International Journal of General Engineering
and Technology (IJGET)
ISSN(P): 2278–9928; ISSN(E): 2278–9936
Vol. 10, Issue 1, Jan–Jun 2021; 41–56
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AN EMERGING COMPUTER NETWORK SECURITY THREATS AND A NEW PROTECTION TECHNIQUE USING BLOCKCHAIN TECHNOLOGY IN ORGANIZATIONS

Hailye Tekleselase

Lecturer, Department of Information Systems, School of Informatics, Wolaita Sodo University, Addis Ababa, Ethiopia

ABSTRACT

Computer network security is any activity designed to protect the usability, integrity and safety of our network and data. With the advancement of networking technology, like mobile communications (5G),"Internet of Things" (IoT) and cloud computing are coming with new information security threats. This study aims to examine an emerging computer network security threats and to create awareness. Case study and survey were conducted. End users still using outdated software, they didn't update the operating system and applications, they use a permanent password, they use weak and default password (name of super hero person). This is due to lack of awareness, no cyber security training programs and culture of end - users. Ransom ware, social engineering, malware (malicious software or program), distributed denial of service attack (DDoS), and phishing were examined. The proposed method is active DNS using block chain technology. Based the findings we conclude that network security protection using current method is not sufficient. A study by Cyber security Ventures predicts these crimes will cost the world $6 trillion a year by 2021.

KEYWORDS: *Network Security, Security Threats, Sensitive Information, Cloud Computing, IoT*

Article History

Received: ***19 May 2021*** **|** ***Revised:*** ***24 May 2021*** **|** ***Accepted:*** ***28 May 2021***

INTRODUCTION

Network security is any activity designed to protect the usability, integrity and safety of the network infrastructure and data. Now a day the most powerful botnets tend to be based on internet of things (IoT) devices as billions of vulnerable IoT devices have deployed and connected and most IoT devices are easy to hack & compromise.

"Cyber security is information system management by individuals or organizations to manage end-users' security behaviors, on the basis of personal perceived behaviors toward potential security breach in work and non-work environment [1].

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Network Security is designed to protect your network and its data from multiple layers of breaches and intrusions with hardware and software solutions. Network Security is a vast and overarching term, and not just one thing, but is a broad term used to describe many different types of technology and various processes used to define a set of rules and configurations relating to network use, threats, accessibility, and overall threat protection.

Ethiopia intelligence intercepts $110 million cyber fraud May 11, 2020.The criminals have used international money transfer system with fake ID and documents. The criminals were caught red-handed after they faked a document including ATM cards, which stated that an American citizen named Neal Charles has ordered a transfer of $110 million from his account.

The 2020 Cyber Security Report highlights the trends cyber-criminals use to attack organizations worldwide across all industries, and gives cyber security professionals and C-Level executives the information they need to protect their organizations from fifth-generation cyber-attacks and threats. By 2021 cyber-attacks will cost the world around $6 billion Dollars.

Global spending on information security and risk management systems will reach $131bn in 2020; increasing to $174bn in 2022 approximately $50bn will be dedicated to protecting the endpoint according to Gartner’s latest information security and risk management forecast.

94% of malware is delivered via email Phishing attacks account for more than 80% of reported security incidents $17,700 is lost every minute due to phishing attacks 60 percent of breaches involved vulnerabilities for which a patch was available but not applied 63 percent of companies said their data was potentially compromised within the last twelve months due to a hardware- or silicon-level security breach Attacks on IoT devices tripled in the first half of 2019.

Through the development of technologies of internet of things (IoT) and cloud computing, enclosed workers and organizations have significantly changed. Cyber security is one of the serious issues in organizations. Complementary the spiteful benefits of technologies, security attacks and deliberate is behavior reason great suffering to people [2].

A ‘Cyber Security Breaches Survey 2018’ revealed that over four in ten (43%) businesses and two in ten (19%) charities in the UK suffered a cyber-attack. The survey found that 38% of small businesses had spent nothing at all to protect themselves from cyber security threats. Information security awareness is about safeguarding that all employees are aware of the rules and regulations regarding securing the information within organization [3].

Figure 1: Cyber Criminals Become More Sophisticated.

Domain Name System (DNS)

Is one of the main Internet protocols. Individuals all around the globe usually access Internet through a browser works by rendering the web pages and portals. First the domain name of the web page is typed by the users in the browser's address bar. Then, Internet assists the users in information exchange. DNS servers can be distinguished into two broad categories: Recursive servers and Non-recursive/Iterative servers. Non-recursive DNS servers basically work as the Start of Authority (SOA), replying to the queries which are inside their governed/local domain only without worrying about the queries of other DNS servers regardless if they can cater to the requested answer or not. On the other hand, Recursive DNS servers reply to the queries of not only local domain but also all types of domains by sending the queries to other servers and then sending back the response to the user. Some of the most serious attacks on the Recursive DNS servers are root name server performance degradation, DNS cache poisoning, Distributed Denial of Service (DDoS) attacks, unauthorized use of resources. As DNS protocol was not basically created with security issues in mind and has vulnerabilities, the large expanse of event data produced by these systems can be used to create situational awareness about Cyber threat. Earlier day's adversary embeds malware with fixed domain name and IP address. This can be detected by using blacklisting methods. In order to bypass the blacklisting method, adversary uses the concept of fluxing.

There are two types of fluxing; they are domain and IP fluxing. Fluxing means an adversary constantly changes the IP address and domain name. Most commonly used method for domain fluxing is domain generation algorithms (DGAs).

Spam and Phishing Email Detection: The most popular form of spam being email spam commonly referred to as junk mail'. The spammers or cybercriminals send us these spam emails in mass amount, either to make money from the small percentage of recipients that actually respond to such emails or to carry out phishing scams to obtain passwords, credit card numbers, bank account details and more or maybe to simply infect the recipient's computer with malicious code. Spam emails are usually used for commercial purposes. Phishing is another online scam where cybercriminals send emails asking for sensitive information. These mails are made in such a way that they appear to be from a legitimate company. In recent days, this phishing email has become one of the major issues of Internet not only resulting in annoying individual users but also creating great financial losses for organizations.

These mails usually consist of links which will direct to website appearing like the company's website to fill in the information but the information provided by you us misused by the criminals since that link will directly take you to the fake website. Phishing mail are basically a form of spam email but is more manipulative and causes more harm since it tries to extract the confidential information from the user and carry out fraudulent activities. This particular type of spam employs two techniques: deceptive phishing and malware-based phishing. The first category uses social engineering scheme, which generates a spam mail which fake the legitimate company ora bank such that the victim is redirected to a fake website to trick the victim to obtain financial data [4].

In recent times, Android OS has earned attention from different organization ranging from academia to industry. An android OS (OS) is an open source, Linux based OS which is most commonly used OS for mobile and handheld devices. Due to its importance in several applications, Android OS has become a target for attackers to conduct criminal and illegal activities. As the attacks to Android OS continue to grow, various methods have been introduced to fight against attacks. The developers use software development kit (SDK) to build and publish their applications. It is basically designed for mobile devices, smartphones, tablets and additionally it can support other platforms like TVs, cars, embedded and wearable devices. Due to this portability nature, many companies have been involved in development of apps for android platform that apparently runs on all the devices. Applications are hosted in official app store called Google Play. Android is being served as most popular OS, third-party distribution centers, a rich SDK and uses Java programming language.

In recent days, Android devices have been largely used by peoples. These devices stores lots of sensitive information like financial information like bank details, user credentials, personal information like photos, and videos. This has become more interesting to the attackers. Malicious authors develop malware to steal the private data or delete or alter the existing data and monitor the user activities with the aim to get benefits. Additionally, Android applications are hosted in various third-party stores which allow the user to repackage Android applications with adding a piece of malicious code. Generally, Android OS automatically assigns a unique Linuxuser ID during the installation phase to know each app runs its own instance of virtual machine. This facilitates to the creation of a sandbox which isolates the apps from each other's. It provides authorization mechanism through the use of Android permissions

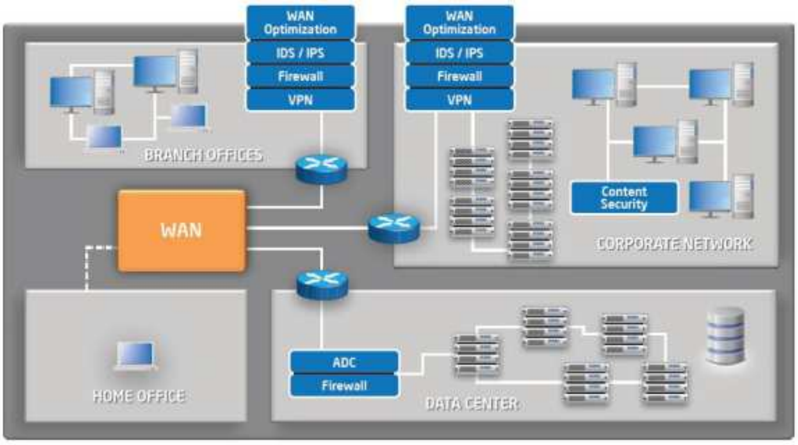


Figure 2: Multiple Layered Network Model.

OBJECTIVE

The main objective of this study is to examine an emerging and the most serious computer security threats, awareness creation, to show an effective method to protect our self and organization from cyber-attacks.

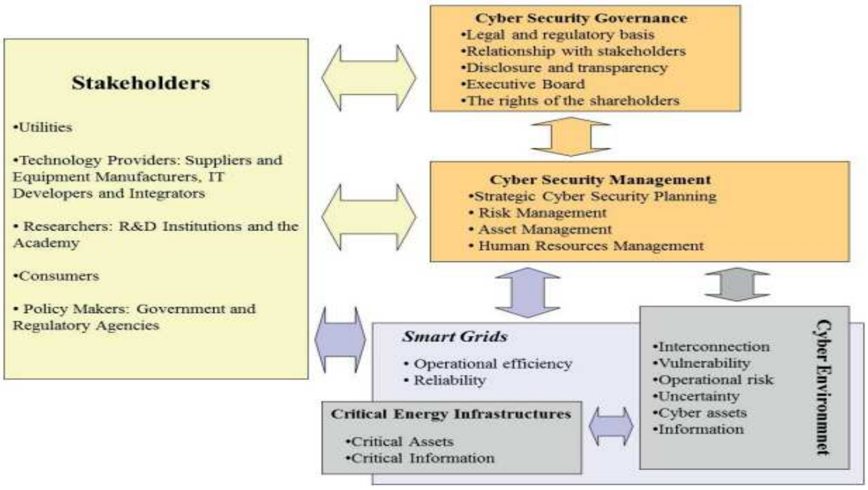

Stakeholders
•Utilities
•Technology Providers: Suppliers and Equipment Manufacturers, IT Developers and Integrators
• Researchers: R&D Institutions and the Academy
•Consumers
• Policy Makers: Government and Regulatory Agencies
Cyber Security Governance
•Legal and regulatory basis
•Relationship with stakeholders
•Disclosure and transparency
•Executive Board
•The rights of the shareholders
Cyber Security Management
•Strategic Cyber Security Planning
• Risk Management
• Asset Management
• Human Resources Management
Smart Grids
• Operational efficiency
• Reliability
Critical Energy Infrastructures
•Critical Assets
•Critical Information
•Interconnection
•Vulnerability
•Operational risk
•Uncertainty
•Cyber assets
•Information
Cyber Environmnet

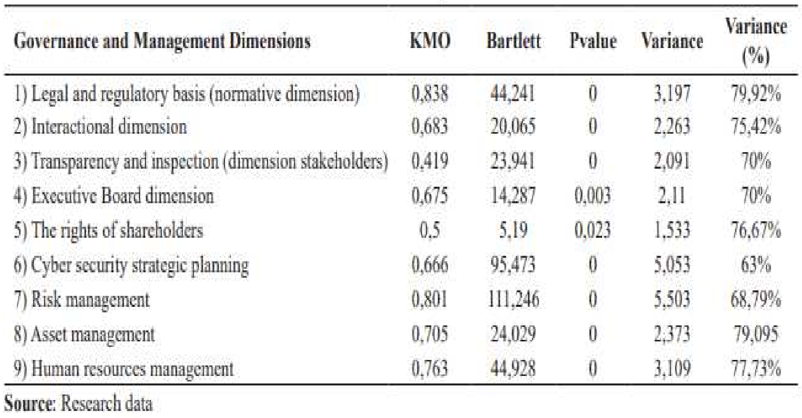
Figure 3: Theoretical Model.

METHODOLOGY

Research Design

A qualitative (interview), survey, case study, and an in-depth literature review approach were used. Survey direct observation and experiment using wire shark and snort network monitoring (security) tools was conducted in sample organizations. Interview related to employees' knowledge and attitudes towards information security and on cyber-attacks.

Table 1: Model Validation



Governance and Management Dimensions	KMO	Bartlett	Pvalue	Variance	Variance (%)
1) Legal and regulatory basis (normative dimension)	0,838	44,241	0	3,197	79,92%
2) Interactional dimension	0,683	20,065	0	2,263	75,42%
3) Transparency and inspection (dimension stakeholders)	0,419	23,941	0	2,091	70%
4) Executive Board dimension	0,675	14,287	0,003	2,11	70%
5) The rights of shareholders	0,5	5,19	0,023	1,533	76,67%
6) Cyber security strategic planning	0,666	95,473	0	5,053	63%
7) Risk management	0,801	111,246	0	5,503	68,79%
8) Asset management	0,705	24,029	0	2,373	79,095
9) Human resources management	0,763	44,928	0	3,109	77,73%

Source: Research data

Emerging Cyber Security Threats

Many companies migrated their data and information to the Cloud in 2019, assuming that this would help mitigate cyber security threats. However, simply moving your data to the Cloud does not guarantee that your data is safer in any manner. Indeed, in 2020, Cloud Jacking will likely become a more prominent cyber security threat due to the increased use of Cloud Computing. A report from Fortune Business indicates that the Internet of Things (IoT) market will reach $1.1 trillion by 2026.

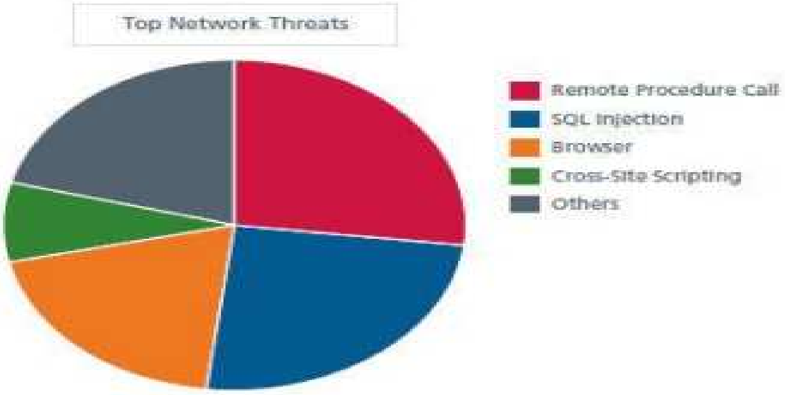


Figure 4

Artificial Intelligence (AI)

Malicious actors may use AI in order to learn about its targets and their environment to then automate tailored attacks. Impersonation scams can imitate the writing style of known and trusted contacts to reduce suspicion when used in email or SMS text-based attacks. However, organizations can also use AI to defend their networks by quickly identifying and analyzing potential attacks [4].

Supply Chains

There will be continued targeting of supply chain vendors and clients via spear-phishing campaigns, business email compromise (BEC) scams, and compromised vendor accounts – particularly to launch ransom ware attacks. Organizations are advised to adopt a vendor management program and implement security protections and controls, including DMARC to help prevent email spoofing [5]

By 2022, 60% of the global GDP will be digitized. Yet today only 45% of people trust that technology will improve their lives. Every sector is beginning to face deep questions about what the implications of this transformation will be [6].

Ransom ware attacks are a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.

This is a type of trojan cyber ware that is designed to gain money from the person or organization’s computer on which it is installed by encrypting data so that it is unusable, blocking access to the user’s system. Ransom ware is a kind of malicious software designed to block access to a computer system or computer files with a demand of paying out a sum of money. Most variants of ransom ware encrypt the files on the affected device, rendering them unavailable and demand a ransom payment in order to restore access to them.

Ransom ware code is often not sophisticated, but it doesn’t have to be, because unlike other forms of conventional malware, it doesn’t generally need to stay undetected for a long time to achieve its target. This relative ease of implementation versus high-profit potential attracts both sophisticated actors of cybercrime and novice actors to run ransom ware campaigns.

In this kind of attack, an adversary collects as much information about your network as he needed for other attacks. This information includes IP address range, server location, running OS, software version, types of devices etc. Packet capturing software, Ping command, trace root command, who is lookup are some example tools which can be used to collect this information. Adversary will use this information in mapping your infrastructure for next possible attack.

Social Engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.

Figure 5

DNS Query Attack

DNS queries are used to discover information about public server on the internet. All OS includes the tool for DNS queries such as lookup in Windows, Dig and Host in Linux. These tools query a DNS server for information about specified domain. DNS server respond with internal information such as Server IP address, Email Server, technical contacts etc. An adversary can use this information in phishing or ping attack.

Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information. Phishing attack is gaining popularity from last couple of years. In this attack an adversary creates fake email address or website which looks like a reputed mail address or popular site. Later attacker sends email using their name. These emails contain convincing message, some time with a link that leads to a fake site. This fake site looks exactly same as original site. Without knowing the truth user tries to log on with their account information, hacker records this authentication information and uses it on real site. [7].

Hijack Attack

This attack usually takes place between running sessions. Hacker joins a running session and silent disconnects other party. Then he starts communicating with active parties by using the identity of disconnected party. Active party thinks that he is talking with original party and may send sensitive information to the adversary.

DNS Query Attack

DNS queries are used to discover information about public server on the internet. All OS includes the tool for DNS queries such as lookup in Windows, Dig and Host in Linux. These tools query a DNS server for information about specified domain. DNS server respond with internal information such as Server IP address, Email Server, technical contacts etc. An adversary can use this information in phishing or ping attack.

Denial of Service Attacks

DoS attack is a series of attacks. In this attack an adversary tires to misuse the legitimate services. Several networking tools are available for troubleshooting. An attacker uses these tools for evil purpose. For example, ping command is used to test the connectivity between two hosts. An adversary can use this command to continuously ping a host with oversized packets. In such a situation target host will be too busy in replying (of ping) that it will not be able run other services.

Insider Attack

According to a survey more than 70% attacks are insider. Insider attacks are divided in two categories; intentionally and accidentally. In intentionally attack, an attacker intentionally damage network infrastructure or data. Usually intentionally attacks are done by disgruntled or frustrated employees for money or revenge. In accidentally attack, damages are done by the carelessness or lack of knowledge.

Internet of Things

A report from Fortune Business indicates that the Internet of Things (IoT) market will reach $1.1 trillion by 2026. To say that IoT is gonna be huge is an understatement. The majority of people know what smart devices are and many own such devices. Google is practically giving away free Google Home Minis. However, the widespread implementation of IoT devices will usher in a larger amount of cyber security threats.

Deep Fakes

We have written before on deep fake technology, and the implications of them. Many people fear that we will start to see malicious uses of deep fakes grow into a massive cyber security threat. Some possibilities include deep fake phishing campaigns, attempts to influence the 2020 election, deep fake-as-a-service companies with bad security, and using deep fakes to commit fraud through synthetic identities. It will be important for the public to maintain a healthy skepticism in the face of fabricated videos. Deep fakes are going to make phishing attempts a lot more convincing, and may end up costing organizations a lot of money in 2020.

Cloud Storage

Many companies migrated their data and information to the Cloud in 2019, assuming that this would help mitigate cyber security threats. However, simply moving your data to the Cloud does not guarantee that your data is safer in any manner. After all, one of the largest 2019 breaches, the Capital One breach, occurred when a hacker infiltrated the servers of a third-party Cloud computing company that Capital One used. This breach resulted in 106 million records exposed, and that will not be an isolated incident.

Indeed, in 2020, Cloud Jacking will likely become a more prominent cyber security threat due to the increased use of Cloud Computing. The infrastructure of Cloud security is going to increase in complexity as the attacks on Cloud services also grow more complex. In fact, in 2020, security will likely be one of the main deciding factors as to which third-party Cloud service organizations will go with.

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There Are A Number of Different Types of Malware, Including

- Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

SQL Injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a data based via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Man-in-the-Middle Attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Social Engineering Attacks

Social engineering attacks like phishing have always been used by attackers to trick victims into surrendering sensitive information like login details and credit card information. Though most organizations are enhancing their email security to block phishing attacks, cybercriminals are coming up with sophisticated phishing kits that aid in data breaches and financial fraud.

Since phishing is an effective, high-reward, and minimal-investment strategy for cybercriminals to gain legitimate access to credentials, it will continue to be a big cybersecurity threat in 2020. In fact, the 2019 Data Breach Investigations Report by Verizon reveals that phishing remains the number one cause of data breaches globally.

SMiShing (SMS phishing) is another form of social engineering attack that will gain prominence in the near future. The immense popularity of apps like WhatsApp, Slack, Skype, WeChat, and Signal among others is encouraging attackers to switch to these messaging platforms to trick users into downloading malware on their phones. According to Experian's 2020 Data Breach Industry Forecast, SMiShing attempts from hackers will target consumers through fraudulent messages disguised as fundraising initiatives.

Cyber securityVenturespredictsthattherewillbe6 billion Internet users by 2022 (75 percent of the projected world population of 8 billion) — and more than 7.5 billion Internet users by 2030 (90 percent of the projected world population of 8.5 billion, 6 years of age and older).

The number and performance of individual "smart" devices is increasing every year, making them a very attractive target for cyber criminals, says the report.

According to the research performed by CompTIA, 26% of the large organizations, 20% of the mid-size organization, and 17% of small businesses make heavy use of security metrics. The same research says that the Cyber security market has recorded a growth of 10.2% in 2018 and has revenue of $91.4 billion[8].

Firewalls

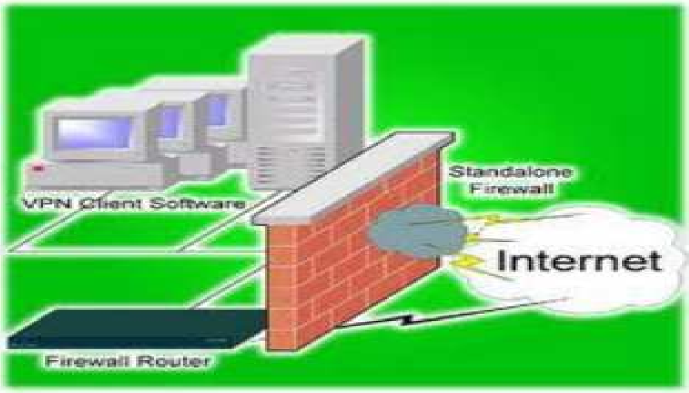


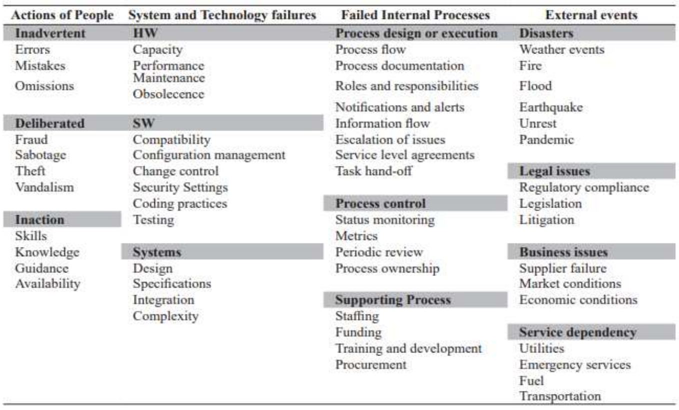
Figure 6: Firewalls.

RESULTS AND DISCUSSIONS

This study is more related to examining the perceptions, consciousness, skills and knowledge of employees in securing sensitive information in organization and critical infrastructure form cyber-attacks. Now a day mobile device are more target especially android operating systems (android version 5.0 and blow), 5G mobile technology, cloud service provider, and IOT devices are more vulnerable for cyber-attacks. So, organizations should have their own Virtual private network (VPN). Besides organization must use intrusion detection systems (IDS), intrusion prevention system (IPS) proactively, and network security tools like snort, wire shark, firewall, vpnaudit record generation and utilization (Argus), unified threat management (UTM), VPN[9].

Besides, it inspects the encounters or vulnerability to secure sensitive information and to create awareness about cyber-attack to all end users. Even by giving free training about cyber security methods, mechanisms, and applications to secure our cyber space in general and our organization in particular even ourselves. Employees in organizations still using obsolete software, they didn't update the software (operating system), they use a permanent password, they are still using weak and default password (Wife/husband name or her/his phone number which is easy to guess) [10].

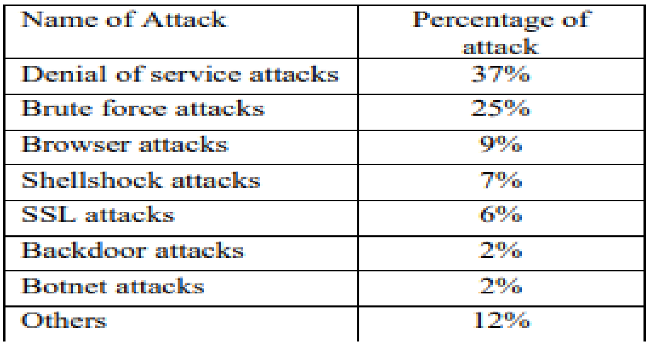
Table 2



Actions of People	System and Technology failures	Failed Internal Processes	External events
Inadvertent	**HW**	**Process design or execution**	**Disasters**
Errors	Capacity	Process flow	Weather events
Mistakes	Performance	Process documentation	Fire
Omissions	Maintenance	Roles and responsibilities	Flood
	Obsolecence	Notifications and alerts	Earthquake
Deliberated	**SW**	Information flow	Unrest
Fraud	Compatibility	Escalation of issues	Pandemic
Sabotage	Configuration management	Service level agreements	
Theft	Change control	Task hand-off	**Legal issues**
Vandalism	Security Settings		Regulatory compliance
	Coding practices	**Process control**	Legislation
Inaction	Testing	Status monitoring	Litigation
Skills		Metrics	
Knowledge	**Systems**	Periodic review	**Business issues**
Guidance	Design	Process ownership	Supplier failure
Availability	Specifications		Market conditions
	Integration	**Supporting Process**	Economic conditions
	Complexity	Staffing	
		Funding	**Service dependency**
		Training and development	Utilities
		Procurement	Emergency services
			Fuel
			Transportation

Source: Adapted from Cebula

Table 3



Name of Attack	Percentage of attack
Denial of service attacks	37%
Brute force attacks	25%
Browser attacks	9%
Shellshock attacks	7%
SSL attacks	6%
Backdoor attacks	2%
Botnet attacks	2%
Others	12%

Types of Attacks

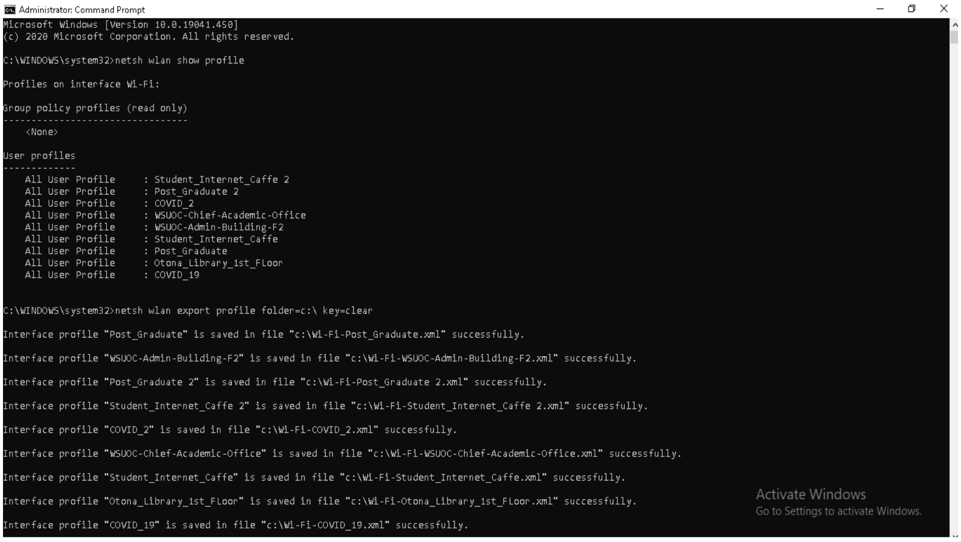
Conclusion based the findings we conclude that cyber security preparations and trained employees are very low at the same time hackers becoming more and more sophisticated. So, awareness creation, behavioral change and training are necessary besides intelligence systems as study show more than 90% cyber-attack occurs due to human factor or human error (carelessness) [11].

As Borkena.org January 9, 2020 Ethio-Telecom reportedly lost an estimated 100 million Ethiopian birr worth of losses. The state-owned company disclosed about it as it is undertaking community engagement in the capital Addis Ababa to discuss about infrastructure security, as reported by Fana Broadcasting Corporate (FBC) on Thursday. The CEO, Firehiwot Tamiru, reportedly said that the problem is worsening from time to time, and it is negatively affecting delivery of quality service and service expansion as well [12].

The initial keyword searches show that there are a substantial number of papers related to blockchain. The technologies of blockchain and truly distributed decentralized systems have only been developed for ten years and are clearly still in their infancy. A sizeable portion of the selected primary studies are experimental proposals or concepts for solutions to today's problems, and they have little quantitative data and few practical applications. Some of the more practical security solutions offered in the remaining primary studies display innovative techniques for solving a wide range of problems concerning data security, mutability and authentication of users. The solutions often depend on a significant change to that system's infrastructure, for example, a change in the network architecture or a reliance on a particular blockchain or platform over a single, centralized server. Due to the labour involved with changing or moving an existing system, it is difficult for some of the practical concepts to be run in an experimental environment for a certain length of time to determine the effectiveness of the blockchain application over conventional security. Notable exceptions included IoT Chain [S39] and their experimentation of different consensus mechanisms. They utilized the well-established Ethereum platform to conduct their development and experimental analysis. It seemed that the most practical and ready-to-deploy solutions were those that had been tested on Ethereum or Bitcoin platforms.

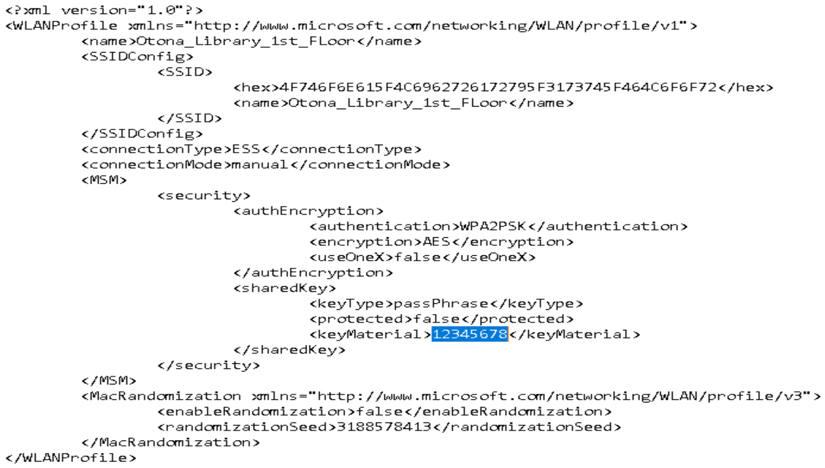
The researchers used established platforms, such as Ethereum and Bitcoin for a few different reasons. Ethereum allows for very customizable programming of smart contracts and blockchain applications in the language Solidity, which is not too far removed from Javascript and Python and as such makes it attractive to developers. The Bitcoin blockchain is the most established, invested in and decentralized blockchain [30] available, and it provides a useful testbed for experimental concepts. However, it can suffer high latency and fees during times of high network demand with the current protocols being employed [12].

Command Prompt and Windows Power Shell Attacks



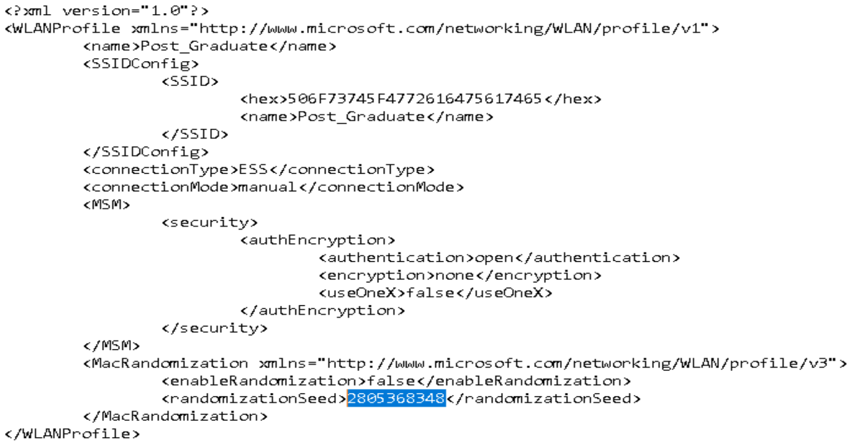
```
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh wlan show profile

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : Student_Internet_Caffe 2
    All User Profile     : Post_Graduate 2
    All User Profile     : COVID_2
    All User Profile     : WSUOC-Chief-Academic-Office
    All User Profile     : WSUOC-Admin-Building-F2
    All User Profile     : Student_Internet_Caffe
    All User Profile     : Post_Graduate
    All User Profile     : Otona_Library_1st_FLoor
    All User Profile     : COVID_19


C:\WINDOWS\system32>netsh wlan export profile folder=c:\ key=clear

Interface profile "Post_Graduate" is saved in file "c:\Wi-Fi-Post_Graduate.xml" successfully.

Interface profile "WSUOC-Admin-Building-F2" is saved in file "c:\Wi-Fi-WSUOC-Admin-Building-F2.xml" successfully.

Interface profile "Post_Graduate 2" is saved in file "c:\Wi-Fi-Post_Graduate 2.xml" successfully.

Interface profile "Student_Internet_Caffe 2" is saved in file "c:\Wi-Fi-Student_Internet_Caffe 2.xml" successfully.

Interface profile "COVID_2" is saved in file "c:\Wi-Fi-COVID_2.xml" successfully.

Interface profile "WSUOC-Chief-Academic-Office" is saved in file "c:\Wi-Fi-WSUOC-Chief-Academic-Office.xml" successfully.

Interface profile "Student_Internet_Caffe" is saved in file "c:\Wi-Fi-Student_Internet_Caffe.xml" successfully.

Interface profile "Otona_Library_1st_FLoor" is saved in file "c:\Wi-Fi-Otona_Library_1st_FLoor.xml" successfully.

Interface profile "COVID_19" is saved in file "c:\Wi-Fi-COVID_19.xml" successfully.
```

Figure 7



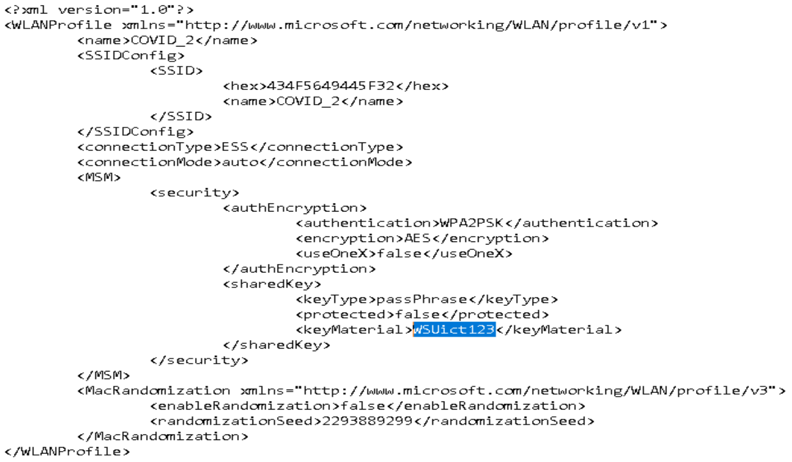
```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>Otona_Library_1st_FLoor</name>
        <SSIDConfig>
                <SSID>
                        <hex>4F746F6E615F4C6962726172795F3173745F464C6F6F72</hex>
                        <name>Otona_Library_1st_FLoor</name>
                </SSID>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>manual</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2PSK</authentication>
                                <encryption>AES</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                        <sharedKey>
                                <keyType>passPhrase</keyType>
                                <protected>false</protected>
                                <keyMaterial>12345678</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
        <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
                <enableRandomization>false</enableRandomization>
                <randomizationSeed>3188578413</randomizationSeed>
        </MacRandomization>
</WLANProfile>
```

Figure 8



```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>Post_Graduate</name>
        <SSIDConfig>
                <SSID>
                        <hex>506F73745F4772616475617465</hex>
                        <name>Post_Graduate</name>
                </SSID>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>manual</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>open</authentication>
                                <encryption>none</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                </security>
        </MSM>
        <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
                <enableRandomization>false</enableRandomization>
                <randomizationSeed>2805368348</randomizationSeed>
        </MacRandomization>
</WLANProfile>
```

Figure 9



```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>COVID_2</name>
        <SSIDConfig>
                <SSID>
                        <hex>434F5649445F32</hex>
                        <name>COVID_2</name>
                </SSID>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>auto</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2PSK</authentication>
                                <encryption>AES</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                        <sharedKey>
                                <keyType>passPhrase</keyType>
                                <protected>false</protected>
                                <keyMaterial>WSUict123</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
        <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
                <enableRandomization>false</enableRandomization>
                <randomizationSeed>2293889299</randomizationSeed>
        </MacRandomization>
</WLANProfile>
```

Figure 10

Effective Ways to Protect Cyber Attacks

Identify Your Sensitive Data

The first step to securing your data is to identify and list all of the private information that you have stored in your network and taking note of whom in your organization has access to it. By gathering all of this information you are able to secure it properly and create a data protection policy which will help keeps your sensitive data secure [13].

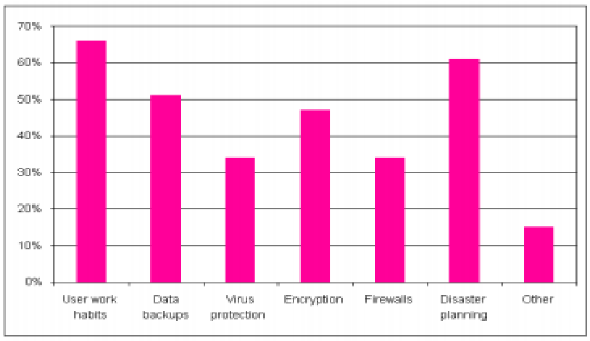


Figure 11: Mechanisms on Cyber Security.

Create a Culture of Accountability

Both employees and managers should be aware of and understand their responsibilities and the responsibilities of their team when it comes to the handling of sensitive information. By making your team aware of their responsibilities and the consequences of mistakes and negative behavior you can create a culture of accountability [14].

Review Accounts and Privileged Access

It is significant that you regularly review your user’s privileges and account logins to ensure that any inactive accounts no longer have access to private information and that users don’t have unnecessary access to data. This helps to reduce the risks of both accidental and malicious insider data breaches [15].

Training

Short- and long-term training to create awareness or knowledge to end users, IT staff, employees in general to all society about cyber-attacks and effective methods or mechanisms to secure our sensitive information.

Firewalls

Network security firewalls monitor the incoming and the outgoing traffic based on a set of predefined rules. It is a barrier that separates trusted networks from untrusted ones. Hardware, software, or both can serve as a firewall.

IDS and IPS

Intrusion Detection System (IDS) is a software application that looks for malicious activity or a policy violation over a network or system, whereas Intrusion Prevention System (IPS) is a network threat prevention technology that actively scans network traffic flow to detect potential threats (or vulnerability exploits) and respond to them accordingly.

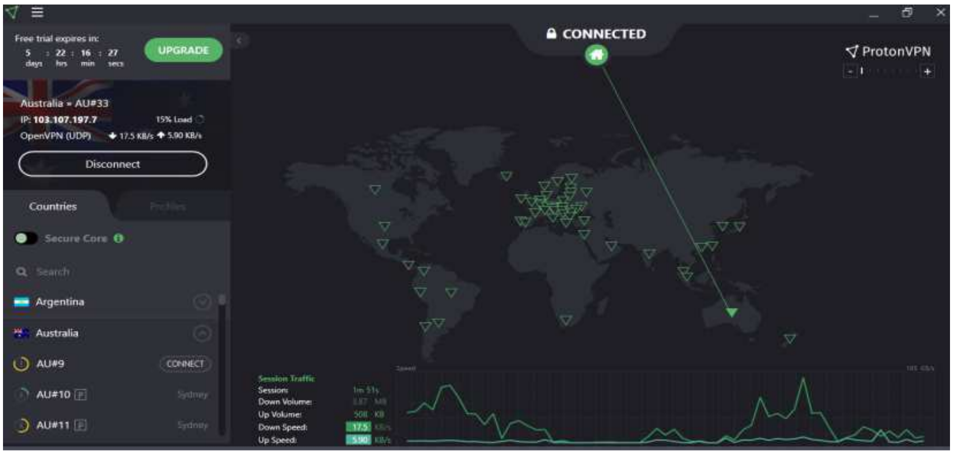
For simple understanding, IDS is considered to be a monitoring system and IPS as a network security control system. Both the systems read network packets to compare them with a database dedicated to known threats. But, IDS never acts on its own as it requires a professional to instruct it whereas IPS works according to its rule set for accepting or rejecting a network packet.

SIEM

Security Information and Event Management (SIEM) is a combination of Security Information Management (SIM) and Security Event Management (SEM). SIEM products ensure that all relevant information is accumulated in one place for your security staff to identify possible threats and respond to them. Everything including physical and virtual appliances to servers of VPN

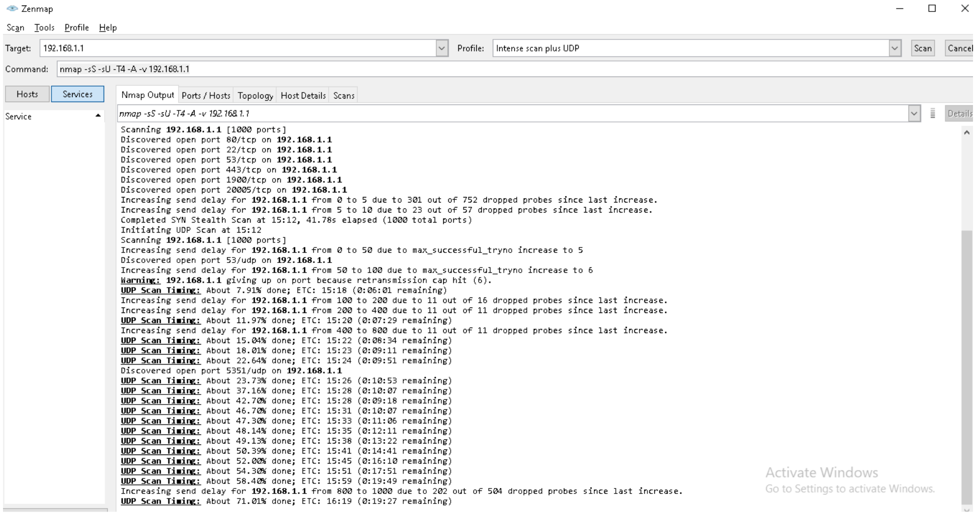
VPN

The act of encrypting a connection over the Internet from its endpoint to a network is defined as a Virtual Private Network (VPN). This technology allows remote access to secure corporate applications or other resources ware can work as an SIEM product.



Australia » AU#33
IP: 103.107.197.7 15% Load
OpenVPN (UDP) 17.5 KB/s 5.90 KB/s
AU#9
AU#10
AU#11
Session Traffic
Session: 1m 51s
Down Volume: 1.87 MB
Up Volume: 508 KB
Down Speed: 17.5 KB/s
Up Speed: 5.90 KB/s

Figure 12: Assess Or Scan Network Vulnerability Using Network Monitoring Tools (Wireshark Or Zen Map).



Target: 192.168.1.1
Profile: Intense scan plus UDP
Command: nmap -sS -sU -T4 -A -v 192.168.1.1

```
nmap -sS -sU -T4 -A -v 192.168.1.1
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 1900/tcp on 192.168.1.1
Discovered open port 20005/tcp on 192.168.1.1
Increasing send delay for 192.168.1.1 from 0 to 5 due to 301 out of 752 dropped probes since last increase.
Increasing send delay for 192.168.1.1 from 5 to 10 due to 23 out of 57 dropped probes since last increase.
Completed SYN Stealth Scan at 15:12, 41.78s elapsed (1000 total ports)
Initiating UDP Scan at 15:12
Scanning 192.168.1.1 [1000 ports]
Increasing send delay for 192.168.1.1 from 0 to 50 due to max_successful_tryno increase to 5
Discovered open port 53/udp on 192.168.1.1
Increasing send delay for 192.168.1.1 from 50 to 100 due to max_successful_tryno increase to 6
Warning: 192.168.1.1 giving up on port because retransmission cap hit (6).
UDP Scan Timing: About 7.91% done; ETC: 15:18 (0:06:01 remaining)
Increasing send delay for 192.168.1.1 from 100 to 200 due to 11 out of 16 dropped probes since last increase.
Increasing send delay for 192.168.1.1 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 11.97% done; ETC: 15:20 (0:07:29 remaining)
Increasing send delay for 192.168.1.1 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 15.04% done; ETC: 15:22 (0:08:34 remaining)
UDP Scan Timing: About 18.01% done; ETC: 15:23 (0:09:11 remaining)
UDP Scan Timing: About 22.64% done; ETC: 15:24 (0:09:51 remaining)
Discovered open port 5351/udp on 192.168.1.1
UDP Scan Timing: About 23.73% done; ETC: 15:26 (0:10:53 remaining)
UDP Scan Timing: About 37.16% done; ETC: 15:28 (0:10:07 remaining)
UDP Scan Timing: About 42.70% done; ETC: 15:28 (0:09:18 remaining)
UDP Scan Timing: About 46.70% done; ETC: 15:31 (0:10:07 remaining)
UDP Scan Timing: About 47.30% done; ETC: 15:33 (0:11:06 remaining)
UDP Scan Timing: About 48.14% done; ETC: 15:35 (0:12:11 remaining)
UDP Scan Timing: About 49.13% done; ETC: 15:38 (0:13:22 remaining)
UDP Scan Timing: About 50.39% done; ETC: 15:41 (0:14:41 remaining)
UDP Scan Timing: About 52.00% done; ETC: 15:45 (0:16:10 remaining)
UDP Scan Timing: About 54.30% done; ETC: 15:51 (0:17:51 remaining)
UDP Scan Timing: About 58.40% done; ETC: 15:59 (0:19:49 remaining)
Increasing send delay for 192.168.1.1 from 800 to 1000 due to 202 out of 504 dropped probes since last increase.
UDP Scan Timing: About 71.01% done; ETC: 16:19 (0:19:27 remaining)
```

Figure 13

CONCLUSIONS

2020 cyber security threats are going to be challenging, weird, and intense. Data breaches have not shown any sign of slowing down, and a slew of new technologies will prove to be challenging. We will need skilled professionals and average individuals with basic cyber hygiene to come together.

Organization should make a continuous cyber security assessment (monitoring) using Intrusion detection system (IDS), intrusion prevention system (IPS), unified threat management (UTM), firewall, secure socket layer (SSL) encryption, WPE protection, SSH, Snort, Wire shark air crack, Nessus and backtrack.

A Cyber Security Software is a must for Cyber Security and Privacy of a business or individual. Cyber security is the method that is used to protect the network, system, or applications from the cyber-attacks. Cyber-attacks have increased from 576 to 791 grand attacks annually during the past three successive years Information Network Security Agency (INSA, 2019).As Borkena.org January 9, 2020 Ethio-Telecom reportedly lost an estimated 100 million Ethiopian birr worth of losses.

Despite the growing trends of using technologies in the country, the awareness and capacity to prevent cyber-attack is still poor; and this makes the situation even worse, Lack of awareness, legal frameworks, and poor cyber security governance, among others, are the major problems identified in organizations in Ethiopia.

RECOMMONDATIONS

- Organization should train their employees.
- Organization should make a continuous cyber security assessment.
- Organization should turn their employees into partners.
- Apply end-to-end encryption to all your confidential files.
- Organizations should have their own virtual private network.

REFERENCES

1. *Y. Lu, "Cyber security Research: A Review of Current Research Topics," Journal of Industrial Integration and Management, vol. Vol. 3, no. No. 4, p. 25, October 2018.*
2. *B. Khan, "Effectiveness of information security awareness methods based on psychological theories," African Journal of Business Management, vol. Vol. 5(26, no. pp. 10862-10868, p. 8, October 2011.*
3. *H. Aldawood, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," MDPI, p. 16, March 2019.*
4. *I. Ghafir, "Security threats to critical infrastructure: the human factor," doi.org, p. 17, March 2018.*
5. *M. D. Donno, "Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era," MDPI, p. 30, June 2019.*
6. *M. M. Kundalakesi, "Network Security with Cryptography," International Journal for Scientific Research & Development, vol. Vol. 6, no. Issue 01, p. 3, September 2018.*
7. *S. Pareek, "Different Type Network Security Threats and Solutions, A Review," International Journal of Computer Science, vol. Volume 5, no. Issue 4, p. 11, April 2017.*
8. *A. Rizal, "Information Security Challenges: A Malaysian Context," International Journal of Academic Research in Business and Social Sciences, vol. Vol. 7, no. No. 9, p. 8, September 2017.*

9. *T. Dargah, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," Journal of Computer Virology and Hacking Techniques, p. 29, July 2019.*

10. *S. Pareek1, "Different Type Network Security Threats and Solutions, A Review," International Journal of Computer Science, vol. Volume 5, no. Issue 4, p. 11, April 2017.*

11. *T. Limba¹, "Cyber Security Management Model for Critical Infrastructure," The International Journal Entrepreneurship and Sustainability Issues, vol. Volume 4, no. Number 4, p. 16, June 2017.*

12. *Y. Rao, "Artificial Intelligence and Big Data for Computer Cyber Security Systems," Journal of Advances in Science and Technology, vol. Vol. 12, no. Issue No. 24, p. 9, November 2016.*

13. *A. Bahalul, "Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh - Hype or Reality?," International Journal of Managing Information Technology (IJMIT), vol. 11, no. 1, p. 14, February 2019.*

14. *V. L, "A Survey on Network Security and Cryptography," International Journal of Advance Research In Science And Engineering, vol. 3, no. 10, p. 10, October 2014.*

15. *T. D, "A Cyber-Kill-Chain based taxonomy of crypto – ransomware features," Journal of Computer Virology and Hacking Techniques, p. 29, July 2019.*

16. *H. A, "A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective," Journal of censor and actuator networks (MDPI), p. 38, April 2019.*

17. *Y. Lu, "Cyber security Research: A Review of Current Research Topics," Journal of Industrial Integration and Management, vol. 3, no. 4, p. 25, October 2018.*

18. *Y. R, "Artificial Intelligence and Big Data for Computer Cyber Security Systems," Journal of Advances in Science and Technology, vol. 12, no. 24, p. 9, November 2016.*

19. *G. A, "On the Effectiveness of Machine and Deep Learning for Cyber Security," 2018 10th International Conference on Cyber Conflict, p. 20, 2018.*

20. *S. Dilek, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," International Journal of Artificial Intelligence & Applications, vol. 6, no. 1, p. 19, January 2015.*

21. *A. A. Sattikar, "A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking," IJCSET, vol. 2, no. 1, p. 4, January 2012.*

22. *H. T. Woldemichael, "Emerging Cyber Security Threats in Organization," Network Security and Communication, vol. 7, no. 6, p. 4, January 2019.*

ABOUT THE AUTHOR

Hailye Tekleselase Michael holds a BSc degree in Information Systems from University of Gondar, and M Sc degree in Information Systems from Addis Ababa University. His current research interests are: Cyber Security, Big Data, AI, ICT and Mobile Computing. He currently Lecturer at Wolaita Sodo University, He is a member of the Ethiopian Space Science Society (ESSS) and the Institution of Electrical and Electronics Engineers (IEEE).