social or political agenda, mainly to protest against a government's actions or military actions [72,73]. They are based on an anonymous or even a covert group which can either be local, regional, or/and international. Such type of hackers relies on targeting and hacking IoT systems, including a government, a military website, or/and an organisation in order to grab some media attention to propagandize their own objectives and goals [74]. Their favorite attack types are (but are not limited to) Denial of Service and Web Defacement.
- **Cryptojackers:** are also called cryptocurrency mining hackers whose aim is to exploit network vulnerabilities to steal end devices' resources to mine cryptocurrencies after exploiting their weaknesses and vulnerabilities [75]. This is usually achieved by spreading a spyware (i.e Trojan or Worm or Virus) across the Web that downloads automatically on the victim's device and works quietly with the victim's knowledge.
- **Gaming Hackers:** have their full focus on the online gaming virtual world, especially with the presence of scammers [76]. Their aim is also to hack the game and exploit its bugs or to even target online streamers, famous players, or professional players and hack their accounts or gaming channels. This can either be for personal reasons or sent by rival competitors to stream snipe them or have their accounts banned or deactivated. AI-based bots can also be used as a means to hack/hijack players gaming accounts or to launch DDoS/-DoS attacks to bring the game servers down [77].
- **Cyber-Spy:** Hackers or even whistle-blowers might also be employed by a given national or international intelligence agency in order to perform cyber-spying, cyber-sabotage, cyber-espionage, cyber-warfare [78,79] or cyber-intelligence [80,81] task(s) [82,83] against a given government, military or terrorist target(s). It is mainly done to conduct cyber-espionage operation(s), or a covert information gathering to retrieve essential information about their targets for further exploitation and further cyber-attacks (i.e Espionage/Reconnaissance) [84]. In fact, they can also be employed by rival organisations to conduct industrial cyber-espionage for industrial data theft.
- **Cyber-Heist:** Cyber-heist is usually achieved when the attackers try to steal as much money as possible from a large number of known online bank accounts, in the least amount of time, mainly targeting Internet of Financial Things (IoFT). Such attacks are usually achieved

either through hacking or even phishing, where they are cashed out in a single unique operation, targeting either the customer of a given bank, or the bank itself [85]. A prime example of that is the Bangladesh bank cyber-heist [86], and the cyber capabilities of North Korea [87].

- **Script Kiddie:** exclusively rely on copying codes and scripts to perform malicious code injection (i.e SQLi) or and modification, mostly. Moreover, Script Kiddies rely on already-made programs in order to use them. Script kiddies also focus on the use of DoS and D-DoS attacks to hit the availability of an IoT-given system, website, or device [88].
- **Cyber-Criminals:** Hackers can also commit cyber-crimes, hence they are known as cyber-criminals [89] when they try to perform and commit their attacks online. All of the crimes mentioned above, along with other crimes can be classified as cyber-criminal acts, and sometimes, cyber-terrorist acts [90].
- **Cyber-Insurgents/Terrorists:** Cyber-terrorists also rely on the internet [74] in order to lead and perform online attacks [91,92] to cause serious economic implications [93] against IoT systems, networks, servers and devices alike. Such cyber-attacks are mainly based on information leakage, web-defacement [94], or even Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. This is all due to the fact that terrorists' knowledge is very limited in the cyber-world. However, it is also evolving using different methods [95], techniques [96] and tactics [97], adopted by different groups [98]. A prime example of that is Houthis [99], Hamas (green hats) [100,101] and the Palestinian Islamic Jihad (PIJ) [102] cyber capabilities [103,104], Al-Qaeda's cyber wing [105], Al-Nusra Front [105] and ISIS's cyber-caliphate, cyber-recruiting [106,107], cyber-Jihad and e-terrorism [108,109].
- **Suicide Hackers:** Suicide hackers are hackers who aim at hacking for a given purpose in order to achieve their intended objectives and goals without taking into consideration the impact of their action [110,111].

2.5. Hackers' motives

It is also important to understand the motives [112] behind IoT attacks, and to shed some light on hackers' backgrounds, and the reasons for launching their cyber-attacks against IoT systems.

- **Political:** Political motives are usually based on targeting government's official websites either through DoS and DDoS attacks or through web defacement. This is done to register a protesting statement against the government's new law, or a new agreement on military action against another government. Such moves can be usually led by anti-war hackers [113] as a cyber-protest and demonstration.
- **Patriotic:** or national motives are based on using hacking as a method to register an official protest as part of condemning a given act against a given country. Hence, relying on hacking as a form of "cyber-protest". In fact, it looks very similar to hacktivism. Except that the main difference is based on a given national group targeting a given country or an individual. The most known example occurred when Chinese hackers did send series of DDoS attacks against American and NATO websites as a form of protest against the bombing of the Chinese embassy in Belgrade, in 1999 [114,115].
- **Religious:** Religious motives are are mostly based on extremist views or/and radicalism (i.e takfir), and is another reason for committing a cyber-crime in the name of a certain religion. Such attacks were formerly led by Al-Qaeda [116] and now ISIS/ISIL [117,118], more specifically, ISIS cyber-wing (cyber-caliphate), to either recruit online, spread propaganda, or communicate with their sleeping cells in western countries to perform terrorist attacks mainly across Africa and the Middle East [119,120].
- **Racism:** Many hacking attacks were also led by racist racial groups including the KKK and Neo-Nazis, QAnon [121], Black Panthers [122], ANTIFA along many other racist groups [123], based on hacking with the purpose of ensuring a racial supremacy, hate preaching [124], or trolling [125]. It can also be classified as a different form of terrorism led and performed in order to target other minorities by spreading fear and terror, online [126].

2.6. Hacking gains

This section is dedicated to classify them into either commercial gains, financial gains, personal gains, or even political. In fact, it depends on the motives of the intended hacking group, their background, and ability to wage cyber-attacks against the IoT domain.

- **Economic:** Hackers do rely on targeting IoT's economy for multiple reasons. Such reasons depend on their intended objectives and aims. In fact, they can be employed by rival organisations to target another competitive organisation and reveal its business secrets and trades. Moreover, they might also be employed to cripple the economy of a given organisation by hitting its online available services [127]. Furthermore, it seems like cyber crimes are responsible for around $12 million per business annually [128].
- **Financial:** Financial gains are on top of priority of hackers. Moreover, they are a crucial pumping source of money theft and money laundering, of which hackers heavily rely on as an illegal source of income and funding. The global cost of a serious cyber-attack can lead to $ 120 billion of losses. According to the PwC's Global State of Information Security Survey 2018 [129], the total cost for a financial incident was 857 000 euros, a cost that is high especially for IoT systems.
- **Personal:** Personal gains are another aspect, especially when a rogue/unsatisfied employee (or whistle-blower) is kicked out of a given organisation. In fact, their aim shifts towards taking revenge against his own organisation. Such a move is done, by selling secrets to rival organisations, or disclosing the organisation's sensitive information [130]. The main aim and goal of this move is to either damage their reputation, scam and blackmail, or disclose their personal information.
- **Political:** Political gains are also of a high priority for a given political party, which can operate within the same country, or even against a foreign country's political law. Therefore, hacking can be the new weapon to affect voting polls, or even election polls. In fact, Russia was accused of interfering with the US elections in 2016 [71]. Such move is aimed at influencing another country through a political alliance achieved by paid propaganda and media, which plays a crucial and essential role in affecting the public's opinion.

3. Targeted IoT cyber-attacks

Targeted attacks are presented according to their aims against IoT systems: network, firmware, users/personnel, device or application. First, it is important to describe the cyber-attacks' structure.

3.1. Cyber-attack types

Cyber-attack structures eventually differ depending on the attack type, as well as the motives, knowledge, experience and skills of the attacker. Moreover, the attack structure also depends on the available resources at the hackers' disposal. As a result, the cyber-attack structure is divided and presented as follows: coordinated, distributed, organised, focused and precised. This is summarised in the following Fig. 4.

In fact, cyber-attacks against IoT are not limited to one aspect and classification since they target a variety of IoT systems within the different IoT domains. In fact, there are endless classifications with countless attacks. The aim of this paper is to present the most common

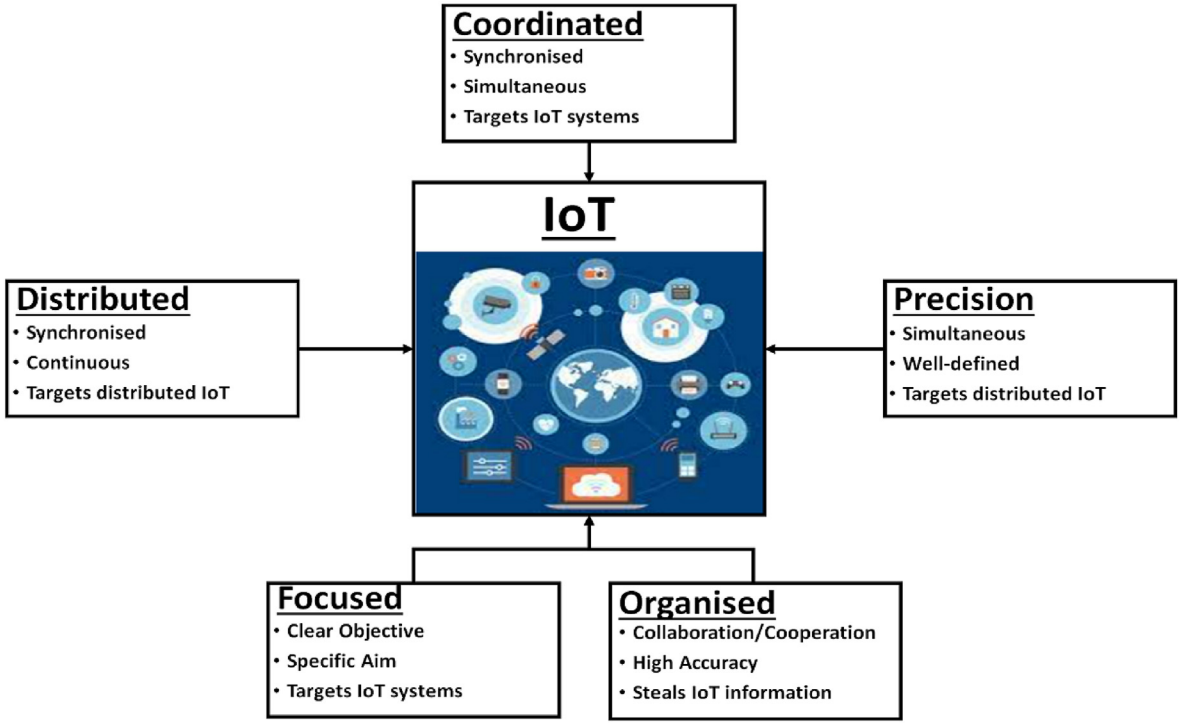

Fig. 4. Attacks against IoT-related domains.

known types of attack that hackers and criminals use, while also presenting suitable security measures to mitigate and overcome them.

3.1.1. Web attacks

Web attacks are primary classified as attacks that target websites, or use websites as a launching platform for their remote cyber-attacks. Among these attacks, their main types are presented as follows:

- **Cookies Hijack:** attack steals the magic cookie that authenticates a user to the remote server. HTTP cookies are also used to a multi-website session, due to the easiness of stealing them from their victim's devices [131].
- **CoAP-based Attacks:** Constrained Application Protocol (CoAP) is an application layer and a specialised web-based transfer protocol used with IoT constrained nodes and constrained networks to enable constrained devices (i.e sensors) [132] to join IoT networks with low bandwidth and low availability. Thus offering lower latency and power consumption [133]. In fact, CoAP is a simplified version of HTTP for IoT or Wireless Sensor Networks (WSNs). Despite its advantage, CoAP is prone to a variety of attacks such as Cross-Protocol, Hijacking, DoS, Man-In-The-Middle, Replay, Relay, Sniffing and Spoofing attacks [134]. A solution to overcome several of CoAP-based attacks was the presentation of a secure authentication and access control scheme for CoAP-based IoT by Obaidat et al. in Ref. [135].
- **DTLS-based Attacks:** since Transport Layer Security (TLS) intends to reliably deliver data stream using end-to-end authenticated encryption, Datagram Transport Layer Security (DTLS), which is a communications protocol is also used to deliver authenticated and encrypted end-to-end datagram-based application data with lower latency [136]. DTLS is used to deal with packet reordering, datagram loss, and data that is larger than the datagram network packet. Thus, offering as a channel security protocol an integrated key management, parameter negotiation, and secure data transfer. DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol to prevent eavesdropping, tampering, or message forgery, and relies on the Secure Real-time Transport Protocol (SRTP) to provide confidentiality, message authentication, and replay protection [137]. Key-reuse (rekeying) can be exploited to perform password attacks. Other attacks include Triple Handshake, as well as SSL Stripping attack, STARTTLS Command Injection (CVE-2011-0411) attack, BEAST (CVE-2011-3389) attack, Padding Oracle and its variant POODLE attack (CVE-2014-3566), which are further described in Ref. [138].
- **Sessions Hijack:** also known as session hijacking or key-to-gain unauthorised access to the IoT device's information session [139]. It usually occur when the "Pass-the-Cookie" technique is used [140] to perform "blind" hijacking or man-in-the-middle attacks using sniffing programs.
- **Masquerade Attacks:** usually target connected networks and devices with weak authorisation by using a fake (network) identity to gain unauthorised access to personal information (E.g usernames, passwords, logons, logins etc.) through legitimate access [141]. This attack can be performed by insiders (whistle-blowers within the organisation) or outsiders (remotely).
- **Buffer Overflow:** or buffer overrun is a program anomaly that overruns and overwrites a buffer's boundary with adjacent memory locations [142]. C and C++, Java and Python are common programming languages associated with buffer overflows. Such attack would result into overwriting adjacent data, overwriting executable code(s), memory access errors, incorrect results, and constant crashing. Cryptographic and non-cryptographic solutions were presented to protect against buffer overflow attacks in Ref. [143]. Bound checking is a suitable solutions, but requires additional processing time. Moreover, randomizing memory layout and deliberately leave buffer space are other suitable solutions to overcome buffer overflow Operating Systems (OS) attacks.
- **Website Spoofing:** includes creating fake (hoax) websites that mislead readers into believing its legitimacy by masquerading it as a legitimate website through a very similar design including similar Uniform Resource Locator (URL) or Cloaked URL, and a shadow copy of the World Wide Web [144]. Website spoofing is always associated with phishing or e-mail spoofing.

- **Malicious Code Injection Attacks:** usually occur on poorly configured and poorly secured web applications [145] for IoT users. In fact, they can be easily exploited by any hacker through a malicious code injection or an SQL injection attack. As a result, this malicious script will be running on the victim's device without their knowledge [146]. Therefore, registering keystrokes or/and retrieving all of the users credentials including emails, passwords, credit card numbers, along with cookies, browsers, and the device's/user's ID.
- **SQL Injection Attacks:** The impact of SQL injection attacks varies depending on the objective and aim of a given hacker [147]. Such an aim is based on either manipulating database information, gathering sensitive data, or even executing a DoS attack. In Ref. [148], SQL injections were divided into three different categories. These categories include three order attacks. The first order attack, is based on the attacker entering a malicious string to modify the executed code. Second order attack, is based on the injection into a storage executed by another action. Third order attack is the later injection, where the attacker manipulates the function by changing its environment variables. On the other hand, there are different SQL injection methods that can be applied [147,149], and they are presented in Table 2. The focus on this type of this attack is due to it being an active method used by hackers mainly to target university websites such as the infamous known cases of Team GhostShell SQL attacks (Oct. 2012, targeting 53 universities), Rasputin SQL attack (Feb. 2017, targeting 60 universities), and LulzSec ITA SQL attack (Feb. 2020, targeting 3 universities) [150]. Further information about SQLi attack types are discussed in Ref. [151].

- **Cross-Site Scripting:** or XSS is a web application security vulnerability based on a malicious code injection by malicious web users. In fact, recent attacks were able to leverage session IDs by relying on JavaScripts functions on other websites to inject them into different pages. This included online banking, instant messaging and emails. Therefore, being capable of stealing a user's session which in turn, can be used to steal stored web cookies. This allows the attacker to replicate a user's session on a different machine [152,153]. Another form of XSS is based on the attacker sending HTTP requests at his own will from his victim's machine, or sending false counterfeited requests relying on the use of an especially sophisticated tool(s).
- **Cross-Site Request Forgery:** Cross-Site Request Forgery (CSRF) takes advantage of any possible lack of authorisation that is either absent or weakly employed in poorly designed web applications. The first step of performing this attack, is based on the hacker making the victims run the malicious script through clicking on malicious link without their knowledge. Therefore, allowing the attacker to use the victims' saved credentials to perform further attacks on their behalf, and without their knowledge. Such attacks usually take place through a network request injection relying on the browser of the user, which permits a website to show every HTTP request to any given network address [153].

Table 2
Different SQL Injection Attacks that can target database applications servers used by IoT users.

SQL Injection Types	Description
Blind Injection	Logical conclusions are derived from the answer to a true/false question regarding the database
Logically Incorrect Queries	Using different error messages to retrieve information to exploit and inject a given database
Piggy-Backed Queries	Malicious queries are additionally inserted into an already injected original query
Stored Procedure	Executing database's built-in functions using malicious SQL Injection scripts/codes
Tautology	SQL injection queries injected so they always result in a true statement
Timing Attack	Collecting information by noticing the database response time
Union Query	Malicious query joined with a safe query using UNION to get other table related information

3.1.2. *Application attacks*

Application attacks against the IoT can take many forms from covert attacks (surveillance) to much more overt ones such as viruses. This paper discusses the main most frequent attacks that take place against the IoT applications.

- **Scareware:** uses social engineering techniques to trick their victims into downloading/purchasing unwanted dangerous rogue software (ransomware) by using fear as their tactic [154]. This is caused by urging users to download a fake software (i.e Anti-Virus) to remove a recently detected (fake) virus to remove it. Scareware can take many forms including antivirus, anti-spyware, firewall application or a registry cleaner. Scareware may include a clickjacking feature that redirects users to malicious website that triggers a malware download once the users clicks on the "Cancel" or the "X" buttons to close the window.
- **Spyware:** is a part of the malware family, masqueraded in a (malicious) software [155,156] that installs itself on a given device to covertly monitor its victims' online/offline behaviour without their knowledge and permission [157] and gain details about them (E.g names, addresses, browsing history, downloads etc). Spyware can act as adware by marketing data firms, or can be a Trojan. Such attack can degrade a system's performance, damages the Central Processing Unit (CPU) capacity, affect the disk usage and cause network traffic overhead.
- **Trojans:** these include two types: Software Trojans (STs) which are often disguised as legitimate software employed by cyber-criminals to gain access to users'systems, and Hardware Trojans (HTs) which cause a malicious modification of the circuitry of an integrated circuit to disable or destroy the entire chip and its components [158]. Once activated, Trojans can steal, spy, exploit, implement backdoors (rootkit) to delete, block, modify, disrupt and modify data [159]. Trojans can take many forms: Trojan-Banker (steal data's account), Trojan-DDoS (denying service), Trojan-Downloader (download/install new malicious program versions), Trojan-Dropper (install viruses), Trojan-FakeAV (fake Anti-Virus), Trojan-Game-Thief (steals online gamers' accounts), Trojan-IM (steals users' usernames/passwords of Skype, Yahoo, Messenger, etc), Trojan-Ransom (modify computer's data as part of ransomware attack), Trojan-SMS (sending text messages from their victims' phones), Trojan-Spy (implement keystroke, keep users under surveillance), and Trojan-Mailfinder (harvest email addresses).
- **Botnet:** bots or zombies tend to exploit IoT devices that suffer from the same vulnerability [160], and can also be used to launch DoS and DDoS attacks by being ordered from a command and control (C&C) software. Botnets can steal data, send spam, or gain remote access. Botnets can take many forms including Hybrid Botnets [161], Internet Relay Chat (IRC) botnets [162], Cloud Botnets [163], Peer-to-Peer (P2P) botnets [164], Hyper Text Transfer Protocol (HTTP) botnets, and Mobile (SMS/Bluetooth) botnets [165], along many other botnet types.
- **Virus:** is designed to target IoT systems and devices by spreading from host to host either through human interaction (Trojan, Logic Bomb [166,167] etc) or without human intervention (worm) [168]. Unlike worms, viruses cannot spread or reproduce without human interaction, since it is a malicious code or program written to alter the way a computer performs. Viruses can be attached to a program, file, funny images, audio/video files, socially shareable content or document, to steal data/passwords, register keystrokes, corrupt files, send spam, erase data or cause hard disk permanent damage [169]. This can also result into having file infection [170]. Infected devices show various symptoms including frequent pop-up windows, homepage changes, frequent crashes, and slow performance. Therefore, its

always important to use trusted/verified up-to-date anti-viruses, avoid clicking on pop-up advertisements, and use spam filters.

- **Rootkit:** is used to gain a remote administrator-level access to a computer or network by stealing an administrator password or exploiting a system's (OS, firmware or application) vulnerability [171]. Rootkits can deactivate/destroy anti-malware software to avoid detection and make its tracking extremely difficult. Moreover, rootkits can ensure a backdoor access through key logging, or turn a given vulnerable device into a bot.

3.1.3. Network attacks

Poorly secure and non-secure IoT networks including servers, channels and gateways are vulnerable to various threats and attacks that exploit their security gaps. The most commonly known type of these attacks are as follows:

- **Eavesdropping:** is known as a passive interception of communication between two parties and can take many forms such as: sniffing by installing a network monitoring software called sniffer, or snooping attack where an eavesdropper passively intercept non-secure or weak communication between two parties to steal their information and credentials via the communication network [172]. To overcome this attack, avoid public Wi-Fi networks, use firewalls, proxies and Virtual Private Networks (VPN).
- **Replay:** are known as playback attacks that are a lower tier versions of a "Man-in-the-middle attack" where an attacker eavesdrops on a secure network communication and intercepts it for further repeated transmission later on to cause delays or disruption of service. To overcome this attack various solutions can be presented such as using timestamps, securing data storage with key update, using security protocols [173], using attentive filtering networks for audio replay attack detection [174], and using Magnitude and Phase Information with Attention-based Adaptive Filters [175].
- **Man-in-the-Middle:** (MITM) is an active eavesdropping form where the attacker impersonates each endpoint to alter, intercept and directly monitor the communications between two parties and tricks them into believing that they are communicating with each other [176]. Therefore, encrypting communication is required and using a mutually a trusted Certificate Authority (CA) between both parties is a must.
- **Packet Sniffing:** intercepts the data through the capture of traffic using a sniffer software [177] over non-secure channels and reads the unencrypted data. Captured data can be analysed to gain access or information. To overcome this issue, channels must be secure and data must be encrypted.
- **Password Cracking:** is a cryptanalysis process that aims to crack passwords to recover credentials and gain access to systems (System Administration privileges) and data [178]. Password cracking can range between brute force [179] (protected using multi-factor authentication), dictionary [180] (protected using a passphrase), Meet-in-the-middle [181] (protected using stronger keys), online/offline password guessing [182] (protected using encrypted password form), rainbow-table [183] (protected using salting technique), and birthday [184] (protected using hashing) attacks with many commercial/free tools being used and available for this task.
- **Traffic Analysis:** intercepts and examines encrypted/unencrypted network traffic to recover any useful information (header, message length, repeated patterns, processing time, transmission delay, etc) [185]. This renders large, periodic, encrypted and plaintext traffic under constant watch. To overcome this attack, sophisticated cryptographic solutions are needed, as well as the use of The Onion Router (TOR).
- **Wireless Jamming:** is used to compromise a secure/non-secure wireless environment (mainly Local Area Networks (LAN)) [186] by denying the access and transceiving services to authorized users, by blocking and jamming all wireless legitimate traffics on all targeted frequencies (mainly FM, GSM, 2.4 and 3, 4 or 5 GHz). To overcome this attack, Wireless LANs can be used, along frequency hopping and shifting techniques.
- **Black-hole:** packet drop attack or blackhole attack is classed as a denial-of-service (DoS) attack by employing a router that (sometimes selectively) relays packets instead of discarding them [187]. Due to the lossy network nature, packet drop attacks are very hard to detect and prevent. Hence, they are frequently deployed to attack wireless ad-hoc networks. This type of attacks can be mitigated using a Timer Based Baited Technique presented in Ref. [188].
- **Byzantine:** attacks have total control on the number of authenticated devices before behaving arbitrarily [189]. This type of attacks turns insider nodes into malicious ones by preventing route establishments, modifying route selections, and dropping route requests. Therefore, disrupting and degrading the performance of both network and routing services. Byzantine takes many forms of attacks including Byzantine Wormhole attacks, and Byzantine Overlay Network Wormhole attack, in addition to other attacks that are further discussed in Ref. [189].
- **DoS/DDoS:** a denial-of-service (DoS) attack prevents legitimate users from accessing their services through an excessive sending of authentication requests with invalid return addresses [190]. A Distributed-Denial-of-Service (D-DoS) compromises multiple systems (compromised through a Trojan and turned into bots) before simultaneously flooding the victims with a massive incoming traffic from multiple sources. DDoS attacks have many types including: traffic attacks, flooding Transmission Control Protocol (TCP) packets, flooding User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) packets, bandwidth attack (sending massive data junk), and application attacks (depleting application layer's resources).

Finally, a penetration testing risk assessment is presented in Table 3 with the appropriate security measures per attack depending on the security target: ((C)onfidentiality, (I)ntegrity, (Av)ailability and (Au)thentication).

3.2. Cyber-activity against IoT

Hacking against IoT can take part or even be part of a cyber-activity led by a hacking group or individual(s), either locally, regionally or globally. As a result, hacking can take many forms, depending on the motives mentioned earlier, depending on goal, cause and objective. Such cyber-activity, can be cyber-crimes, cyber-terrorism, cyber-warfare, and cyber-espionage, targeting IoT systems including (but not limited to) Medical IoT [5], Industrial IoT (i.e Cyber-Physical Systems [20] and power-line stations [22] and long range communication [21]), Military IoT (i.e Drones/UAVs [23] and robotics [24]).

The possible cyber-activities that can benefit from the exploitation of IoT devices are listed in the following:

- **Cyber-Crimes:** Hackers mainly rely on cyber-theft, cyber extortion, and skimming [196] in order to steal financial or personal information via IoT systems, computers, devices or insecure browsers to target businesses, organisations, installations and sometimes for cyber-bullying purposes against the youth [197]. This was done by breaching the security measures to intercept data by also targeting engines, wikis and blogs by constantly sending empty messages. This was mitigated by using adaptive neuro-fuzzy inference systems [198]. This concept was adopted by the attackers to carry out various types of malware attacks [199]. In fact, cyber-heist is a large scale monetary theft which can be realised by relying on digital devices such as IoT one to perform their cyber-crimes through hacking, with Crime-ware kits [200] including SpyEye [201], Butterfly Bot [202] and Zeus [203] being the most used hacking tools. The most infamous cyber-heist act was MIRAI attack.

Table 3
Security attacks against IoT entities and users with possible security measures.

Attack		Targeted Security Goals				Security Goals	
Target	**Type**	**C**	**I**	**Av**	**Au**	**Cryptography**	**Non-Cryptography**
Web Attacks	Cookies Hijack	✓	X	X	✓	Encrypted Connection	HTTPS, Secure Websites
	Session Hijack	✓	X	X	✓	Encrypted Connection	Session Key Management, Secure SSL/TLS, HTTPS
	Masquerade Attack	✓	✓	X	✓	Encrypted Communication	Code Signing, Execution Prevention, File/Directory Permissions
	Buffer Overflow	X	X	✓	X	–	Bound Checking, Randomized Memory Layout
	Website Spoofing	✓	X	✓	X	–	Secure Websites, Web Filtering, Anti-Phishing Training, Netcraft
	Malicious Code Injection	✓	✓	X	X	–	Proper Secure Coding
	SQL Injection	✓	✓	✓	X	Secure Coding	Input Validation
	Cross-Site Scripting	✓	✓	✓	X	Secure Coding	Filter Input/Output, Security Policy
	Cross-Site Request Forgery	✓	✓	X	X	Read-only GET requests	Cross-Site Request Forgery
Application Attacks	Scareware	✓	✓	X	✓	–	Anti-Virus, Anti-Ransomware, Awareness
	Cookies Hijack	✓	X	X	✓	Encrypted Connection	HTTPS, Secure Websites
	Spyware	✓	X	X	X	–	Anti-Spyware, Updated Software Patches, Trusted Third Parties
	Trojan	✓	✓	✓	X	–	Anti-Virus, Updated Software Patches, Awareness
	Botnet	✓	✓	✓	X	–	Anti-Malware Software, Updated Systems, Disabled Unused Ports, Awareness
	Virus	✓	✓	✓	X	–	Anti-Virus, Firewalls, Awareness, Updated Systems
	File Infection	✓	✓	X	X	–	Anti-Virus, Prevented P2P File Sharing, IDS, Awareness
	Rootkit	✓	✓	✓	✓	–	Advanced Anti-virus, Awareness, Updated Systems, IDS/IPS
Network Attacks	Eavesdropping	✓	X	X	X	Encrypted Data & Communication	Personal Firewall, Proxies, VPN
	Replay	X	X	X	✓	Encrypted Data & Communication	VPN & Personal Firewall
	Man-in-the-Middle	✓	✓	X	✓	Digital Certificate & Encrypted Communication	VPN, Strong Authentication & Tamper Detection
	Packet Sniffing	X	X	✓	X	PKI [191]	VPN, TLS & SSL [191]
	Password Cracking	✓	X	X	✓	Strong Hashing	Strong Multi-Factor Constant Password Changing, Strong Passwords
	Traffic Analysis	X	X	✓	X	Encrypted SIP [192], Secure Communication	Network Filtering, Network Monitoring & Analysis
	Wireless Jamming	X	X	✓	X	Encrypted Channels, Secure Communication Lines	FHSS and DSSS [193]
	Black-hole	X	X	✓	X	ECC [194]	HMM [195], R-AODV [194]
	Byzantine	X	X	✓	✓	–	Secure Endpoints, Advanced Firewalls, IDS/IPS, Traffic Monitoring/Analysis

- **Cyber-Espionage:** became another dangerous emerging field seriously targeting IoT, especially when a Stuxnet worm attack targeted the Iranian nuclear power grids [204], followed by other similar attacks (i.e Flame, Duqu and Gauss variants) [205]. Another aspect of cyber-espionage. Moreover, industrial cyber-espionage [206] took place in 1997, where engineers disclosed sensitive business information to the company's competitors. In fact, such attack was revealed through received emails and faxes. The engineer was accused of industrial espionage and was sentenced for around two and a half years in jail. A large spy network called GhostNet [207] was revealed by Canadian researchers in 2009. It was responsible for more than a thousand computer intrusions in more than 103 countries, gaining unauthorised access, and compromising different devices. Operation Shady RAT is the most infamous cyber-espionage case that affected more than 70 companies and organisations since 2006 [208]. It was spread through an e-mail with a malicious link attached to it as a self-loading remote-access tool, or Remote Access Trojan (RAT). Thus, gaining unauthorised access to legal entities and sensitive data. This is similar to the cases of studies of Smallcase, Derusbi, and Sakula RATs [209].
- **Cyber-Terrorism:** Due to the availability of hacking tools and internet with high speed real-time data transmission, and the easiness to obtain laptops, computers, and mobile phones at low prices, it became a source of attraction for terrorists with psychological effects [210]. As a result, terrorists started using it as a new emerging type of cyber-warfare, known as the asymmetric cyber-warfare, in order to lead cyber-attacks against IoT systems mainly belonging to Western governments and military installations [211]. Their extremist motives are usually either religious-based or racial-based via the spread of hate, terror, fear and/or racism through hacking. This was mainly done through defacing/hacking websites, or mostly DoS/D-DoS attacks [212].

In fact, terrorists are now also relying on online methods to perform their online cyber-attacks in a cheaper but much more effective way to express or impose extreme politico-religious views [213–215].

- **Cyber-Warfare:** or information dominance or/and information warfare [216], which became a new type of cyber-war and part of an electronic warfare being waged against sensitive IoT systems and domains. This was achieved through cyber-space against different countries [217], in order to cripple their cyber-ability and capability and smart infrastructure with a group of cyber-army or cyber-warriors [218,219]. A global cyber-war [107] was already waged against ISIS/ISIL in Ref. [220]. This war managed to decisively defeat their cyber-caliphate online, and freezing their online activities. Another attack was led by Russia against Georgia and Estonia in 2007–2008, by sending multiple waves of D-DoS attacks, as well as against Ukraine following the Russo-Ukraine conflict since 2014 [221], which was renewed in January, February and March 2022. Therefore, crippling their online available services [222,223]. In fact, cyber-warfare can be part of the electronic warfare domain to ensure the Battlefield's Situational Awareness (BSA) using Cyber Electronic Warfare (CEW) [224,225]. One example is the ongoing cyber-war between the North Atlantic Treaty Organisation (NATO) members

and both Russia and China [226,227], especially in the Balkans [228].

3.3. Targeted IoT fields

The new adaptation and the widespread use of the internet and recently the IoT was based on digitizing data and records that are stored and processed by cloud services. This gave hackers the opportunity to launch cyber-attacks against numerous IoT sectors such as banks, enterprises, governments, military installations, hospitals, and individuals.

- **Organisations:** any national/international organisation or small/medium enterprise is also prone to a wide range of cyber-attacks [229], which can severely impact their operational performance [230]. These cyber attacks are based on targeting the organisations' devices, relying on phishing and spear-phishing attacks [231,232]. These attacks can infect a given organisation device with a malware capable of recording keystrokes, or injecting a spyware, or a Trojan horse (RAT), which turns the devices into botnets, or enables advanced access privileges.
- **Banks:** The most common attacks against banks can be based on hitting the availability of a given bank and preventing legitimate users from accessing and using the available services. This can have devastating effects on systems and people alike, targeting and compromising both systems and data confidentiality, integrity or/and availability. Moreover, cyber-heist [233,234] can also occur. This leads to stealing online money as much as possible, in the least amount of time.
- **Enterprises:** are also prone to cyber-attacks led by hackers to disrupt their services and interrupt them. In fact, smaller enterprises are the most enterprises vulnerable to attacks by hackers. By quantifying a given risk [235], financial losses managed to reach up to more than $445 Billion yearly, which is a quite high number.
- **Governments:** are mainly targeted either by hacktivists, cyber-terrorists [236], or even cyber-espionage attacks. Hacktivists perform their attacks as a form of protest, relying on hacking as a tool in order to make a clear statement. However, cyber-espionage is led by foreign rival governments against other governments by relying on cyber-intelligence agencies. In fact, it is a part of information gathering in order to lead a much more sophisticated cyber-attacks against smart infrastructure or even affect election polls [237,238].
- **Hospitals:** also became the perfect target for hackers in order to steal patients' private data and sell them to malicious parties. In May 2017, the National Health Service (NHS) came under a WannaCry ransomware attack, led by North Korea's Cyber-Unit 180 (Lazarus) [239], before establishing a security operations center and investing £ 250 000 to raise awareness and train NHS employees. In January 11th, 2018, Hancock Regional Hospital in Indianapolis was infected by malware via an e-mail, known as a phishing attack [239]. Hackers locked the hospital's computer systems and demanded a ransom in Bitcoin crypto-currency. Therefore, luring the hospital to pay $55,000 as a ransom [240].

Fig. 5. Proposed cyber-classification taxonomy.

- **Military Websites:** A new emerging technique has two main aspects, cyber-warfare [241,242] (i.e Russian-Ukraine case [243], or cyber-terrorism [78,91]. It can also take a secondary aspect by being part of a hacktivism campaign led by protesters (i.e anonymous) [74], or led by state-sponsored hackers such as the Iranian and Iranian-backed hackers, state-sponsored proxies (i.e Hezbollah [244]) and the Syrian Electronic Army group [245] against a given (US/Israeli) military action [246]. Therefore, the military seems to be a recent cyber-target by different hackers [247], where bits and bytes are replacing bullets and bombs in the cyber-physical world.

Finally, this paper summarizes them in Fig. 5.

4. Real-case IoT-Related events

In this section, we present some real-time security events that took place against IoT servers, gateway, and end-devices, including real case vulnerability and database exploit, along with real cyber attack events, and we highlight some possible security measures.

4.1. Real case vulnerability exploitation

Several real case studies are mentioned and briefly discussed to highlight how such vulnerabilities were exploited to conduct cyber-attacks including:

- **Adobe Flash Incident:** in 2013, Adobe suffered a breach [248]. In 2015, the Adobe Flash came under attack. The exploited vulnerabilities were zero-day types including mainly CVE-2015-5119, CVE-2015-5122 and CVE-2015-5123.
- **Equifax Data Breach Incident:** took place in March 2017, where an unpatched Apache Struts vulnerability coded CVE-2017-5638 running on Equifax's web servers was exploited due to a security failure caused by Equifax's administrators not applying least privilege controls. After accessing the web server, the attackers successfully sneaked into the database, held and siphoned private information of 143 million consumers including social security names, addresses, dates of birth, social security, and credit card numbers, costing around $3 billions to sort the breach. Hence, the importance of a zero-trust approach to Privileged Access Management (PAM) [249].
- **Exploit - CVE Variants Incidents:** CVE variants were prone to various exploits [250]. In 2020, Microsoft successfully managed to detect attacks that leveraged vulnerabilities in the Microsoft Exchange Server. These attacks were classified as Zero-Day, and were tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. The exploitation took place when attackers managed to successfully inject malicious codes into the resources used in the Exchange Offline Address Book (OAB) service [251,252].
- **Exploit - CVE-2020–1472-Zerologon:** was a critical Microsoft vulnerability which allowed a attacker to escalate privilege to the highest level without having any credentials. This was done when the attacker managed to reset the password with or without reestablishing the original password [253].
- **Exploit - CVE-2020–0688 Incident:** was initially discovered on February 26, 2020, when the credentials of an already compromised account were leveraged to authenticate to Outlook Web Access (OWA). The credential harvesting attack was achieved by either password guessing or poor password policy, allowing the attacker to exploit the Exchange Control Panel (ECP).
- **Exploit - 05–2022–0438.doc Incident:** was revealed on May 30, 2022, which is a zero-day flaw in Microsoft Office that allows the ability to achieve arbitrary code execution on affected Windows systems. The word document was uploaded to VirusTotal from an IP address in Belarus but was discovered. The exploit uses Word's

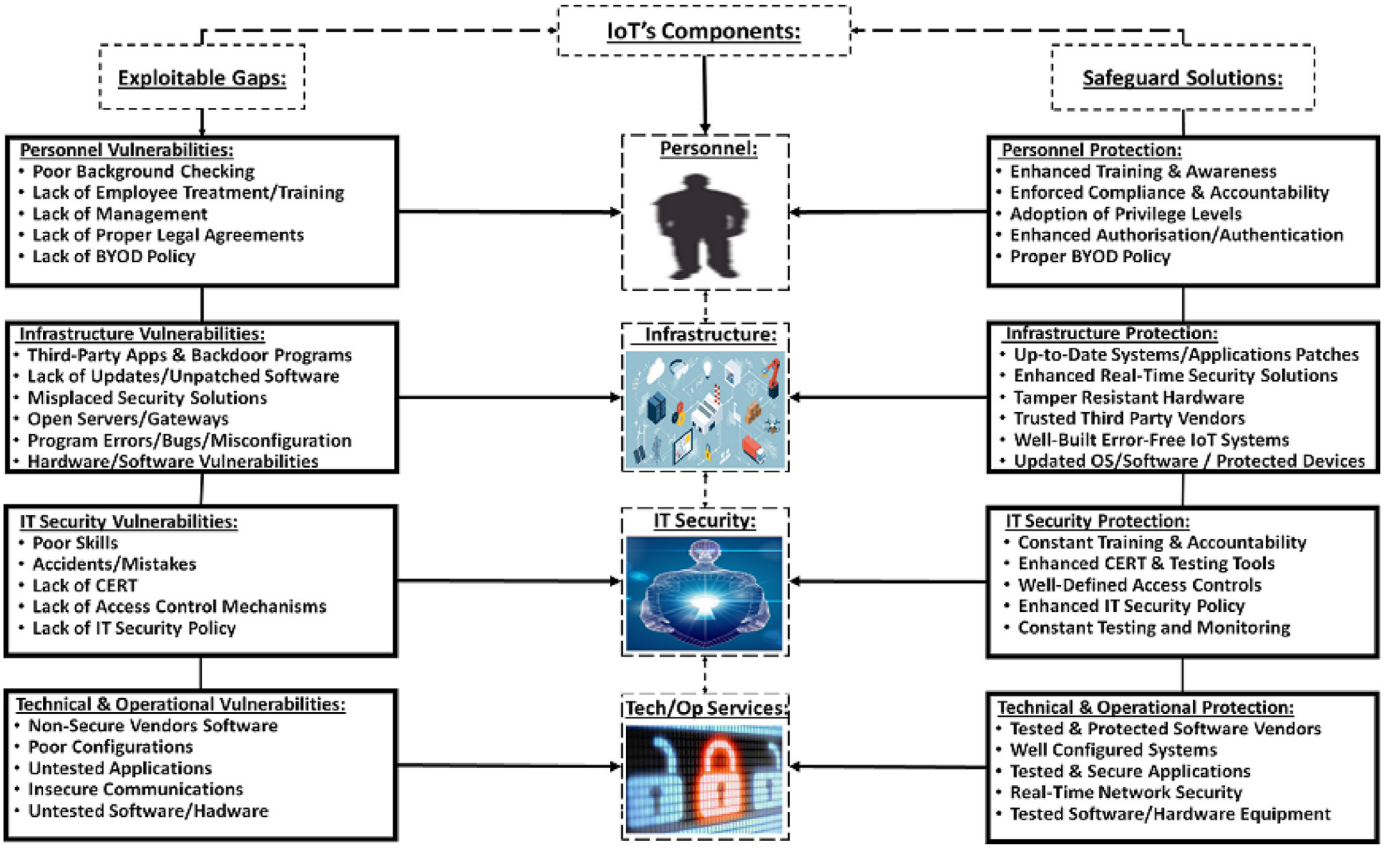

Fig. 6. Vulnerability & Security Solutions at different IoT's Components.

external link to load the HTML file ("RDF842l.html"), then the 'ms-msdt' scheme to execute PowerShell code. Its severity level is similar to the CVE-2021-40444 exploit.

In fact, it is also important to highlight the yearly increase in number of cyberattacks, which according to CISCO's 2021 Cybersecurity Threat Trends report, (Spear) Phishing attacks were responsible for more than 80% of security incidents and 90% of data breaches. Increasing the year-over-year in phishing attacks by 400%. On the other hand, ransomware attacks increased by 48%, with a 17% increase between 2020 and 2021 [254,255].

4.2. Vulnerability assessment

Untested IoT systems tend to be more vulnerable to various types of attacks such as the ones presented above, which puts them at a higher risk of being targeted due to their exploitable security gaps. Therefore, it is important to assess vulnerabilities before specifying the risk(s) associated with them.

In order to evaluate a given vulnerability, it is highly recommended to assess it first starting by identifying it. In Ref. [256], Votipka et al. were among the first to conduct a study and a comparison analysis between ethical hackers and pen testers. The analysis included ways to scan, find and discover vulnerabilities. Also, the paper included how testers and hackers develop their own skills, knowledge and experience, as well as the tools they use. Moreover, the authors provided their own recommendations to support and improve security training for testers, along with better communication between ethical hackers and developers, where hackers were also encouraged to participate.

In fact, there is a huge number of tools for Vulnerability Assessment Penetration Testing (VAPT) [257] that can be used to perform penetration testing and vulnerability assessment for ethical hacking purposes. Different papers mentioned various types of vulnerability assessment and penetration testing tools such as [257,258]. However, we shall focus on the main VAPT tools, which are typically used during ethical hacking training.

Hence, Table 4 presents a summary of the most frequently used Vulnerability Assessment Penetration Testing (VAPT) and Network Vulnerability Scanning (NVS) tools in order to secure IoT systems from any exploits and protect them from any attack.

4.2.1. IT security vulnerability

IT security (ITSec) vulnerability, once exploited, can cause a serious blow to both IoT systems and users/clients since they target the confidentiality, integrity or/and availability of a given IoT system, which drastically affect its performance.

Table 4
Vulnerability Assessment Penetration Testing (VAPT) & Network Vulnerability Scanning (NVS) tools that can be employed on IoT entities (end devices with OS and/or servers), in addition to the user's desktop/mobile.

Name	Type	Description
Kali Linux	VAPT/ NVS	Various collection of different tools
Paros Proxy	VAPT	Web vulnerabilities scanner
Core Impact	VAPT	Vulnerability exploitation & Scanning
Parrot Security OS	VAPT	Designed for vulnerability assessment and mitigation, penetration testing, computer forensics and anonymous web browsing
Nexpose	VAPT/ NVS	Vulnerability Scanner & Vulnerability Management Life-cycle
Microsoft Baseline Security Analyzer (MBSA)	NVS	Identify any missing service packs, security patches, and security misconfigurations, scans IP addresses, scan weak passwords, or SQL administrative vulnerabilities
Retina CS Community	NVS	Finds network vulnerabilities, configuration issues, and missing patches, provides free scanning and patching for 256 IPs (max), supports vulnerability scanning in mobile devices, servers, and web applications

- **Lack of Access Control Mechanisms:** The lack of the right access control mechanisms can make any IoT system prone to various types of attacks and vulnerabilities. In many cases, employees are given access privileges to perform more than their intended task(s), along with being left with these privileges even after their task(s) have been performed. However, in other cases, physical access control is another concern, since locks can be easily broken and keys can be easily obtained. Therefore, the adoption of biometric access control mechanisms [259,260] is important and deserves a new aspect of attention, especially since many biometric features can be imitated [261].
- **Third-Party Applications:** are usually untrusted or semi-trusted applications that are used for a specific task or to fix a given IoT system, such as debugging processes. Such applications can be rogue applications that can be used to gain unauthorised access to the network, inject malicious codes or eavesdrop/spy on the transmitted message to retrieve confidential information.
- **Backdoor Programs:** are typically set by vendors for fast access to any given IoT system. However, they can also open the door for hackers who exploit them as a weakness to gain an illegal covert access. In fact, hidden backdoors are intentionally-created computer security vulnerabilities, which allow the covert installation of a program or the execution of a given code to provide remote access to a given system via the exploited device.
- **Lack of Patching/Updates:** (OS) systems must always be updated to avoid patching vulnerabilities in older versions. Otherwise, they can be easily exploited. This, especially recently, has proven to be a main vulnerability such as the case of Log4j variant that has exploited and keeps on exploiting thousands of devices. This leaves not only OSs vulnerable, but also systems and devices that rely or run on this platform vulnerable to older and much newer exploits such as zero-day attacks [262]. Therefore, systems, devices and OSs updates is a must [263].
- **Program Errors & Unknown System Bugs:** these issues are usually caused by coding errors or software bugs, which can be exploited to install a given malware (mainly Trojan or worm) to establish access to a given device or for reconnaissance purposes. In fact, they can also be related to security, software or programming bugs especially when different systems are communicating with each other. Such bugs are usually vulnerabilities that are exploited to gain or maintain access over a given system.
- **Unknown System Vulnerabilities:** are usually exploited by zero-day attacks such as the recent case of the Log4j (i.e CVE-2021-44228, CVE-2021-442288, CVE-2021-45046 variants) [264] that caused a cyber-security flaw (December 2021) since such vulnerabilities are only known to the attacker, and they are very difficult to prevent. Hence, the importance of adopting penetration testing.
- **Hardware Vulnerability:** is related to the IoT hardware equipment that are fragile and not tamper resistant, making them more prone to destruction, physical tampering, damage or damage beyond recovery. Other vulnerabilities may cause systems to overheat, melt down, burn down or even explode. Therefore, it is also important to check the quality of the hardware and hardware equipment in-use, and ensure that their use will be in a safe, secure and suitable environment.
- **Poor IT Skills:** are usually caused by the lack of training of IT security personnel who would have limited experience and skills. Therefore, continuous training must be maintained to ensure a high level of readiness and a low risk of failure.
- **Accidents:** can be intentional as the ones caused by rogue employees, or unintentional due to lack of employees' training. The associated errors can be minor, but sometimes they can be major causing the system to crash and thus, affecting its availability. Hence, accountability must be enforced, while creating a team spirit among co-workers to avoid mistreatment and lack of performance.

- **Lack of CERT:** Described as the lack of training that the IT security staff undergoes in order to become part of the "Computer Emergency Response Team" (CERT) [265]. In fact, it is highly recommended to address to such a vulnerability and threat accurately, effectively, efficiently, and on time.

4.2.2. *Technical & operational vulnerability*

Operational vulnerabilities requires constant scanning to assess their exploitable vulnerability level [266], as well as to detect and identify the Advanced Persistent Threat (APT) strategy [267]. However, it is important to identify and classify them first.

- **System Privileges:** admin privileges that are not properly assigned, or exploited access controls, or unchanged defaults can also be misused and exploited, especially by insiders or leaked by whistleblowers.
- **Resource-Constrained Devices:** especially IoT devices with limited battery life, or that are resource-constrained in terms of memory and computational power require more a much more specialised compatible version to rely on in order to operate [268]. This also requires a special security measures being adopted to ensure an active security measure in a timely manner and without affecting their performance.
- **Vendors Software:** In many cases, vendors employ software without taking into consideration the security aspect of its given design, especially when left unpatched or misconfigured [269]. Moreover, software is either employed with no security protection, or with very weak security protection, which compromises the software [270]. In fact, using sandboxing can be a good practice for an IoT system's poor or misconfiguration [271].
- **Untested Applications:** Many applications remain untested and unevaluated to check their security and vulnerability levels. Therefore, these applications are left unevaluated without being deemed as either secure or non-secure. Thus, leaving them prone to various attacks types including surveillance attacks.
- **Hardware Components:** Many hardware components lack of the necessary physical protection and security against any possible physical attack based on an unauthorised access. Therefore, it is essential to protect servers and storage areas from any possible and unwanted physical access to prevent any physical/logical damage.

In brief, all these vulnerabilities are summarised in Fig. 6, along with their most suitable solution.

5. Ethical hacking

In the era where ethical hacking is gaining a great fame and popularity with an increased adoption and appliance to test the IoT security, it is important to identify its life-cycle. Moreover, the tools used in its life-cycle events must also be highlighted in order to know how the process proceeds.

5.1. *Ethical hacking life-cycle*

Ethical hacking life-cycle is closely similar to normal hacking life-cycle with only a slight difference based on the fact that ethical hackers aim to cause no harm nor damage to a given IoT server, system, device or domain unlike black-hat hackers (see Fig. 7 and Fig. 8). In fact, it is further illustrated in Fig. 8.

- **Reconnaissance:** The reconnaissance phase is based on the use of the available processes and techniques that can either be used covertly, or deliberately in order to gather information about IoT systems or/and users via open or less-secure IoT servers or/and ports through network mapping. This includes IoT-related details such as the Wi-Fi/network in use, type of connected machines/devices, along their software, hardware and Operating System (OS).
- **Scanning:** aims to discover any IoT-related security or/and vulnerability gap(s) that can be used to conduct the attack. This includes the search for open or/and unused open ports, live hosts, devices, systems and services, along configuration/security vulnerabilities in firewalls, Intrusion Detection Systems/Intrusion Preventing Systems (IDS/IPS), as well as routers and switches [188,272].
- **Gaining Access:** is based on gaining unauthorised but simulated access to an IoT system, application, server or device. This is achieved by relying on various penetration testing tools and techniques to

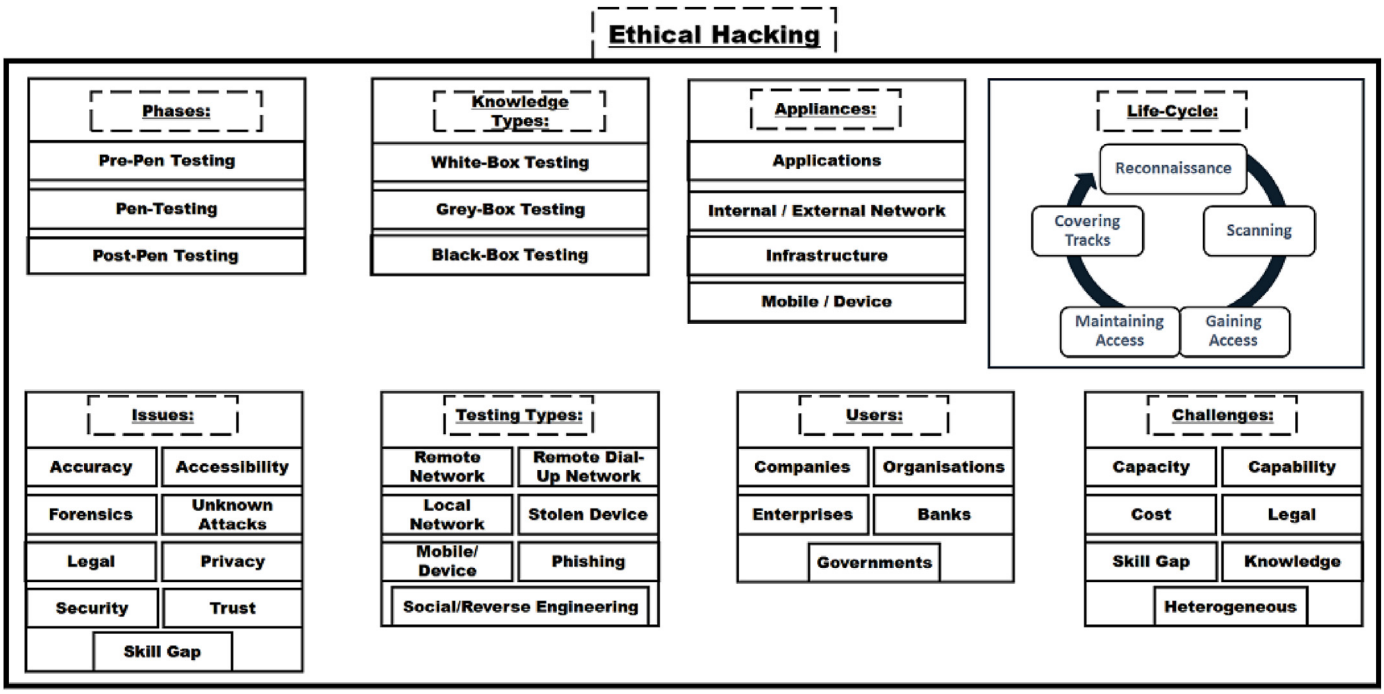

Fig. 7. Proposed general taxonomy for ethical hacking process.

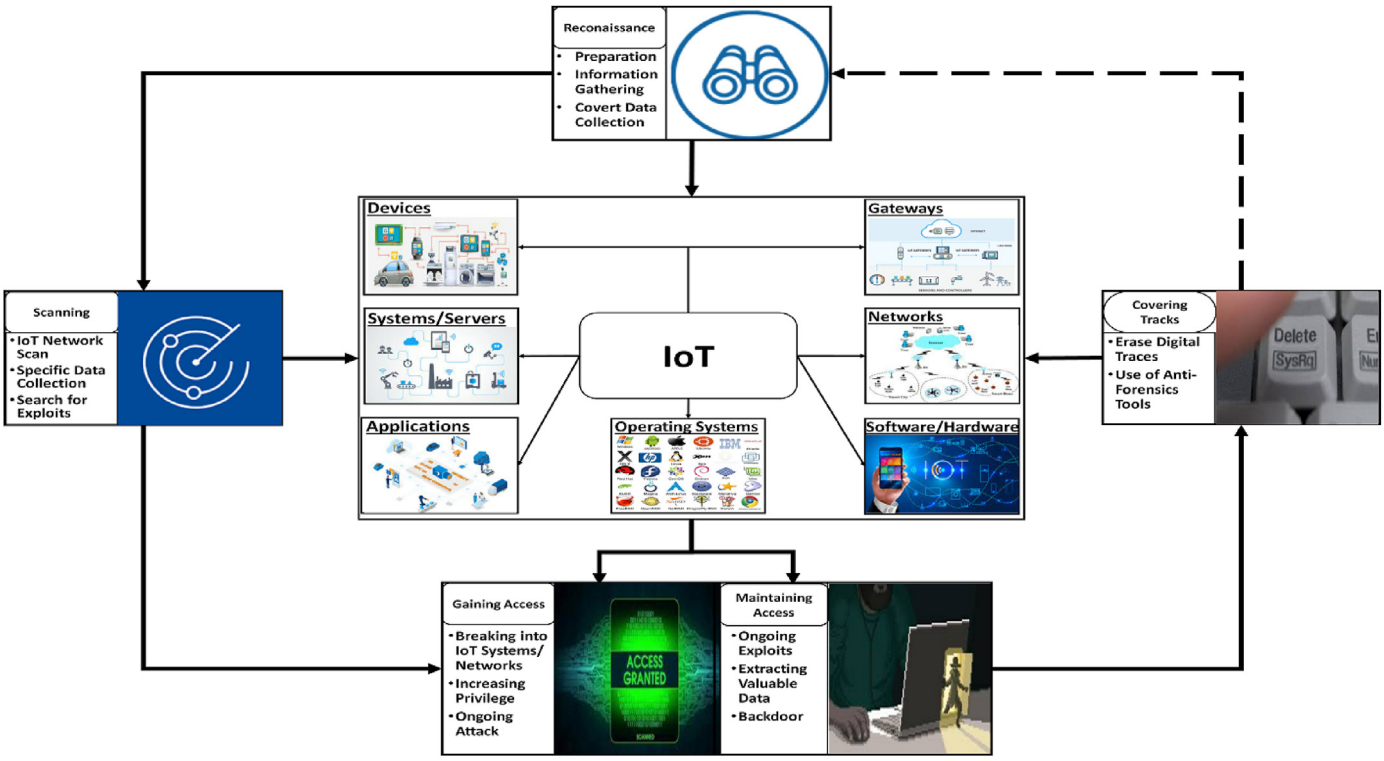

Fig. 8. Appliance of the hacking concept on IoT-related domains and components, where ethical hackers stop at gaining access.

virtually break into the system and bypass the security measures. Thus, targeting the authorisation or authentication of a given IoT system.

- **Maintaining Access:** Once access into a given IoT system, device, or server is gained using tools [110], the system's resources can be exploited by seeking other common vulnerable devices [273,274].

Table 5
Web-based Ethical Hacking tools that can be employed with the IoT Web-applications servers.

Tools	Definition	Description	Operating System(s)	Tasks	Type	Programming Language
Acunetix	Web-based	Web Application Security Scanner	RedHat, Mac, Windows-based	End-to-end web security scanning	Commercial	C++
Netsparker	Web-based	Hacking Web Applications	Web-servers, application server-based	Accurate/automated application security tester	Commercial	JavaScript, Ajax
Sqlmap	Web-based	SQL Injection	CentOS, Red Hat, Linux, Windows-based	Detects and exploits SQL injection flaws	Open Source	Python
Nikto	Web-based	Web Server Scanning Tool	Unix, Mac, Linux, Windows-based	Hacks web servers, Scans for dangerous files, suspicious/outdated versions	Open Source	Perl
Burp Suite	Web-based	Web Vulnerability Scanning	Mac, Linux, Windows-based	Web vulnerability scanner and web application security	Commercial	Java, Python, Ruby
OWASP ZAP	Web-based	Web Application Security Scanner	Mac, Linux, Windows-based	hijacks sessions, manipulates passing traffic, tests the security of web applications	Open Source	Java
Recon-ng	Web-based	Web Reconnaissance Framework	Linux-based	Used for quick and efficient web-based reconnaissance	Open Source	Python
Invicti	Web-based	Web Application Security Scanner	Linux, Windows-based	Detects SQL Injection, XSS and other vulnerabilities	Commercial	C++
Fortify WebInspect	Web-based	Dynamic Application Security Testing	Web-servers, application server-based	Identifies security vulnerabilities, informs on vulnerability trending, compliance management, and risk oversight	Commercial	C/C++, C#, VB.NET, and ASP.NE
Sboxr	Web-based	Web Application Vulnerability Testing	Web-servers, application server-based	Customises security scanners, detects false positives/negatives	Open-Source	Python, Ruby, C# or VB.NET
Uniscan	Web-based	Web Application Penetration Testing Tool	Linux-based	Performs stress test, web or server fingerprinting, dynamic or static test option	Open Source	Perl
Ping Utility	Web-based	Ping Service Scanner	Linux, Windows-based	Pings to any IP or domain and gives their approximate geographical location	Open Source	HTML
OUILookup	Web-based	MAC Address Vendor Lookup Tool	Linux, Windows-based	Easy to use, allows partial MAC address search	Open Source	NodeJS, PHP, Python

- **Security Reports:** following the successful completion of the previous phases, a security report is presented to show the main systems' and personnel's vulnerabilities and how they were exploited or can be exploited in each phase. Weak security measures and practices are also flagged and highlighted to enhance the adoption of more protective and proactive security solutions to reduce the risk of exposure to cyber-attacks. Risk and vulnerability assessment methods are also suggested to maintain or reduce risks to an acceptable level.

5.2. Ethical hacking tools

In order to achieve the intended ethical hacking cycle, different tools should be used so ethical hackers can perform and conduct their simulated attack against any IoT system, server, application or device. Furthermore, Tables 5-8, present a summary of the most famous tools used for ethical hacking purposes. To further divides this, Ethical Hacking for IoT (EHIoT) can be adopted over different IoT parts including:

1. **Web-based:** where EHIoT tools are used to scan web applications and web-servers to detect security gaps and vulnerabilities to prevent their exploit by malicious entities. These main tools are summarised in Table 5.
2. **Cloud-Based:** where EHIoT tools primary used to track and trace attacks using forensics tools and also to monitor performance issues and reduce security risks, while trying to re-ensure compliance and accountability. The main tools are presented in Table 6.
3. **Network-based:** where EHIoT tools are used to monitor and scan IoT networks for any security vulnerability or gap, as well as to test the strength of the password/encryption that is used to secure IoT communications/connections. These main tools are summarised in Table 7.
4. **Application-based:** where EHIoT tools are used to evaluate the security level of IoT applications, and to check if they still perform well in case of an event taking place, while also adding the forensics part to retrieve artefacts in case of attacks. The main used tools are summarised in Table 8.

5.3. Ethical hacking challenges

There are various challenges that the surround the ethical hacking domain. In fact, it is very important to highlight them to identify the problem, verify the challenge and overcome them both. However, these challenges are not limited to one or two aspects, but to various different aspects instead.

- **Capability Challenges:** Many challenges are related to the lack of experience and skills gained over time. In fact, there's a threshold difference between different ethical hacking teams [276]. Moreover, there's no standardised threshold that unifies the skills and experience of ethical hackers into a single capability and capacity. Therefore, some ethical hacking teams may have more skills, experience, and knowledge, compared to other groups when performing their penetration testing to secure an IoT system/device, along with the availability of a much more sophisticated tools and kits.
- **Capacity Challenges:** Another challenge is performing the necessary penetration testing in order to evaluate the level of security and immunity of a given IoT system or organisation against cyber-attacks, especially in terms of risk management [277]. The capacity is based on the limited experienced manpower, and the available resources, used to perform the penetration testing technique(s) and attack(s). Therefore, this is another challenge that requires a deeper focus and attention in order to address to it.
- **Cost Challenges:** The cost of performing a penetration testing attack is not cheap, but rather expensive. However, it is necessary to avoid any exploitation of any vulnerability or security gap [276]. In fact, penetration testing is divided into two main steps. The first one requires the identification of already existing exploitable IoT vulnerabilities which requires a defined cost. The next step is based on the ability to offer security measures to further protect the IoT system, which also requires an additional cost.
- **Legal Challenges:** Many legal challenges also surround the ethical hackers within the ethical hacking domain, especially when its conducted against an IoT system or domain. In other terms, ethical hackers do not perform their penetration testing without signing a legal document called the Non-Disclosure Agreement (NDA). This also requires notifying the required authorities so their testing is not classified as a cyber-crime. Therefore, without the signing of legal processes, ethical hackers risk being legally prosecuted and arrested [278]. This is due to the absence of a uniform/universal and legal jurisdiction processing system to achieve a unified mutual cooperation between pen testers and ethical hackers.
- **Knowledge Challenges:** Knowledge challenges are based on the ability of ethical hackers to perform their penetration testing against IoT's exploitable vulnerabilities and security gaps. This includes software bug, misconfiguration or other bugs (i.e hardware, configuration, or coding). However, their penetration testing and knowledge are based on the ability to identify and overcome the only already existing attacks. In other terms, penetration testing is unable to detect new attacks such a zero-day attacks [279]. This is due to these attacks being based on exploiting a vulnerability that was not detected by ethical hackers who were conducting their penetration testing. This also includes the birthday attack [280,281] in a way, which is quite similar to zero-day. Also, the presence polymorphic malware [282] and encrypting services that keep on changing their signature and behaviour patterns. Thus, their identification and mitigation process remains as a serious challenge. This is all due to their ability to avoid and evade being detected by intrusion detection systems, firewalls and anti-viruses.
- **Data Management Challenges:** especially when it comes to processing the intercepted data, which depends on its volume, size, type, compatibility, processing speed, homogeneous/heterogeneous nature, validation, consistency, trust, and location, especially in case where ethical hackers are dealing with big data [283,284]. This also depends on data compatibility with the in-use ethical hacking tools to ensure that the collected data would not result into it being damaged, altered or modified in a way that damages the IoT system, server, application, etc, nor would result into further security breach nor information/data leaks.

Table 6
Cloud-based Ethical Hacking tools that can be employed with IoT-Cloud domains.

Tools	Definition	Description	Operating System(s)	Tasks	Type	Programming Language
Intruder	Cloud-based	Cloud-based Finding	Cloud platforms	Finding/fixing vulnerabilities	Commercial	Python
LiveAction	Cloud-based	Powerful Network Forensics Software	Mac, Linux, Windows-based	monitors performance issues and reduces security risks using Omnipeek	Commercial	C++
QualysGuard	Cloud-based	Scalable Online Hacking Tools	UNIX, Windows-based	helps businesses streamline their security and compliance solutions	Commercial	Java

Table 7
Network-based Ethical Hacking tools that can be employed to detect vulnerability within IoT networks.

Tools	Definition	Description	Operating System(s)	Tasks	Type	Programming Language
Nmap	Network-based	Network Vulnerability Scanner	OpenBSD, Solaris, Mac, Linux, Windows-based	Computer security/Network management, network and port security scanner	Open Source	C, Python, Lua, C++
Aircrack-Ng	Network-based	Packet Sniffer/WiFi Cracker	BSD, Solaris, eComStation 2, Mac, Linux, Windows-based	Supports wireless network security and interface controllers	Open Source	C
Wireshark	Network-based	Data Packet Analyser	BSD, Mac, Linux, windows-based	Analyses data packets, decrypts many protocols, performs live capture and offline analysis	Open Source	C
OpenVAS	Network-based	Open Vulnerability Assessment Scanner	Linux, Windows-based	Unauthenticated and authenticated testing, uses high-level and low-level internet/industrial protocols	Open Source	C
NetStumbler	Network-based	Wireless Networking Tool	Windows-based	Verifies network poor coverage, detects wireless interference/rogue access points	Open Source	C
Maltego	Server-based	Link Analysis and Data Mining Tool	Mac, Linux, Windows	Real-time data mining and information gathering	Commercial	Python
Ettercap	Network-based	Network Sniffing	BSD/Solaris/MAC, Linux, Windows-based	Network/host analysis, Content filtering, live connections sniffing	Open Source	C
John the Ripper	Network-based	Password Cracking Tool	DOS/Open VMS, Windows-based	Performs dictionary attacks, detects weak UNIX passwords	Open Source	C
Angry IP Scanner	Network-based	IP Scanner Tool	Mac, Linux, Windows-based	Scans IP addresses and ports on local networks and Internet	Open Source	Java
HOIC	Network-based	Network Stress Testing Tool	Mac, Linux, Windows-based	Denial-of-service application, floods targeted systems with requests	Open Source	C#
L0phtCrack	Network-based	System Hacking Tool	Solaris, BSD, Linux, Windows-based	Deduces passwords, uses password hashes, searches for weak passwords	Commercial	C
NetBIOS	Netwok-based	Non-routable OSI Session Layer 5 Protocol	Linux, Windows-based	Reads/writes on remote systems, initiate DoS attacks	Open Source	C
The Hydra	Network-based	Fast Network Logon Password Cracking Tool	QNX, Mac, Linux-based	Password/username guessing, login credential cracking, targets specific ports	Open Source	C++
Security Event Manager	Network-based	Network Security Event Manager	Mac, Linux, Windows-based	Detects threats, monitors security policies, and protects networks	Commercial	C and C++
Traceroute NG	Network-based	Network Path Analyser Tool	ReactOS, Linux, Windows-based	Provides accurate analysis, allows continuous network probing	Open Source	TCL [275]
Kismet	Network-based	Wireless Network Scanner Tool	Mac, Linux, Windows-based	Identifies networks, collects packets and detects hidden/non-beaconing networks	Open Source	Python, C++
Zenmap	Network-based	Official Nmap Security Scanner Software	BSD, Mac, Linux, Windows-based	Tracks new hosts, new and existing downed services	Open Source	Python
SuperScan	Network-based	Network Mapper	FreeBSD, Unix, Linux, Windows-based	Scans TCP ports and fixes the issues with hostnames and views their response, performs ping and port scans	Open Source	Python, C#, Java and PHP
Hping/Hping3	Network-based	Network Security Scanner	BSD, Solaris, Mac, Linux, Windows-based	Sends packets and displays target replies, handles packet body and size, used to transfer files, tests firewall rules, performs port scanning and network performance	Open Source	C/TCL
Fluxion	Network-based	Wireless Network Security Tool	Linux, Windows-based	Audits the Access Point (AP) security, recovers Wifi-Protected Access (WPA/WPA2) keys, conducts Handshake Snopper and Captive Portal attacks	Open Source	Bash, Python
MAC lookup	Network-based	MAC Address Scanner	Android Mac, Linux, Unix, Windows-based	Identifies the type of the device and the manufacturer, ensures real-time geographical location	Open Source	Python

- **Forensics Challenges:** in many cases the use of forensics and anti-forensics in the phase to cover tracks is not always taken into consideration, or it was lightly considered. This, in turn, proves to be challenging for ethical hackers to fulfill the whole ”hacking phase”, which on the same time would also affect how First Incident Responders Team (FIRT) would react and what forensics tools do they need to use to track and trace the attacker and counter his use of anti-forensics tools [285].
- **Cloud Computing Challenges:** cloud computing is one of the main key challenges that surround the ethical hacking domain [286], especially since according to FinTech News, attacks against cloud computing increased by 630% between January and April 2020 [287]. These attack included data breaches, malware injection, DoS, and account hijacking.

5.4. Ethical hacking issues

Ethical hacking has been prone to lots of different issues that surround this domain, especially when being applied on IoT, due to ethical hackers lacking skills, experience and knowledge for a start [288]. There is also different varieties of performing different ethical hacking tests. As a result, these varieties have their own advantages and drawbacks. However, there are far more important issues that require attention first.

- **Privacy:** The privacy issue must be taken very seriously, especially when an IoT system’s vulnerability is being exposed due a simulated penetration testing attack being conducted by ethical hackers. Such a simulated attack mainly targets the privacy of this organisation including data, information, and user’s privacy [289].
- **Security:** Security issues are more related to the lack of experience, knowledge and skills among the ethical hacking team that is performing the penetration testing [290]. It is also related to the weak security measures and access control mechanisms employed by a given organisation to protect itself from any given physical access attempt(s).
- **Trust:** issues are primary related to fully trusting a third (suspicious) party [291] in order to evaluate the IoT system’s security level(s) [292]. In fact, performing penetration testing would allow ethical

Table 8
Application-based Ethical Hacking tools that can be employed to detect security vulnerabilities/gaps found within IoT entities (End devices with OS, Servers/Fog), in addition to user desktop or mobile.

Tools	Definition	Description	Operating System(s)	Tasks	Type	Programming Language
Metasploit	Application-based	Anti-forensic Tool Builder	Mac, Linux, Windows-based	Covering Tracks/artefacts, provides remote machine testing, understand security vulnerabilities	Open Source	Perl
Metasploit Pro	Application-based	Pen Testing Software	Mac, Linux, Windows-based	Develops and executes exploit codes against remote machines, create security testing tools	Commercial	Ruby
Kiuwan	Application-based	Code Security	Unix, Mac, Linux, Windows-based	Reviews software source codes to identify sources of vulnerabilities	Commercial	Java
SET	Application-based	Social Engineering Toolkit	Mac, Linux-based	Provides a phishing utility, performs social engineering activities	Open Source	Python
njRAT	Application-based	RAT Hacking Tool	Linux, Windows-based	Gets remote access, registers keystrokes, steals passwords, activates webcam	Commercial	Python
Sn1per	Application-based	Automated Security Vulnerability Scanner	Linux, Windows-based	Duplicate sites for phishing and social designing purposes	Open Source	Ruby
Cain and Abel	Application-based	Password Recovery Tool	Windows-based	Sniffs networks, recovers MS Access passwords, and cracks encrypted ones	Open Source	Visual C++
Hashcat	Application-based	Robust Password Cracking and Ethical Hacking Tool	Mac, Linux, Windows-based	Recovers lost passwords and audits password security	Open-Source	OCL and C
RainbowCrack	Application-based	Password Cracking and Ethical Hacking Tool	Linux, Windows-based	Generates rainbow tables for password cracking, while reducing the time length	Commerical	Python
IKECrack	Application-based	Authentication Cracker Tool	Mac, Linux, Windows-based	Performs brute-force/dictionary attacks, Pre-Shared-Key analysis and cryptography tasks	Open-Source	C, Perl
Medusa	Application-based	Best Parallel Password cracker Tool	SunOS, BSD, Linux, Mac, Windows-based	Supports many services with remote authentication, performs Thread-based parallel/Brute-force testing	Open-Source	Python, Ruby

hackers to know all information about the organisation. This includes their exploitable vulnerabilities and available security gaps.

- **Legal and Law Issues:** issues are highly emerging, especially since ethical hackers need to perform a simulated cyber-attack or/and hacking which, in real cases, would be classified as a cyber-crime [293]. Therefore, the reliance on signing a non-disclosure agreement to protect both sides is mandatory. Moreover, when performing simulated insider attacks, police law enforcement and local authorities must be notified, so that in case the organisation managed to capture an ethical hacker, there will not be any prosecution(s) nor arrest(s). Therefore, this is another important issue that requires some serious attention.
- **Forensics:** Many ethical hackers lack the ability to make use of forensic tools and techniques to retrieve any data from logs and audits to check for failed login attempt(s) or abnormal network behaviour. In some cases, ethical hackers rely on the use of anti-forensic techniques to simulate an advanced attack to uncover the attacker's track(s). This method is performed and applied in order to check the ability of a given organisation to defend, detect and locate the attacker. In fact, it is classified as another issue, where most ethical hackers have little knowledge in the digital forensics domain [10,11,294], including cloud forensics [258], mobile/computer forensics [295], and web-applications [296], especially when these fields are linked and connected to the IoT domain.
- **Budget Constraints:** are still challenging since the budget limit is not sufficient to purchase a software package quality to use it on different IoT devices.
- **Compatibility Issues:** are still challenging as its still difficult to conduct ethical hacking tasks due to them requiring a specialised interface, hardware/software, and locating/extracting digital file systems from volatile/non-volatile computer memory. This also raises compatibility issues due to having different manufacturers.

6. Penetration testing

Penetration testing requires the presence of ethical hackers in a certified/verified professional way that guarantees their safety and the organisation's safety and security in any IoT domain. Therefore, it is highly important to know how penetration testing is linked to ethical hackers, and how ethical hackers perform their duties and tasks.

Penetration tests are conducted to evaluate the levels of IoT security and immunity of a given IT and non-IT systems and personnel against security gaps and/or exploitable vulnerabilities [297] from already known or unknown attacks. A vulnerability can possibly exist in an OS due to design flaw, mis-configuration, software bug or even failure. Therefore, the aim of penetration testing is to safeguard the information from any alteration, modification or disclosure from already known threats and/or attacks. As such, different security measures were suggested and presented by different papers including [298,299]. Such papers, presented the implementation of the right Access Control mechanisms, along with a strong authentication process. This was accompanied by the implementation of additional firewalls, Intrusion Detection/Intrusion Prevention systems, and cryptographic mechanisms to protect data's Confidentiality, Integrity and Availability (CIA), as well as privacy and authentication.

Penetration testing has its own advantages and drawbacks that one must understand before diving deeper into the this subject, especially when its being applied to the IoT domain. The main advantages of penetration testing are based on ensuring the right evaluations through the tests to achieve a proactive security approach [297]. Such approach allows the exploration and detection of security risks accurately, whilst ensuring a system's adaptation to real-time changes. Moreover, penetration testing helps with the investigation of data breaches and network intrusions. As a result, advanced penetration testing was introduced in Ref. [300], based on the latest available security exploitation and research. Unlike traditional penetration testing, the organisation is made aware of the importance and reliance on solid, well-built incident response team and program to adhere to any emerging threat before it even occurs [301].

6.1. Penetration testing tools

To ensure the most effective and successful penetration testing for IoT, different tools are being effectively used for this specific task, of which many in-use tools were presented in Ref. [258], with a brief comparison between vulnerability assessment and penetration testing being made in Ref. [302]. Nonetheless, these main penetration testing tools will be highlighted and summarised in Table 9.

Table 9
Famous penetration testing tools that can be used on IoT devices, servers in addition to user(s) devices that have operating system.

Penetration Testing Tools	Description
Acunetix	Scans and detects web vulnerabilities including XSS, SQL Injection, Code execution and File inclusion/upload form
Burp Suite	Used for Pen-Test and security websites, capable of Proxy Interception, write plugins, and Automatic vulnerability detection
Backbox Linux	Focuses on penetration testing and safety assessment and penetration testing, mainly used for the analysis of web applications and networks
Kali Linux	An advanced penetration testing and Security Auditing, with hundreds of tools to perform PenTesting, Forensics and Reverse Engineering, and other wireless, web an network security analysis
Nessus	Deals with a large number of network devices, also used for web applications penetration testing
Parrot Security OS	Highly efficient lightweight OS designed for ethical hacking, computer forensics testing, cryptography and other security tasks
Samurai Web Testing Framework	Preconfigured framework that functions as a web pen -testing platform, capable of detection website code vulnerabilities
SQLmap	Automated command line capable of detecting and exploiting any SQL Injection vulnerability, whilst extracting information from databases

6.2. Penetration testing knowledge types

Penetration testing knowledge is usually divided into three main types [303]. Each type is classified as part of the conducted penetration testing in order to evaluate the level of security and immunity of a given organisation in each tested case [304,305].

Moreover, box testing technique are presented in Table 10.

Table 10
Existing Box testing Techniques [306,307].

Testing Type	Testing Technique	Description
White Box Testing	Statement Coverage	Used to test every statement more than once. Tool in use: Cantata++
	Decision Coverage	Used to test every decision condition including conditional loops more than once. Tool in use: TCAT-PATH
	Condition Coverage	Ensures a one-time code execution mandatory once conditions are tested
	Decision/Condition Coverage	Used to test all the Decision/Condition coverage during the code execution
	Multiple Condition Coverage	Each system entry point is executed more than once
Black Box Testing	Finds errors in the input values boundaries	Finds errors in the input values boundaries
	Equivalence Class Partitioning	Excessive application testing to input redundancy. Inputs divided into classes with values for each class
	Decision Table Based Testing	Employed when the action is applied under unstable varying conditions
	Cause-Effect Graphing Technique	Operates on a system's external behaviour only, and helps selecting and creating test cases
	Error Guessing	Success rate depends on the experience of the tester. Test cases are written while reading a document or when encountering an undocumented error
Grey box Testing	Matrix Testing	Defines all the existing variables on a given program
	Regression Testing	Relies on retest all, retest risky use cases, retest within a firewall strategies to check if previous changes regressed other program's new version aspects
	Pattern Testing	Goes through the code to identify the cause of failure by retrieving historical data of the previously defected system
	Orthogonal Array Testing	Offers the most code coverage with the least test cases

- **White-Box Testing:** is also known as open box testing [306]. It is based on having full knowledge regarding the intended and targeted IoT system in addition to all its software and firmware components. White box testing is based on the attacker's ability to have an insider (i.e whistle-blower) with a full knowledge over how a program runs. However, White-Box testing is less time consuming since there's a prior full knowledge of the IoT system. This makes it very suitable for testing algorithms. It also ensures that all logical decisions are being verified, and ensures syntax checking with any possible design error.
- **Grey-Box Testing:** is also known as translucent testing. It is based on having a secondary knowledge about the IoT system, due to the internal programming being partially known. Unlike White box testing, it is not time consuming [307]. However, it is not suitable for testing algorithms. In fact, it is non-intrusive and unbiased, with the least risk of conflicts between testers and developers.
- **Black-Box Testing:** can also include application black-box testing [308]. In fact, testers do not have any prior knowledge regarding the internal/external IoT system, nor over the software and firmware structure used [306]. Moreover it can also be tested on android applications [309]. As a result, such a test is conducted based on the user's perspective and not the designer's perspective. Despite that the program used is not known. A pen-tester may be an expert, since testers rely on any system contradictions. This testing form is very time consuming as there is no prior knowledge to the tested system. However, it is not useful for testing algorithms, nor complex segments of code since many program paths are left untested. In fact, it is also known as **Behavioural Testing** and can either be functional or non-functional.

6.3. Penetration testing appliance

Penetration Testing can also be applied to other IoT domains such as the applications and networks domains. In fact, it is applied to evaluate the levels of security in a given application and network both internally and externally, to avoid any possible exploitation. In other terms, penetration testing can be applied in application penetration testing, internal/external network penetration testing, and infrastructure/application penetration testing.

- **Application Penetration Testing:** including mobile and web application pen testing [310], aims to reveal possible application vulnerabilities, security risks, weaknesses and flaws by relying on real-case strategies and attacks. This is done via a close cooperation and collaboration in-between IoT applications and IT infrastructure through servers, networks and devices alike to detect and overcome any exploitable vulnerability or security gap. Application and Web Application penetration testing focuses on reviewing the authorisation, data protection and security configuration mechanisms.
- **Internal & External IoT Network Penetration Testing:** aims to detect the main IoT network vulnerabilities [311] by conducting a series of simulation attack scenarios using the Kali Linux Operating System platform [312]. It tries to identify the exploited vulnerability(ies) or/and security gap(s) along the path of the attack in order to assess its likelihood and impact. Thus, offering the necessary recommendations to protect a network both internally and externally.
- **Cloud Penetration Testing:** is applied to the cloud infrastructure domains as part of pen testing in clouds or cloud pen testing [313] and includes both corporate applications and integrated networks [314]. The aim is to identify any attack's path based on identified security gap, while assessing the likelihood and impact of a similar potential attack type against the IoT in cloud [315].

6.4. Existing solutions

To ensure a much more accurate and successful penetration testing process, various solutions were presented using different techniques and tools to safeguard and maintain a secure IoT environment. Different protective precautions and actions have been already taken into consideration [12] to protect a system from any cyber-attack based on ethical hacking techniques, rather than only training managers [316].

- **Ethical Hacking:** is an essential method to simulate the lifecycle adopted by a hacker or an attacker to simulate an attack against an IoT system, application/OS, or network. Therefore, a variety of solutions was presented. Greenwald et al. developed a methodology that provides an automated generation and execution of remote testing plans by using modeling techniques from partially observable Markov decision processes (POMDPs) [317]. The authors demonstrated the efficiency of the approximation algorithm used to satisfy performance requirements of penetration test planning. Trivedi presented an online comprehensive solution for network administrators that use popular exploits and network intrusion tools on their own private network to detect any breach/flaw and preserve confidential data [318]. As a result, an IDS was presented to prevent cross-scripting vulnerabilities.

In [319], Lu et al. analysed the Shadowcrew network to examine the social organisation of a hacking community using social networking methods for text mining and network analysis. Their analysis revealed the hackers' decentralized network structure as well as their organisation's structure. Zhou et al. presented a system that offers ethical hackers computer forensics training to maintain data protection under attack, while also analysing the organisation's security policies and strategies [320]. Thus, offering a proper Analysis System for Computer Forensic Education, Training & Awareness (ASCFETA) plan. However, the system is prone to various limitations including the accuracy of data-limits, which affect the decision-making process. In Ref. [321], Alazab et al. surveyed the existing trends in crime toolkits and offered a case study on the Zeus botnet.

A variety of exploit types was presented to predict future attack trends, while stating that security measures such as behavioural analysis or whitelists are necessary as countermeasures. In Ref. [201], Sood et al. analysed the components and techniques used by the SpyEye botnet malware and presented an example and analysis of the third-generation botnets. The analysis was a static-behavioural one to understand SpyEye's characteristics and exploitation techniques. In Ref. [322], Abbasi et al. presented a scalable and generalised framework that identified expert hackers and characterised their specialities by analysing their forum content on social media platforms, using text analytics for a key hacker identification and analysis. Results revealed the hackers' interaction network along the content-based clustering of key actors within the hacking community. Angmo et al. discussed and analysed the use of selenium suite in Ref. [323], which combines different automated testing tools and provides testers with various frameworks for different web testing cases. A performance evaluation shows how the selenium web-driver is a better tool than Watir web-driver.

In [316], Hajdarevic et al. addressed the threat of resource starvation attacks by presenting a simulation-based training scenario that allows trainees to experience the effect of new/old DDoS attack forms and how to initiate a response in a simulated environment. However, accurate results were not offered. Sandhya et al. presented an approach based on the use of the Wireshark packet sniffing tool to allow ethical hackers to reveal the system security flaws at the user authentication level to check whether a website is secure or not [324]. The adoption of this approach offered a faster vulnerability identification at a higher success rate. In Ref. [325], Tetskyi et al. described the web service design that relied on the use of neural networks to create a decision support tool for web applications penetration testing. However, this solution was prone to various setbacks related mainly to the high expertise and flexibility requirements. In Ref. [326], Bailey et al. presented an innovative approach based on an ethical hacking game, Self-Adaptive Authorisation Framework (SAAF), which is protected by a self-adaptive authorisation infrastructure to allow the observation of the user's activity pre/post-adaptation. Live experiments managed to capture a wide range of malicious behaviour, related to exploiting vulnerabilities, in an effective and efficient manner without any administrator interference.

- **Penetration Testing:** Penetration testing is an essential method to reveal how a system or network is vulnerable or how the adopted security measures suffer from an exploitable security gap. As a result, various solutions were presented. Rushing et al. described a software project named Collaborative Penetration-testing and Analysis Toolkit (CPAT) that helps network security analysts with performing penetration tests by using network analysis technologies and tools in a collaborative environment with reactive data management [327]. However, results are still to be reported. Visoottiviseth et al. developed a PENTOS as a penetration testing system for IoT devices designed for ethical hacking and used to determine both IoT risks and vulnerabilities [328]. Moreover, PENTOS offers penetration testing on IoT devices including password, web, and wireless attacks followed by a summary on the result of attacks while offering security recommendations.

Ning et al. presented a penetration attack tree model that describes, organises, classifies, manages, and schedules the attacks for Attack Resistance Test (ART) [329]. Results show how this model offers a detailed description of the logical relationship of attacks while providing guidance for penetration attacks. Almubairik et al. presented a systematic penetration testing algorithm guided by a threat model to ensure that all threat models are checked [330]. The appliance of this model to a real system reduced the consequences that can result from malicious attacks in a shorter time since the tester is relieved from monotonous tasks. However, further research is required to cover other threats such as SQL threats, cross-site scripting, and mail threats.

Bechtsoudis et al. revealed how a comprehensive security level can be reached through extensive Penetration Tests (Ethical Hacking) [331]. A Penetration Test methodology and framework were presented to expose any exploitable vulnerability per network layer. Results show how a common network mis-configuration was exploited to compromise the internal network. This provided evidence on how regular penetration tests must be conducted on the organisation network. Jiajia offered a penetration testing method based on mobile internet that uses the actual network to build a platform to complete the plan of executing a pen test based on the existing vulnerabilities of mobile internet [332]. Results show that the mobile communication terminal is mostly affected by the web pressure test and the energy consumption. In Ref. [333], a mobile penetration testing specialised company named Attify, started giving courses, writing books and conducting live penetration testing on different IoT domains to offer a more secure use of mobile devices.

Lastly, Hu et al. presented an automated penetration testing framework that employs deep reinforcement learning based on the Deep Q-Learning Network (DQN) method to help with the automation of the penetration testing process. This framework can also be used for defense training by recreating simulated attacks in the training environment [334]. Optimal results show that DQN's accuracy in fighting the optimal attack path is 86%

- **Vulnerability Assessment:** VA solutions are presented to assess and evaluate the threats related to IoT websites, networks, OS/applications, and devices through simulation attacks to prevent their exploitation. As a result, various VAPT tools are presented. Shah et al. worked on developing NetNirikshak 1.0 as a new automated Vulnerability Assessment and Penetration Testing (VAPT) Tool to address the threats that target data/services' Integrity and

Confidentiality [335]. NetNirikshak 1.0 was reportedly useful against SQL injection (SQLi) vulnerabilities while tracing back the source of the attack. However, NetNirikshak 1.0 is only limited to the SQLi and cannot detect Cross Site Scripting (XSS), OS Command Injection, etc.

Goel et al. explained how the VAPT concept can be used as an effective cyber defence technology, while offering further details about VAPT's life cycle, and techniques along the top 15 vulnerability assessment tools [257]. The authors presented an Ensemble approach called 'VEnsemble 1.0' model that combines multiple VAPT tools (open source/premium) to achieve a higher accuracy than previous solutions [336]. Simulations show how VEnsemble 1.0 offers a higher accuracy in detecting different types of vulnerabilities at a reduced cost.

The above solutions are summarised in Table 11.

7. IoT Security & Safety Procedures

Despite the different preventive and protective IoT security measures being recommended, many steps need to be considered to ensure that the adopted security and safety measures are both enforced and properly introduced into the IoT domain. As a result, (first) incident responders must be distinguished and classified to maintain the right response against a given event(s). Once achieved, preventive and protective security measures must be employed for further protection. Finally, these security measures must be employed to maintain and ensure the right level of protection, while respecting the main security goals.

Table 11
Existing solutions of Penetration Testing that can be applied to IoT.

Year	Reference	Authors	Solution	Details
2008	[329]	Ning et al.	Penetration testing Solutions	List and description of existing PT solutions
2010	[318]	Trivedi et al.	Comprehensive online tool [WR-3]	Analyses any network security flaw
2012	[320]	Zhou et al.	ASCFETA	Part of an Organisation's security policy
2013	[321]	Alazab et al.	Crime tool kit investigation	Study of malware type, variation & quality
2014	[335]	Shah et al.	"Net-Nirikshak 1.0" model	Facilitates VAPT in Indian banks
2014	[322]	Abbasi et al.	Social media analytical model	Extracts interactions between users & hacking communities
2015	[327]	Rushing et al.	CPAT	Suitable for penetration testing data reconnaissance phase
2016	[336]	Goel et al.	"VEnsemble 1.0" approach	A VAPT that detects different vulnerability types
2016	[330]	Almubairik et al.	Threat model driven approach	Evaluates the immunity of tested systems against attack types
2017	[328]	Visoottiviseth et al.	PENTOS	Determines risks/ vulnerabilities of IoT devices
2017	[324]	Sandhya et al.	Use of Wireshark	Assesses website security
2018	[325]	Tetskyi et al.	Neural Network based	Creates decision support tool for Web application penetration testing
2018	[326]	Bailey et al.	Ethical game of hacking	Handles malicious behaviour of real & intelligent users

7.1. IT security policy

A great deal of emphasis should be placed on the security and safety procedures, where each employee must respect and adhere to in any IoT domain. This can only be achieved through continuous training and awareness while maintaining accountability. The list of various policies involved in the process is presented below:

1. **Adoption of Cyber-Security for IoT standards:** which are essential to maintain the right security measures and standards that are compatible with the IoT market (i.e users, customers, manufacturers, etc) and domain (IoT servers, systems, devices, etc).
   - **ETSI EN 303 645:** ETSI EN 303 645 v2.1.1 is a global standard that is applicable for consumer IoT cyber security, which covers all consumer IoT devices with a good security baseline being established [337]. It consists of 13 high-level recommendations to establish 35 recommendations, 68 provisions, 33 mandatory requirements. This standard serves as a guidance tool for IoT manufacturers as it also offers examples of how each provision's implementation can be provided [338]. A test specification was also released by the European Telecommunications Standards Institute (ETSI) named ETSI TS 103 701, to describe in a comprehensive way how conformity assessment can be achieved, to harmonize the evaluation methodologies and support manufacturers, suppliers for their internal security processes [339].
   - **NISTIR 8259:** provides guidance for both manufacturers and their supporting third parties to design, test and support IoT devices. The series consists of three final documents and one draft document [340].
   - **NISTIR 8259:** includes recommendations for IoT device manufacturers.
   - **NISTIR 8259A:** includes the IoT core device cyber-security technical capability baseline [341].
   - **NISTIR 8259B:** includes the IoT non-technical supporting capability core baseline [341].
   - **NISTIR 8259C (DRAFT):** creates a profile using the IoT Core and Non-Technical Baselines (NISTIR 8259A/B) to create tailored IoT cyber-security requirements sets [342].

7.2. Incident response

In case of an incident, a response is automatically triggered, where responders are called upon the occurrence of a security event for them to respond with the right security measures and countermeasures to mitigate any attack that targets the IoT domain in a real-time manner and reduces the risk's occurrence and likelihood. Such responses can either be active, passive, or hybrid. This depends on the responders' training, skills, experience, available resources, and manpower, as well as on the attacker's motives and gains. As such, they can be classed as active (i.e ability to "counter-back" any given attack against an IoT system [343]), passive (i.e taking defensive counter-measures to overcome it) or hybrid (i.e using a "Smart Response" using smart AI-based security measures). Preventive and protective security measures can be adopted to protect IoT's network, system and users' data [344], such as the use of symmetric encryption [345,346] including the post-quantum cryptography [347, 348].

8. Learnt lessons

After conducting this survey, the main weak and strong points of penetration testing for IoT are identified, along with those found in the ethical hacking domain.

- **Standard Security Solutions:** are required and more specialised security (counter) measures should be applied instead, as vulnerabilities differ from one IoT device, system, or protocol to another. This is due to the heterogeneous nature of IoT devices, protocols, operating systems, etc, making them more prone to a larger variety of different and dangerous vulnerability types and exploitable security gaps.
- **Continuous Security/Awareness Training:** which is recommended while adopting specialised security guidelines, especially accountability, depending on the IoT layers, systems, devices, etc, as well as the adoption of seminars and training sessions to keep the users posted and updated.
- **Enhanced Security Designs:** which are essential ahead of their implementation and adoption using ethical hacking and penetration testing tools for IoT, which can be built based on the Artificial Intelligence (AI) based on Machine Learning (ML) solutions to ensure higher accuracy and reduce false negatives and false positives with a lesser response time to react and interact.
- **More Investment:** is needed in this domain, which requires a higher budget to be spent to raise awareness, train uniform/non-uniform personnel, assert both responsibility and accountability, as well as to train more ethical hackers and penetration testers to specialize, improve their knowledge, experience, skills and available tools.
- **Legal Authorisation:** laws must protect and support ethical hackers during their simulated attacks, where pre and post-agreements are needed to be established first, to legally maintain their safety and security.
- **Forensics Knowledge:** the need for more knowledge about forensics and expertise is also required to conduct much more effective and efficient penetration testing.

9. Future research directions

Securing IoT systems have undergone great progress in the last few years, but there are still several challenges that lurk ahead, which may be tackled in the next few years and decades. Security, safety, and privacy are still causing a serious challenge since a given attacker (i.e hacker) can maliciously exploit these IoT end devices, which in turn, can lead to complete or partial control of other IoT end devices, servers, or the whole systems. Therefore, We present several potential research directions in the following to improve PT for IoT systems:

- **Enable AI-based Solutions:** especially since AI plays a key role to enable innovative penetration testing and ethical hacking solutions. This is due to the ability to react to any discovered security vulnerabilities in one of the following ways:
  1. **Detect:** AI-based solutions can detect IoT-based security gaps and vulnerabilities with higher accuracy, with lesser time, and lesser false positives and false negatives.
  2. **Prevent:** AI-based solutions can ensure a much more effective solution at mitigating threats and preventing IoT-based attacks at a faster rate, more effectively, and more accurately.
  3. **Correct:** AI-based solutions can also offer a corrective process similar to the "self-healing" concept especially for hybrid [349] and distributed [350] IoT systems and applications [351] more accurately and with lesser execution time, fault tolerance and error rates.
  4. **Mixed:** AI-based solutions are usually adopted when the process requires either "Detection and Prevention" or "Detection and Correction" tasks or both, depending on the incident's occurrence or type (i.e. attack or accident).

Sometimes, the detection process cannot be achieved especially in the case of advanced passive attack types (i.e Footprinting, War driving, or Spying) [352,353]. Hence, an urgent and persistent need for more sophisticated tools to detect attacks in their early phase to prevent them from further spreading and damaging the IoT system, network, application, or device.

- **Enable smart automated PT Solutions:** which should be enabled in a real-time manner to achieve the necessary functionalities of IoT entities and application requirements. This can be achieved by relying on AI-based solutions which play a key role in detecting security vulnerabilities.
- **Enhanced IoT Corrective Solutions:** must be maintained to "correct" and overcome detected IoT security vulnerabilities. This includes enhanced Intrusion Prevention Systems, and next-generation firewalls while ensuring a secure and verified data backup, with alternative devices being available for necessary computational requirements.

on the other hand, existing PT detection solutions (network or host) or correction ones can benefit from the advancements of AI to enhance PT accuracy level.

10. Suggestions & recommendations

Despite having different IoT security measures available for implementation and deployment, in this paper we present several suggestions and recommendations to support the ethical hacking domain and to enhance penetration testing for IoT systems. Also, we propose the following "Personnel and User Security Awareness Training (PaUSAT)" (see Fig. 9) assigned to each working staff depending on their job nature in a given enterprise or organisation, to establish and achieve both compliance and accountability.

- **Maintaining Privacy:** and respecting it, especially of both IoT users and companies during the conduction of ethical hacking and penetration testing processes to ensure that it is protected during the whole process.
- **Multi-Factor Authentication** must be adopted to prevent any unauthorised access or abused legal access to IoT systems or devices that transmit, receive, or store sensitive data or information.
- **Lightweight Security Mechanisms:** such as lightweight encryption and lightweight intrusion detection systems can be applied to resource-constrained IoT devices to ensure that they are also protected against any possible malicious event(s) such as security exploits or attacks, and to ensure a safer transmission of real-time IoT data based on a trade-off between IoT's system performance, security and privacy mechanisms.
- **Enforced policies:** the adoption of identification, authorisation, and authentication policies prevents unauthorised entities/users from accessing IoT systems, which makes them less prone to insider threats and attacks.
- **Real-time isolation:** the need to implement real-time proactive and protective security/safety mechanisms that instantly disconnect or forcibly shutdown any compromised IoT device(s) once a security threat is detected. This will ensure that the compromised IoT device(s) will not be (remotely) controlled nor exploited by an adversary.
- **Safer IoT Designs:** all IoT systems, applications, operating systems, and end-devices must undergo a safety check test before and after achieving the required design to reduce the likelihood and the occurrence of any potential risk that may target any of the presented IoT parts.
- **Fulfilling Skill-Gaps:** is caused due to the lack of available skilled ethical hackers. Hence, more advertisements and recruitment campaigns, seminars, and conferences are needed to encourage and educate more people to join the ethical hacking domain.
- **Specialised Training:** especially security training must be assigned for each staff/employee category to overcome and address different attack types that they might encounter in their fields.

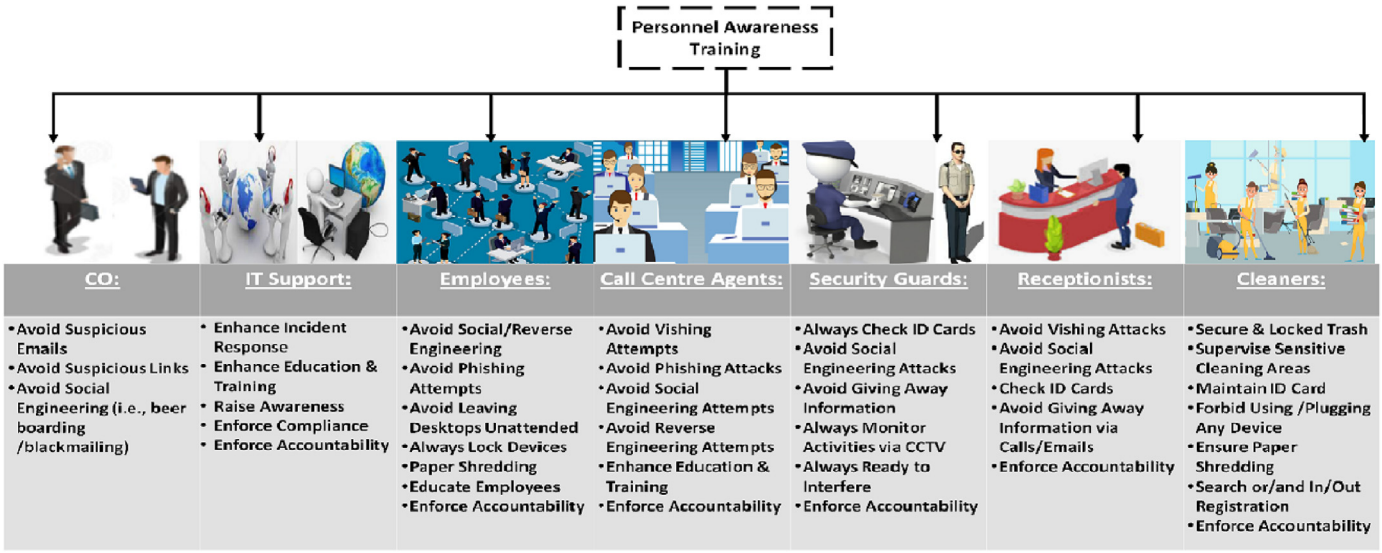

Fig. 9. Suggested User/Personnel Security Awareness Training for IoT User-related fields.

- **International Exchange & Competitions:** are needed to enhance the experience and skills that can be acquired via gaming challenges, along with the establishment of new fundamentals for (potential) ethical hackers to follow. This also includes workshops, formations, and educative online courses.
- **Cyber threat intelligence:** CTI is also important and should be considered as a means to mitigate mainly external threats (and internal ones) since it focuses on their ongoing gained knowledge, experience, and skills based on previous attack occurrences [354]. This is always done before assessing both cyber and physical threats and identifying/defining their threat actors [355] to identify potential attacks to mitigate them and overcome harmful events before their occurrence and how to cyber defenders will react in case of an attack [356].

In fact, the recommended security and safety measures regarding the IoT can be summarised in the following Fig. 10.

Nonetheless, future perspectives and scope regarding ethical hacking and penetration testing for IoT domains should also be highlighted.

- **New Jobs & Opportunities:** ethical hacking and penetration testing jobs are the fastest growing jobs in IT (security) units of prominent organisations and industries. Such jobs are available in the private sector, governments, military, and law enforcement including investigative agencies such as the National Security Agency (NSA) and the Federal Bureau of Information (FBI).
- **Outside the Box Thinking:** ethical hackers need to be creative problem-solvers to be able to detect and fix unknown system vulnerabilities before their exploitation. This type of thinking is being adopted now in an attempt to remain one step ahead of the attacker.
- **Enhanced Critical Decision Making:** is another aspect that security firms are looking for, especially among the new generation of ethical hackers, as they are expected to remain vigilant, on high alert, and in some cases part of the rapid incident response team.
- **New Skills:** are always required depending on which organization the ethical hacker and pen tester are working for. It is important to

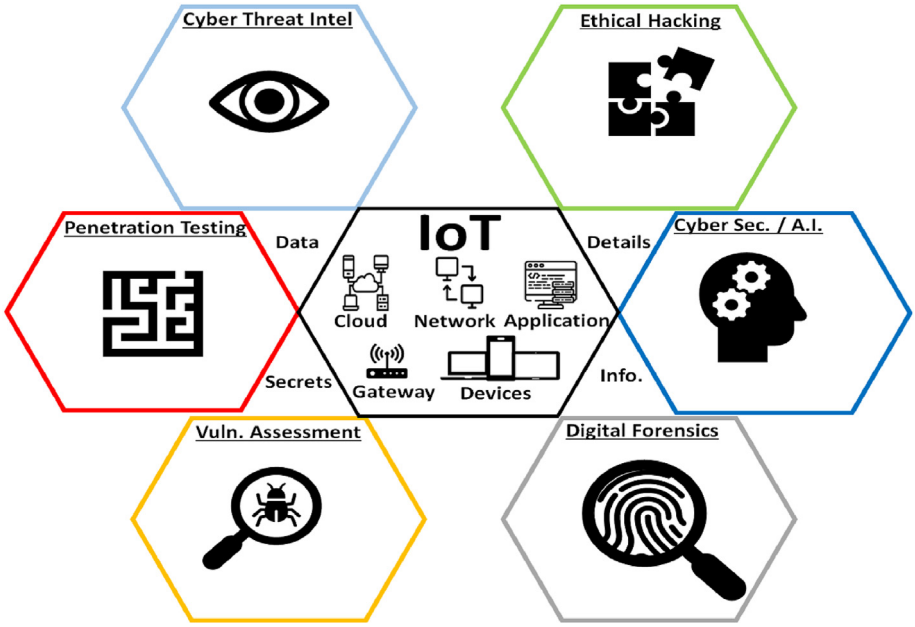

Fig. 10. Recommended security and safety measures to secure and protect the IoT domain.

enhance their collaboration and communication skills, as well as their project planning, task handling, project planning, and management.

11. Conclusion

In this paper, the importance of conducting penetration testing for IoT systems along with the reliance on trusted ethical hackers to perform simulated attacks are highlighted and discussed thoroughly. This enables the assessment of the security level against common IoT threats and attacks and provides a better understanding of the evaluation, assessment, and mitigation of any given risk against the IoT domain, including options to detect, patch, and update IoT systems. Moreover, we highlight the key differences between hacking and ethical hacking in IoT systems. On the other hand, we describe how hackers operate according to their objectives, goals, motives, gains, and benefits. We present various taxonomies and frameworks as an overview regarding the hacking domain in general that are in common with the IoT domain. Finally, many recommendations and suggestions are proposed to further train employees, IT staff, and security personnel, in addition to insights about future work to protect IoT systems by using smart automated ethical hacking and penetration testing solutions.

Authorship clarified

Jean-Paul A. Yaacoub: Writing- Original draft preparation, conceptualization, methodology. **Hassan N. Noura**: Validation, writing- Original draft preparation, conceptualization, methodology. **Ola Salman**: Validation, writing- Original draft preparation, conceptualization, methodology. **Ali Chehab**: Validation, writing- Original draft preparation, conceptualization, methodology.

Funding

This research was supported by funds from the EIPHI Graduate School (contract "ANR-17-EURE-0002").

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Prabhat Thakur. Mathematical Modelling of Spectrum Sharing in Cognitive Radio Communication Systems.
[2] Kaneez Fizza, Abhik Banerjee, Karan Mitra, Prem Prakash Jayaraman, Rajiv Ranjan, Pankesh Patel, Dimitrios Georgakopoulos, Qoe in iot: a vision, survey and future directions, Discover Internet of Things 1 (1) (2021) 1–14.
[3] Rabie Ramadan, Internet of things (iot) security vulnerabilities: a review, PLOMS AI 2 (1) (2022).
[4] Binbin Zhao, Shouling Ji, Jiacheng Xu, Tian Yuan, Qiuyang Wei, Qinying Wang, Chenyang Lyu, Xuhong Zhang, Changting Lin, Jingzheng Wu, et al., A large-scale empirical analysis of the vulnerabilities introduced by third-party components in iot firmware, in: Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis, 2022, pp. 442–454.
[5] Jean-Paul A. Yaacoub, Mohamad Noura, Hassan N. Noura, Ola Salman, Yaacoub Elias, Raphaël Couturier, Chehab Ali, Securing internet of medical things systems: limitations, issues and recommendations, Future Generat. Comput. Syst. 105 (2020) 581–606.
[6] Shriya S. Shetty, Rithika R. Shetty, Tanisha G. Shetty, Divya Jennifer D'Souza, Survey of hacking techniques and it's prevention, in: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), IEEE, 2017, pp. 1940–1945.
[7] Radana Dvorak, Heather Dillon, Nicole Ralston, Jeffrey Matthew Welch, Exploring ethical hacking from multiple viewpoints, in: 2020 ASEE Virtual Annual Conference Content Access, 2020.
[8] Urshila Ravindran, Raghu Vamsi Potukuchi, Yufei Peng, Hua Li, Xiaoyan Li, Jikang Wang, Xinyu Zhang, Amruta Khare, Ganesh M. Kakandikar, Omkar K. Kulkarni, A review on web application vulnerability assessment and penetration testing, J. homepage 9 (1) (2022) 1–22, journals/rces.
[9] Sib tul Hassan, Analysis of vulnerabilities in system by penetration testing, Pakistan J. Sci. Res. 2 (1) (2022) 22–25.
[10] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Chehab Ali, Digital Forensics vs. Anti-digital Forensics: Techniques, Limitations and Recommendations, 2021 *arXiv preprint arXiv:2103.17028*.
[11] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Chehab Ali, Advanced Digital Forensics and Anti-digital Forensics for Iot Systems: Techniques, Limitations and Recommendations, Internet of Things, 2022, 100544.
[12] Michael Kassner, Ethical Hackers' Top Motivation Isn't Money, According to Hackerone - Techrepublic, February 2018. https://www.techrepublic.com/article/ethical-hackers-top-motivation-isnt-money-according-to-hackerone/. (Accessed 11 January 2019).
[13] Jacob G. Oakley, Why human hackers?, in: Professional Red Teaming Springer, 2019, pp. 15–28.
[14] Aaron Yi Ding, Gianluca Limon De Jesus, Marijn Janssen, Ethical hacking for boosting iot vulnerability management: a first look into bug bounty programs and responsible disclosure, in: Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing, ACM, 2019 pages 49–55.
[15] Sara N. Matheu, Jose L. Hernandez-Ramos, Antonio F. Skarmeta, Gianmarco Baldini, A survey of cybersecurity certification for the internet of things, ACM Comput. Surv. 53 (6) (2020) 1–36.
[16] Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, Mohsen Guizani, A survey of machine and deep learning methods for internet of things (iot) security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1646–1685.
[17] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, Biplab Sikdar, A survey on iot security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.
[18] Wan Haslina Hassan, et al., Current research on internet of things (iot) security: a survey, Comput. Network. 148 (2019) 283–294.
[19] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi, Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28.
[20] Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Chehab Ali, Mohamad Malli, Cyber-physical systems security: limitations, issues and future trends, Microprocess. Microsyst. 77 (2020), 103201.
[21] Noura Hassan, Tarif Hatoum, Ola Salman, Jean-Paul Yaacoub, Chehab Ali, Lorawan security survey: issues, threats and possible mitigation techniques, Int. Things 12 (2020), 100303.
[22] Jean Paul A. Yaacoub, Javier Hernandez Fernandez, Hassan N. Noura, Chehab Ali, Security of power line communication systems: issues, limitations and existing solutions, Comp. Sci. Rev. 39 (2021), 100331.
[23] Jean-Paul Yaacoub, Ola Salman, Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations, Internet of Things, 2020, 100218.
[24] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Chehab Ali, Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations, Int. J. Inf. Secur. (2021) 1–44.
[25] Danielle Griffith, Innovation at the edge: iot 2.0, in: 2022 IEEE Asian Solid-State Circuits Conference (A-SSCC), IEEE, 2022, pp. 2–3.
[26] Ian Zhou, Imran Makhdoom, Negin Shariati, Muhammad Ahmad Raza, Rasool Keshavarz, Justin Lipman, Mehran Abolhasan, Abbas Jamalipour, Internet of things 2.0: concepts, applications, and future directions, IEEE Access 9 (2021) 70961–71012.
[27] Emily Chow, Ethical Hacking & Penetration Testing, vol. 626, University of Waterloo, Waterloo, Canada, No. AC, 2011.
[28] Matt Bishop, About penetration testing, IEEE Secur. Priv. (6) (2007) 84–87.
[29] Patrick Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier, 2013.
[30] Rafay Baloch, Ethical Hacking and Penetration Testing Guide, Auerbach Publications, 2017.
[31] Bharat S. Rawal, Gunasekaran Manogaran, Alexender Peter, The basics of hacking and penetration testing, in: Cybersecurity and Identity Access Management, Springer, 2023, pp. 21–46.
[32] Shicheng Zhu, Shunkun Yang, Xiaodong Gou, Yang Xu, Tao Zhang, Yueliang Wan, Survey of testing methods and testbed development concerning internet of things, Wireless Pers. Commun. 123 (1) (2022) 165–194.
[33] Stephen Russell, Tarek Abdelzaher, The internet of battlefield things: the next generation of command, control, communications and intelligence (c3i) decision-making, in: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), IEEE, 2018, pp. 737–742.
[34] Vishal Gotarane, Sandeep Raskar, Iot practices in military applications, in: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, 2019, pp. 891–894.
[35] Chinonso Okereke, Nur Haliza Abdul Wahab, Mohd Murtadha Mohamad, et al. Autonomous Underwater Vehicle in Internet of Underwater Things: A Survey.
[36] Yutian Zhang, Jun Ni, Hanqing Tian, Wei Wu, Jibin Hu, Integrated robust dynamics control of all-wheel-independently-actuated unmanned ground vehicle in diagonal steering, Mech. Syst. Signal Process. 164 (2022), 108263.

[37] Bisma Bashir, Aqeel Khalique, A review on security versus ethics, Int. J. Comput. Appl. 151 (11) (2016) 13–17.
[38] Somosri Hore, Kumarshankar Raychaudhuri, Cyber espionage—an ethical analysis, in: Innovations in Computational Intelligence and Computer Vision, Springer, 2021, pp. 34–40.
[39] AF Almeida Virgilio, Danilo Doneda, Jacqueline de Souza Abreu, Cyberwarfare and digital governance, IEEE Int. Comput. 21 (2) (2017) 68–71.
[40] Raji Youssef Al-Bayati, Cyber terrorism (models of international efforts to reduce it), Tikrit J. Polit. Sci. 2 (28) (2022) 91–121.
[41] Victoria Jangada Correia, An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom, SN Comput. Sci. 3 (1) (2022) 1–31.
[42] Denham Byron, Ransomware and Malware Sandboxing, 2022.
[43] César Brito, Luis Pinto, Victor Marinho, Sara Paiva, Pedro Pinto, A review on recent advances in implanted medical devices security, in: 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, 2021, pp. 1–6.
[44] Ying He, Ruben Suxo Camacho, Soygazi Hasan, Cunjin Luo, Attacking and defence pathways for intelligent medical diagnosis system (imds), Int. J. Med. Inf. 148 (2021), 104415.
[45] Dennis Broeders, Els de Busser, Fabio Cristiano, Tatiana Tropina, Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand? J. Cyber Pol. (2022) 1–39.
[46] Oxford Analytica. Unequal Israeli-Iranian Cyberwar Will Escalate. Emerald Expert Briefings, (oxan-es).
[47] Eduardo Izycki, Eduardo Wallier Vianna, Critical infrastructure: a battlefield for cyber warfare?, in: ICCWS 2021 16th International Conference on Cyber Warfare and Security Academic Conferences Limited, 2021, p. 454.
[48] Mohee Ahmad, Cyber War: the Hidden Side of the Russian-Ukrainian Crisis, 2022.
[49] George M. Moore, How International Law Applies to Attacks on Nuclear and Associated Facilities in ukraine, 2022.
[50] Don C. Smith, Playing with Fire: Military Attacks against a Civilian Nuclear Power Station, 2022.
[51] Sourav Banerjee, Chinmay Chakraborty, Sumit Chatterjee, A survey on iot based traffic control and prediction mechanism, in: Internet of Things and Big Data Analytics for Smart Generation, Springer, 2019, pp. 53–75.
[52] Fenghua Zhu, Yisheng Lv, Yuanyuan Chen, Xiao Wang, Gang Xiong, Fei-Yue Wang, Parallel transportation systems: toward iot-enabled smart urban traffic control and management, IEEE Trans. Intell. Transport. Syst. 21 (10) (2019) 4063–4071.
[53] Sara Oleiro Araújo, Ricardo Silva Peres, José Barata, Fernando Lidon, José Cochicho Ramalho, Characterising the agriculture 4.0 landscape—emerging trends, challenges and opportunities, Agronomy 11 (4) (2021) 667.
[54] Bam Bahadur Sinha, R. Dhanalakshmi, Recent advancements and challenges of internet of things in smart agriculture: a survey, Future Generat. Comput. Syst. 126 (2022) 169–184.
[55] PRZETACZNIK Jakub, Russia's War on ukraine: Timeline of Cyber-Attacks, 2022.
[56] Réka Szabó, Cyber Warfare in the Ukrainian Conflict—A Determinant of the Outcome of the War?, 2022.
[57] Sanjeet Kumar and Sahila Chaudhry. Risk of Hacking in E-Banking: A Study of Private Sector Banks.
[58] Pierre Thalamy, Piranda Benoit, Julien Bourgeois, Engineering efficient and massively parallel 3d self-reconfiguration using sandboxing, scaffolding and coating, Robot. Autonom. Syst. 146 (2021), 103875.
[59] Melanie Schranz, Martina Umlauft, Micha Sende, Wilfried Elmenreich, Swarm robotic behaviors and current applications, Front. Robot. AI 7 (2020) 36.
[60] Rune Langleite, Carsten Griwodz, Frank T. Johnsen, Military Applications of Internet of Things: Operational Concerns Explored in Context of a Prototype Wearable, 2021.
[61] Lin Zhu, Suryadipta Majumdar, Chinwe Ekenna, An invisible warfare with the internet of battlefield things: a literature review, Hum. behav. emerg. technol. 3 (2) (2021) 255–260.
[62] Martti Lehto, Cyber-attacks against critical infrastructure, in: Cyber Security, Springer, 2022, pp. 3–42.
[63] Vasile Coman, et al., The use of cyber attacks during traditional armed conflicts. specific and the commitment of state responsibility, J. Law and Publ. Administr. 8 (15) (2022) 35–44.
[64] Emily Caroscio, Jack Paul, John Murray, Suman Bhunia, Analyzing the ransomware attack on dc metropolitan police department by babuk, in: 2022 IEEE International Systems Conference (SysCon), IEEE, 2022, pp. 1–8.
[65] Andrew Feutrill, Dinesha Ranathunga, Yuval Yarom, Matthew Roughan, The effect of common vulnerability scoring system metrics on vulnerability exploit delay, in: 2018 Sixth International Symposium on Computing and Networking (CANDAR), IEEE, 2018, pp. 1–10.
[66] Mikhail Buinevich, Konstantin Izrailov, Andrei Vladyko, Testing of utilities for finding vulnerabilities in the machine code of telecommunication devices, in: 2017 19th International Conference on Advanced Communication Technology (ICACT), IEEE, 2017, pp. 408–414.
[67] Petar Čisar, Sanja Maravić Čisar, General vulnerability aspects of internet of things, in: 2015 16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI), IEEE, 2015, pp. 117–121.
[68] Butun Ismail, Patrik Österberg, Houbing Song, Security of the internet of things: vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. Tutor. 22 (1) (2019) 616–644.
[69] Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese, Andrea Zanella, Iot: internet of threats? a survey of practical security vulnerabilities in real iot devices, IEEE Internet Things J. 6 (5) (2019) 8182–8201.
[70] Tim Jordan, Paul Taylor, A sociology of hackers, Socio. Rev. 46 (4) (1998) 757–780.
[71] Jens David Ohlin, Did Russian cyber interference in the 2016 election violate international law, Tex. Law Rev. 95 (2016) 1579.
[72] Steve Mansfield-Devine, Hacktivism: Assessing the Damage, vol. 2011, Network Security, 2011, pp. 5–13, 8.
[73] Tracey Caldwell, Hacktivism Goes Hardcore, vol. 2015, Network Security, 2015, pp. 12–17, 5.
[74] E Denning Dorothy, Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy, Netw. netwars: The future of terror, crime, and militancy 239 (2001) 288.
[75] Gabriel Jozsef Berecz, István Gergely Czibula, Hunting traits for cryptojackers, ICETE (2) (2019) 386–393.
[76] John Glynn, Online gaming: a virtual experiment in the dark side of human nature, Skeptic 24 (1) (2019) 14–18.
[77] Bruce Schneier, Invited talk: the coming ai hackers, in: International Symposium on Cyber Security Cryptography and Machine Learning, Springer, 2021, pp. 336–360.
[78] Lech Janczewski, Andrew Colarik, Cyber Warfare and Cyber Terrorism, IGI Global, 2007.
[79] Randy Borum, John Felker, Sean Kern, Kristen Dennesen, Tonya Feyes, Strategic cyber intelligence, Inf. & Comput. Secur. 23 (3) (2015) 317–332.
[80] Sanjay Goel, Cyberwarfare: connecting the dots in cyber intelligence, Commun. ACM 54 (8) (2011) 132–140.
[81] Libicki Martin, The coming of cyber espionage norms, in: 2017 9th International Conference on Cyber Conflict (CyCon), IEEE, 2017, pp. 1–17.
[82] Nadav Morag, Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats, Colorado Technical University, October, 2014 media/CTU/Files/ThoughtLeadership/cybercrime-white-paper. ashx.
[83] Mihoko Matsubara, Countering cyber-espionage and sabotage: the next steps for Japanese–uk cyber-security co-operation, Rusi 159 (1) (2014) 86–93.
[84] Ellen Nakashima, Report on 'operation Shady Rat'identifies Widespread Cyber-Spying, vol. 3, 2011. Washington Post.
[85] Timothy Sablik, et al., Cyberattacks and the digital dilemma, Econ. Focus (3Q) (2017) 8–11.
[86] Sultana Sharmeen Karim, Cyber-crime Scenario in Banking Sector of bangladesh: an Overview, –44, 2016, pp. 12–19.
[87] Emma Chanlett-Avery, John W. Rollins, Liana W. Rosen, Catherine A. Theohary, North Korean cyber capabilities, Brief. Congr. Res. Ser. (2017).
[88] Kargl Frank, Joern Maier, Michael Weber, Protecting web servers from distributed denial of service attacks, in: Proceedings of the 10th International Conference on World Wide Web, ACM, 2001, pp. 514–524.
[89] Stas Filshtinskiy, Cybercrime, cyberweapons, cyber wars: is there too much of it in the air? Commun. ACM 56 (6) (2013) 28–30.
[90] Steve M. Furnell, Matthew J. Warren, Computer hacking and cyber terrorism: the real threats in the new millennium? Comput. Secur. 18 (1) (1999) 28–34.
[91] Andrew M. Colarik, Cyber Terrorism: Political and Economic Implications, Igi Global, 2006.
[92] James Andrew Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic & International Studies, Washington, DC, 2002.
[93] Jian Hua, Sanjay Bapna, The economic impact of cyber terrorism, J. Strat. Inf. Syst. 22 (2) (2013) 175–186.
[94] Mohammed Alhamed, Omar M. Alsuhaibany, Website Defacement Incident Handling System, Method, and Computer Program Storage Device, US Patent 8,549,637, October 1 2013.
[95] Robert W. Taylor, Eric J. Fritsch, John Liederbach, Digital Crime and Digital Terrorism, Prentice Hall Press, 2014.
[96] Maurice Dawson, Marwan Omar, Jonathan Abramson, Understanding the methods behind cyber terrorism, in: Encyclopedia of Information Science and Technology, third ed., IGI Global, 2015, pp. 1539–1549.
[97] J.P.I.A.G. Charvat, Cyber terrorism: a new dimension in battlespace, The virt. battlefield: Perspect. cyber warfare 3 (2009) 77–87.
[98] Paulo Shakarian, Shakarian Jana, Andrew Ruef, Introduction to Cyber-Warfare: A Multidisciplinary Approach, Newnes, 2013.
[99] Andy Scollick, The Irish defence forces in the drone age, in: E.U. The (Ed.), Irish Defence Forces and Contemporary Security, Springer, 2023, pp. 295–314.
[100] Fabio Cristiano, Deterritorializing cyber security and warfare in Palestine: hackers, sovereignty, and the national cyberspace as normative, CyberOrient 13 (1) (2019) 28–42.
[101] Anthony J. Mattazaro, The Future Fight: Cyberwar at the Operational Level of War, ARMY COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH KS, 2020. Technical report.
[102] Daniel Cohen, Danielle Levin, Cyber infiltration during operation protective edge, Forbes vol. 12 (August, 12, 2014).
[103] Ilias Kapsis, 7 crypto-assets and criminality, Organised Crime, Financial Crime, and Criminal Justice: Theoretical Concepts and Challenges (2023) 122.
[104] Fabio Cristiano, Palestinian Territory Occupied1, Routledge Companion to Global Cyber-Security Strategy, 2020, p. 35.
[105] Kyung-shick Choi, Claire Seungeun Lee, Robert Cadigan, Spreading propaganda in cyberspace: comparing cyber-resource usage of al qaeda and isis, Int. J. Cybersecur. Int. Cyber. 1 (1) (2018) 21–39.

[106] Sabrine Saad, Muriel Chamoun, Stéphane B. Bazan, Infowar on the web: when the caliphate goes online, in: Proceedings of the ACM Web Science Conference, 2015, pp. 1–3.
[107] Malcolm Nance, Christopher Sampson, Hacking ISIS: How to Destroy the Cyber Jihad, Simon and Schuster, 2017.
[108] Christina Schori Liang, Unveiling the" united cyber caliphate" and the birth of the e-terrorist, Georgetown J. Int. Aff. (2017) 11–20.
[109] David H. McElreath, Daniel Adrian Doss, Leisa McElreath, Ashley Lindsley, Glenna Lusk, Joseph Skinner, Ashley Wellman, The communicating and marketing of radicalism: a case study of isis and cyber recruitment, Int. J. Cyber Warf. Terror. (IJCWT) 8 (3) (2018) 26–45.
[110] Sonali Patil, Ankur Jangra, Mandar Bhale, Akshay Raina, Pratik Kulkarni, Ethical hacking: the need for cyber security, in: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), IEEE, 2017, pp. 1602–1606.
[111] Caroline G. Jones, Computer hackers on the cul-de-sac myspace suicide indictment under the computer fraud and abuse act sets dangerous precedent, Widener L. Rev. 17 (2011) 261.
[112] John McBrayer, Exploiting the Digital Frontier: Hacker Typology and Motivation, The University of Alabama, 2014.
[113] Sandor Vegh, Classifying forms of online activism: the case of cyberprotests against the world bank, in: Cyberactivism, Routledge, 2013, pp. 81–106.
[114] Peter Hays Gries, Tears of rage: Chinese nationalist reactions to the belgrade embassy bombing, China J. (46) (2001) 25–43.
[115] John Sweeney, Jens Holsoe, Ed Vulliamy, Nato bombed Chinese deliberately, Guardian 17 (10) (1999).
[116] Rohan Gunaratna, Inside Al Qaeda: Global Network of Terror, Columbia University Press, 2002.
[117] James P. Farwell, The media strategy of isis, Survival 56 (6) (2014) 49–55.
[118] Judith Tinnes, Bibliography: islamic state (is, isis, isil, daesh)[part 4], Perspectives on Terrorism 12 (2) (2018).
[119] Shehabat Ahmad, Teodor Mitew, Yahia Alzoubi, Encrypted jihad: investigating the role of telegram app in lone wolf attacks in the west, J. Strat. Secur. 10 (3) (2017) 3.
[120] Abdel Bari Atwan, Islamic State: the Digital Caliphate, Univ of California Press, 2015.
[121] Darren Linvill, Matthew Chambers, Jennifer Duck, Steven Sheffield, Mapping the Messenger: Exploring the Disinformation of Qanon, First Monday, 2021.
[122] Martin A. Miller, The dynamics of entangled political violence: from the greensboro massacre (1979) to the war on terror (2001), in: Terrorism and Transatlantic Relations, Springer, 2022, pp. 33–42.
[123] Nigel Copsey, Samuel Merrill, Violence and restraint within antifa, Perspect. terror. 14 (6) (2020) 122–138.
[124] Jessie Daniels, Cyber Racism: White Supremacy Online and the New Attack on Civil Rights, Rowman & Littlefield Publishers, 2009.
[125] Andrew Jakubowicz, et al., Alt_right white lite: trolling, hate speech and cyber racism on social media, Cosmopolitan Civ. Soc.: An Interdiscip. J. 9 (3) (2017) 41.
[126] Jessie Daniels, Cloaked websites: propaganda, cyber-racism and epistemology in the digital era, New Media Soc. 11 (5) (2009) 659–683.
[127] Brian Cashell, William D. Jackson, Mark Jickling, Baird Webel, The Economic Impact of Cyber-Attacks, Congressional Research Service Documents, CRS RL32331, Washington DC), 2004.
[128] Hilary Tuttle, Cybercrime costs businesses $11.7 million per year, Risk Manag. 64 (10) (2017), 36–36.
[129] The global state of information security survey 2018: pwc. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html, October 2017.
[130] Devin Marsh, Are Ethical Hackers The Best Solution For Combating The Growing World Of Cyber-Crime?, PhD thesis University Honors College, Middle Tennessee State University, 2017.
[131] Suphannee Sivakorn, Iasonas Polakis, Angelos D. Keromytis, The cracked cookie jar: http cookie hijacking and the exposure of private information, in: 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 2016, pp. 724–742.
[132] S. Arvind, V Anantha Narayanan, An overview of security in coap: attack and analysis, in: 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), IEEE, 2019, pp. 655–660.
[133] Zach Shelby, Klaus Hartke, Carsten Bormann, The Constrained Application Protocol (Coap), Technical report, 2014.
[134] Wolfgang Müller, Evaluating the Security and Resilience of Typical off the Shelf Coap Iot Devices: Assessing Coap and Wi-Fi Vulnerabilities, 2022.
[135] Muath A. Obaidat, Jian Lim Choong, Kutub Thakur, A secure authentication and access control scheme for coap-based iot, in: 2022 5th Conference on Cloud and Internet of Things (CIoT), IEEE, 2022, pp. 145–149.
[136] Eric Rescorla, Hannes Tschofenig, Nagendra Modadugu, The Datagram Transport Layer Security (Dtls) Protocol Version 1.3, Internet Engineering Task Force, 2019.
[137] Jasone Astorga, Marc Barcelo, Aitor Urbieta, Eduardo Jacob, Revisiting the feasibility of public key cryptography in light of iiot communications, Sensors 22 (7) (2022) 2561.
[138] Yaron Sheffer, Ralph Holz, Peter Saint Andre, Summarizing Known Attacks on Transport Layer Security (Tls) and Datagram Tls (Dtls), Technical report, 2015.
[139] Dahlia Sam, K. Nithya, S. Deepa Kanmani, Adlin Sheeba, A Shamila Ebenezer, B Uma Maheswari, Jennifer Daffodils Amesh, Survey of Risks and Threats in Online Learning Applications, Secure Data Management for Online Learning Applications, 2023, p. 2.
[140] Prakash Umasankar Mukkara, Ajith Kumar, Subbaraju Uppalapati, Vishnu Vardhan, Sureshkumar Thangavel, Secure Network Communications, US Patent 8,468,347, June 18 2013.
[141] Salvatore J. Stolfo, Malek Ben Salem, Shlomo Hershkop, Methods, Systems, and Media for Masquerade Attack Detection by Monitoring Computer User Behavior, US Patent 8,769,684, July 1 2014.
[142] Crispin Cowan, F. Wagle, Calton Pu, Steve Beattie, Jonathan Walpole, Buffer overflows: attacks and defenses for the vulnerability of the decade, in: Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, vol. 2, IEEE, 2000, pp. 119–129.
[143] Krerk Piromsopa, Richard J. Enbody, Survey of protections from buffer-overflow attacks, Eng. J. 15 (2) (2011) 31–52.
[144] Jeremiah Grossman, Whitehat Website Security Statistics Report, 2007. Retrieved March, 8:2010.
[145] Donald Ray, Jay Ligatti, Defining code-injection attacks, ACM Sigplan Not. 47 (2012) 179–190. ACM.
[146] Xing Jin, Xuchao Hu, Kailiang Ying, Wenliang Du, Heng Yin, Gautam Nagesh Peri, Code injection attacks on html5-based mobile apps: characterization, detection and mitigation, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 66–77.
[147] Puspendra Kumar, R.K. Pateriya, A survey on sql injection attacks, detection and prevention techniques, in: Computing Communication & Networking Technologies (ICCCNT), 2012 Third *International Conference on*, IEEE, 2012, pp. 1–5.
[148] Bharti Nagpal, Nanhay Singh, Naresh Chauhan, Angel Panesar, Tool based implementation of sql injection for penetration testing, in: Computing, Communication & Automation (ICCCA), 2015 International Conference on, IEEE, 2015, pp. 746–749.
[149] Diallo Abdoulaye Kindy, Al-Sakib Khan Pathan, A survey on sql injection: vulnerabilities, attacks, and prevention techniques, in: Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on, IEEE, 2011, pp. 468–471.
[150] Yunkai Bai, Andrew Stern, Jungmin Park, Mark Tehranipoor, Domenic Forte, Rascv2: enabling remote access to side-channels for mission critical and iot systems, ACM Trans. Des. Autom. Electron. Syst. 27 (6) (2022) 1–25.
[151] Ahmed Abdullah and Maryam Malik. A Survey on Sql Injection Attacks: Detection and Prevention.
[152] Jonathan Held, Cross-site scripting (xss), in: Encyclopedia of Information Assurance-4 Volume Set (Print), Auerbach Publications, 2010, pp. 638–645.
[153] Ammar Atef Al Azab, Malware Detection and Prevention, Deakin University, 2013. Technical report.
[154] Christian Seifert, Jack Stokes, Long Lu, David Heckerman, Christina Colcernian, Sasi Parthasarathy, Navaneethan Santhanam, Scareware Detection, US Patent 9,130,988, September 8 2015.
[155] Amir Afianian, Salman Niksefat, Babak Sadeghiyan, David Baptiste, Malware dynamic analysis evasion techniques: a survey, ACM Comput. Surv. 52 (6) (2019) 1–28.
[156] Ori Or-Meir, Nir Nissim, Yuval Elovici, Lior Rokach, Dynamic malware analysis in the modern era—a state of the art survey, ACM Comput. Surv. 52 (5) (2019) 1–48.
[157] Qing Hu, Qing Hu, Tamara Dinev, Is spyware an internet nuisance or public menace? Commun. ACM 48 (8) (2005) 61–66.
[158] Swarup Bhunia, M. Tehranipoor, The Hardware Trojan War, Springer, Cham, Switzerland, 2018.
[159] Mohammad Tehranipoor, Farinaz Koushanfar, A survey of hardware trojan taxonomy and detection, IEEE design & test of comput. 27 (1) (2010) 10–25.
[160] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Szydlowski Martin, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna, Your botnet is my botnet: analysis of a botnet takeover, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, ACM, 2009, pp. 635–647.
[161] Heloise Pieterse, Martin Olivier, Design of a hybrid command and control mobile botnet, J. Inf. Warf. 12 (1) (2013) 70–82.
[162] Arash Habibi Lashkari, Seyedeh Ghazal Ghalebandi, Shahab Alizadeh, Rohini Devi, Irc botnet major issues and solutions, in: 2011 2nd International Conference on Networking and Information Technology, vol. 17, IPCSIT, 2011.
[163] Kassidy Clark, Martijn Warnier, Frances MT. Brazier, Botclouds-the future of cloud-based botnets, in: CLOSER. Citeseer, 2011.
[164] Ping Wang, Baber Aslam, Cliff C. Zou, Peer-to-peer botnets, in: Handbook of Information and Communication Security, Springer, 2010, pp. 335–350.
[165] Karim Ahmad, Syed Adeel Ali Shah, Rosli Bin Salleh, Muhammad Arif, Rafidah Md Noor, Mobile botnet attacks–an emerging threat: classification, review and open issues, KSII Trans. Internet and Inf. Syst. (TIIS) 9 (4) (2015) 1471–1492.
[166] E Denning Dorothy, Cyberterrorism: the logic bomb versus the truck bomb, Global Dialog. 2 (4) (2000) 29.
[167] Stephen Northcutt, Logic Bombs, Trojan Horses, and Trap Doors, SANS, 2005, pp. 2005–2016.
[168] Pele Li, Mehdi Salour, Xiao Su, A survey of internet worm detection and containment, IEEE Commun. Surv. Tutor. 10 (1) (2008) 20–35.
[169] Feri Sulianta, Comparison of the computer viruses from time to time, 10.37178/ca-c. 23.1. 139, CENTRAL ASIA AND THE CAUCASUS 23 (1) (2022) 1386–1391.
[170] Peter Szor, The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1, Pearson Education, 2005.
[171] Ken Chiang, Levi Lloyd, A case study of the rustock rootkit and spam bot, HotBots 7 (2007), 10–10.
[172] Zhanjun Zhang, Zhongxiao Man, Yong Li, Improving wójcik's eavesdropping attack on the ping–pong protocol, Phys. Lett. 333 (1–2) (2004) 46–50.

[173] Jr Hubert Rae McLellan, Secure Data Storage with Key Update to Prevent Replay Attacks, US Patent App. 12/015,770, July 23 2009.
[174] Cheng-I Lai, Alberto Abad, Korin Richmond, Junichi Yamagishi, Najim Dehak, Simon King, Attentive filtering networks for audio replay attack detection, in: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2019, pp. 6316–6320.
[175] Meng Liu, Longbiao Wang, Jianwu Dang, Seiichi Nakagawa, Haotian Guan, Xiangang Li, Replay attack detection using magnitude and phase information with attention-based adaptive filters, in: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2019, pp. 6201–6205.
[176] Callegati Franco, Cerroni Walter, Marco Ramilli, Man-in-the-middle attack to the https protocol, IEEE Secur. Priv. 7 (1) (2009) 78–81.
[177] Bhupendra Singh Thakur, Sapna Chaudhary, Content sniffing attack detection in client and server side: a survey, Int. J. Adv. Comput. Res. 3 (2) (2013) 7.
[178] Matt Weir, Sudhir Aggarwal, Breno De Medeiros, Bill Glodek, Password cracking using probabilistic context-free grammars, in: 2009 30th IEEE Symposium on Security and Privacy, IEEE, 2009, pp. 391–405.
[179] Jim Owens, Jeanna Matthews, A study of passwords and methods used in brute-force ssh attacks, in: USENIX Workshop on Large-Scale Exploits and Emergent Threats, LEET), 2008.
[180] Arvind Narayanan, Vitaly Shmatikov, Fast dictionary attacks on passwords using time-space tradeoff, in: Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM, 2005, pp. 364–372.
[181] Hüseyin Demirci, Ali Aydın Selçuk, A meet-in-the-middle attack on 8-round aes, in: International Workshop on Fast Software Encryption, Springer, 2008, pp. 116–126.
[182] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Julio Lopez, Guess again (and again and again): measuring password strength by simulating password-cracking algorithms, in: 2012 IEEE Symposium on Security and Privacy, IEEE, 2012, pp. 523–537.
[183] Panagiotis Papantonakis, Dionisios Pnevmatikatos, Ioannis Papaefstathiou, Charalampos Manifavas, Fast, fpga-based rainbow table creation for attacking encrypted mobile communications, in: 2013 *23rd* International Conference on Field Programmable Logic and Applications, IEEE, 2013, pp. 1–6.
[184] Mihir Bellare, Tadayoshi Kohno, Hash function balance and its impact on birthday attacks, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2004, pp. 401–418.
[185] Sachin Kadloor, Xun Gong, Negar Kiyavash, Tolga Tezcan, Nikita Borisov, Low-cost side channel remote traffic analysis attack in packet networks, in: 2010 IEEE International Conference on Communications, IEEE, 2010, pp. 1–5.
[186] S Praveen Kumar, S. Swapna, Jamming attacks in wireless networks, Int. J. Comput. Sci. Netw. Secur. 13 (10) (2013) 110–113.
[187] Latha Tamilselvan, V. Sankaranarayanan, Prevention of blackhole attack in manet, in: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), IEEE, 2007, 21–21.
[188] Adwan Yasin, Mahmoud Abu Zant, Detecting and isolating black-hole attacks in manet using timer based baited technique, Wireless Commun. Mobile Comput. 2018 (2018).
[189] A. Geetha, N. Sreenath, Byzantine attacks and its security measures in mobile adhoc networks, IJCCIE 2016 (2016).
[190] Anderson Bergamini de Neira, Burak Kantarci, Michele Nogueira, Distributed Denial of Service Attack Prediction: Challenges, Open Issues and Opportunities, Computer Networks, 2023, 109553.
[191] Ivan Ristic, *Bulletproof* SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, Feisty Duck, 2013.
[192] Jani Hautakorpi, Gonzalo Camarillo, R. Penfield, Alan Hawrylyshen, Medhavi Bhatia, Requirements from Session Initiation Protocol (Sip) Session Border Control (Sbc) Deployments. *RFC5853*, IETF, 2010.
[193] M. Hasan, Jag Mohan Thakur, Prajoy Podder, Design and implementation of fhss and dsss for secure data transmission, Int. j. signal proc. syst. 4 (2) (2016) 144–149.
[194] Fahmina Taranum, Ayesha Sarvat, Nooria Ali, Shamekh Siddiqui, Detection and prevention of blackhole node, in: 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), IEEE, 2020, pp. 1–7.
[195] Hanane Kalkha, Satori Hassan, Khalid Satori, Preventing black hole attack in wireless sensor network using hmm, Proc. Comput. Sci. 148 (2019) 552–561.
[196] M.M. Mogunova, Criminal Law Analysis of Cyber Threats in the Business Environment, OF OMSK UNIVERSITY, 2021.
[197] Shaheen Shariff, Confronting Cyber-Bullying: what Schools Need to Know to Control Misconduct and Avoid Legal Consequences, ERIC, 2009.
[198] Shivender Singh, Anil K. Sarje, Manoj Misra, Client-side counter phishing application using adaptive neuro-fuzzy inference system, in: Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, IEEE, 2012, pp. 788–792.
[199] Yanping Zhang, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang, Hongmei Deng, A survey of cyber crimes, Secur. Commun. Network. 5 (4) (2012) 422–437.
[200] Vadim Kotov, Fabio Massacci, Anatomy of exploit kits, in: International Symposium on Engineering Secure Software and Systems, Springer, 2013, pp. 181–196.
[201] Aditya K. Sood, Richard J. Enbody, Rohit Bansal, Dissecting spyeye–understanding the design of third generation botnets, Comput. Network. 57 (2) (2013) 436–450.
[202] Benoit Dupont, Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime, Crime Law Soc. Change 67 (1) (2017) 97–116.
[203] Abedelaziz Mohaisen, Alrawi Omar, Unveiling zeus: automated classification of malware samples, in: Proceedings of the 22nd International Conference on World Wide Web, ACM, 2013, pp. 829–832.
[204] James P. Farwell, Rafal Rohozinski, Stuxnet and the future of cyber war, Survival 53 (1) (2011) 23–40.
[205] Boldizsár Bencsáth, Pék Gábor, Levente Buttyán, Mark Felegyhazi, The cousins of stuxnet: Duqu, flame, and gauss, Future Internet 4 (4) (2012) 971–1003.
[206] A. Coskun Samli, Laurence Jacobs, Counteracting global industrial espionage: a damage control strategy, Bus. Soc. Rev. 108 (1) (2003) 95–113.
[207] Ronald J Deibert, Rafal Rohozinski, A. Manchanda, Nart Villeneuve, G.M.F. Walton, Tracking Ghostnet: Investigating a Cyber Espionage Network, 2009.
[208] Dmitri Alperovitch, et al., Revealed: Operation Shady RAT, ume 3, McAfee, 2011.
[209] Deana Shick, OMeara Kyle, Unique Approach to Threat Analysis Mapping: A Malware Centric Methodology for Better Understanding the Adversary Landscape, CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, 2016. Technical report.
[210] Michael L. Gross, Daphna Canetti, Dana R. Vashdi, The psychological effects of cyber terrorism, Bull. At. Sci. 72 (5) (2016) 284–291.
[211] Mitko Bogdanoski, Drage Petreski, Cyber terrorism–global security threat, Contemp. Macedonian Defense-Int. Sci. Defense, Secur. Peace J. 13 (24) (2013) 59–73.
[212] Marwan Albahar, Cyber attacks and terrorism: a twenty-first century conundrum, Sci. Eng. Ethics 25 (4) (2019) 993–1006.
[213] Jonalan Brickey, Defining cyberterrorism: capturing a broad range of activities in cyberspace, Combat. Terror. Centre at West Point 5 (8) (2012).
[214] Catherine Lotrionte, State sovereignty and self-defense in cyberspace: a normative framework for balancing legal rights, Emory Int'l L. Rev. 26 (2012) 825.
[215] Gregory L. Keeney, Detlof Von Winterfeldt, Identifying and structuring the objectives of terrorists, Risk Anal.: Int. J. 30 (12) (2010) 1803–1816.
[216] Mica Endsley, William M. Jones, Situation Awareness Information Dominance & Information Warfare, LOGICON TECHNICAL SERVICES INC DAYTON OH, 1997. Technical report.
[217] John Arquilla, Rebuttal cyberwar is already upon us, Foreign Pol. 192 (2012) 84.
[218] Jennifer J. Li, Lindsay Daugherty, Training Cyber Warriors: what Can Be Learned from Defense Language Training? Technical Report, RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA, 2015.
[219] Tom Gjelten, First strike: us cyber warriors seize the offensive, World Aff. 175 (2012) 33.
[220] Christina Schori Liang, Cyber jihad: understanding and countering islamic state propaganda, GSCP Policy Paper (2) (2015) 4.
[221] Andrew James, Kenneth Geers, et al., 'compelling opponents to our will': the role of cyber warfare in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCDCOE, 2015, pp. 39–48.
[222] Rain Ottis, Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective, in: Proceedings of the 7th European Conference on Information Warfare, 2008, p. 163.
[223] Ian Traynor, Russia accused of unleashing cyberwar to disable Estonia, Guardian 17 (5) (2007).
[224] Nurgul Yasar, Fatih Mustafa Yasar, Yucel Topcu, Operational advantages of using cyber electronic warfare (cew) in the battlefield, in: Cyber Sensing 2012, vol. 8408, International Society for Optics and Photonics, 2012, 84080G.
[225] Askin Osman, Riza Irmak, Mustafa Avsever, Cyber warfare and electronic warfare integration in the operational environment of the future: cyber electronic warfare, in: Cyber Sensing 2015, vol. 9458, International Society for Optics and Photonics, 2015, 94580H.
[226] Elizabeth Van Wie Davis, Shadow Warfare: Cyberwar Policy in the United States, Russia and China, Rowman & Littlefield Publishers, 2021.
[227] Keir Giles, The Next Phase of Russian Information Warfare, vol. 20, NATO Strategic Communications Centre of Excellence Riga, 2016.
[228] Even Mediu, Nato and Russia in the Balkans, Power Struggle for Influence between Two Security Zones. Case Studies of Albania, Montenegro, and Croatia, PhD thesis, Webster University, 2021.
[229] Wrightson Tyler, Advanced Persistent Threat Hacking: the Art and Science of Hacking Any Organization, McGraw-Hill Education Group, 2014.
[230] Jibran Saleem, Bamidele Adebisi, Ande Ruth, Mohammad Hammoudeh, A state of the art survey-impact of cyber attacks on sme's, in: Proceedings of the International Conference on Future Networks and Distributed Systems, 2017.
[231] Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, M Eric Johnson, Going spear phishing: exploring embedded training and awareness, IEEE Secur. Priv. 12 (1) (2014) 28–38.
[232] Jason Hong, The state of phishing attacks, Commun. ACM 55 (1) (2012) 74–81.
[233] M.T. Chadwick, J.G. Soussan, T.C. Martin, D. Mallick, S.S. Alam, Bank robbery: the real losers in the 1998 Bangladesh flood, Land Degrad. Dev. 12 (3) (2001) 251–260.
[234] Mike Lennon, Hackers Hit 100 Banks in Unprecedented $1 Billion Cyber Heist: Kaspersky Lab, Security Week, 2015.
[235] Ashish Garg, Jeffrey Curtis, Hilary Halper, Quantifying the financial impact of it security breaches, Inf. Manag. Comput. Secur. 11 (2) (2003) 74–83.
[236] J. Bergal, Hacktivists Launch More Cyberattacks against Local, State Governments, 2017.
[237] Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, 2011.

[238] Ellen Nakashima, Russian Government Hackers Penetrated Dnc, Stole Opposition Research on Trump, 2016. *Washington Post online*.
[239] D. Maron, Us hospitals not immune to crippling cyber-attacks: outdated systems and earlier breaches underscore America's healthcare data security risks, Sci. Am. 15 (2017). Last modified May.
[240] Lynne Coventry, Dawn Branley, Cybersecurity in healthcare: a narrative review of trends, threats and ways forward, Maturitas 113 (2018) 48–52.
[241] Jason Andress, Steve Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier, 2013.
[242] Michael Robinson, Kevin Jones, Helge Janicke, Cyber warfare: issues and challenges, Comput. Secur. 49 (2015) 70–94.
[243] Stinissen Jan, Kenneth Geers, A legal framework for cyber operations in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCDCOE Publications, Tallinn, 2015, pp. 123–134.
[244] Filiz Katman, The Islamic Republic of Iran's cyber security strategy: challenges in an era of cyber uncertainty, in: Routledge Companion to Global Cyber-Security Strategy, Routledge, 2021, pp. 435–447.
[245] Ahmed K. Al-Rawi, Cyber warriors in the middle east: the case of the syrian electronic army, Publ. Relat. Rev. 40 (3) (2014) 420–428.
[246] Dina Matar, The syrian regime's strategic political communication: practices and ideology, Int. J. Commun. 13 (19) (2019).
[247] Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, World war c: understanding nation-state motives behind today's advanced cyber attacks, FireEye, Milpitas, CA, USA, Tech. Rep. Sep (2014).
[248] Long Cheng, Fang Liu, Danfeng Yao, Enterprise data breach: causes, challenges, prevention, and future directions, Wiley Interdisciplinary Reviews: Data Min. Knowl. Discov. 7 (5) (2017), e1211.
[249] Ping Wang, Christopher Johnson, Cybersecurity incident handling: a case study of the equifax data breach, Issues in Information Systems 19 (3) (2018).
[250] Gerhard Eschelbeck, The laws of vulnerabilities, Black Hat Briefings 2606 (2004).
[251] Zuzana Hromcová and Anton Cherepanov. Anatomy of Native Iis Malware.
[252] Rui Li, Wenrui Diao, Li Zhou, Shishuai Yang, Shuang Li, Shanqing Guo, Android Custom Permissions Demystified: A Comprehensive Security Evaluation, IEEE Transactions on Software Engineering, 2021.
[253] S.V. Bezzateev, S.G. Fomicheva, G.A. Zhemelev, Agent-based zerologon vulnerability detection, in: 2021 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), IEEE, 2021, pp. 1–5.
[254] Shaen Corbet, John W. Goodell, The reputational contagion effects of ransomware attacks, Finance Res. Lett. 47 (2022), 102715.
[255] Hannah T. Neprash, Claire C. McGlave, Dori A. Cross, Beth A. Virnig, Michael A. Puskarich, D Huling Jared, Alan Z. Rozenshtein, Sayeh S. Nikpay, Trends in ransomware attacks on us hospitals, clinics, and other health care delivery organizations, 2016-2021, in: JAMA Health Forum, vol. 3, American Medical Association, 2022, e224873 e224873.
[256] Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, Michelle Mazurek, Hackers vs. testers: a comparison of software vulnerability discovery processes, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 374–391.
[257] Jai Narayan Goel, B.M. Mehtre, Vulnerability assessment & penetration testing as a cyber defence technology, Proc. Comput. Sci. 57 (2015) 710–715.
[258] Rina Elizabeth Lopez De Jimenez, Pentesting on web applications using ethical-hacking, in: Central American and Panama Convention (CONCAPAN XXXVI), 2016 *IEEE 36th*, IEEE, 2016, pp. 1–6.
[259] Muzhir Shaban Al-Ani, Maha Abd Rajab, Biometrics hand geometry using discrete cosine transform (dct), Sci. Technol. 3 (4) (2013) 112–117.
[260] Anil K. Jain, Ajay Kumar, Biometric recognition: an overview, in: Second Generation Biometrics: the Ethical, Legal and Social Context, Springer, 2012, pp. 49–79.
[261] Mandy Douglas, Karen Bailey, Mark Leeney, Kevin Curran, An overview of steganography techniques applied to the protection of biometric data, Multimed. Tool. Appl. 77 (13) (2018) 17333–17373.
[262] Raphael Hiesgen, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch, The Race to the Vulnerable: Measuring the Log4j Shell Incident, 2022 *arXiv preprint arXiv:2205.02544*.
[263] Hritik Gupta, Alka Chaudhary, Anil Kumar, Identification and analysis of log4j vulnerability, in: 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), IEEE, 2022, pp. 1580–1583.
[264] Critical vulnerability in Apache log4j library. https://www.riello-ups.com/news/14255-critical-vulnerability-in-apache-log4j-library, December 2021.
[265] Kevin J. Houle, Trends in Denial of Service Attack Technology, 2001 archive/pdf/DoS_trends. pd.
[266] Yien Wang, Jianhua Yang, Ethical hacking and network defense: choose your best network vulnerability scanning tool, in: Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on, IEEE, 2017, pp. 110–113.
[267] Colin Tankard, Advanced Persistent Threats and How to Monitor and Deter Them, vol. 2011, Network security, 2011, pp. 16–19, 8.
[268] Sa'ed Abed, Reem Jaffal, Bassam Jamil Mohd, A review on blockchain and iot integration from energy, security and hardware perspectives, Wireless Pers. Commun. (2023) 1–44.
[269] Jeffrey R. Jones, Estimating software vulnerabilities, IEEE Secur. Priv. 5 (4) (2007) 28–32.
[270] Amas Phillips, Carsten Maple, Florian Lukavsky, Ian Pearson, Michael Richardson, Nigel Hanson, Paul Kearney, Robert Dobson, Software Bills of Materials for Iot and Ot Devices, IoT Security Foundation, 2023.
[271] Chris Greamo, Anup Ghosh, Sandboxing and virtualization: modern tools for combating malware, IEEE Secur. Priv. 9 (2) (2011) 79–82.
[272] S.G. Rameshkumar, G. Mohan, Counter and timer based baited method for separating blackhole attacks in manet, Ann. Roman. Soc. Cell Biol. 25 (6) (2021) 897–904.
[273] Samuel Adu-Gyimah, George Asante, and Oliver Kufuor Boansi. Social engineering attacks: a clearer perspective. Int. J. Comput. Appl.s, 975:8887.
[274] Kristan Stoddart, Gaining access: attack and defense methods and legacy systems, in: Cyberwarfare, Springer, 2022, pp. 227–280.
[275] Jielin Dong, Network Dictionary, Javvin Technologies Inc., 2007.
[276] E Pike Ronald, The "ethics" of teaching ethical hacking, J. Int. Technol. Inf. Manag. 22 (4) (2013) 4.
[277] Syed A. Saleem, Ethical hacking as a risk management technique, in: Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, ACM, 2006, pp. 201–203.
[278] Bushra Siddiqua Oosman, Ravishankar Dudhe, Review on the ethical and legal challenges with iot, in: 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), IEEE, 2021, pp. 529–534.
[279] Leyla Bilge, Tudor Dumitras, Before we knew it: an empirical study of zero-day attacks in the real world, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security, ACM, 2012, pp. 833–844.
[280] Don Coppersmith, Another birthday attack, in: Conference on the Theory and Application of Cryptographic Techniques, Springer, 1985, pp. 14–17.
[281] Marc Girault, Robert Cohen, Mireille Campana, A generalized birthday attack, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1988, pp. 129–156.
[282] Ilsun You, Kangbin Yim, Malware obfuscation techniques: a brief survey, in: Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on, IEEE, 2010, pp. 297–300.
[283] Alana Maurushat, Ethical Hacking, University of Ottawa Press, 2019.
[284] G.S. Sriram, Security challenges of big data computing, Int. Res. J. Modern. Eng. Technol. Sci. 4 (1) (2022) 1164–1171.
[285] Jean-Paul A. Yaacoub,and Hassan N. Noura, Ola Salman, Ola and Ali Chehab, Advanced digital forensics and anti-digital forensics for iot systems: techniques, limitations and recommendations, Int. Things 19 (2022), 100544.
[286] Mark Crosbie, Hack the cloud: ethical hacking and cloud forensics, in: Cloud Technology: Concepts, Methodologies, Tools, and Applications, IGI Global, 2015, pp. 1510–1526.
[287] A Alfred Raja Melvin, G.Jaspher W. Kathrine, S Sudhakar Ilango, S. Vimal, Seungmin Rho, Neal N. Xiong, Yunyoung Nam, Dynamic malware attack dataset leveraging virtual machine monitor audit data for the detection of intrusions in cloud, Trans. Emerg. Telecommun. Technol. 33 (4) (2022) e4287.
[288] Ben Rafferty, Dangerous skills gap leaves organisations vulnerable, Netw. Secur. 2016 (8) (2016) 11–13.
[289] Jamil Danish, Muhammad Numan Ali Khan, Is ethical hacking ethical, Int. J. Eng. Sci. Technol. 3 (5) (2011) 3758–3763.
[290] Philip Brey, Ethical aspects of information security and privacy, in: Security, Privacy, and Trust in Modern Data Management, Springer, 2007, pp. 21–36.
[291] Georg Thomas, Burmeister Ok, Gregory Low, Issues of implied trust in ethical hacking, in: Proceedings of the 28th Australasian Conference on Information Systems, December, 2017, pp. 4–6.
[292] Bhawana Sahare, Ankit Naik, Shashikala Khandey, Study of ethical hacking, Int. J. Comput. Sci. Trends Technol 2 (4) (2014) 6–10.
[293] Harper Allen, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, Gray Hat Hacking the Ethical Hackers Handbook, McGraw-Hill Osborne Media, 2011.
[294] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Chehab Ali, A Survey on Ethical Hacking: Issues and Challenges, 2021 *arXiv preprint arXiv:2103.15072*.
[295] Keyun Ruan, Cybercrime and Cloud Forensics: Applications for Investigation Processes: Applications for Investigation Processes, IGI Global, 2012.
[296] Ajinkya A. Farsole, Amurta G. Kashikar, Apurva Zunzunwala, Ethical hacking, Int. J. Comput. Appl. 1 (10) (2010) 14–20.
[297] Lunne Tom, John JM. Powell, Peter K. Robertson, et al., Cone Penetration Testing in Geotechnical Practice, CRC Press, 2014.
[298] James P. McDermott, Attack net penetration testing, in: Proceedings of the 2000 Workshop on New Security Paradigms, ACM, 2001, pp. 15–21.
[299] Thomas M. Chen, Guarding against network intrusions, in: Computer and Information Security Handbook, third ed., Elsevier, 2017, pp. 149–163.
[300] Lee Allen, Advanced Penetration Testing for Highly-Secured Environments: the Ultimate Security Guide, Packt Publishing Ltd, 2012.
[301] Thomas J Mowbray, Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions, John Wiley & Sons, 2013.
[302] Andrew Tang, A guide to penetration testing, Netw. Secur. 2014 (8) (2014) 8–11.
[303] Sven Türpe, Jörn Eichler, Testing production systems safely: common precautions in penetration testing, in: 2009 Testing: Academic and Industrial Conference-Practice and Research Techniques, IEEE, 2009, pp. 205–209.
[304] Tracey Caldwell, Ethical hackers: putting on the white hat, Netw. Secur. 2011 (7) (2011) 10–13.
[305] Hessa Mohammed Zaher Al Shebli, Babak D. Beheshti, A study on penetration testing process and tools, in: Systems, Applications and Technology Conference (LISAT), 2018 IEEE Long Island, IEEE, 2018, pp. 1–7.
[306] Srinivas Nidhra, Jagruthi Dondeti, Black box and white box testing techniques-a literature review, Int. J. Embed. Syst. Appl. (IJESA) 2 (2) (2012) 29–50.
[307] Mohd Ehmer Khan, Farmeena Khan, et al., A comparative study of white box, black box and grey box testing techniques, Int. J. Adv. Comput. Sci. Appl. 3 (6) (2012).

[308] Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell, State of the art: automated black-box web application vulnerability testing, in: 2010 IEEE Symposium on Security and Privacy, IEEE, 2010, pp. 332–345.
[309] Yury Zhauniarovich, Anton Philippov, Olga Gadyatskaya, Crispo Bruno, Fabio Massacci, Towards black box testing of android apps, in: Availability, Reliability and Security (ARES), 2015 10th International Conference on, IEEE, 2015, pp. 501–510.
[310] Henry Raúl González Brito, Raydel Montesino Perurena, Riesgos de seguridad en las pruebas de penetración de aplicaciones web: security risks in web application penetration testing, Revista Cubana de Transf. Digit. 2 (2) (2021) 98–117.
[311] G. Jayasuryapal, P. Meher Pranay, Harpreet Kaur, et al., A survey on network penetration testing, in: 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), IEEE, 2021, pp. 373–378.
[312] Renas R. Asaad, Penetration testing: wireless network attacks method on kali linux os, Acad. J. Nawroz Univ. 10 (1) (2021) 7–12.
[313] Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2010.
[314] Subashini Subashini, Veeraruna Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11.
[315] Harshdeep Singh, Jaswinder Singh, Penetration testing in wireless networks, Int. J. Adv. Res. Comput. Sci. 8 (5) (2017).
[316] Kemal Hajdarevic, Adna Kozic, Indira Avdagic, Zerina Masetic, Nejdet Dogru, Training network managers in ethical hacking techniques to manage resource starvation attacks using gns3 simulator, in: 2017 *XXVI* International Conference on Information, Communication and Automation Technologies (ICAT), IEEE, 2017, pp. 1–6.
[317] Greenwald Lloyd, Robert Shanley, Automated planning for remote penetration testing, in: MILCOM 2009-2009 IEEE Military Communications Conference, IEEE, 2009, pp. 1–7.
[318] Aakash Trivedi, A comprehensive online tool [wr-3] that detects security flaws in networks, in: Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 2, IEEE, 2010, pp. 316–320.
[319] Yong Lu, Xin Luo, Michael Polgar, Yuanyuan Cao, Social network analysis of a criminal hacker community, J. Comput. Inf. Syst. 51 (2) (2010) 31–41.
[320] Yangbin Zhou, Keyu Jiang, An analysis system for computer forensic education, training, and awareness, in: Computing, Measurement, Control and Sensor Network (CMCSN), 2012 International Conference on, IEEE, 2012, pp. 48–51.
[321] Ammar Alazab, Jemal Abawajy, Michael Hobbs, Robert Layton, Ansam Khraisat, Crime toolkits: the productisation of cybercrime, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2013, pp. 1626–1632.
[322] Abbasi Ahmed, Weifeng Li, Victor Benjamin, Shiyu Hu, Hsinchun Chen, Descriptive analytics: examining expert hackers in web forums, in: Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, IEEE, 2014, pp. 56–63.
[323] Rigzin Angmo, Monika Sharma, Performance evaluation of web based automation testing tools, in: Confluence the Next Generation Information Technology Summit (Confluence), 2014 5th *International Conference*, IEEE, 2014, pp. 731–735.
[324] S. Sandhya, Sohini Purkayastha, Emil Joshua, Akash Deep, Assessment of website security by penetration testing using wireshark, in: Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, IEEE, 2017, pp. 1–4.
[325] Artem Tetskyi, Vyacheslav Kharchenko, Dmytro Uzun, Neural networks based choice of tools for penetration testing of web applications, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2018.
[326] Christopher Bailey, Rogério de Lemos, Evaluating self-adaptive authorisation infrastructures through gamification, in: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2018.
[327] Darrien Rushing, Jason Guidry, Ihssan Alkadi, Collaborative penetration-testing and analysis toolkit (cpat), in: Aerospace Conference, 2015 IEEE, IEEE, 2015, pp. 1–9.
[328] Vasaka Visoottiviseth, Phuripat Akarasiriwong, Siravitch Chaiyasart, Siravit Chotivatunyu, Pentos: penetration testing tool for internet of thing devices, in: Region 10 Conference, TENCON 2017-2017 IEEE, IEEE, 2017, pp. 2279–2284.
[329] Ning Zhu, Chen Xin-yuan, Yong-fu Zhang, Xin Si-yuan, Design and application of penetration attack tree model oriented to attack resistance test, in: Computer Science and Software Engineering, 2008 International Conference on vol. 3, IEEE, 2008, pp. 622–626.
[330] Norah Ahmed Almubairik, Wills Gary, Automated penetration testing based on a threat model, in: Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for, IEEE, 2016, pp. 413–414.
[331] Anestis Bechtsoudis, Nicolas Sklavos, Aiming at higher network security through extensive penetration tests, IEEE latin am. trans. 10 (3) (2012) 1752–1756.
[332] Jiajia Wang, Research of penetration test based on mobile internet, in: Computer and Communications (ICCC), 2016 2nd *IEEE International Conference on*, IEEE, 2016, pp. 2542–2545.
[333] Aaron Guzman, Aditya Gupta, IoT Penetration Testing Cookbook: Identify Vulnerabilities and Secure Your Smart Devices, Packt Publishing Ltd, 2017.
[334] Zhenguo Hu, Razvan Beuran, Yasuo Tan, Automated penetration testing using deep reinforcement learning, in: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2020, pp. 2–10.
[335] Sugandh Shah, B.M. Mehtre, An automated approach to vulnerability assessment and penetration testing using net-nirikshak 1.0, in: Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, IEEE, 2014, pp. 707–712.
[336] Jai Narayan Goel, Mohsen Hallaj Asghar, Vivek Kumar, Sudhir Kumar Pandey, Ensemble based approach to increase vulnerability assessment and penetration testing accuracy, in: Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on, IEEE, 2016, pp. 330–335.
[337] Marc Langheinrich, The internet of thugs? IEEE Pervasive Comput. 20 (3) (2021) 4–6.
[338] Bohdana Sereda, Jason Jaskolka, An evaluation of iot security guidance documents: a shared responsibility perspective, Proc. Comput. Sci. 201 (2022) 281–288.
[339] Barakat Raman, Faruk Catal, Sascha Hackel, Axel Rennoch, Martin A. Schneider, Towards a certification scheme for iot security evaluation, Informatik 2021 (2021).
[340] Michael Fagan, Katerina Megas, Karen Scarfone, Matthew Smith, Core Cybersecurity Feature Baseline for Securable Iot Devices: A Starting Point for Iot Device Manufacturers, National Institute of Standards and Technology, 2019. Technical report.
[341] Michael Fagan, Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith, IoT Device Cybersecurity Capability Core Baseline, US Department of Commerce, National Institute of Standards and Technology, 2020.
[342] Michael Fagan, Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith, Foundational Cybersecurity Activities for IoT Device Manufacturers, US Department of Commerce, National Institute of Standards and Technology, 2020.
[343] Kenneth Einar Himma, Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking, The handbook of information and computer ethics, 2008, p. 191.
[344] Ross Brewer, Cyber threats: reducing the time to detection and response, Netw. Secur. 2015 (5) (2015) 5–8.
[345] Eman Salim Ibrahim Harba, Secure data encryption through a combination of aes, rsa and hmac, Eng. Technol. Appl. Sci. Res. 7 (4) (2017) 1781–1785.
[346] Gorjan Alagic, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al., Status Report on the First Round of the NIST Post-quantum Cryptography Standardization Process. US Department of Commerce, National Institute of Standards and Technology, 2019.
[347] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Perlner Ray, Daniel Smith-Tone, Report on Post-quantum Cryptography, US Department of Commerce, National Institute of Standards and Technology, 2016.
[348] Jintai Ding, Rainer Steinwandt, Post-quantum Cryptography: 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers, vol. 11505, Springer, 2019.
[349] João Pedro Dias, Tiago Boldt Sousa, André Restivo, Hugo Sereno Ferreira, A pattern-language for self-healing internet-of-things systems, in: Proceedings of the European Conference on Pattern Languages of Programs 2020, 2020, pp. 1–17.
[350] Ronny Seiger, Stefan Herrmann, Uwe Aßmann, Self-healing for distributed workflows in the internet of things, in: 2017 IEEE International Conference on Software Architecture Workshops (ICSAW), IEEE, 2017, pp. 72–79.
[351] Rafael Angarita, Responsible objects: towards self-healing internet of things applications, in: 2015 IEEE International Conference on Autonomic Computing, IEEE, 2015, pp. 307–312.
[352] Kimberly Graves, CEH Certified Ethical Hacker Study Guide, John Wiley & Sons, 2010.
[353] M.E. Elhamahmy, Tarek S. Sobh, Preventing information leakage caused by war driving attacks in wi-fi networks, in: International Conference on Aerospace Sciences and Aviation Technology, vol. 14, The Military Technical College, 2011, pp. 1–9.
[354] Vasileios Mavroeidis, Siri Bromander, Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence, in: 2017 European Intelligence and Security Informatics Conference (EISIC), IEEE, 2017, pp. 91–98.
[355] Md Sahrom Abu, Siti Rahayu Selamat, Aswami Ariffin, Robiah Yusof, Cyber threat intelligence–issue and challenges, Indon. J. Electr. Eng. Comput. Sci. 10 (1) (2018) 371–379.
[356] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, Ali E. Abdallah, Cyber threat intelligence sharing: survey and research directions, Comput. Secur. 87 (2019), 101589.