VOL 3 (2019) NO 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises

Said F. Aboelfotoh[#], Noha A. Hikal[#]

[#] *IT dept. , Faculty of Computers and Information Systems, Mansoura University, Egypt*
E-mail: said_994@yahoo.com, dr_nahikal@mans.edu.eg

***Abstract*— Regarding the huge spread of technology among individuals and enterprises, technologies and electronic communications become one of the most important pillars of the operation of small and large enterprises alike, and the source of education and entertainment for individuals, this led to thinking about the risks of reliance on this technology and the impact on the economic index of enterprises market, reputation and the safety of individuals and enterprises, these fears forced the experts and decision-makers to think about information security and develop new methods to measure and assess the level of protection of information and data in enterprises and privacy of individuals. This paper introducing a review of recent cyber-security measuring and assessment methodologies and tools based on industry best practices for the measure and assesses of network security and protection of a modern enterprise data network. The analysis is based on a study the methods for the measurement and assessment of information security at the physical and technical level, penetration testing and identification of weaknesses in the cyber-security system followed and policies used in modern enterprises. A comprehensive description of the strengths, weaknesses, and licensing conditions for tools is presented. Moreover, major security requirements associated with modern enterprises is discussed and analyzed to discover vulnerability in the existing systems and explain the potential impact of this vulnerability.**

***Keywords*— Cyber Security, Performance Measures, Risk Assessment, Vulnerability Scanner.**

I. Introduction

Cyber security refers generally to the ability to save and manage access to networked systems and the information they include [1], aiming to ensure that the privacy of identity of organizations and individuals are saved. It also involves the confidentiality, availability and integrity (CAI) of data, which are necessary for the quality and safety of organizations and individuals. Typical cyber security methods are sets of techniques, Policy, countermeasures and safeguards taken and used to avoid or minify the risk of a cyber-attack to save Institutions, organizations and individuals from the intentional exploitation of their assets (i,e; systems, networks, data and applications). These set of techniques varies depending on procedure and measurements that are developed to keep systems, networks, data and applications safe from cyber threats.

Importance of cyber security

Information security occupies great interests in recent technologies and enterprises. These interests are growing rapidly to accommodate the tremendous technological advances that are taking place these days. Moreover, most studies and experiences had proved that controlling cyber risks in real time is a preferable move than resolving it in the next stage. Cyber-attacks affect badly starting from individuals ending, not endless, by countries and economics. According to the Data Breach Investigation in 2018, there were more than 53,000 cyber security crime and 2,216 successfully data breaches [2], it is obvious that cybercrime is still on the rise. The next subsections introduce a brief preview on the importance of cyber-security in different directions [3,4].

i. Information wars: Information has become wealth for countries such as petroleum and priceless metals as well as for the organizations and individuals, so the information wars became more prevalent and dominated by many developed countries that have seek to wage wars without blood and tears using information obtained and acquired by various means, This information is used as a weapon in economic wars between the organizations, and as a weapon to blackmail individuals, weaken them and humiliate.

ii. Simplicity is the peak of complexity: Since the harnessing of technology for human service and has been witnessing rapid development in order to facilitate human life led that to the concept of "simplicity is the peak of complexity" for this simplicity the technology has become a very complex and drove to the emergence of new vulnerabilities and increased opportunities for exposure to cyber-attacks.

iii. Huge data: The spread of technology in the finer details of our lives ‹force the organizations to deal with millions of digital transaction daily more than ever before, leading to a large number of stored data and give rise to gigantic data warehouses and the emergence of new data types and formats that would be less structured unlike ordinary data, in return more vulnerable and less protected.

iv. Cloud storage: Due to the weakness of the normal storage tools and huge data stored, this has always led to the dependence on cloud storage for its ease of use and data accessibility , so there can be a dangerous threat to the privacy and mismanagement of stored data.

v. Internet of Things IoT: Many devices are connected to the internet. These are known as Internet of Things, these devices are increasingly common in homes and offices, used to simplify and speed up tasks, as well as show better levels of control and accessibility. this proliferation cause a threat to the privacy of individuals who own them If not managed completely, every IoT device that is connected to the internet could lead to the formation of an army of sleepers used to destroy major economic markets. Expert guess there will be 27.1 billion connected devices globally by 2021, so this problem will only worsen with time.

vi. Spreading hacking tools: Since highly skilled hackers and well-funded pose a big risk, the less skilled individuals pose big risk also because of spreading hacking tools and programs on the internet for free led to their presence and there is also a growing threat because of them. The commercialization of cybercrime makes it easy for anyone to possess the tools they need to start an attack and cause damage, such as ransom ware and crypto-mining malware, or crypto-currency mining malware or simply crypto-jacking[5].

II. Cyber-security System Decomposition

Typical actions of Cyber security system are shown in Table 1. These components are considered the standard essential steps that must be followed by successful Cyber security system. A brief definition of these components as follows [6]:

A. *Analyze:*

Analyze and identify potential risk that surrounding the organization to know its nature, characteristics and methods of coping it, Identify information at risk and identify vulnerability in existing systems.

B. *Defend:*

Once the organization identifies and analyzes its cyber-security threats and identifies vulnerability in existing systems, it must set a cyber-security system appropriate to its security needs to address these internal and external cyber-security threats, and implement policies and procedures that defend sensitive information from unauthorized use.

C. *Detect:*

If a cyber-security system is built to fit the security needs of the organizations, it will be easy to detect breakthroughs and identify internal and external cyber-attacks, the time factor is very important for detecting security breaches so organizations will need to take on a set of advanced techniques and best practices to successfully detect cyber-attacks attempts.

D. *Revival* :

Once the process of detecting and defend of attacks ends, the process of reviving of systems that have been hacked begins. It aims to restore the system to its previous state and recover lost data, the process of the revival is a costly process of time and effort on the level of data restoration and system security updates in the absence of resilient recovery framework.

E. *Investigate:*

After detecting and defend against these cyber-attacks, organizations must investigate these attacks and know when the attack occurred and how? And who did this attack and what data he was able to reach?

The process of investigating cyber-attacks is an important component of any successful cyber security system and act as main pillar of the cyber security system, and organizations must be record these investigations to be used later and avoid falling into the same vulnerability, and developing the policies and practices used in the organization based on these investigations.

F. *Oversight and Development:*

The process of Oversight and Development is a permanent process in the cyber security system, which includes oversight of all online systems and activities, as well as people, and monitor all the alerts issued by intrusion detection system IDS and investigate these alerts and know the cause it, and also considers the development process is very important at the level of different systems in the organization and individuals, Systems should be up to date and have recent security updates and only use of original systems issued by a reliable source. for the process of development of individuals come through the development of security awareness and training them on various forms of cyber-attacks that target the organization through them and also try to raise the degree of loyalty to them.

TABLE I

Cyber-security components

Analyze	analyze and identify potential risk that surrounding the organization
Defend	set a cyber-security system appropriate to its security needs to address these internal and external cyber-security threats
Detect	detect breakthroughs and identify internal and external cyber attacks
Revival	reviving of systems that have been hacked and restore the system to the state and recover lost data
Oversight & development	oversight of all online systems and activities, as well as people, and monitor all the alerts issued by IDS, Systems development by get latest updates and have recent security updates and use of original systems, development of security awareness and training individuals on various forms of cyber attacks that target them

III. Cyber-security impact

Cyber-attacks are costly in terms of expense, the efforts, recovery time and reputation damage. Over the last two years, the cost of cybercrime increased rapidly by 23 percent more than last year and organizations have been lost, on average, US$11.7 million because of these cyber-attacks [7]. The impact of cyber-security can be divided into two parts as [8],[9]: its impact on individuals, and its impact on organizations.

The impact on individuals may occur in the form of ppenetrating personal accounts on social networking platforms and stealing personal information, hacking personal computers or smart phones and stolen data stored on it, The penetration of devices connected to the Internet in the home (IoT), resulting in: financial loss represented in stolen financial information such as credit card or other data, reputation damage as a result of extortion to steal personal information, causing psychological and physical pain as a result.

The impact on the organizations may be have many of images, the most common threat is social engineering, relying on weak security awareness among employees in organizations, which leads to: financial loss as a result of steal of organization information, steal of financial information (bank accounts details or credit card details), steal of money(via phantom transfers), Disable services (disability to perform transactions online), loss of new business contract, The cost of maintaining systems, networks and devices affected by the penetration, damage to the reputation of the Organization, which led to: loss existing or new customers, loss in the sales share due to the disruption of services, reduction in profits due to loss in the sales and customers, And legal consequences, which led to face fines and regulatory sanctions.

IV. Cyber Attacks

Cyber-attacks refer to attempts to deliberately violate by an anonymous person to cause damage to the organization for personal, financial or political reasons:

DoS/DDoS: DoS or DDoS attacks is an attempt to block and delay operations by exhausting victim resources using a huge flood of data packets sent sequentially using the millions of Internet-related devices called botnet, and it can be divided into three main categories[12] :

Volume-based attacks: - which includes ICMP floods and UDP floods or any of other spoofed packet attacks. The aim of this attack is too exhausting the bandwidth of the victim.

Protocol-based attacks: - which includes fragmented packet attacks, Smurf attack, SYN floods, Ping of death, The main aim of this attack is too exhausting actual server resources, such as memory or firewall.

Application layer based attack: - and it includes attacks like Zero-day attack, the aimed goal of the attack is to target Windows, open BSD or Apache vulnerabilities.

Cryptomining malware, or cryptocurrency mining malware or simply crypto jacking, is new term that refers to malicious software programs and malware designed to use the resources of the victim machine in the process of mining digital currencies such as Bitcoin without a user's permission, it also allowed website owners to set up Monero coin miners using a soft code of Javascript, This code run in the background of visitors' browsers, using CPU power to mining digital coins causing excess CPU power without the approval or awareness of the website users [5].

Ransomware is a rising threat which encrypts a user’s files and asks victim paid a ransom then can release the decryption key. This type of malware is in charge of for hundreds of millions of dollars in blackmail annually. but the worse is still, there is new developing variants, helping to evasion from many malware detection, antivirus and intrusion detection systems IDS[13].

V. Real Cyber Offense

In January 2003, the penetration of the safety control system at the nuclear power plant in Davis-Besse Ohio, to disable the plant and shut down for maintenance, and on the basis of reports issued by the administration of the plant, the penetration has done through the connection of a computer infected with Slammer worm that was connected via local network [10].

In 2010, Stuxnet worm exploited some weaknesses in the Microsoft Windows operating system, according to Symantec reports. Around 45,000 networks around the world have been infected so far. The Iranian government also confirmed that the Bushehr nuclear power plant in the country Was attacked by Stuxnet worm [10].

In 2019 using Phishing Email to target the National Bank of Malawi by adding worms payload to the PDF file and then send the file via e-mail address of one of the bank's branches in another area and when the reception branch receive the file and interact with it, the local network for the bank has been infected [11].

VI. Assessment Importance

Cyber-security assessment helps enterprises keep their systems and network up to date. Cyber-security assessments are very efficient for discovering and fixing issues within your enterprise’s network, systems, applications and policies. Furthermore, by reviewing policies, countermeasure, and standards to identify weaknesses in cyber-security, better cyber-security assessment prepares your enterprise against potential attacks and prevents breaches, reduce the impact of success breaches, and keep your enterprise reputation from damage.

VII. Assessment Methods

Usually, vulnerability assessment is considered as an only method of cyber-security assessment, while there are a number of other methods that are no less important than evaluating the vulnerability that is used to assess the performance of the cyber-security system in the enterprise. In this paper, nine methods will be identified to assess cyber security:

1. Vulnerability assessment method.
2. Network assessment method.
3. Virus detection assessment method.
4. Authentication assessment method.
5. Penetration testing assessment method.
6. Human assessment method.
7. Hardware threats assessment method.
8. Policy & countermeasure assessment method.
9. Natural threats assessment method.

VIII. CYBER SECURITY ASSESSMENT METHODS

Nowadays increasingly, the latest research is focusing on cyber-security issues and its challenge in modern enterprises, however, research in this area is still at an early phase, a cyber-security assessment is important to check and examine the integrity of networks and associated systems. orderly testing and scanning of network security controls help ensure that vulnerabilities, miss updates and misconfigurations are identified and classify to minify the probability of system attacks.

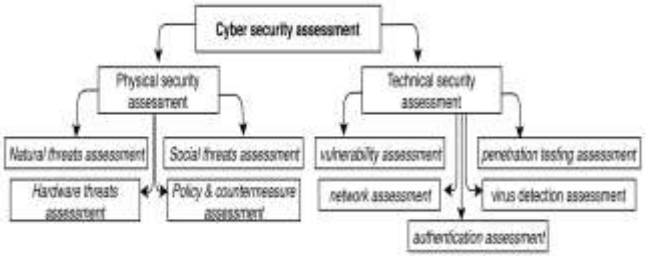

Cyber security assessment
Physical security assessment
Technical security assessment
Natural threats assessment
Social threats assessment
vulnerability assessment
penetration testing assessment
Hardware threats assessment
Policy & countermeasure assessment
network assessment
virus detection assessment
authentication assessment

Fig. 1 Cyber-security assessment

Typical assessment methods of Cyber security system are shown in figure 1 can be divided to two groups depending on the nature of the security risks, a-Technical security assessment methods which include five methods 1.vulnerability assessment, 2.network assessment, 3. penetration testing assessment, 4.authentication assessment and 5.virus detection assessment and the second group is b-Physical security assessment methods which include four methods, 1. Social threats assessment method, 2.Hardware threats assessment method, 3.Policy & countermeasure assessment method and 4.Natural threats assessment method.

A. Technical security assessment:

1) *Vulnerability assessment*

Vulnerability assessment is an examination of the potential points that can be used in attack on a system or network by identifying out-of-date software versions, identifies open ports in operating systems, and applications that run on network, it used to detects system weaknesses in networks, applications and communications devices and measure the performance of cybersecurity system applied, However, vulnerability scanners also use predefined huge databases of vulnerabilities[14] to detect deficiencies and potential reduction for those deficiencies. Vulnerability scans are also used by attackers seeking system holes to enter the network[15].

1.1. Vulnerability classification:

i. Policy and Procedure vulnerabilities[15]: policies and procedures are a set of rules, principles, and guidelines which formulated by an organization in order to maintain the internal order of the organization, and must be adhered to by all within the boundaries of the organization.

ii. Hardware vulnerability[16]: Vulnerability resulting from the lack of the equipment in an isolated or protected area of physical access to it, use of non-genuine parts and not of a reliable source, and providing physical protection for sensitive and critical systems, such as data centers, Supervisory control and data acquisition (SCADA) ,process control and safety systems, monitoring systems.

iii. Software vulnerability [16]: These include vulnerability caused by non-use of genuine programs from trusted sources, use erroneous settings, lack of recent updates special security updates, lack of training of personnel, erroneous use, installation of updates without testing, lack of backups.

iv. 4-Data vulnerability[16]: Vulnerability resulting from data access to unauthorized persons through hacking or intruding, non-use of data encryption, or data corruption with no alternative versions, Lack of interest in backups regularly and periodically, theft of backup tapes or damage due to retention in an inappropriate climate.

1.2. Vulnerability groups:

There are more vulnerabilities databases that contain more than 18,000 vulnerability so far, and these lists increase by 25 new vulnerabilities every week, If we try to classify this vulnerability into groups we will get more than 25 sets as it shown in table 2[17].

TABLE II
VULNERABILITIES DATABASES [17]

Malware	Brute Force Attack	CGI scripts	DATABASE
E-COMMERCE	FILE TRANSFER	PROTOCOL	FINGER
GENERAL REMOTE SERVICES	HARDWARE	INFORMATION (NiS, YP, WHOIS)	INFORMATION GATHERING
NEWS SERVER	TCP/IP	WEB SERVER	Network File System
WINDOWS	PROXY	Remote Procedure Call	SMB/NETBIOS
DNS AND BIND	FIREWALL	Simple Network Management Protocol	MAIL SERVICES

1.3. Vulnerability Scanning Tools:

Vulnerability scanners help IT staff in a modern enterprise to identify weaknesses inside its network, such as open ports that could be exploited by users that not having official permission or approval, and applications that are missing the latest security updates, it helps to make sure that the network follows the policy used in the organization.

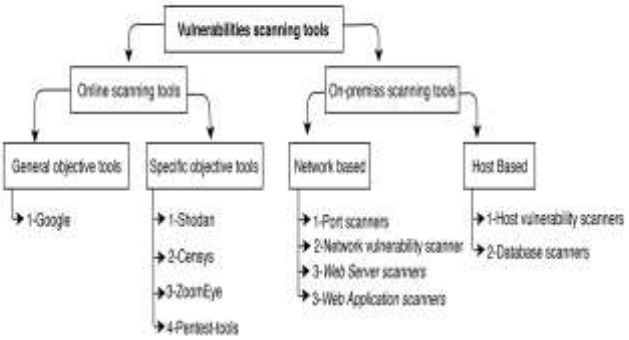


Fig. 2 Vulnerabilities scanning tools

There are two types of vulnerability scanners are shown in figure 2. Online scanning tools which able to retrieve vulnerabilities that are exposed public and can be exploited by hackers and On-premises scanning tools that monitoring network traffic. Both types of vulnerability scanner complete each other's capabilities and can work together within a network, to get the best possible result, Vulnerabilities scanning tools can be considered as search engines that demand for specific information about a specific thing, Vulnerabilities scanning tools can classified into two categories: Online scanning tools and On-premises scanning tools.

first group classified into two categories: general objective and Specific objective. The first group exemplified by Google which works based on specific queries that can be text, image, audio or special queries (i.e site: target.com filetype:xls username password email). the second group do the scanning for a specific objective, such as hosted services, open ports, SSL/TLS vulnerabilities or specific protocol vulnerabilities, such as SQL injection or XSS (Cross Site Scripting).

1.3.1. Online scanning tools:

it can be grouped to i. Specific objective tools which contain i. a - Shodan, i.b- Censys, i.c-ZoomEye, i.d-Pentest-tools and ii.General objective tools which contain ii.a- google

1.3.1.1. Specific objective tools

for the first group they are important tools that are used when conducting a vulnerabilities assessment or penetration testing, and the most common ones (such as Shodan, Pentest-tools, Censys and Zoomeye) which share their data online for the public.

i. Shodan is a search engine that was founded in 2009 by John Matherley, an engine that scans open ports for any devices connected to internet and IOT such as home access controls, refrigerators, webcams, Smart TVs, smart grids and modern enterprises. It scans for devices that connected to the internet and are publicly accessible through the web[18]. it is available as an online service which tries to gather information about IP addresses, by scanning it, tries to identify the services are under execution and which port are used, and generate report about the services, status, ports, headers and metadata, This information is shared online for the public[19], example of online webcam search result as it showed in figure 3 [18].

Fig. 3 shodan scanning result[18]

Shodan scanning process checks if target port is open with TCP SYN scan, if is open, it extract target's banner string which includes details such as name and version of the service, operating system, according to Shodan official web site, there are 41 known ports are scanned from distributed servers around the world and extract each banner separately and saved in the database [18]. Shodan advantages and disadvantages are shown in table 3.

TABLE III
SHODAN ADVANTAGES AND DISADVANTAGES[18]

advantages	disadvantages
Easy to use, simple search query	Paid and not free
Provide its data through API, and support API for developer	The source code is not available for participation and modification by the public
Generate downloaded report in different format like JSON, CSV or XML	Dissemination of information gained for the public and presents weaknesses and Vulnerabilities discovered, which leads to misuse
Support search by map	No fresh data
Technical support	Not support IPv6
Have enterprise platform for enterprises	Scan only devices that connected directly to network
Support RSS feed	the search results can be used by hackers to demand this information and use it for malicious works.
It can scan 41 ports	No Automatically scan

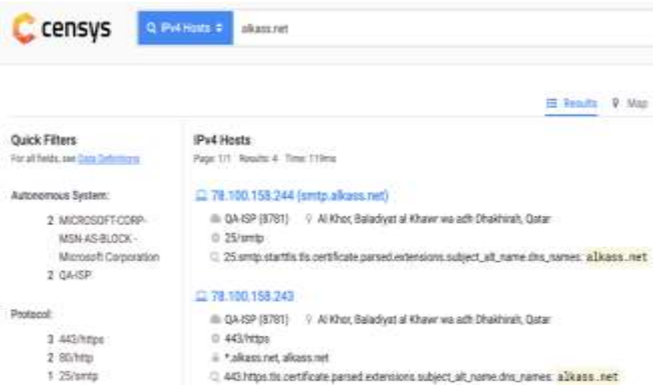
ii. Censys: It is an IP Search Engine, like Shodan, that is used to scan and gather information about connected devices on the internet and details services and open ports[20].

Censys have updated databases that contain information on the devices that are scanned on the Internet and the services, open ports that are exposed by connected devices.

Censys is similar to Shodan in the scan and data collection process both are used Banner grab using Zgrab and the SYN Scan mechanism using Zmap, and gathering data on hosts and websites out of periodical and horizontal scan of the giving IPv4 address range using ping scan technique[21], that is used to recognize all taken IP addresses then report open ports, services running on the scanned addresses.

What distinguishes Censys from others is that it is capable of checking the following protocols: HTTPS, HTTP, POP3(S), FTP, HTTP, Proxies, SSSH, Modbus, SMTP(S), IMAP(S), CWMP, StartTLS, Heartbleed and SSLv3 [21] using Zgrab banner grabber tool.

As it shown in figure 4 Censys is able to retrieve the description of the connected devices that scanned, and technical details, services provider, service owner, Contact Information, hackers used it to obtain goals based on their weaknesses and are ranked according to the weaknesses and the date of the scanned, its data are saved and accessible through API.



censys

alkass.net

Quick Filters
For all fields, see Data Definitions

Autonomous System:
2 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation
2 QA-ISP

Protocol:
3 443/https
2 80/http
1 25/smtp

IPv4 Hosts
Page: 1/1 Results: 4 Time: 119ms

78.100.158.244 (smtp.alkass.net)
QA-ISP (8781) Al Khor, Baladiyat al Khawr wa adh Dhakhirah, Qatar
25/smtp
25.smtp.starttls.tls.certificate.parsed.extensions.subject_alt_name.dns_names: alkass.net

78.100.158.243
QA-ISP (8781) Al Khor, Baladiyat al Khawr wa adh Dhakhirah, Qatar
443/https
*.alkass.net, alkass.net
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: alkass.net

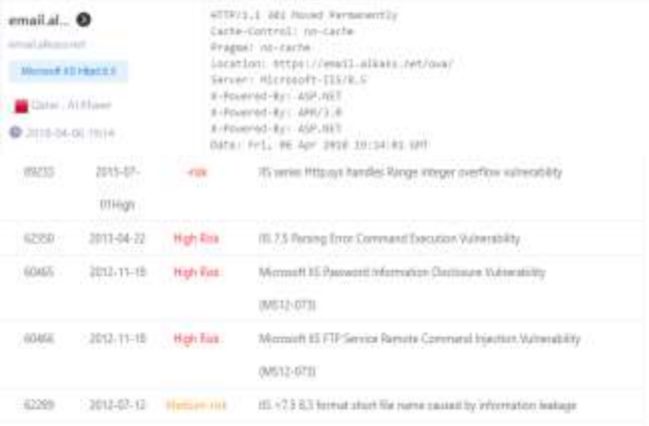
Fig. 4 censys scanning result [20]

Censys is built on three main tools, i. ZMap The Fast Internet Scanner, is a network scanning tool for scanning the entire network (or large scale). It is able to scan the entire public IPv4 address space in less than one hour with a 10gigE connection[22]. ii. ZGrab is application-layer scanner tool for a banner grabber, written in Go programming language and supports HTTPS, HTTP, SSH, FTP, Telnet, SMTP, POP3, IMAP, Modbus, Siemens S7, BACNET, and Tridium, it can execute a TLS connection and gather HTTP page of all hosts which founded on ZMap on TCP/443 port[22]. iii. ZTag is a tool used to processes the ZGrab output and writes raw scan data with metadata that are grabbed such as device information and vulnerabilities and protocol handshakes information to more descriptive data[22]. censys advantages and disadvantages are shown in table 4 [20] [21].

TABLE IV
CENSYS ADVANTAGES AND DISADVANTAGES[20,21]

advantages	disadvantages
Easy to use	Paid and not free
Provide its data through API	The source code is not available for participation and modification by the public
Provide contact information about service provider	Dissemination of information gained for the public and presents weaknesses and Vulnerabilities discovered, which leads to misuse
Have data filtering	No fresh data
Passive scan	Not support IPv6
Technical support	Scan only devices that connected directly to network
It can scan 35 ports	use external tools for vulnerability analysis
Automatically scan scheduled	the search results can be used by hackers to demand this information and use it for malicious works.

iii. ZoomEye is a search engine for Internet space, it works to scan Internet related devices and scan open ports and services on which it operates, It relies on two of the most powerful tools, Xmap and Wmap that targeting devices and websites in the cyberspace and work to detect vulnerability and open ports, as it showed in its report in figure 5.



email.al...
email.alkass.net
Microsoft IIS httpd 8.5
Qatar , Al Khawr
2018-04-06 19:14

```
HTTP/1.1 301 Moved Permanently
Cache-Control: no-cache
Pragma: no-cache
Location: https://email.alkass.net/owa/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Powered-By: ASP.NET
Date: Fri, 06 Apr 2018 10:14:01 GMT
```

89235 2015-07-01High risk IIS series Http.sys handles Range integer overflow vulnerability
62959 2013-04-22 High Risk IIS 7.5 Parsing Error Command Execution Vulnerability
60465 2012-11-15 High Risk Microsoft IIS Password Information Disclosure Vulnerability (MS12-073)
60466 2012-11-15 High Risk Microsoft IIS FTP Service Remote Command Injection Vulnerability (MS12-073)
62299 2012-07-12 Medium risk IIS <7.5 8.3 format short file name caused by information leakage

Fig. 5 ZoomEye scanning result [23]

ZoomEye is able to be used to discover all the services and devices through continuous scan all the time, It analyzes the acquired information and converts it to reports that enable researchers and information seeking to understand the vulnerabilities discovered, ZoomEye is considered to be a hacker tool but is designed for security and research purposes[23]. zoomeye advantages and disadvantages are shown in table 5[23].

TABLE V
ZOOMEYE ADVANTAGES AND DISADVANTAGES[23]

advantages	disadvantages
Easy to use, simple search query	Advanced data are paid in enterprise platform
Basic data are free	Manual scan
Provide its data through API, and support API for developer	No periodical scan
Generate downloaded report in different format like JSON, CSV or XML	
Generate chart report	
Search based on text query with advanced parameter	

iv. Pentest-tools is an online cyber security and vulnerability assessment platform, provide utilities and tools that can be used to test and assess the security of the modern enterprise's infrastructure such as servers, applications and network, generating assessment report containing vulnerabilities, Network failure and recommendations for fixing them.

Pentest-tools contain a set of classifications each containing a vast set of tools that are used to conduct the test and most of these tools rely mainly on Google dorks queries and other Linux tools, such as:

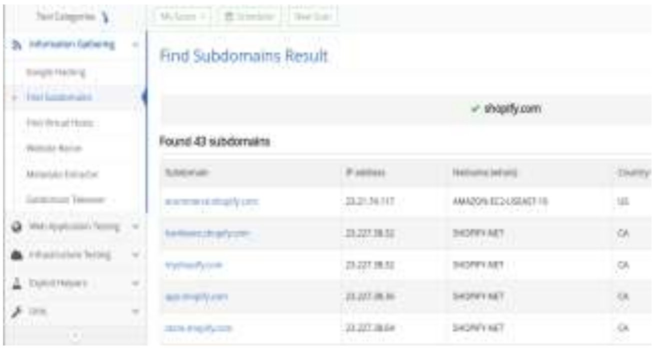
1. an information-gathering group that is contained:

A. Find Subdomains Responsible for detecting all the services associated with the specified Domain as shown in figure 6.

B. Find Virtual Hosts “vhosts” is a web server configured to hold multiple websites at the same time, with different domain names [26].

C. Website Recon is the process of getting the largest amount of information available about the target, and it is the first stage of the penetration test, Website Recon tool employ Wappalyzer tool as a scanning engine, which can identify more than 900 web technologies from over 50 categories using a vast database of web signatures[26].

D. Subdomain Takeover is a type of vulnerability which appears when using a DNS CNAME entry for subdomains refers to a foreign service (like. Heroku, Bitbucket, Github, Shopify, Desk, Squarespace). the attacker could use the foreign service and expose the linked subdomain[26].



Find Subdomains Result

✓ shopify.com

Found 43 subdomains

Fig. 6 pentest Find Subdomains sample report [26]

E. Google hacking “Google Dorks”, Google search engine has a set of special queries “Google Dorks” that can be used to obtain motivating information about the target, the tool combines all useful and common queries used in one place.

2. Web Application Testing the second group from pentest-tools which contain:

A. SQL Injection (SQLi) Is one of the most known web application vulnerabilities yet, it occurs when the application allows users to input unvalidated text that may be executed on a database, the Toole is building on top of OWASP ZAP, which is one of the most popular security tools[26].

here is an example URL which retrieves the type and version of MySQL database that is running by using the SQL Injection vulnerability and execute this query: http://vulnapp.example.com/travel.jsp?id=x' UNION SELECT NULL, NULL, @@version -- '

B. XSS Scan Cross-Site Scripting (XSS) is a type of injection, and consider as one of the most known web application vulnerabilities yet, it occurs when the application allows users to input un-validated text 'malicious scripts' that may be executed on a web application, the Toole is building on top of OWASP ZAP, which is one of the most popular security tools[26].

C. URL Fuzzer used to discovery resources that not accessible to the public (such as /backups, /source_code.zip, /index.php.old, /archive.tgz), The URL Fuzzer tool uses a vast custom wordlist which contains over 1000 names of known files and directories for obtain hidden files and directories, For each WORD in the list tool will create an HTTP request like: Base_URL/WORD/ or to Base_URL/WORD.EXT [26].

D. Web Server Scan tool used to obtain vulnerabilities which affect web applications like SQL injection, Directory Traversal, OS Command Injection, XSS, others and identifies specific web server configuration issues, tool it builds on top of Nikto Vulnerability Scanner it use updated signature database and each signature contains a set of request that obtains vulnerability[26].

E. CMS Tests try to scan CMS applications to obtain vulnerability, target server issues, by using a black box test approach which does varied tests to obtain weaknesses in the target website, it has different tools for performing scan on different CMS like:WordPress Scan, Drupal Scan, Joomla Scan, SharePoint Scan[26].

3. Infrastructure Testing the third group from pentest-tools which contain: A. Network Scan OpenVAS, B. TCP Port Scan, C. UDP Port Scan, D. Ping Sweep, E. DNS Zone Transfer, F. SSL Tests[26].

Table 6 shown advantages and disadvantages of online cyber security and vulnerability assessment platform, pentest [26].

TABLE VI
PENTEST ADVANTAGES AND DISADVANTAGES

advantages	disadvantages
combine a vast of open source tools	Complex for normal users
Using Google Dorks	paid
Provide its data through API	Manual scan
Multi category for each type of hack	No report available

Table 7 shows the comparison between common Specific objective tools [18,19, 20, 23, 26]:

TABLE VII
COMPARISON BETWEEN COMMON SPECIFIC OBJECTIVE TOOLS

-	Shodan	Censys	ZoomEye	pentest-tools
Platform	Web based search engine	Web based search engine	Web based search engine	Web based search engine
Pricing	Paid	Paid	Basic data are free and advanced data are paid	Paid
Scan methods	SYN Scan / Banner grab	SYN Scan / Banner grab	SYN Scan / Banner grab	Open source tools and google

TABLE VII
COMPARISON BETWEEN COMMON SPECIFIC OBJECTIVE TOOLS

-	Shodan	Censys	ZoomEye	pentest-tools
				dorks
Syn scan tool	none	Zmap	Xmap	Zmap/Xmap/OpenVS
banner scan tool	none	Zgrab	Wmap	none
scan range	Horizontal Scan	Horizontal Scan	Horizontal Scan	Horizontal Scan
Scanned ports	41 port target	35 port target	none	none
scan option	Manual search	automatic/scheduled search	Manual search	Manual search
API	Available but paid	Available two type free and paid	Available free	Available but paid
Reports	Generate downloaded report in different format	Have Report Builder	Chart report	Rwa data/ no downloaded report
Friendly	Easy to use	Easy to use	Easy to use	Complex
RSS feed	Available	none	none	none

1.3.1.2 General objective tools

which contain ii.a- google, ii.b- yahoo, ii.c- bing or any Search sites that can be used to obtain information about the target, whatever the information is simple it will be important and influential, and the most famous of this sites is Google search engine.

i. Google-hacking is a new hacking method used by hackers to gather information about targets and discover vulnerabilities on applications and get its error messages, discover the pages that contains credentials data or login fields, by using special queries “Google Dorks”. usually, this information include systems configuration data, source code files, username and password data, database information and services version. This method use Google engine to search for any information regarding targets in general, by using of advanced operators in the Google search text in order to obtain related information about the targets in the search results. The result may be include the version of services that are used, list of a vulnerable application or a specific file-type (like username and password, database config file, CGI scripts).

Special queries Syntax “Google Dorks”: are a queries that take advantage of advanced search features provided by the search engine to obtain sensitive information or discover list of systems vulnerability, Google allows users to search about keyword in specific web pages using special queries, let them to search about specific parts in web pages, This is useful when you have billions of web pages and need every chance to tight the search results. For example, a Special queries to locate all the pages that containing Login Portals:“inurl:/sap/bc/bsp” [24] the queries depend on three parts, the factor, the colon (:) and the demand keyword that be searched, three parts are wrote one string without spaces, Google engine recognize the pattern and use it to reduce the search result using provided information, as is shown in table 9 for most common google dorks factors. For example, using this search query, “intitle:index.of filetype:sql”[24] engine will search for the word ‘index.of’ in the title of a website ‘intitle:’ and will restrict the result to sql files ‘filetype:sql’ that have been indexed by engine.

Dorks classification[24]: Special queries “Google Dorks” can be divided into 14 categories based on the goal of query or data retrieved.

Table 8 shows a brief and number of dorks available for each category, 89.5% of the dorks are depended on banners and URL patterns in their query syntax as the classification show[25].

TABLE VIII
DORKS CLASSIFICATION[24]

Category	Brief	No	Query
Advisories and Vulnerabilities	queries that are able to retrieve vulnerable servers	215	inurl:"q=user/password"
Error Message	queries that retrieve the pages with errors messages	68	intitle:"CGIWrap Error"
Files containing juicy info	queries that retrieve valuable info	230	inurl:apspassword
Files containing passwords	queries that retrieve files have pass	135	filetype:txt 9 JunOS
Files containing usernames	queries that retrieve files contains	15	"username.xlsx" ext:xlsx

TABLE VIII
DORKS CLASSIFICATION[24]

Category	Brief	No	Query
	username or login info		
Footholds	queries that retrieve log files	21	inurl:/install/stringnames.txt
Pages containing login portals	This factor finds indexed pages that contains login fields.	232	inurl:/login.zul
Network or Vulnerabilities data	queries that retrieve pages which have vulnerability	59	inurl:/scripts/wgate
Sensitive Directories	queries that retrieve directories exposed online	61	inurl:"/irj/go/km/docs/"
Sensitive Online Shopping info	queries that retrieve online shops pages	9	inurl:shopdbtest.asp
Various Online Devices	queries that retrieve online devices that are connected to internet and have setup pages.	201	inurl:/setup.cgi@next_file=
Vulnerable Files	queries that retrieve sites that have vulnerable files	56	inurl:"simplenews/admin"
Vulnerable Servers	queries that retrieve servers have vulnerability	48	inurl:/proc/self/cwd
Web Server Detection	queries that detect web servers and database server	72	intitle: "Welcome to nginx!" + "Thank you for using nginx."

TABLE IX
COMMON GOOGLE DORK FACTORS[24]

Factor	Description	Example
site:	This factor used to limit the search for a specific website or domain.	site:alkass.com

TABLE VIII
DORKS CLASSIFICATION[24]

Category	Brief	No	Query
filety pe:	This factor is used to search for files of a particular type.		password filetype:sql
link:	This factor will search for pages that link to the demand URL.		link:www.alkass. net
cache:	This factor order to finds a copy of the page even if that page is not available		cache:testphp.vu lnweb.com
intitle :	This factor used for searching a string inside a page.		intitle:index.of
inurl:	This factor run the search in the given URI.		inurl:passwords.t xt

1.3.2. On-premises scanning tools

On-premises scanners can be classified into two groups of vulnerability scanners network-based scanners that work through the network, and host based scanners that work on the target itself[27], There are also another classification of vulnerability scanners used by some users: active scanners that are able to simulating cyber attacks and also have the ability to fixing weaknesses points in the network to avoid the risk of being exploited by hackers, and Passive scanners that monitoring network traffic[28], In the proposed paper we will use the first classification because it is more general and comprehensive in terms of use.

1.3.2.1. network-based scanners: often is installed and run on a single machine usually it is a server that scans other live systems on the network. It helps to discover dangerous vulnerabilities like misconfigurations systems, firewall, vulnerable web servers, non-updated software, and risks associated with system authentication inside the scanned network[27].

i. network-based scanners types: network-based scanner can be divided into four groups a. Port scanners, b. network vulnerability scanners, c. Web Server Scanners, d. Web Application Scanners.

A. Port scanners: is an application designed to obtain the open ports in network hosts, this process is done by sends client requests to a range of network nods and attempting to connect to predefined ports on a systems, there are many scanners tools used for discovering open ports, in proposed paper we will mention only common tools, *Nmap* and *superscan,* as shown in table 10.

TABLE X
PORT SCANNERS TOOLS[15,29]

-	Nmap “Network Mapper"	Superscan
Vendor	open source application	Foundstone (now McAfee)
Cost	free and open source application	Free
Platform	Linux, Windows and Mac	Windows

TABLE X
PORT SCANNERS TOOLS[15,29]

-	Nmap “Network Mapper"	Superscan
	OS	
Interface	command line terminal ‘CLI’	GUI
Mode	Active	Passive

B. Network vulnerability scanners: Network scanners are typically used to identify active hosts in a user-specified address range. Once active hosts have been identified, they are scanned for open ports, network services that are running on hosts, monitoring network device such as a human-machine interface (like fingerprint devices, access control devices) , printers, mobiles, switches, firewalls, IP Camera and routers, in proposed paper we will mention only common tools, Wireshark, Nessus and GFI, as shown in table 11.

TABLE XI
NETWORK VULNERABILITY SCANNERS TOOLS[15,29]

-	Wireshark	Nessus	GFI LanGuard
Vendor	open source application	Tenable	GFI
Cost	Free	Paid	Paid
Platform	multi-platform	multi-platform	Windows
Interface	GUI	GUI	GUI
Mode	Both	Both	Active

C. Web Server scanners: it will scan and assess servers for potential vulnerabilities that can be discovered and used by hackers to compromise and control a server, Examples of this vulnerabilities are Open ports, administrator accounts that improperly configured, anonymous access to private files and directories on server, CGI scripts, mis security updates, in proposed paper we will mention only common tools, Nikto, Wikto and HPWebInspect, as shown in table 12.

TABLE XII
WEB SERVER SCANNERS TOOLS[29]

-	Nikto	Wikto	HPWebInspect
Vendor	open source application	open source application	HP
Cost	Free	Free	Paid
Platform	multi-platform	Windows	Windows
Interface	CLI	GUI	GUI
Mode	Both	Both	Passive

D. Web Application scanners: It measures and evaluates the security levels used in web applications like Cross-Site Scripting (XSS), Broken Authentication and Session Management, Cross-Site Request Forgery (CSRF) and SQL injection that hosted on web servers, and noted that cannot do comprehensive security assessment on all security aspect of a scanned web application using web application scanners there are some aspect issue have to manual checking (like authentication, URL Obfuscation) would be needed in order to complete web applications security assessment, in proposed paper we will mention only common tools, skipfish, DirBuster, Paros proxy and Acunetix, as shown in table 13.

TABLE XIII
WEB APPLICATION SCANNERS TOOLS[29]

-	skipfish	DirBuster	Paros proxy	Acunetix
Vendor	Google	open source	open source	Acunetix
Cost	Free	Free	Free	Paid
Platform	multi-platform	multi-platform	multi-platform	multi-platform
Interface	CLI	GUI	GUI	GUI
Mode	Both	Passive	Passive	Both

1.3.2.2. host based scanners: often is installed and run on the host itself to be scanned, and has permission to access operating systems low-level files, such as specific services, application, registry files and configuration details. It can thus provide deep know into risky activities. It can also detect if the system has been compromised by track its effect, detect suspicious file names, unexpected system files or personal files ،unexpected program activity, and unexpected installed programs. Host-based scanners able also to do kernal system checks, So this advantage is outperformed by the host-based scanner for network-based scanners where they can access the low level of system scan files[27]. Host-based scanner can divide into two groups 1. Host vulnerability scanners, 2. Database vulnerability scanners.

A. Host vulnerability scanners:

It scans the installed system to detect potential vulnerabilities, It can examine the system files itself, the programs installed on it, observe the programs suspicious activities, check user activities and trace the hackers' traces on the compromised system. There are many tools that can do this, in the proposed paper we will mention only common tools, Microsoft Baseline Security Analyser (MBSA) and OpenVS, as shown in Table 14.

TABLE XIV
HOST VULNERABILITY SCANNERS [29]

-	MBSA	OpenVS
Vendor	Microsoft	open source
Cost	Free	Free
Platform	Windows	multi-platform
Interface	GUI	GUI

B. Database vulnerability scanners:

A database scanner is a type of a host-based vulnerability scanner, It executes full security scan of database systems, and can discover any potential s vulnerability in database systems, such as mis-configurations, mis-updates, missing patches, weak passwords and Trojan horses, in proposed paper we will mention only common tools, *Scuba Database Vulnerability Scanner, as shown in table 15.*

TABLE XV
DATABASE VULNERABILITY SCANNERS [30]

-	Scuba
Vendor	Imperva
Cost	Free
Platform	multi-platform
Interface	GUI

2) ***Network assessment:***

Network assessment is the second method of cyber security assessment and measuring, Network assessment is an expression that refers to several things in the context of the network. It could include the analysis of network devices to discover which devices are old, not updated, out of support. It could also include the assessment of network performance, check of network architecture, review a security of network (configuration, access points, bugs, vulnerabilities), network assessment term also could be used to find what network devices are work on the network, it also includes applications, PCs, servers and operating systems assessment, networks assessment can be divided into three groups: 1. Assessment of network infrastructure, 2. Assessment of network performance and availability, 3. Assessment of network security.

2.1. Network assessment groups:

2.1.1. Assessment of network infrastructure:

Evaluation of the infrastructure, consisting of an inventory of the devices used in the network, the old devices, the devices that are out of support and others that lack the latest updates or miss-configuration, the design of the routing protocol, Windows ADS, auditing the authentication system used in the Wi-Fi points, monitor the equipment temperature during the day, The data obtained from the inspection process for the infrastructure must be analyzed to identify potential issues in the current infrastructure of the network and to record all information about the equipment working in the network.

2.1.2. Assessment of network performance and availability:

Measuring the performance of traffic running in the network and record peak time of traffic and compare the amount of traffic consumed in relation to the activities executed by the network and measuring the network response time, errors that may affect the performance of the network and availability.

2.1.3. Assessment of network security:

A Network Security Assessment is an evaluation that is prepared to identify vulnerabilities that could cause damage to business or potential attack on modern enterprises, or disclosure of critical information, it can appears in several forms and are always use different technology to disguise to escape from intrusion detection system, such as viruses, backdoors, trojans, and applications, it can be classified into three groups. External vulnerabilities, internal vulnerabilities, and social vulnerabilities, so network security has to be top seniority for all modern enterprises and security assessments have to be done regularly.

2.2. Network Assessments methods:

2.2.1. Log review and analysis:

Log review and analysis include auditing different system logs in order to discover anomaly about security policy[15]. network log review is important for some of the reasons. First of all, to discover an attack and identify the harm caused, it can be done by analyzing the network log events. By reviewing and analyzing network logs, you can know what happens within your network, network log file have much valuable information that can help to discover an attack and identify the harm caused, by proper analysis for network log you can discover intrusion attempts, errors, alerts, misconfigured devices, by proper analysis for network log, you can easily catch what is worrying and easily to handle it. It is very important to analyze the log to know the original cause, to get useful data from log and make analysis efficient, you have to collect and merge log data across all the systems, and get together events from numerous devices in real-time within the network, the most common network log review and analysis tools are Sguil tools is open source and support multi-platforms and GUI, SolarWinds Log & Event Manager is paid and support multi-platforms and GUI.

2.2.2. Vulnerability scan:

Identifying weaknesses in the network that can lead to potential risks, discussed in section 1.

2.2.3. Penetration testing:

also called ethical hacking, is the process of testing networks, computer systems or web application to find vulnerabilities and use it to attack, the process includes gathering information about the target, identifying possible vulnerabilities points, attempting to use it then reporting the result, it will be discussed in section 3.

***2.3.* Network *Assessments* tools:**

Network scanners are designed and hired to implement volume automated network scanning of predefined IP ranges to discover vulnerable components inside the scanned network. The most common network scanners are Nmap, Nessus, Retina Network Security Scanner and Acunetix.

2.3.1. **Nmap "Network Mapper"** is a port scanner tool used to scan vast networks, is able to perform analysis of ICMP, TCP, and UDP low-level. Nmap performs scanning with multi techniques, and have some advanced features such as IP fingerprinting, stealth scanning, service protocol fingerprinting, network packet sniffing and network traffic filter analysis[29].

2.3.2. **Nessus:** Nessus is a network vulnerability scanning package that able to perform vast automated scanning and assessment perform for a target network, Nessus has the ability to scan ICMP, TCP, and UDP, scan of specific services in the network such as Microsoft IIS, MySQL, Apache, Oracle and many others[29].

2.3.3. **Retina Network Security Scanner tool** is a vulnerability scanner implemented and designed by Beyond Trust's company, it provides security patch for Microsoft, Firefox, and Adobe applications and have the ability to assess the risk based on best network performance, network component and Operating System, It is a paid tool which requires a Windows server that provides security patches for IPs, the scanning process is done based on permission provided by the user and also generate the report based on user preference and allows the user to choose the way of report delivery[31].

2.3.4. **Acunetix:** is a paid tool, implemented and designed for a comprehensive network security scanner and a fully automated scanning tool that able to detects more than 50,000 vulnerabilities and misconfigurations and reports them, It able to detect open ports and discover running services, have the ability to assesses security of routers, switches and load balancers servers, poor configured Proxy Servers, apply tests for passwords, DNS zone transfer and TLS/SSL ciphers[32].

3) ***Virus*** **detection assessment**

Virus detection is the third method of cyber security assessment and measuring, viruses detection involves using software to detect viruses, spyware ،worms, back-doors, Trojan horses, rootkits , keystroke loggers or any tool that works to disclose information to unauthorized persons or cause damage or harm to the systems, because modern enterprises are becoming more and more dealing with IP networks and most of its transactions have become online, and, thus, have become a target for cyber attacks, It is, therefore, necessary for the modern enterprises to pay attention to the virus detectors and the interest in evaluating their performance and updating periodically.

3.1. **Virus detection groups:**

Virus detection can be divided into two groups depending on the method of installation, a- Network-based detector and b- Host-based detector, Both of them have advantages and disadvantages[15].

3.1.1. Network-based detector:

Network-based detector generally installed on a remote server in the network[15], detecting virus before it access the network by analyzing network traffic for detect virus communications when it using network traffic to communicate with attackers, carry stolen information, control victim machine, and propagation from device to other in the network. all of these actions can be observed at the network easily by the network-based detector and can provide definitive evidence of virus infection rather than scanning a user's PC directly[33]. In general, Network-based detectors enjoy the following advantages[33]: A. Network-based detectors are not sensitive to the modern methods used in viruses that use to bypass host-based detectors systems, because the network-based detector needs only to monitor communication protocols that are difficult to modify and it is embedded to network and invisible to attackers and viruses. B. Network-based detectors do not affect the performance of the user's machine, because it is usually installed on a remote server. C. Always up to the date of the latest threats, because it is managed only by the service provider, not the end user.

3.1.2. Host-based detector:

Host-based virus detectors software is usually installed on end users systems and able to detect malicious code in files, applications, removable media and documents for the local host. Host-based virus detectors does not affect the performance of the network, but it does significantly affect the performance of the system installed on it[15], In general, Host-based virus detectors enjoy the following advantages[33]: A. able to detect malicious code on end-user system, B. does not affect the performance of the network, C. able to automatically update the database of signatures.

3.2. **Virus detection Methods:**

There are many methods available and used to detect viruses based on different points of view, such as a- signature based methods and b- heuristic based methods.

3.2.1. signature based Methods: Signature-based methods is the most methods used to detect virus nowadays in both host-based detectors and network-based detectors, A signature is a predefined pattern of bytes that are stored in database to be used to distinguish between malicious code and positive one[34], or analyzes network traffic to look for a suspect traffic pattern and used as a signature which known to be related with virus command and control activity[33], Signature databases are developed and created in labs by analyzes samples of malware[33], detectors based on signature methods are fast, simple and effective against many common viruses. One of the disadvantages of signature-based methods is that it always requires an up to date signature database, new viruses, if not added to the signature database, will not be discovered, Also, viruses that use new techniques such as obfuscation will not be detected [35].

3.2.2. heuristic based Methods: Heuristic based methods has some other names like behaviour based or anomaly based detection, this methods observe and focuses on the actions done by the software during execution to discover whether it is malicious software or not[35], In detectors that are build on heuristic-based methods, It consists of two stages, the training phase where the detector observes and analyzes the behaviour of the harmful program and benign, and then in the second stage is the test phase the detector classifies the program to Harmful or benign based on the actions carried out by the program based on the patterns that trained the detector in the training phase[35], The power of detectors that are built on heuristic-based methods is the ability to detect harmful programs that are unable to detect by detectors that are built on signature-based methods, but on the other hand, the disadvantages of detectors that are build on heuristic-based methods the time and performance required to conduct a scan and it gives a significant positive false rate PFR [34].

3.3. **Virus detection Tools:**

There are two types of virus detectors, some of which are based on the network and the other depends on the host and both have free tools and another commercial, but the most effective now are commercial tools because of its full support and continuous updating of the signature databases, as well as most of the commercial tools are built on both methods followed In the discovery of viruses, signature-based methods and heuristic based methods, the following table 17 is the most important tool used to detect viruses[36]:

TABLE XVII
VIRUS DETECTION TOOLS [36]

-	Bitdefender +	Norton	Avira	Trend Micro
Vendor	Bitdefender	Symantec	Avira	Trend Micro
Cost	Paid	Paid	Free/Paid	Paid
Platform	multi-platform	multi-platform	multi-platform	multi-platform
Interface	GUI, Ease of use	GUI	GUI	GUI
performance	10/10	10/10	8.5/10	8/10
Signature / Heuristic	Both	Both	Both	Both

4) **Authentication assessment:**

Authentication refers to the identification of a user's identity based on a set of characteristics such as something owned by the user or something he knows or something that distinguishes him. The Authentication process also consists of a set of methods that are determined based on the level of protection required. Evaluation of authentication is also a very important method of measuring and assessment methods of cyber-security for modern enterprises because it is one of the most methods used in the authentication of the system, as it is more common to hacked by hackers due to the lack of evaluation by the user and modern enterprises.

4.1. Authentication types:

Authentication process can be divided into three types 1. Proof of Knowledge, 2. Proof of Possession, 3. Proof of Characteristics[37].

4.1.1. Proof of Knowledge: refers to something user know, it may be any authentication that consists of information that the user knows only, such as PIN "a personal identification number", a user name and password or a secret question.

4.1.2- Proof of Possession: refers to something user have, it may be any authentication based on something the user own, such as mobile phone, smartcards, tokens numbers, ID license, driver's license.

4.1.3. Proof of Characteristics: refers to something that is characteristic of the user, it may be any authentication that consist of physiologically or behaviorally information that distinguishes the user , such as fingerprints templates, hand geometry read, length and weight, face recognition, iris recognition, retina recognition, DNA analysis, voice recognition, signature patterns.

4.2. Authentication methods:

Authentication methods are the way of using different types of authentication according to the required security protection system, which is divided into two methods according to the factors used, 1. single factor, and 2. multi factors[37].

4.2.1. Single factor: is a process of using one factor from authentication types for user identification such as user name and password, smartcards or fingerprints templates.

4.2.2. multi-factors: Multi factors authentication are consists of using more than one factor of authentication types, two or more factors are employed with each other in the process of authentication, which would raise the level of protection above the level available when using single-factor authentication, such as user name and password with smartcards or fingerprints templates.

4.3. Authentication assessment tools:

Most authentication methods depend on the user name and password as a basic factor of authentication, whether using single-factor authentication or Multi factors authentication, so more cyber attacks on the authentication process target user name and password factor, so modern enterprises should always be measuring and assessment the authentication process, especially that one using single-factor authentication, Following table 18 shown the most popular authentication assessment tools that can be used:

TABLE XVIII
AUTHENTICATION ASSESSMENT TOOLS [15]

-	Aircrack	Brutus	Cain and Abel	John Ripper	THC Hydra
Vendor	Open source	-	Open source	Open source	Open source
Cost	Free	Free	Free	Free	Free
Platform	multi-platform	Windows	Windows	Multi-platform	Multi-platform
Interface	CLI	GUI	GUI	CLI	CLI/ GUI
Mode	Both	Active	Both	Active	Active

5) **Penetration testing assessment**

Is a simulated actual cyber-attack on target systems, to test the effectiveness and stability of systems in the face of such real cyber-attacks, and to detect vulnerabilities that can be exploited by attackers, this process can be called ethical hacking because it is based on a prior authorization of the target in order to measure and assess the performance of cyber-security in the enterprise, the penetration test process can be classified into five types, 1. Network Penetration Test, 2. Web Application Penetration Testing, 3. Wireless Penetration Test, 4. Social Engineering Penetration Test, 5. Client-Side Penetration Test, and three methods to conduct the test, based on the information authorized for the tester during the agreement on the testing process[38], 1. black box testing, 2. white box testing, 3. gray box testing , but in this research, we will develop nine methods depending on four parameters to carry out the test based on the nature of the penetration test, such as 1. Knowledge of penetration test, 2. location of penetration test, 3. executor of penetration test, 4. precognition of penetration test, whatever the type of the penetration test process, it is consists of six stages, start with Planning and Preparation for the penetration test and terminate with preparing a comprehensive report of the results of the process of penetration test.

5.1. penetration test types:

a penetration test can be classified into five types based on the area of the test, 1. Network Penetration Test: This type of penetration testing is a common and basic penetration test and is aims to detect gaps and discover vulnerabilities in the infrastructure of networks under the test. 2. Web Application Penetration Testing: Since this penetration test, check the endpoints of all web applications that a user may have to interact with regularly, so he needs careful planning and time investment. Also, as threats from Web applications increase, the ways they test are constantly evolving. 3. Wireless Penetration Test: This penetration test is designed to analyze wireless devices that deployed on the enterprise's sites, which includes items such as laptops, tablets, notebooks, smartphones, IOT devices. the penetration test have to attend tests for the protocols that used to configure Wireless, this will help to discover weakness areas, check access points for wireless, this will help to identify points that break access rights and expose the vulnerability. Typically, these tests should be performed at the end of the system test. 4. Social Engineering Penetration Test: This type of test consider as an important part of penetration testing and falls under the category of physical security assessment that we will discuss in the next section. This type of test is designed for examination of the Human Network of the enterprise. This penetration test mimic attacks which the employees of an enterprise could attempt to breach. However, it can be divided into two subcategories, 4.1. Remote Tests: it aims to trick an employee to stolen sensitive information using electronic methods. The penetration executor can perform such an attack via a phishing email. 4.2. Physical Tests: This type of test demand direct communication with the employee to get sensitive information. It might involve human handling technic like Imitation, Intimidation, Dumpster Diving or convince the employee via phone calls. 5. Client-Side Penetration Test: these tests aim to discover security threats on users local workstations. such as a flaw and bugs in a software applications that running on the user’s workstation which can be exploit easily by hackers like web browsers (Chrome, Firefox, Safari, IE, Opera), Putty, Sniffers, Git clients, MS PowerPoint, Photoshop, Adobe flash player, media players, third-party software, and OSS (open source software). Therefore, these in house developed applications must pass through the penetration test.

5.2. penetration test methods:

The penetration test can be performed using one of these methods based on the factors which determined based on the nature of the penetration test, such as 1. Knowledge of penetration test, 2. location of penetration test, 3. executor of penetration test, 4. precognition of penetration test.

5.2.1- Knowledge of penetration test:

this factor depends on how much information can be shared with the test executor for use in the penetration test process and can be divided into three methods, 1. black box testing: in this method of penetration testing, the penetration executor has no information about the system architecture that is under the test. so, the black box penetration test method is a simulation for an actual cyber attack on target systems. This means that the penetration executor will try to discover all possible vulnerabilities, and all potential system gaps are used to expose the system, one of black box testing disadvantage is very expensive for fund and time, it is also the possibility to cause disruption of service and damage to systems during the testing process[38]. 2. white box testing: this method of testing is the opposite of a black box test, the penetration executor has detailed information about the systems that are under the test, this information may be network architecture, the operating system running, and maybe applications source code, This method of penetration tests are often used with new systems or new modifications that are being used. So, these method of penetration tests are routinely proceeding, as a result, they are the best way to identify system vulnerabilities without excessive cost or time, but one of disadvantage is the penetration executor is not so much interested with a simulated actual cyber-attack on target systems that are under the assessment [38]. 3. gray box testing: this method of a penetration test is a mix of black and white box testing method, the executor will own limited information about the systems under the test, such as operating systems are running, network architecture. The purpose of this type of penetration test is often to verify the security elements in the system[38].

5.2.2- location of penetration test:

The location of execution of the penetration test, this factor affects the result of the test, it can be divided into two methods, 1. External penetration test method: it performs the penetration test from the outside the enterprise and this type of test simulates actual external cyber-attacks, and 2. Internal penetration test method: it performs the penetration test from inside the enterprise and this method is similar to the white box testing method, when the information about the system under the test will be available when compared to an external penetration test method.

5.2.3- executor of penetration test:

A test executor is one of the methods to choose between them. When choosing the method for conducting the penetration test, it can be divided into two methods: 1. In-house executor: It is usually from a member of the security staff at the enterprise. This method is very appropriate when there is no budget to conduct the test, As well as the fear of spreading vulnerability available to other individuals, but one of its disadvantages is that it can't simulate actual cyber-attacks, because it will be aware of all information about the system under the test, and this type of penetration test is similar to the White Box testing method. 2. Third party executor: enterprises often hire third-party company to execute these tests, this is called to a third party penetration testing, and it can simulate actual external cyber-attacks, but on the other side, it will be spreading vulnerability available to other individuals outside, as it will be expensive in time and cost.

5.2.4- precognition of penetration test:

precognition is one of the methods of penetration testing. It can be divided into two types: 1. blind: which is to provide very limited information to the test executor, such as information that is available to the public like the name of the enterprise and its website, and notified the concerned parties of the implementation of the test, in this type of test often hire a third party to execute the penetration test, 2. double-blind: In this method, the enterprise's IT and security crew are not notified beforehand and they are blind to the penetration testing, in this method can exam the enterprise's security monitoring, rules, policy and response procedures and countermeasure, in this method only a few people in the enterprise are made aware of the penetration testing. often it's only the project manager who carefully watches the whole process to ensure that the testing procedures performed correctly.

5.3. penetration test Stages:

The penetration test consists of a set of stages to be followed in order to obtain a successful test and obtain satisfactory results. These include the following

5.3.1. Planning and reconnaissance: In this stage, the test executor gathers as much information about the target as possible. this information can be target website, domain details, IP addresses, mail servers any information even if it is simple. This stage is considered one of the most time-consuming stages when using a black box testing, but this will help with further stages of the penetration test.

5.3.2**. Scanning:** This is the stage where the test executor will deal with the target with an aim to discover the vulnerabilities, gaps. the test executor will send different requests to the target and records the target response to various inputs. This request can be sent to the network with different tools, to identify open FTP portals, services that are running, open share drives, and much more. or use these requests with the web application, to identify libraries and logic implemented, code comments or the vulnerable functions like injection, remote code execution, cross-site scripting.

5.3.3**. Gaining access:** Once the vulnerabilities and gaps have been discovered and identified in the previous stage, the next stage is to exploit these vulnerabilities and gaps to gain access to the target.

5.3.4**. Maintaining access:** once the test executor gaining access to the target systems and sneak into the network, the next stage will be the most important, maintenance of this access and keep it, to ensure that the access is persistence. This is important to ensure that the access is available even if the system is modified, rebooted or reset**.**

5.3.5**. Exploitation:** after gaining access to target systems and maintain this access, start with the next stage where the actual data breaches are done. the test executor will try to compromise the system, get the data, launch dos attacks, start with another type of penetration test from inside the network. Usually, this stage is very dangerous so should be controlled and monitored to ensure that the damage on the network is limited.

5.3.6. Evidence collection and report generation: Once most of the stages of the penetration test are done, the final stage is to collect the flags, the evidence of the exploited and explain the vulnerabilities, gaps discovered and report it to the target management for review and action.

5.4. penetration test tools:

Each stage of the penetration requires a set of tools that help the penetration test executor to complete the stage, each tool differs from the other in the method used and results, and is selected based on the type and method of penetration, but there are machines designed specifically to penetration test, these machines "designed to destroy", It contains a wide range of tools that serve each stage of the penetration. The following table 19 shown the most common of these machines:

TABLE XIX
PENETRATION TEST TOOLS[15,38]

-	Kali Linux	Metasploit
Vendor	Rapid7	Rapid7
Cost	Free	Paid
Platform	Linux	Linux, Windows
Interface	Both	Both
Mode	Both	Both

B. **Physical security assessment**

Physical security is the second method of cybersecurity for modern enterprises, and it is no different from technical security in terms of importance. However, most of the research in cyberspace security ignores physical security and focuses only on technical security. In this proposed research, we will discuss physical security and its components. Physical security is the security of assets, networks, hardware, data and personnel from unauthorized actions that might cause breach or damage to an enterprise or lead to cyber-attack. Physical security includes protection from natural disasters such as fire, flood, it can be divided into four items 1-social threats assessment, 2-hardware threats assessment, 3-policy and countermeasures assessment, 4-natural threat assessment.

1) **Social threats assessment**

Social means our daily lives actions which include both personal and professional actions, and social threats mean risks that can occur as a result of our social daily dealings, Social threat is also called “Hacking the Human” or Social engineering, is the way to obtain information and break security procedures through tricking other people and exploitation of human vulnerability [39].

1.1. Social engineering phases:

Social attacks are different from each other and in the way they are implemented, but most of them consist of four phases, 1. Information gathering phase, 2. Confidence-building phase 3. Exploitation phase, 4. Implementation phase [40].

1.1.1. **Information gathering phase**: In this phase, tries to obtain information about the target from several resources and ways, such as social network, dumpster diving, website, observation, physical interactions, and so on.

1.1.2. **Confidence building phase:** In this phase, tries to build the relationship with the target by trying to start a conversation or another way using the information you gathered about the target at the previous phase**.**

1.1.3. Exploitation phase: In this phase use the relationship that was built in the previous phase in order to get the information required to move to the next phase. 4-Implementation phase: This phase is the last phase in which the attack is carried out and the goal is achieved[40].

1.2. Social engineering types:

Social attacks can be divided into two types depending on the way in which they are carried out,

1.2.1. human-based social attacks: In this type of attacks, the hacker interacts directly with the target and tries to extract the information required directly by using some of the skills associated with this method, such as using social network sites, deception, intimidation, etc. Often the targets in this type are very limited.

1.2.2. technical based social attacks: In this type of attack, it is done by the help of technical ways which used to trick the target such as phishing email, fake social networking sites, counterfeit advertisements, in this type the targets are too many and on a wide scale and often target the human force in the enterprises[40].

1.3. Social engineering methods[40]:

There are methods of social attacks followed by attackers to carry out this type of attack. These are four methods:

1.3.1. physical method: Is one of the methods used by the attacker to collect information about the target, such as dumpster diving, which is the way of inspection in the garbage in order to obtain some information or papers or other uses in the composition of information about the target, and also observation of the target and know his daily events. **1.3.2. technical method:** This method depends on the Internet in a large way where the use of search engines as well as social networking sites and there are also some programs that help in this, such as Moltego, one of the most famous tools used in this area.

1.3.3. Social method: A social method is the most important method of social engineering attacks. Depending on the development of the relationship between the attacker and the target through, the use of some psychological techniques such as persuasion to manipulate their targets like the use of purported authority. Or uses the most successful psychological techniques of curiosity, like, used in the phishing email. But most social attacks are performed by phone and be quite successful.

1.3.4. socio-technical method: This method combines the former techniques but contains an innovative technique, the gift, where the attacker distributes storage devices containing a Trojan horse as a kind of gifts or propaganda for the product to the victims, and always does the process near the real target so that it can be manipulated and convinced.

2) **hardware threats assessment:**

hardware threat is any breach of data resulting from the potential risk of physical access to information technology hardware, such as improper use of the hardware by users, the theft or cyber-attacks, and the threat of hardware can be divided into two sections:

2.1. hardware threats classification:

2.1.1. User threat: This section includes the risks caused by the user to hardware such as misuse which leads to the infiltration of intruders to the network and data breaches, or the use of external storage devices such as hard disks, CD, DVD or flash drive, which leads to infection with viruses, which in turn lead to data breaches, as well as the use of non-original parts, which may be infected with viruses in advance, or adversely affect the performance of the device, , as well as leaking sensitive information through the user himself through the phone camera or screen capture.

2.1.2. Access threat: This section represents the risks caused by unauthorized access to IT hardware. This can result in hardware theft, or hacking, through a re-operation of a password using password reset tools or the spread of a Trojan virus on the hardware, which leads to a data breach.

2.2. Countermeasures for protection from hardware threats:

Hardware threats can cause significant damage to your data whether this damage is caused by external sources such as theft or unauthorized access, or from internal sources such as improper use or use of non-genuine parts. Here are some actions you can take to protect your data from hardware threats: 2.2.1. make sure to install computers in safe places. 2.2.2. Close and use the device ports with permission. 2.2.3. the use of surveillance cameras. 2.2.4. Review computer events periodically. 2.2.5. Scheduled maintenance regularly. 2.2.6. Use original parts. 2.2.7. Training employees on the optimal use of computers.

3) **Policy & countermeasure assessment:**

information security policy and countermeasures are law and a constitution that governs IT transactions in enterprises, written and agreed on by IT, management and legal, to outlining things like passwords, employee access controls, physical access controls, network security, mobile device management, server security, risk management practices, data security, data backup and recovery, disaster recovery Plan, logs and event monitoring.

The modern enterprises must develop information security policy and countermeasures consistent with their objectives and business goals[41], information security policy and countermeasures assessment are conducted fundamentally to evaluate compliance to policy and mandatory standards[41].

3.1. Importance of IT security policies and countermeasures for Modern enterprises:

These days, with the constant change in business and technology and the adoption of most of the business on information technology, the resources of companies, whether small or large as the target of many of the hackers. Therefore, security policies and countermeasures are considered to be the methods of prevention that most companies that deal with technology should follow. They help them defend against potential violations or help restore the network and information if a breach occurs.

A security policy is necessary and important for any organization because it determines what to do if users misuse the network assets or if there is a cyber-attack on the network or a network outage due to a natural disaster.

3.2. Key elements of IT security policies and countermeasures for Modern enterprises:

There are a number of key elements that must be met in the information security policy, which should be reviewed when assessing the information security policy[42]:

3.2.1. Purpose of Policy Creation: Prior to the establishment of a security policy, the purpose and objective of such a policy should be defined, such as the need of development of a general approach to information security, the detection and elimination of information security flaws, such as misuse of data, networks, computer systems and applications, and keep enterprise assets from theft[42].

3.2.2. Scope of information security policy: The scope of policy should be defined, so it should treat all enterprise data, applications, systems, facilities, network infrastructure, users, IT staff and IT third parties without any exception[42].

3.2.3. Information security objectives: Usually the objectives of the policy of safety are represented in, Confidentiality – data and information assets should be confined to authorized users to access and not be disclosed to unauthorized users ‹Integrity – keeping the data complete, intact and accurate, as well as operational applications to ensure accuracy and integrity ‹Availability – Ensure that information is available and available at the time of the request[42].

3.2.4. Authority and Access Control Policy: Access to a company's network and servers, must be through unique logins that require an authentication process in the form of passwords, tokens, biometrics, IDs. Monitoring should be carried out on all systems, Login attempts successful ones and failures, the date and time of login and logout exactly[42].

3.2.5. Data classification: Data may have different values so they should be classified based on the confidentiality to be met. The data classification policy may sort the whole information set as follows: High-risk data, confidential data, public data[42].

3.2.6. Data support and operations: Organization of mechanisms of public order responsible for data protection and handlings such as data backup and data traffic[42].

3.2.7. Security Awareness: Sharing information security policies with employees is an important step. A training course will involve employees in a positive situation, towards information security policy, ensuring that they have an idea of existing procedures and mechanisms for data protection, for example, levels of confidentiality and data sensitivity issues. This awareness training should address a wide range of critical topics: how to collect data, process data, delete data, manage records, maintain data quality, privacy, confidentiality, appropriate use of IT systems, use of appropriate social networks and cyber-attacks[42].

3.3. assessment method of Information security policies and countermeasures for Modern enterprises:

Information security policy and countermeasures assessments are important to maintain enterprises security assurance from cyber-attacks and multiple risks in Cyberspace. There are many tools and methods used to evaluate security policies and countermeasures, The most popular of these methods is auditing lists [41].

3.3.1. Auditing lists: Auditing lists method of information security policy and countermeasures assessment include reviewing policy component, security techniques and controls with auditing lists provided by security best practices and security standards. The checklists define the criteria that will be used for evaluation of the security characteristics of systems and IT products ‹it may also include the internal controls, The auditing lists method is usually utilized for high-level security audit for purposes of obtaining certification[41].

4) Natural threats assessment:

Natural threats that can threaten the security and privacy of information and information technology devices, such as floods, earthquakes or thunderstorms, these natural threats can lead to fires, high temperatures and even electric shocks to IT devices, causing potential physical damage and loss of data. , Natural threats are considered as unintended and unpredictable threats. However, they have a very significant impact on the security of information. Therefore, they must be taken into consideration during the assessment of information security, and while preparing security policies and countermeasures. Therefore, they are considered as elements of cybersecurity in the proposed research.

4.1. Countermeasures for protection from natural threats:

Natural threats can cause considerable damage to your data and information technology devices. Here are measures you can take to protect your data and information technology devices from natural threats:

4.1.1. Back up data: Backing up data include creating multiple copies of your data. threats like fire, floods and earthquakes can happen without caution. having a backup helps you to recover your data and systems in case of any loss happen, using an external hard drive, magnetic tape or use an online data backup site such as Cloud storage. This way, you can keep your data online. It should take into account the safety procedures during the backup process such as data encryption before copying to maintain the misuse, keeping them in separate locations away from the main site such as other buildings or cities, keeping them in a moderate climate and suitable to protect them from damage.

4.1.2. Install IT devices in secure locations: Install your information technology devices in a place where it is unlikely to be affected by natural factors. For example, avoid installing IT equipment in rooms exposed to dust or excessive moisture.

4.1.3. set up protective electrical devices: set up devices such as (UPS) an Uninterruptible Power Supply that can provide an alternative battery to IT devices in case of a power failure. Software damage can occur as a result of sudden power failure, spikes and surges on the power line, so the UPS device protects against such damage.

4.1.4. Isolate IT devices from fire: Isolate the IT devices from fire by placing them in fire retardant environment. In addition, you can set up an adequate fire safety system and procedures in order to quick damage control.

4.1.5. Ensure appropriate temperatures and humidity: You must Ensure proper temperature and humidity level to ensure the smooth operation of your IT devices. You can do this by setting up devices such as humidifiers and air conditioners.

IX. Challenges

Cybersecurity faces many challenges, which are constantly increasing with the tremendous technological progress we are witnessing. Among the most prevalent challenges in modern enterprises:

1. Human, The human element is the weakest part of the security chain in any modern enterprise. The success of cyber attacks is the result of the mistakes they make. The modern enterprises must pay special attention to staff training of specially trained non-technical staff in order to increase their security awareness and avoid the mistakes that cause security breaches.
2. Understand the importance of cybersecurity, The lack of understanding of management and individuals in the enterprises the importance of cybersecurity is one of the challenges to cybersecurity. The lack of awareness of the managers of the importance of cybersecurity leads to the lack of support for their systems of protection and update them continuously, creating gaps in it, and also the lack of awareness of the individuals of the importance of cybersecurity, which leads to serious mistakes that lead to security violations.
3. Big Data, The big data from the cybercrime challenges, enterprises want to extract value from those data, but the central nature of large data stores creates new security challenges; data must be guaranteed to be secure during the process of processing. So you should put the controls around the same data, you should also put controls around the applications and systems that store and process the data.
4. IoT, Internet-related home appliances pose a major challenge to cybersecurity but they lack the means to protect them, so they pose a serious threat to the privacy of individuals and the security of enterprises. These devices, known as Internet objects, represent an army of sleepers that can be misused to hit the most powerful systems in moments. There will be 27.1 billion connected devices globally by 2021, so this problem will get worse over time. Several recent cybersecurity conferences have revealed serious security flaws in the Internet of things. Some showed how self-driving cars can be hijacked, and how to controlled remotely medical devices, such as pacemakers. Although this is undoubtedly worrisome, which makes it even more shocking is how people pay attention to cybersecurity importance.
5. lack of appropriate cybersecurity skills, the lack of people with appropriate cybersecurity skills is one of the biggest challenges faced by cybersecurity. The gap between modern threats and current skills is increasing in such a way that these threats are difficult for enterprises.
6. Spreading hacking tools, Since highly skilled hackers and well funded pose a big risk, the less skilled individuals pose big risk also because of spreading hacking tools and programs on the internet for free led to their presence and there is also a growing threat because of them.
7. Keeping up with changing technologies, Not keeping pace with changing technology periodically is one of the most serious challenges faced by cyber-security.
8. Lack of budgets for cyber-security development, Failure to provide a special budget for the development of cyber-security leads to weak security systems in enterprises and lead to security breaches resulting from the development of security vulnerabilities by the hackers.
9. Security assessments on a regular basis, One of the most serious challenges that cyber-security faces are the lack of interest by enterprises and individuals to conduct security assessments on a regular basis, security assessment help enterprises keep their systems and network up to date. Security assessments are very efficient for discovering and fixing issues within your enterprise's network, systems, applications and policies. Furthermore, by reviewing policies, countermeasure, and standards to identify weaknesses in cyber-security, better security assessment prepares your enterprise against potential attacks and prevents breaches, reduce the impact of success breaches, and keep your enterprise reputation from damage.

X. Proposed solutions

The proposed solution presented in this research paper for the above challenges is to assess the performance of cybersecurity by dividing the security risks into two parts based on their nature and then developing methods to measure the effective cybersecurity system for each part:

1. *Technical security*: which represent the potential risks due to security gaps in systems which running In the enterprise, these technical risks are evaluated using five methods, 1.1. vulnerability assessment: Evaluation of vulnerability, by examining the gaps existing in all systems and applications and then fixing these gaps, 1.2. network assessment: Evaluation of the network, through the examination of the security of the network, and performance, and check the infrastructure of the network and identify the weaknesses in them and then solve these problems, 1.3. penetration testing assessment: The penetration test is a complete simulation of the hacking process carried out by hackers, but it is done by security experts and with prior permission. Its purpose is to determine the effectiveness and stability of the system against cyber attacks and identify and repair potential vulnerabilities. 1.4. authentication assessment: The authentication process is one of the most targeted operations by hackers, so evaluation is performed by testing the authentication factors and determining their

strength against potential attacks. 1.5. virus detection assessment: Virus detectors are used to avoid viruses that are deployed and used as a primary access point to the network, so the tool is identified according to security requirements. and the second part is an examination and assessment of the potential security risks of the surrounding physical elements

2. *Physical security* which can be assessed through four methods, 2.1. Social threats assessment method: It is an assessment of the weakest link in the security chain, which is the human element by conducting a set of tests like social engineering to identify their weaknesses that can be targeted by the hackers. 2.2. Hardware threats assessment method: Identify the potential risks arising from the physical elements of the computer and the network and identify the most important procedures to be followed to avoid such a type of risk. 2.3. Policy & countermeasure assessment method: Evaluate the efficiency and effectiveness of the policies and countermeasure of the organization and its conformity with international policies for information security. 2.4. Natural threats assessment method: Identify potential risks from disasters and natural factors and identify the most important actions to be taken to avoid such risks.

One of the best ways to prevent cyber-attacks is to increase the security awareness of cyber-security importance for individuals and the administration, and to train them in the simplest possible security measures to deal with potential risks which can be face in light of the tremendous technological progress that swept all daily transactions on the personal level and business.

XI. Conclusion

Security assessment methods can be considered as a standard used for measuring and assess an enterprise's security posture. Security assessment methods are essential to comprehensive network security, systems and data integrity. Without good Security assessment method, management cannot answer the common question today "Are you secured enough?", making appropriate decisions and identify the points to be developed and time, effort and money required to invest in information security development.

XII. Suggestions and future work

Measuring information security at enterprise is difficult. efficient measurement is important in order to prove compliance, improve efficiency and effectiveness of controls at the enterprise. This research provides a comprehensive set of variables that can be used to measure and evaluate the performance of information security in modern enterprises, in accordance with the security needs, and to ensure the safety, confidentiality, integrity and availability of data.

References

[1] J. L. Bayuk, J. Healey, P. Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss. "Cyber Security Policy Guidebook", First Edition. © 2012 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc)2012(.

[2] Verzon Data Breach Investigations Report https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf (2018)

[3] IoD Policy Report, Cyber Security Underpinning the digital economy,https://www.iod.com/Portals/0/PDFs/Campaigns%20and%20Reports/Digital%20and%20Technology/Cyber%20Security%20-Underpinning%20the%20digital%20economy.pdf?ver=2016-09-13-171033-407, (2016)

[4] R. Bronson, 4 Reasons Cybersecurity Is More Important Than Ever, https://www.techwell.com/techwell-insights/2018/12/4-reasons-cybersecurity-more-important-ever, (2018)

[5] Sucuri security provider, Cryptocurrency Mining Malware Trends & Threat Predictions, https://sucuri.net/documentation/Sucuri-eBook-Cryptomining-Malware.pdf (2018)

[6] Components of a Cyber Security Program at maricopa countyaz, USA, https://www.maricopa.gov/1948/Components-of-a-Cyber-Security-Program

[7] Accenture company, "COST OF CYBER CRIME STUDY" Ponemon Institute LLC Attn: Research Department, 2308 US 31 North Traverse City, Michigan 49629 USA, 1.800.887.3118, research@ponemon.org (2017).

[8] D. Worth, negative impacts from cyber-attacks, University of Kent,https://phys.org/news/2018-10-negative-impacts-cyber-attacks.html, (2018)

[9] M. Gerami, Impact of Cyber Threats on Business Profitability, ITU-ICT Faculty training on "Cybersecurity", Iran, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Impact%20of%20Cyber%20Threats%20on%20Business%20Profitability.pdf, (2018)

[10] Yang, Y., Littler, T., Sezer, S., McLaughlin, K., & Wang, H. F.. Impact of cyber-security issues on Smart Grid. 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (2011).

[11] Antiy CERT. Report on the Worm Stuxnet's Attack. Antiy Corp., Harbin, China. [Online]. Available: http://www.antiy.net/en/analysts/Report_On_the_Attacking_of_Worm_ Struxnet_by_antiy_labs.pdf . (2019).

[12] W. Bhaya, M. Ebady Manaa" Review Clustering Mechanisms of Distributed Denial of Service Attacks", Journal of Computer Science 10 (10): 2037-2046,ISSN: 1549-3636 (2014).

[13] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B.. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. IEEE 36th International Conference on Distributed Computing Systems (ICDCS). doi:10.1109/icdcs.2016.46 (2016).

[14] Databases of vulnerabilities generally include information from active vulnerability repositories, such as the United States Computer Emergency Readiness Team (US-CERT) (http://www.kb.cert.org/vuls/), or vendor advisories, such as BugTraq (http://www.securityfocus.com/archive/1).

[15] Cynthia K. Veitch, Susan Wade, and John T. Michalski, Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants, Sandia National Laboratories P.O. Box 5800 Albuquerque, New Mexico 87185 (2012)

[16] Kavita S.Kumavat, Ranjana P. Dahake, Dr.M.U.Kharat, Overview of Vulnerability Analysis, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 10,October (2013)

[17] K. Williams,Vulnerability list, VISTA Penetration Study Internet and inter-nal network security testing, Available at: http://www.internetbankingaudits.com/list_of_vulnerabilities.htm.

[18] John Matherly. Shodan official Website. hps://www.shodan.io/

[19] S. Lee, S. H. Shin, and B. h. Roh. Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning. In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN). 1048–1052. DOI:hp://dx.doi.org/10.1109/ICUFN.2017.7993960, (2017)

[20] Censys, official Website: https://www.censys.io/

[21] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. Alex Halderman." A Search Engine Backed by Internet-Wide Scanning" In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, New York, NY, USA, (2015).

[22] The Zmap Project, official Website https://zmap.io/

[23] zoomeye official Website. www.zoomeye.org

[24] Google Hacking Database (GHDB). [Online]. Available: https://www.exploit-db.com/google-hacking-database/

[25] Toffalini, F., Abbà, M., Carra, D., & Balzarotti, D. Google Dorks: Analysis, Creation, and New Defenses. Lecture Notes in Computer Science, 255–275.doi:10.1007/978-3-319-40667-1_13, (2016)

[26] pentest-tools official Website. https://pentest-tools.com

[27] Lee, N. M. Z., Ooi, S. Y., & Pang, Y. H.. Vulnerability Reports Consolidation for Network Scanners. Computational Science and Technology, 11–20.doi:10.1007/978-981-10-8276-4_2, (2018)

[28] N. JHALA Network Scanning and Vulnerability Assessment with Report Generation, CSE-INS,IT,Nirma University May 13, 2014 CSE Department CSE-INS,IT,Nirma University, (2014)

[29] Security tools https://sectools.org

[30] Imperva official Website www.imperva.com

[31] Retina Network Security Scanner official Website: https://www.beyondtrust.com/products/retina-network-security-scanner/

[32] Acunetix Network Security Scanner official Website: https://www.acunetix.com/

[33] Kindsight Security Labs, The Case for Network-based Malware Detection https://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9599-case-network-based-malware-detection.pdf, (2014)

[34] R. Sihwail, K. Omar, K. Akram Zainol Ariffin. A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysi, DOI: http://dx.doi.org/10.18517/ijaseit.8.4-2.6827, (2018).

[35] Damodaran, A., Troia, F. D., Visaggio, C. A., Austin, T. H., & Stamp, M. A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 13(1), 1–12. doi:10.1007/s11416-015-0261-z, (2015).

[36] Best Antivirus Software of 2019 https://www.toptenreviews.com/software/security/best-antivirus-software/

[37] D. P. Tshilombo , V. V. Gopala Rao, Two Way Authentication for Analytics as a Service in Cloud, ISSN (Online): 2581-5792, (2019)

[38] G.Johansen, L.Allen, T.Heriyanto, S.Ali, Kali Linux 2 Assuring Security by Penetration Testing, Copyright © 2016 Packt Publishing,(2016)

[39] R. Singh Patel, Kali Linux Social Engineering, Ref: 1171213,(2013)

[40] A.KOYUN, E.Al Janabi, Social Engineering Attacks, Journal of Multidisciplinary Engineering Science and Technology (JMEST) (2017)

[41] M. Corpuz, Enterprise Information Security Policy Assessment - An Extended Framework for Metrics Development Utilising the Goal-Question-Metric Approach, IS Institute, Queensland University of Technology, Brisbane, Queensland/4000, Australia, (2011).

[42] Key Elements of an Information Security Policy, https://resources.infosecinstitute.com/key-elements-information-security-policy/#gref , (2018).