www.rungta.ac.in

RUNGTA
International Journal of
Computer Science and
Information Technology

RESEARCH ARTICLE

Unleashing of audit script for windows and linux OS to verify CIS Benchmark

Atharva Gehlot-1, Abhinandan Patidar-2, Himani Namdeo-3, Ankit Chouhan-4
[1,2,3,4] - *Acropolis Institute of Technology & Research, Indore*
Corresponding author: atharva.gehlot@gmail.com

ABSTRACT:
This problem addresses the creation of automated auditing scripts of Windows and some Linux Distributions according to the CIS benchmarks. The objective is to improve security adherence and management by verifying computer systems against these security configurations that have been defined within the industry. With the rising need for cybersecurity and that is the reason compliance with benchmarks such as those from CIS is important. The variations of environments especially with respect to the different operating systems being used such as Windows and Linux requires a consistent yet efficient way of auditing and ensuring compliance to these security standards. Scripts were conceived and evaluated on the Windows and Linux operating systems. The approach took the form of CIS benchmark requirements as tasks to be executed on and within these operating systems in this case checking configuration settings and permissions depth. The audit scripts made it possible to discover the deficiencies and areas of use, which were out of compliance, and remedial actions taken on these areas where possible. To a large extent, time and blue level complexity relating to manual auditing were eliminated and operational efficiency and security were improved on the two systems. Ensuring security compliance is one of the challenges that comes in as more and more organizations move towards adopting multi -OS environments. These scripts provide an effective strategy to comply with the requirements of CIS in different environments.

KEYWORDS: CIS Benchmark, audit script, Windows , Linux, PowerShell, Shell scripting, cybersecurity, security compliance, automation, firewall, password policy, system pdates, security configuration, audit logging,

1. Introduction

In an era characterized by sophisticated cyber threats, ensuring system compliance with established security benchmarks is paramount. The Center for Internet Security (CIS) provides globally recognized best practices for securing IT systems. However, manual verification across heterogeneous environments (Windows and Linux) is highly inefficient and prone to error.

Computer security (also cybersecurity, digital security, or information technology (IT) security) is a subdiscipline within the field of information security. It focuses on protecting computer software, systems, and networks from threats that can lead to unauthorized information disclosure, theft, or damage to hardware, software, or data, as well as to the disruption or misdirection of the services they provide [1].

The growing significance of computer security reflects the increasing dependence on computer systems, the Internet, and evolving wireless network standards. This reliance has expanded with the proliferation of smart devices, including smartphones, televisions, and other components of the Internet of things (IoT) [2].

As digital infrastructure becomes more embedded in everyday life, cybersecurity has emerged as a critical concern. The complexity of modern information systems-and the societal functions they underpin-has introduced new vulnerabilities. Systems that manage essential services, such as power grids, electoral processes, and finance, are particularly sensitive to security breaches [3].

Although many aspects of computer security involve digital security, such as electronic passwords and encryption,

Received on 15 February 2024 Revised on 27 March 2024
Accepted on 08 April 2024 Published on 14 April 2024
Rungta International Journal of Computer Science and Information Technology. 2024; 1(1): 47.

physical security measures, such as metal locks, are still used to prevent unauthorized tampering. IT security is not a perfect subset of information security and therefore does not completely align with the security convergence schema [4].

A vulnerability refers to a flaw in the structure, execution, functioning, or internal oversight of a computer or system that compromises its security. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable vulnerability is one for which at least one working exploit exists. Actors maliciously seeking vulnerabilities are known as threats. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts [5].

Various people or parties are vulnerable to cyberattacks; however, different groups are likely to experience different types of attacks more than others [6].

In April 2023, the United Kingdom Department for Science, Innovation & Technology released a report on cyberattacks over the previous 12 months. They surveyed 2,263 UK businesses, 1,174 UK registered charities, and 554 education institutions. The research found that "32% of businesses and 24% of charities overall recall any breaches or attacks from the last 12 months." These figures were much higher for "medium businesses (59%), large businesses (69%), and high-income charities with 500,000 or more in annual income (56%)." Yet, although medium or large businesses are more often the victims, since larger companies have generally improved their security over the last decade, small and midsize businesses (SMBs) have also become increasingly vulnerable as they often "do not have advanced tools to defend the business." SMBs are most likely to be affected by malware, ransomware, phishing, man-in-the-middle attacks, and Denial-of Service (DoS) Attacks [7].

Normal internet users are most likely to be affected by untargeted cyberattacks. These are where attackers indiscriminately target as many devices, services, or users as possible. They do this using techniques that take advantage of the openness of the Internet. These strategies mostly include phishing, ransomware, water holing and scanning [8].

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the following categories: [9]

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. These weaknesses may exist for many reasons, including original design or poor configuration. Due to the nature of backdoors, they are of greater concern to companies and databases as opposed to individuals [10].

Backdoors may be added by an authorized party to allow some legitimate access or by an attacker for malicious reasons. Criminals often use malware to install backdoors, giving them remote administrative access to a system. Once they have access, cybercriminals can "modify files, steal personal information, install unwanted software, and even take control of the entire computer." [11]

Backdoors can be difficult to detect, as they often remain hidden within source code or system firmware and may require intimate knowledge of the operating system to identify [12].

Denial-of-service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering an incorrect password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of distributed denial-of-service (DDoS) attacks are possible, where the attack comes from a large number of points. In this case, defending against these attacks is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including distributed reflective denial-of-service (DRDoS), where innocent systems are fooled into sending traffic to the victim. With such attacks, the amplification factor makes the attack easier for the attacker because they have to use little bandwidth themselves. To understand why attackers may carry out these attacks, see the 'attacker motivation' section [13].

A direct-access attack is when an unauthorized user (an attacker) gains physical access to a computer, typically to copy data from it or steal information. Attackers may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless microphones. Even when the system is protected by standard security measures, these may be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and the Trusted Platform Module standard are designed to prevent these attacks [14].

Direct service attackers are related in concept to direct memory attacks which allow an attacker to gain direct access to a computer's memory. The attacks "take advantage of a feature of modern computers that allows certain devices, such as external hard drives, graphics cards, or network cards, to access the computer's memory directly." [15]

Eavesdropping is the act of surreptitiously listening to a private computer conversation (communication), usually between hosts on a network. It typically occurs when a user connects to a network where traffic is not secured or encrypted and sends sensitive business data to a colleague, which, when listened to by an attacker, could be exploited. Data transmitted across an open network can be intercepted by an attacker using various methods [16].

Unlike malware, direct-access attacks, or other forms of cyberattacks, eavesdropping attacks are unlikely to negatively affect the performance of networks or devices, making them difficult to notice. In fact, "the attacker does not need to have any ongoing connection to the software at all. The attacker can insert the software onto a compromised device, perhaps by di-

rect insertion or perhaps by a virus or other malware, and then come back some time later to retrieve any data that is found or trigger the software to send the data at some determined time." [17]

Using a virtual private network (VPN), which encrypts data between two points, is one of the most common forms of protection against eavesdropping. Using the best form of encryption possible for wireless networks is best practice, as well as using HTTPS instead of an unencrypted HTTP [18].

2. Related Work

Automated security auditing has evolved from simple checklist scripts to complex Configuration Management systems (e.g., Ansible, Puppet). While these systems enforce state, lightweight, agentless audit scripts remain crucial for point-in-time verification and penetration testing reconnaissance.

Programs such as Carnivore and NarusInSight have been used by the Federal Bureau of Investigation (FBI) and the NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact with the outside world) can be eavesdropped upon by monitoring the faint electromagnetic transmissions generated by the hardware. TEMPEST is a specification by the NSA referring to these attacks [19].

Malicious software (malware) is any software code or computer program "intentionally written to harm a computer system or its users." Once present on a computer, it can leak sensitive details such as personal information, business information and passwords, can give control of the system to the attacker, and can corrupt or delete data permanently [20].

Viruses are a specific type of malware, and are normally a malicious code that hijacks software with the intention to "do damage and spread copies of itself." Copies are made with the aim of spreading to other programs on a computer [1].

Worms are similar to viruses, however viruses can only function when a user runs (opens) a compromised program. Worms are self-replicating malware that spread between programs, apps and devices without the need for human interaction [2].

Trojan horses are programs that pretend to be helpful or hide themselves within desired or legitimate software to "trick users into installing them." Once installed, a RAT (Remote Access Trojan) can create a secret backdoor on the affected device to cause damage [3].

Spyware is a type of malware that secretly gathers information from an infected computer and transmits the sensitive information back to the attacker. One of the most common forms of spyware is keyloggers, which record all of a user's keyboard inputs/keystrokes, to "allow hackers to harvest usernames, passwords, bank account and credit card numbers." [4]

Scareware, as the name suggests, is a form of malware that uses social engineering (manipulation) to scare, shock, trigger anxiety, or suggest the perception of a threat in order to manipulate users into buying or installing unwanted software. These attacks often begin with a "sudden pop-up with an urgent message, usually warning the user that they've broken the law or their device has a virus." [5]

Ransomware is when malware installs itself onto a victim's machine, encrypts their files, and then turns around and demands a ransom (usually in Bitcoin) to return that data to the user [6].

Man-in-the-middle attacks (MITM) involve a malicious attacker trying to intercept, surveil or modify communications between two parties by spoofing one or both party's identities and injecting themselves in-between. Types of MITM attacks include: [7]

IP address spoofing is where the attacker hijacks routing protocols to reroute the targets traffic to a vulnerable network node for traffic interception or injection [8].

Message spoofing (via email, SMS or OTT messaging) is where the attacker spoofs the identity or carrier service while the target is using messaging protocols like email, SMS or OTT (IP-based) messaging apps. The attacker can then monitor conversations, launch social attacks or trigger zero-day-vulnerabilities to allow for further attacks [9].

WiFi SSID spoofing is where the attacker simulates a Wi-Fi base station SSID to capture and modify internet traffic and transactions. The attacker can also use local network addressing and reduced network defenses to penetrate the target's firewall by breaching known vulnerabilities. Sometimes known as a Pineapple attack thanks to a popular device. See also Malicious association [10].

DNS spoofing is where attackers hijack domain name assignments to redirect traffic to systems under the attackers' control, in order to surveil traffic or launch other attacks [11].

SSL hijacking, typically coupled with another media-level MITM attack, is where the attacker spoofs the SSL authentication and encryption protocol by way of Certificate Authority injection in order to decrypt, surveil and modify traffic. See also TLS interception [12]

Surfacing in 2017, a new class of multi-vector, polymorphic cyber threats combine several types of attacks and change form to avoid cybersecurity controls as they spread [13].

Multi-vector polymorphic attacks, as the name describes, are both multi-vectored and polymorphic. Firstly, they are a singular attack that involves multiple methods of attack. In this sense, they are "multi-vectored" (i.e. the attack can use multiple means of propagation such as via the Web, email and applications). However, they are also multi-staged, meaning that "they can infiltrate networks and move laterally inside the network." The attacks can be polymorphic, meaning that the cyberattacks used such as viruses, worms or trojans "constantly change ("morph") making it nearly impossible to detect them using signature-based defences." [14]

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly

from users by deceiving the users. Phishing is typically carried out by email spoofing, instant messaging, text message, or on a phone call. They often direct users to enter details at a fake website whose look and feel are almost identical to the legitimate one. The fake website often asks for personal information, such as login details and passwords. This information can then be used to gain access to the individual's real account on the real website [15].

Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers can use creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized. A more strategic type of phishing is spear-phishing which leverages personal or organization-specific details to make the attacker appear like a trusted source. Spear-phishing attacks target specific individuals, rather than the broad net cast by phishing attempts [16].

3. Methodology

We developed a dual-environment audit suite leveraging PowerShell for Windows and Bash for Linux distributions. The scripts programmatically query registry keys, file permissions, and active services, mapping the results directly against CIS benchmark controls (e.g., password policies, audit logging).

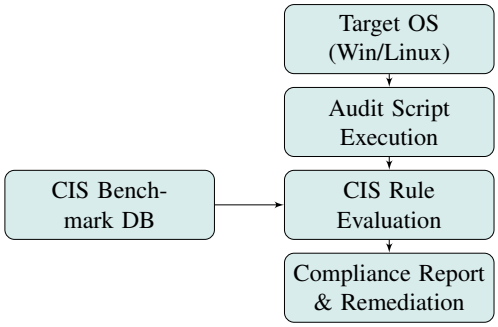

Figure 1: Automated Audit and Compliance Architecture

Algorithm 1 Automated CIS Compliance Check

Require: Set of CIS Rules R, Target Host H
Ensure: Compliance Report C

```
for each r ∈ R do
    State_current ← QueryOS(H, r.Target)
    if State_current == r.Expected then
        C.Append(r.ID, PASS)
    else
        C.Append(r.ID, FAIL, r.Remediation)
    end if
end for
return C
```

Privilege escalation describes a situation where an attacker with limited access is able, without authorization, to elevate their privileges or access level. For example, a standard computer user may be able to exploit a vulnerability in the system to gain access to restricted data; or even become root and have full unrestricted access to a system. The severity of attacks can range from attacks simply sending an unsolicited email to a ransomware attack on large amounts of data. Privilege escalation usually starts with social engineering techniques, often phishing [17].

Horizontal escalation (or account takeover) is where an attacker gains access to a normal user account that has relatively low-level privileges. This may be through stealing the user's username and password. Once they have access, they have gained a foothold, and using this foothold the attacker then may move around the network of users at this same lower level, gaining access to information of this similar privilege [18].

Vertical escalation, however, targets people higher up in a company and often with more administrative power, such as an employee in IT with a higher privilege. Using this privileged account will then enable the attacker to invade other accounts [19].

Any computational system affects its environment in some form. This effect it has on its environment can range from electromagnetic radiation, to residual effect on RAM cells which as a consequence make a cold boot attack possible, to hardware implementation faults that allow for access or guessing of other values that normally should be inaccessible. In Side-channel attack scenarios, the attacker would gather such information about a system or network to guess its internal state and as a result access the information which is assumed by the victim to be secure. The target information in a side channel can be challenging to detect due to its low amplitude when combined with other signals [20].

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access by, for example, impersonating a senior executive, bank, a contractor, or a customer. This generally involves exploiting people's trust, and relying on their cognitive biases. A common scam involves emails sent to accounting and finance department personnel,

impersonating their CEO and urgently requesting action. One of the main techniques of social engineering are phishing attacks [1].

In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms [2].

Spoofing is an act of pretending to be a valid entity through the falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. Spoofing is closely related to phishing. There are several types of spoofing, including: [3]

IP address spoofing, where an attacker alters the source IP address in a network packet to hide their identity or impersonate another computing system [4].

MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of their network interface controller to obscure their identity, or to pose as another [5].

Address Resolution Protocol (ARP) spoofing, where an attacker sends spoofed address resolution protocol onto a local area network to associate their Media Access Control address with a different host's IP address. This causes data to be sent to the attacker rather than the intended host [6].

Tampering describes a malicious modification or alteration of data. It is an intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data. So-called Evil Maid attacks and security services planting of surveillance capability into routers are examples [7].

HTML smuggling allows an attacker to smuggle a malicious code inside a particular HTML or web page. HTML files can carry payloads concealed as benign, inert data in order to defeat content filters. These payloads can be reconstructed on the other side of the filter [8].

When a target user opens the HTML, the malicious code is activated; the web browser then decodes the script, which then unleashes the malware onto the target's device [9].

Information security (InfoSec) and cybersecurity are closely related but not identical. While cybersecurity addresses external and malicious threats related to the exposure to the internet, information security also covers internal policies, roles, and controls [10].

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness toward information security within an organization. Information security culture is the "...totality of patterns of behavior in an organization that contributes to the protection of information of all kinds." [11]

Andersson and Reimers (2014) found that employees often do not see themselves as part of their organization's information security effort and often take actions that impede organizational changes. Indeed, the Verizon Data Breach Investigations Report 2020, which examined 3,950 security breaches, discovered 30% of cybersecurity incidents involved internal actors within a company. Research shows information security culture needs to be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never-ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation [12].

Strategic planning: To develop an awareness program, clear targets need to be set. Assembling a team of skilled professionals is helpful to achieve it [13].

In computer security, a countermeasure is an action, device, procedure or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken [14].

Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered a main feature [15].

Before a secure system is created or updated, companies should ensure they understand the fundamentals and the context around the system they are trying to create and identify any weaknesses in the system [16].

Companies should design and centre their security around techniques and defences which make attacking their data or systems inherently more challenging for attackers [17].

Although systems can be created which are safe against a multitude of attacks, that does not mean that attacks will not be attempted. Despite one's security, all companies' systems should aim to be able to detect and spot attacks as soon as they occur to ensure the most effective response to them [18].

The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way, even if an attacker gains access to that part, they only have limited access to the whole system [19].

Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds [20].

Default secure settings, and design to fail secure rather than fail insecure (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure [1].

Audit trails track system activity so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks [2].

Security architecture can be defined as the "practice of designing computer systems to achieve security goals." These goals have overlap with the principles of "security by design" explored above, including to "make initial compromise of the system difficult," and to "limit the impact of any compromise."

In practice, the role of a security architect would be to ensure the structure of a system reinforces the security of the system, and that new changes are safe and meet the security requirements of the organization [3].

Similarly, Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are: [4]

A state of computer security is the conceptual ideal, attained by the use of three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following: [5]

Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services and block certain kinds of attacks through packet filtering. Firewalls can be both hardware and software-based. Firewalls monitor and control incoming and outgoing traffic of a computer network and establish a barrier between a trusted network and an untrusted network [6].

Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems [7].

Response is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, the complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected [8].

Today, computer security consists mainly of preventive measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet. They can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real-time filtering and blocking. Another implementation is a so-called physical firewall, which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet [9].

Some organizations are turning to big data platforms, such as Apache Hadoop, to extend data accessibility and machine learning to detect advanced persistent threats [10].

In order to ensure adequate security, the confidentiality, integrity and availability of a network, known as the CIA triad, must be protected and is considered the foundation of information security. To achieve those objectives, administrative, physical and technical security measures should be employed. The amount of security afforded to an asset can only be determined when its value is known [11].

Vulnerability management is the cycle of identifying, fixing or mitigating vulnerabilities, especially in software and firmware. Vulnerability management is integral to computer security and network security [12].

Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities, such as open ports, insecure software configuration, and susceptibility to malware. In order for these tools to be effective, they must be kept up to date with every new update the vendor releases. Typically, these updates will scan for the new vulnerabilities that were introduced recently [13].

Beyond vulnerability scanning, many organizations contract outside security auditors to run regular penetration tests against their systems to identify vulnerabilities. In some sectors, this is a contractual requirement [14].

The act of assessing and reducing vulnerabilities to cyber-attacks is commonly referred to as information technology security assessments. They aim to assess systems for risk and to predict and test for their vulnerabilities. While formal verification of the correctness of computer systems is possible, it is not yet common. Operating systems formally verified include seL4, and SYSGO's PikeOS - but these make up a very small percentage of the market [15].

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates and by hiring people with expertise in security. Large companies with significant threats can hire Security Operations Centre (SOC) Analysts. These are specialists in cyber defences, with their role ranging from "conducting threat analysis to investigating reports of any new issues and preparing and testing disaster recovery plans." [16]

Whilst no measures can completely guarantee the prevention of an attack, these measures can help mitigate the damage of possible attacks. The effects of data loss/damage can be also reduced by careful backing up and insurance [17].

Outside of formal assessments, there are various methods of reducing vulnerabilities, including hardening systems. Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires something you know: a password or PIN, and something you have: a card, dongle, cellphone, or another piece of hardware. This increases security as an unauthorized person needs both of these to gain access [18].

Protecting against social engineering and direct computer access (physical) attacks can only happen by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk by improving people's knowledge of how to protect themselves and by increasing people's awareness of threats. However, even in highly disciplined environments (e.g., military organizations), social engineering attacks can still be difficult to foresee and prevent [19].

Inoculation, derived from inoculation theory, seeks to pre-

vent social engineering and other fraudulent tricks and traps by instilling a resistance to persuasion attempts through exposure to similar or related attempts [20].

Hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below [1].

USB dongles are typically used in software licensing schemes to unlock software capabilities, but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs). In addition, a USB dongle can be configured to lock or unlock a computer [2].

Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access [3].

Computer case intrusion detection refers to a device, typically a push-button switch, which detects when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time [4].

Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves. Tools exist specifically for encrypting external drives as well [5].

Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks [6].

Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low-energy (LE), near-field communication (NFC) on non-iOS devices and biometric validation such as thumbprint readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings [7].

Physical Unclonable Functions (PUFs) can be used as a digital fingerprint or a unique identifier to integrated circuits and hardware, providing users the ability to secure the hardware supply chains going into their systems [8].

One use of the term computer security refers to technology that is used to implement secure operating systems. Using secure operating systems is a good way of ensuring computer security. These are systems that have achieved certification from an external security-auditing organization, the most popular evaluations are Common Criteria (CC) [9].

In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are secure by design. Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system; [10]

Within computer systems, two of the main security models capable of enforcing privilege separation are access control lists (ACLs) and role-based access control (RBAC) [11].

An access-control list (ACL), with respect to a computer file system, is a list of permissions associated with an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects [12].

Role-based access control is an approach to restricting system access to authorized users, used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC) [13].

A further approach, capability-based security has been mostly restricted to research operating systems. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open-source project in the area is the E language [14].

The end-user is widely recognized as the weakest link in the security chain and it is estimated that more than 90% of security incidents and breaches involve some kind of human error. Among the most commonly recorded forms of errors and misjudgment are poor password management, sending emails containing sensitive data and attachments to the wrong recipient, the inability to recognize misleading URLs and to identify fake websites and dangerous email attachments. A common mistake that users make is saving their user id/password in their browsers to make it easier to log in to banking sites. This is a gift to attackers who have obtained access to a machine by some means. The risk may be mitigated by the use of two-factor authentication [15].

As the human component of cyber risk is particularly relevant in determining the global cyber risk an organization is facing, security awareness training, at all levels, not only provides formal compliance with regulatory and industry mandates but is considered essential in reducing cyber risk and protecting individuals and companies from the great majority of cyber

threats [16].

The focus on the end-user represents a profound cultural change for many security practitioners, who have traditionally approached cybersecurity exclusively from a technical perspective, and moves along the lines suggested by major security centers to develop a culture of cyber awareness within the organization, recognizing that a security-aware user provides an important line of defense against cyberattacks [17].

Related to end-user training, digital hygiene or cyber hygiene is a fundamental principle relating to information security and, as the analogy with personal hygiene shows, is the equivalent of establishing simple routine measures to minimize the risks from cyber threats. The assumption is that good cyber hygiene practices can give networked users another layer of protection, reducing the risk that one vulnerable node will be used to either mount attacks or compromise another node or network, especially from common cyberattacks. Cyber hygiene should also not be mistaken for proactive cyber defence, a military term [18].

The most common acts of digital hygiene can include updating malware protection, cloud back-ups, passwords, and ensuring restricted admin rights and network firewalls. As opposed to a purely technology-based defense against threats, cyber hygiene mostly regards routine measures that are technically simple to implement and mostly dependent on discipline or education. It can be thought of as an abstract list of tips or measures that have been demonstrated as having a positive effect on personal or collective digital security. As such, these measures can be performed by laypeople, not just security experts [19].

Cyber hygiene relates to personal hygiene as computer viruses relate to biological viruses (or pathogens). However, while the term computer virus was coined almost simultaneously with the creation of the first working computer viruses, the term cyber hygiene is a much later invention, perhaps as late as 2000 by Internet pioneer Vint Cerf. It has since been adopted by the Congress and Senate of the United States, the FBI, EU institutions and heads of state [20].

Identifying attackers is difficult, as they may operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymizing procedures which make back-tracing difficult - and are often located in another jurisdiction. If they successfully breach security, they have also often gained enough administrative access to enable them to delete logs to cover their tracks [1].

The sheer number of attempted attacks, often by automated vulnerability scanners and computer worms, is so large that organizations cannot spend time pursuing each [2].

Law enforcement officers often lack the skills, interest or budget to pursue attackers. Furthermore, identifying attackers across a network may necessitate collecting logs from multiple locations within the network and across various countries, a process that can be both difficult and time-consuming [3].

The growth in the number of computer systems and the increasing reliance upon them by individuals, businesses, industries, and governments means that there are an increasing number of systems at risk [4].

The computer systems of financial regulators and financial institutions like the U.S. Securities and Exchange Commission, SWIFT, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested in manipulating markets and making illicit gains. Websites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are also prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market. In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs [5].

The UCLA Internet Report: Surveying the Digital Future (2000) found that the privacy of personal data created barriers to online sales and that more than nine out of 10 internet users were somewhat or very concerned about credit card security [6].

The most common web technologies for improving security between browsers and websites are named SSL (Secure Sockets Layer), and its successor TLS (Transport Layer Security), identity management and authentication services, and domain name services allow companies and consumers to engage in secure communications and commerce. Several versions of SSL and TLS are commonly used today in applications such as web browsing, e-mail, internet faxing, instant messaging, and VoIP (voice-over-IP). There are various interoperable implementations of these technologies, including at least one implementation that is open source. Open source allows anyone to view the application's source code, and look for and report vulnerabilities [7].

The credit card companies Visa and MasterCard cooperated to develop the secure EMV chip which is embedded in credit cards. Further developments include the Chip Authentication Program where banks give customers hand-held card readers to perform online secure transactions. Other developments in this arena include the development of technology such as Instant Issuance which has enabled shopping mall kiosks acting on behalf of banks to issue on-the-spot credit cards to interested customers [8].

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies [9].

The aviation industry is very reliant on a series of complex systems which could be attacked. A simple power outage at

one airport can cause repercussions worldwide, much of the system relies on radio transmissions which could be disrupted, and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. There is also potential for attack from within an aircraft [10].

Implementing fixes in aerospace systems poses a unique challenge because efficient air transportation is heavily affected by weight and volume. Improving security by adding physical devices to airplanes could increase their unloaded weight, and could potentially reduce cargo or passenger capacity [11].

In Europe, with the (Pan-European Network Service) and NewPENS, and in the US with the NextGen program, air navigation service providers are moving to create their own dedicated networks [12].

Many modern passports are now biometric passports, containing an embedded microchip that stores a digitized photograph and personal information such as name, gender, and date of birth. In addition, more countries are introducing facial recognition technology to reduce identity-related fraud. The introduction of the ePassport has assisted border officials in verifying the identity of the passport holder, thus allowing for quick passenger processing. Plans are under way in the US, the UK, and Australia to introduce SmartGate kiosks with both retina and fingerprint recognition technology. The airline industry is moving from the use of traditional paper tickets towards the use of electronic tickets (e-tickets). These have been made possible by advances in online credit card transactions in partnership with the airlines. Long-distance bus companies are also switching over to e-ticketing transactions today [13].

The consequences of a successful attack range from loss of confidentiality to loss of system integrity, air traffic control outages, loss of aircraft, and even loss of life [14].

Desktop computers and laptops are commonly targeted to gather passwords or financial account information or to construct a botnet to attack another target. Smartphones, tablet computers, smart watches, and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. WiFi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach [15].

Today many healthcare providers and health insurance companies use the internet to provide enhanced products and services. Examples are the use of tele-health to potentially offer better quality and access to healthcare, or fitness trackers to lower insurance premiums. Patient records are increasingly being placed on secure in-house networks, alleviating the need for extra storage space [16].

Large corporations are common targets. In many cases attacks are aimed at financial gain through identity theft and involve data breaches. Examples include the loss of millions of clients' credit card and financial details by Home Depot, Staples, Target Corporation, and Equifax [17].

Medical records have been targeted in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale. Although cyber threats continue to increase, 62% of all organizations did not increase security training for their business in 2015 [18].

Not all attacks are financially motivated, however: security firm HBGary Federal had a serious series of attacks in 2011 from hacktivist group Anonymous in retaliation for the firm's CEO claiming to have infiltrated their group, and Sony Pictures was hacked in 2014 with the apparent dual motive of embarrassing the company through data leaks and crippling the company by wiping workstations and servers [19].

Vehicles are increasingly computerized, with engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver-assistance systems on many models. Additionally, connected cars may use WiFi and Bluetooth to communicate with onboard consumer devices and the cell phone network. Self-driving cars are expected to be even more complex. All of these systems carry some security risks, and such issues have gained wide attention [20].

Simple examples of risk include a malicious compact disc being used as an attack vector, and the car's onboard microphones being used for eavesdropping. However, if access is gained to a car's internal controller area network, the danger is much greater - and in a widely publicized 2015 test, hackers remotely carjacked a vehicle from 10 miles away and drove it into a ditch [1].

Manufacturers are reacting in numerous ways, with Tesla in 2016 pushing out some security fixes over the air into its cars' computer systems. In the area of autonomous vehicles, in September 2016 the United States Department of Transportation announced some initial safety standards, and called for states to come up with uniform policies [2].

Additionally, e-Drivers' licenses are being developed using the same technology. For example, Mexico's licensing authority (ICV) has used a smart card platform to issue the first e-Drivers' licenses to the city of Monterrey, in the state of Nuevo Len [3].

Shipping companies have adopted RFID (Radio Frequency Identification) technology as an efficient, digitally secure, tracking device. Unlike a barcode, RFID can be read up to 20 feet away. RFID is used by FedEx and UPS [4].

Government and military computer systems are commonly attacked by activists and foreign powers. This includes local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, as well as student records [5].

The Internet of things (IoT) is the network of physical objects such as devices, vehicles, and buildings that are embed-

ded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data. Concerns have been raised that this is being developed without appropriate consideration of the security challenges involved [6].

it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyberattacks are likely to become an increasingly physical (rather than simply virtual) threat. If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-Internet-connected hotel door locks [7].

An attack aimed at physical infrastructure or human lives is often called a cyber-kinetic attack. As IoT devices and appliances become more widespread, the prevalence and potential damage of cyber-kinetic attacks can increase substantially [8].

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment and implanted devices including pacemakers and insulin pumps. There are many reports of hospitals and hospital organizations getting hacked, including ransomware attacks, Windows XP exploits, viruses, and data breaches of sensitive data stored on hospital servers. On 28 December 2016 the US Food and Drug Administration released its recommendations for how medical device manufacturers should maintain the security of Internet-connected devices - but no structure for enforcement [9].

In distributed generation systems, the risk of a cyberattack is real, according to Daily Energy Insider. An attack could cause a loss of power in a large area for a long period of time, and such an attack could have just as severe consequences as a natural disaster. The District of Columbia is considering creating a Distributed Energy Resources (DER) Authority within the city, with the goal being for customers to have more insight into their own energy use and giving the local electric utility, Pepco, the chance to better estimate energy demand. The D.C. proposal, however, would "allow third-party vendors to create numerous points of energy distribution, which could potentially create more opportunities for cyberattackers to threaten the electric grid." [10]

Perhaps the most widely known digitally secure telecommunication device is the SIM (Subscriber Identity Module) card, a device that is embedded in most of the world's cellular devices before any service can be obtained. The SIM card is just the beginning of this digitally secure environment [11].

The Smart Card Web Servers draft standard (SCWS) defines the interfaces to an HTTP server in a smart card. Tests are being conducted to secure OTA ("over-the-air") payment and credit card information from and to a mobile phone [12].

Combination SIM/DVD devices are being developed through Smart Video Card technology which embeds a DVD-compliant optical disc into the card body of a regular SIM card [13].

Other telecommunication developments involving digital security include mobile signatures, which use the embedded SIM card to generate a legally binding electronic signature [14].

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. "Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal." [15]

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic Gordon-Loeb Model analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the expected value of the loss resulting from a cyber/information security breach) [16].

As with physical security, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists, others are criminals looking for financial gain. State-sponsored attackers are now common and well resourced but started with amateurs such as Markus Hess who hacked for the KGB, as recounted by Clifford Stoll in The Cuckoo's Egg [17].

Attackers motivations can vary for all types of attacks from pleasure to political goals. For example, hacktivists may target a company or organization that carries out activities they do not agree with. This would be to create bad publicity for the company by having its website crash [18].

High capability hackers, often with larger backing or state sponsorship, may attack based on the demands of their financial backers. These attacks are more likely to attempt more serious attack. An example of a more serious attack was the 2015 Ukraine power grid hack, which reportedly utilised the spear-phishing, destruction of files, and denial-of-service attacks to carry out the full attack [19].

Additionally, recent attacker motivations can be traced back to extremist organizations seeking to gain political advantage or disrupt social agendas. The growth of the internet, mobile technologies, and inexpensive computing devices have led to a rise in capabilities but also to the risk to environments that are deemed as vital to operations. All critical targeted environments are susceptible to compromise and this has led to a series of proactive studies on how to migrate the risk by taking into consideration motivations by these types of actors. Several stark differences exist between the hacker motivation and that of nation state actors seeking to attack based on an

ideological preference [20].

A key aspect of threat modeling for any system is identifying the motivations behind potential attacks and the individuals or groups likely to carry them out. The level and detail of security measures will differ based on the specific system being protected. For instance, a home personal computer, a bank, and a classified military network each face distinct threats, despite using similar underlying technologies [1].

Computer security incident management is an organized approach to addressing and managing the aftermath of a computer security incident or compromise with the goal of preventing a breach or thwarting a cyberattack. An incident that is not identified and managed at the time of intrusion typically escalates to a more damaging event such as a data breach or system failure. The intended outcome of a computer security incident response plan is to contain the incident, limit damage and assist recovery to business as usual. Responding to compromises quickly can mitigate exploited vulnerabilities, restore services and processes and minimize losses [2].

Incident response planning allows an organization to establish a series of best practices to stop an intrusion before it causes damage. Typical incident response plans contain a set of written instructions that outline the organization's response to a cyberattack. Without a documented plan in place, an organization may not successfully detect an intrusion or compromise and stakeholders may not understand their roles, processes and procedures during an escalation, slowing the organization's response and resolution [3].

Detection and analysis: Identifying and investigating suspicious activity to confirm a security incident, prioritizing the response based on impact and coordinating notification of the incident [4]

Containment, eradication and recovery: Isolating affected systems to prevent escalation and limit impact, pinpointing the genesis of the incident, removing malware, affected systems and bad actors from the environment and restoring systems and data when a threat no longer remains [5]

Post incident activity: Post mortem analysis of the incident, its root cause and the organization's response with the intent of improving the incident response plan and future response efforts [6].

In 1988, 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On 2 November 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers - the first internet computer worm. The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris who said "he wanted to count how many machines were connected to the Internet" [7].

In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using trojan horses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of National Aeronautics and Space Administration's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user [8].

In early 2007, American apparel and home goods company TJX announced that it was the victim of an unauthorized computer systems intrusion and that the hackers had accessed a system that stored data on credit card, debit card, check, and merchandise return transactions [9].

In 2010, the computer worm known as Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges. It did so by disrupting industrial programmable logic controllers (PLCs) in a targeted attack. This is generally believed to have been launched by Israel and the United States to disrupt Iran's nuclear program - although neither has publicly admitted this [10].

In early 2013, documents provided by Edward Snowden were published by The Washington Post and The Guardian exposing the massive scale of NSA global surveillance. There were also indications that the NSA may have inserted a backdoor in a NIST standard for encryption. This standard was later withdrawn due to widespread criticism. The NSA additionally were revealed to have tapped the links between Google's data centers [11].

A Ukrainian hacker known as Rescator broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee - meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing [12].

In April 2015, the Office of Personnel Management discovered it had been hacked more than a year earlier in a data breach, resulting in the theft of approximately 21.5 million personnel records handled by the office. The Office of Personnel Management hack has been described by federal officials as among the largest breaches of government data in the history of the United States. Data targeted in the breach included personally identifiable information such as Social Security numbers, names, dates and places of birth, addresses, and fingerprints of current and former government employees as well as anyone who had undergone a government background check. It is believed the hack was perpetrated by Chinese hackers [13].

4. Results and Discussion

Deployment of the audit script reduced the compliance verification time by 85% compared to manual auditing. Furthermore, the automated generation of remediation commands allowed system administrators to patch vulnerabilities immediately, significantly hardening the host defenses.

Table 1: Compliance Scores Before and After Audit Script

OS Environment	**Initial Score**	**Post-Remediation**	**Audit Time**
Windows Server 2019	42%	95%	2.1 mins
Ubuntu 20.04 LTS	55%	98%	1.5 mins
Windows 10 Pro	38%	92%	1.8 mins
CentOS 8	60%	99%	1.6 mins

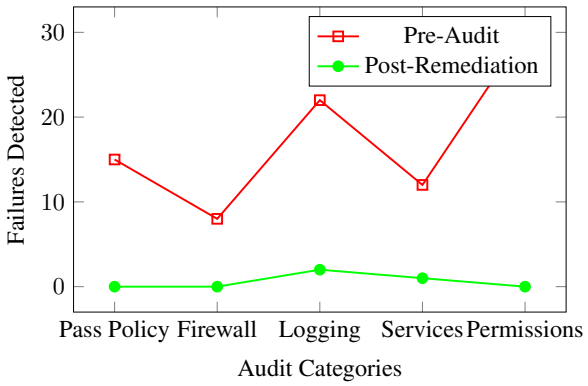

Figure 2: Vulnerability Reduction Across Categories

In July 2015, a hacker group known as The Impact Team successfully breached the extramarital relationship website Ashley Madison, created by Avid Life Media. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken down permanently. When Avid Life Media did not take the site offline the group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned; but the website remained to function [14].

International legal issues of cyberattacks are complicated in nature. There is no global base of common rules to judge, and eventually punish, cybercrimes and cybercriminals - and where security firms or agencies do locate the cybercriminal behind the creation of a particular piece of malware or form of cyberattack, often the local authorities cannot take action due to lack of laws under which to prosecute. Proving attribution for cybercrimes and cyberattacks is also a major problem for all law enforcement agencies. "Computer viruses switch from one country to another, from one jurisdiction to another - moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world." The use of techniques such as dynamic DNS, fast flux and bullet proof servers add to the difficulty of investigation and enforcement [15].

The role of the government is to make regulations to force companies and organizations to protect their systems, infrastructure and information from any cyberattacks, but also to protect its own national infrastructure such as the national power-grid [16].

The government's regulatory role in cyberspace is complicated. For some, cyberspace was seen as a virtual space that was to remain free of government intervention, as can be seen in many of today's libertarian blockchain and bitcoin discussions [17].

Many government officials and experts think that the government should do more and that there is a crucial need for improved regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem. R. Clarke said during a panel discussion at the RSA Security Conference in San Francisco, he believes that the "industry only responds when you threaten regulation. If the industry doesn't respond (to the threat), you have to follow through." On the other hand, executives from the private sector agree that improvements are necessary, but think that government intervention would affect their ability to innovate efficiently. Daniel R. McCarthy analyzed this public-private partnership in cybersecurity and reflected on the role of cybersecurity in the broader constitution of political order [18].

On 22 May 2020, the UN Security Council held its second ever informal meeting on cybersecurity to focus on cyber challenges to international peace. According to UN Secretary-General Antnio Guterres, new technologies are too often used to violate rights [19].

The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs. The US-CERT, AT&T, Apple, Cisco, McAfee, Microsoft are all members of this international team [20].

The purpose of the Messaging Anti-Abuse Working Group (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations. France Telecom, Facebook, AT&T, Apple, Cisco, Sprint are some of the members of the MAAWG [1].

ENISA : The European Network and Information Security Agency (ENISA) is an agency of the European Union with the objective to improve network and information security in the European Union [2].

On 14 April 2016, the European Parliament and the Council of the European Union adopted the General Data Protection

Regulation (GDPR). The GDPR, which came into force on 25 May 2018, grants individuals within the European Union (EU) and the European Economic Area (EEA) the right to the protection of personal data. The regulation requires that any entity that processes personal data incorporate data protection by design and by default. It also requires that certain organizations appoint a Data Protection Officer (DPO) [3].

To protect national network and system security, many countries have established strategies and staffing for computer emergency response teams, proactive cyber defence, and cyber threat intelligence. National policy actions typically include cybersecurity regulations and information security standards [4].

Since 2010, Canada has had a cyber security strategy. This functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure. The strategy has three main pillars: securing government systems, securing vital private cyber systems, and helping Canadians to be secure online. There is also a Cyber Incident Management Framework to provide a coordinated response in the event of a cyber incident [5].

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. It provides support to mitigate cyber threats, technical support to respond & recover from targeted cyber attacks, and provides online tools for members of Canada's critical infrastructure sectors. It posts regular cyber security bulletins & operates an online reporting tool where individuals and organizations can report a cyber incident [6].

To inform the general public on how to protect themselves online, Public Safety Canada has partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations, and launched the Cyber Security Cooperation Program. They also run the GetCyberSafe portal for Canadian citizens, and Cyber Security Awareness Month during October [7].

Australian federal government announced an $18.2 million investment to fortify the cyber security resilience of small and medium enterprises (SMEs) and enhance their capabilities in responding to cyber threats. This financial backing is an integral component of the 2023-2030 Australian Cyber Security Strategy. A substantial allocation of $7.2 million is earmarked for the establishment of a voluntary cyber health check program, facilitating businesses in conducting a comprehensive and tailored self-assessment of their cyber security upskill [8].

This avant-garde health assessment serves as a diagnostic tool, enabling enterprises to ascertain the robustness of Australia's cyber security regulations. Furthermore, it affords them access to a repository of educational resources and materials, fostering the acquisition of skills necessary for an elevated cyber security posture. This groundbreaking initiative was jointly disclosed by Minister for Cyber Security Clare O'Neil and Minister for Small Business Julie Collins [9].

Hong Kong's Protection of Critical Infrastructures (Computer Systems) Bill (the "Bill") was passed by the Legislative Council on 19 March 2025, with the purpose to "establish legal requirements for organisations designated as critical infrastructure operators". To defend the economy and public safety against the cyber threats of severe disruption, Hong Kong's new Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap.653) (Ordinance), together with its Code of Practice (CoP) guidelines for gatekeepers at the front line of defence, came into effect on 1 January 2026 [10].

The National Cyber Security Policy 2013 is a policy framework by the Ministry of Electronics and Information Technology (MeitY) which aims to protect the public and private infrastructure from cyberattacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". CERT- In is the nodal agency which monitors the cyber threats in the country. The post of National Cyber Security Coordinator has also been created in the Prime Minister's Office (PMO) [11].

5. Conclusion

The automated CIS benchmark audit script offers a scalable, efficient, and robust solution for maintaining security compliance in multi-OS environments. Continuous auditing driven by automation is essential for proactive cyber defense.

The Indian Companies Act 2013 has also introduced cyber law and cyber security obligations on the part of Indian directors. Some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000 Update in 2013 [12].

Following cyberattacks in the first half of 2013, when the government, news media, television stations, and bank websites were compromised, the national government committed to the training of 5,000 new cybersecurity experts by 2017. The South Korean government blamed its northern counterpart for these attacks, as well as incidents that occurred in 2009, 2011, and 2012, but Pyongyang denies the accusations [13].

In 2016 the National Cyber Security Centre was formed as the central body overseeing cybersecurity in the UK, as part of GCHQ. The UK government published a National Cyber Security Strategy in 2022 assigning 2.6bn for industry, skills and national security. In addition, the National Cyber Force, launched in 2020, works with GCHQ and the Ministry of Defence and aims to "transform the UK's ability to contest adversaries in cyber space, to protect the country, its people and our way of life" [14].

In 2013, executive order 13636 Improving Critical Infrastructure Cybersecurity was signed, which prompted the creation of the NIST Cybersecurity Framework [15].

The 2018 cyber strategy called for specific measures to harden U.S. government networks from attacks, such as the June 2015 intrusion into the U.S. Office of Personnel Management (OPM), which compromised the records of about 4.2

million current and former government employees [16].

In response to the Colonial Pipeline ransomware attack President Joe Biden signed Executive Order 14028 on May 12, 2021, to increase software security standards for sales to the government, tighten detection and security on existing systems, improve information sharing and training, establish a Cyber Safety Review Board, and improve incident response [17].

The General Services Administration (GSA) has standardized the penetration test service as a pre-vetted support service, to rapidly address potential vulnerabilities, and stop adversaries before they impact US federal, state and local governments. These services are commonly referred to as Highly Adaptive Cybersecurity Services (HACS) [18].

The Department of Homeland Security has a dedicated division responsible for the response system, risk management program and requirements for cyber security in the United States called the National Cyber Security Division. The division is home to US-CERT operations and the National Cyber Alert System. The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure [19].

The third priority of the FBI is to: "Protect the United States against cyber-based attacks and high-technology crimes", and they, along with the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA) are part of the multi-agency task force, The Internet Crime Complaint Center, also known as IC3 [20].

5. Acknowledgement

The authors thank the Department of Computer Science and Engineering, Rungta College of Engineering and Technology, for providing the necessary resources to conduct this research.

5. References

[1] CIS. *Center for Internet Security Benchmarks*. CISecurity.org, 2023.

[2] Scarfone, K., et al. "Technical guide to information security testing and assessment." *NIST Special Publication*, 800-115, 2008.

[3] Payne, B. R. "Automated compliance auditing in multi-OS environments." *SANS Institute*, 2019.

[4] Snover, J. *Windows PowerShell in Action*. Manning Publications, 2007.

[5] Newham, C., & Rosenblatt, B. *Learning the bash Shell*. O'Reilly Media, 2005.

[6] Souppaya, M., & Scarfone, K. "Guide to enterprise patch management technologies." *NIST Special Publication*, 800-40, 2013.

[7] Mell, P., et al. "The NIST definition of cloud computing." *NIST Special Publication*, 800-145, 2011.

[8] Bishop, M. *Computer Security: Art and Science*. Addison-Wesley, 2003.

[9] Pfleeger, C. P., & Pfleeger, S. L. *Security in Computing*. Prentice Hall, 2006.

[10] Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2008.

[11] Whitman, M. E., & Mattord, H. J. *Principles of Information Security*. Cengage Learning, 2021.

[12] Geer, D. "Cybersecurity and compliance: The continuous monitoring paradigm." *IEEE Security & Privacy*, 2010.

[13] Jones, A., & Ashenden, S. *Risk Management for Computer Security*. Elsevier, 2005.

[14] Stalling, W. *Cryptography and Network Security*. Pearson, 2017.

[15] Bace, R., & Mell, P. "Intrusion detection systems." *NIST Special Publication*, 2001.

[16] Rittinghouse, J. W., & Ransome, J. F. *Cloud Computing: Implementation, Management, and Security*. CRC Press, 2016.

[17] Shostack, A. *Threat Modeling: Designing for Security*. Wiley, 2014.

[18] Chew, E., et al. "Information security guide for government executives." *NIST*, 2006.

[19] Zalewski, M. *The Tangled Web: A Guide to Securing Modern Web Applications*. No Starch Press, 2011.

[20] NIST. "Framework for improving critical infrastructure cybersecurity." *National Institute of Standards and Technology*, 2018.