

Assignment part 2

by Adam Spencer McGowan

FILE	3046_ADAM_SPENCER_MCGOWAN_ASSIGNMENT_PART_2_113613_2092207276.DOCX		
TIME SUBMITTED	28-MAY-2018 11:54PM (UTC+0100)	WORD COUNT	2939
SUBMISSION ID	90010329	CHARACTER COUNT	19727

Risks to security of a computer network

Student: Adam McGowan

Lecture: Tim Bashford

Table of Contents

Introduction	3
What are risks to security?	4
How do risks topple security?	4
Type of attacks:	4
Denial of Service	4
How to prevent?	5
Rogue DHCP Servers	6
How to prevent?	6
Packet sniffing.....	6
How to prevent?	7
Password cracking.....	7
Guessing:.....	7
Brute Force.....	7
What is a Hacker(s)?	8
How to prevent?	8
Crackers.....	9
Scams	9
How to prevent?	9
Type of security:.....	9
Antivirus	9
Conclusion.....	11
Fire sale	12
References	13

Introduction

The introduction is about how network security and computers get attacked and how to prevent and protect the network security and computers from falling into the attacks hands and prevent a user from being the victim of that attack. How to DDoS attack and how to prevent them, what are rogue DHCP and what to do if one discovered, how to prevent a sniffer from monitoring users data. This is also about how hackers and crackers and what those are and do, how to prevent them from happening and what damage does the hackers and crackers cause to network and computer system. Then to talk about the difference between the difference of protection and what can it do what it prevents.

What are risks to security?

Security risks are when a security is either breached or broken by a hacker, malware or out of date. The system has been compromised and that the security in the system has become useless to stop/prevent the attack. These attacks are called Cyber-attacks, these are carried out in order for many reasons such as: stealing data, challenge, and privacy, personal. "The Internet of Things (IoT) security breaches seem to affect businesses regularly with the proliferation of hackers stealing data" [1]. The reason of hackers stealing data can be many:

- To sell for currency
- To blackmail,
- To know the victim.

These three main points are common as these put number of people at risk of feeling violated from the breach of privacy. This is usually happens to high profile targets who work in the inner circle such as "Big Websites: AdultFriendFinder, Dropbox, MySpace, LinkedIn, Yahoo whom more than 2 billion usernames, passwords, and email addresses both professional and private, at risk" [2].

How do risks topple security?

Toppled security is when the security is wiped out or partly destroyed and that there are attacked from all directions that taken control of the servers, computers and console network. "Online gaming networks for Sony's PlayStation and Microsoft's Xbox consoles have gone offline in what hackers have said was a coordinated attack" [3]. The hackers that toppled security usually DDoS (distributed denial of service.) This is by flooding the network with loads of incoming messages by targeting a system to slow it down or crash it.

Type of attacks:

Denial of Service

Distributed denial of service attacks is when a hacker or a group of hacktivist target a network or company servers by flooding the entire network with messages or disrupting the traffic that is connected to the internet. "The cyber criminals using a number of mix volume of attacks on applications which is

difficult to detect the hackers getting into the network infrastructure such as firewalls and IPS" [4]. There are many other type of DDoS attacks:

- Volumetric Attacks
- TCP State-Exhaustion Attacks
- ICMP Flood
 - ICMP Flood is when a hacker takes it for either fun or personal by flooding its victim's server or computer by echoing. "The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets" [5].
- IP/ICMP Fragmentation
- BGP Hijacking
 - BGP Hijacking is when a hacker takes over a server or some IP address by corrupting the BGP. "Prefix hijacking, route hijacking or IP hijacking) is the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables maintained using the Border Gateway Protocol" [4].
- IPSEC Flood

How to prevent?

When it comes to DDoS attacks, they are almost impossible to fight back or get to stop. This is because these attacks can last for days or weeks and this depends on how long the attacker keeps doing it for. To prevent the attacks from happening and to protect the system from the attacks, is to have a good updated security along with a software the protects networks from DDoS.

There is a site called SiteLock, "SiteLock Website Security protects organizations against all types of DDoS threats—including the most sophisticated forms" [6]. SiteLock can protect a network from the largest DDoS attacks such as Layer7.

There is also another software that protects users from DDoS attacks called StackPath, this type of security gives the same type of protection as SiteLock does. StackPath has a layer of security that stops any floods that a DDoS causes the "layers of security that protect against SYN floods and UDP floods. When activated, our Web Application Firewall provides even more DDoS protection" [7].

Rogue DHCP Servers

A rogue DHCP Server is when an attacker plugs in its own DHCP Server into the network and takes or changes the IP Addresses from the other computers that are connected to that network, it also like the attacker can monitor other user's websites and spy on what the users are looking at. The attack can stop the user of other computers to connect to the internet and the attack can take the whole traffic for itself. "A rogue DHCP server on your network will interrupt the normal DHCP server and offer a new gateway and IP address to the requesting PC" [8].

How to prevent?

Rogue DHCP Server can be detected on the network if the user checks for an IP/MAC address that doesn't match up to the IP for the DHCP, there are a few ways to tell if there a Rogue DHCP server is being used, this can be done by using a software called Wireshark or can be done by looking through the commands by ipconfig/all and check the Original DHCP address and the IP's that are for the clients. If there an IP/MAC address that doesn't look right or doesn't match, then there another command to check for sure that is used called ARP-a this will locate the Rogue DHCP address that doesn't fit in well. Using Wireshark: "Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible" [9].

Packet sniffing

A packet sniffer is when a hacker uses to collect and steal data from another user. The hacker who is snooping on the network doesn't cause damage to the network but can encrypted control and gain access to a lot of sensitive materials that are flowing through the data. "The sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution" [10]. Packet Sniffing allows hackers to gain more access to anything that comes and goes from the network, the tool a free software and easy, this gives hackers a layback job to get what the hacker wants. The packet sniffer isn't just Ethernet only, it can also be wireless sniffing which is called Wi-Fi Sniffer. The Wi-Fi sniffer is just the same as Ethernet just the hacker is using wireless rather a cable. "Wireless sniffer tools, their ability to monitor, intercept, and decode data" [11].

How to prevent?

To prevent a user being a victim to a packet sniffer is to secure the network and all the data is by the following steps:

- Encrypted the sensitive data under a zip before sending them over networks
- Check if the site the user is on is trusted by with a signature of a lock symbol and says "secure" along in highlighted in green  this will show that it safe and encrypted.
- The user can use an Antivirus tool that always protects computers and networks from attacks. "Method as [antisniff](#), that scan networks to determine if any NICs are running in promiscuous mode. These detection tools since they act as an alarm of sorts, triggered by evidence of a sniffer" [12].

Password cracking

Password cracking is when a hacker cracks the victim's password and gains access to the account, network or computer. This is done either by a software or by a genius who used the top of its mind by studying the victim's personal life.

Guessing:

As sometimes a genius who cracks password by guessing is because the victim password isn't strong, it contains a birthday number, dates, victim's names and pets, etc... "Even with the advanced programs, algorithms, and techniques, the easiest way of cracking a user password is by using logic or try commonly used passwords" [13].

Brute Force

Brute Force is a software that is used to crack on passwords, this software tries all combinations for a password from a small weak password to a long effective password. "Even on modern hardware, with a password of 7 characters or larger" [13], this depends on the length of a password when the software is guessing. Brute Force software's are:

- John the Ripper – it combines cracking modes, "John is available for several different platforms which enables you to use the same cracker" [14].
- Rarcrack

- Oracle – Oracle password cracker is one of brute force ways of attacking victim's passwords. "The tool uses particular usernames and tries to combination it's tries every second" [15].

What is a Hacker(s)?

Hacker is a single person, or hacktivist is a group of hackers working together, these type are either expert or skilled. Each type of teams or individuals are different. A single hacker could be hacking for fun, challenge or to steal data. A team of hackers that work together hack for the same goal. There are three different type of hackers:

- White Hat Hacker
- Grey Hat Hacker
- Black Hat Hacker

A white hat hacker are usually the "Good Samaritan" who does hacking for purpose for a big pay check and challenge, also to help detect a security breach for companies that hire or asks for the white hat hackers help. But the white hat hacker are sometimes either grey or black hat hackers or were once one. "white hat hacker is a specialist who breaks into protected systems and networks to test the security and assist the problem" [16].

Black hat hackers are everybody's worse nightmares. These type of hackers doesn't just hack for fun or challenge, it mostly to steal data, sell on black market or destroy the data. "Not only black hat hackers seek to steal data, but also to modify or destroy data" [17]. The black hat hacker are also nicknamed "cracker" as the hacker usually crack passwords and network security by causing damage. Black hat hackers common targets are companies that hold sensitive data to financial this is how the hacker gets it's pay by either blackmail or sell it. "the hackers are malicious, tech-savvy, and dangerous online outlaws, who steal thousands of currency of network infrastructure damage for personal gain" [18].

How to prevent?

When a hacker hacks, it causes terrible loss of personal to loss of currency which is distressing to the victims as this causes either more currency to repair damaged computer/server to changing every details and pray that the hacker doesn't use this information against the victims. To protect against hackers is to scan the computer with a good anti virus installed, updated firewall and security, keep away from corrupted websites and emails from unknown figure and always keep an backup of hard disk. "A common security practice

when connected to a public Wi-Fi network use a VPN, encrypts all traffic, making it impossible for a hacker” [19].

Crackers

Just like a black hat hacker, a cracker is the same. Both parties do the same job in breaking the system and stealing the sensitive data. An individual that cracking a network or a computer system to gain access does heavy damage to the system or the whole computer/network, bringing it down to its knees. “A cracker performing cracking for malicious activities, profit or causes, sometimes break the network's security system deliberately” [20].

Scams

Scams or another name fraudster or phishing, a way to gain money from the victims, this is done by either a website pop up or a trojan horse ransomware that got passed the network security. Scams can be sent by emails out of the blues which might have a file/download/fake photo attached, waiting to attack the computer and steal data then hold it as a blackmail after the victim opens that file. This type of scam can sometimes be a family of another type of attack called ransomware. “when an attacker, masquerading as a trusted entity and tricks the victim into opening a file from email or text, to a malicious link the malware installs and causes damage to system” [21].

How to prevent?

To avoid scams is to take precaution on what emails has been send and who it is from. To check where it came from to also think before click on the email or website. Installing an anti-scam tool that protects users while browser the internet. “Anti-phishing toolbars quick checks on the sites that are visiting and compare them to list of list known phishing sites” [22].

Type of security:

Antivirus

There are a lot of antivirus protections that help to protect networks and computer systems from attacks.

- Norton Security
- Kaspersky
- McAfee
- Total AV

- Malwarebytes
- Avast

Some antivirus charges every year to keep the user protected from attacks, while some are free completely or semi free. The reason of antivirus is to keep a system or network safe and that data doesn't get destroyed or fall into the wrong hands. "Antivirus software's help protect computer against viruses, worms, Trojan horses, and other unwanted invaders" [23].

Conclusion

The network security on what type of attacks and how to prevent them from in theory, this is also about what happens when network security is under attack by a hacker or a malware attacks. The protection that the network or computer seeks to keep the system safe and to keep the users personal data and currency from falling into the wrong hands or destroyed. This was an difficult part to work out as there was a lot of information required to read and write out. To write out an assignment like this is to understand the information a lot deeper to get a clear idea.

Fire sale

A fire sale is an attack, a cyberwarfare which is either caused by a group of hacktivist, Cyber Terrorism, or another Government Military from another country attacks in cyberspace. A fire sale means "Everything MUST GO!" The fire sale is named out from each letter:

- F stand for Financial – Such as Collapses the Exchange, market prices, crash the Banks and ATM's
- I stand for Infrastructure – Cause transports to be closed and communications brought down and security disabled.
- R stand for Resources - Emergency services out of order, electric and gas and water shut off.
- E stand for Environment – Unlike resources, environment is about the background such as sewage, storm drains, such as dam controls which could also be disasters.

References

- [J. Feit, "Do Your IoT Devices Risk a Security Breach?," *Buildings*, vol. 111, no. 7, pp. 18-20,22, 1 2017.
]
- [C. staff, "Top celebrity online security screwups in 2016," XSS - CROSS SITE SECURITY, 13 2 December 2016. [Online]. Available: <https://www.csoonline.com/article/3150035/data-protection/top-celebrity-online-security-screwups-in-2016.html>. [Accessed 21 May 2018].
- ["Sony and Microsoft 'hack' brings down PlayStation and Xbox," *Made for minds.*, 26 December 3 2014. [Online]. Available: <http://www.dw.com/en/sony-and-microsoft-hack-brings-down-playstation-and-xbox/a-18152612>. [Accessed 22 May 2018].
- ["WHAT IS DDOS?," NETSCOUT, [Online]. Available: <https://www.netscout.com/what-is-ddos>. 4 [Accessed 22 May 2018].
]
- ["PING FLOOD (ICMP FLOOD)," IMPERVA INCAPSULA, [Online]. Available: 5 <https://www.incapsula.com/ddos/attack-glossary/ping-icmp-flood.html>. [Accessed 22 May 2018].
]
- ["SiteLock DDoS Protection," SiteLock, [Online]. Available: <https://www.sitelock.com/ddos-protection>. [Accessed 23 May 2018].
]
- ["Security Protection that's built in, not bolted on.," StackPath, [Online]. Available: 7 https://www.stackpath.com/security/?utm_campaign=DDoS%20Mitigation&utm_source=ppc&utm_medium=Google%20Paid%20Search&utm_content=DDoS&gclid=EAIaIQobChMlgZaoi_uW2wIVDZPtCh1tYwdGEAAAYAiAAEgl08PD_BwE#DDoS&ads_cmpid=882145813&ads_adid=45973073964&ads_matchtype=. [Accessed 23 May 2018].
- [R. Slosser, "How a Rogue DHCP Server Works," Plixer, 17 December 2014. [Online]. Available: 8 <https://www.plixer.com/blog/detect-network-threats/how-a-rogue-dhcp-server-works/>.
] [Accessed 23 May 2018].
- ["Chapter 1. Introduction," Wireshark, [Online]. Available: 9 https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs.
] [Accessed 23 May 2018].
- ["Sniffer," techopedia, [Online]. Available: <https://www.techopedia.com/definition/4113/sniffer>. 1 [Accessed 23 May 2018].
0
]
- [N. DuPaul, "WIRELESS SNIFFER: TOOLS, SOFTWARE TO DETECT PACKET OR NETWORK SNIFFERS," 1 VERACODE, [Online]. Available: <https://www.veracode.com/security/wireless-sniffer>. [Accessed 22 May 2018].

1
]

[M. Tanase, "Sniffers: What They Are and How to Protect Yourself," Symantec Connect , 26
1 February 2002. [Online]. Available: <https://www.symantec.com/connect/articles/sniffers-what-2-they-are-and-how-protect-yourself>. [Accessed 23 May 2018].

]

["Password Cracking," Mitchell Forensics Information Pass_crack, [Online]. Available:
1 http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html. [Accessed 23 May 2018].

3
]

["John the Ripper," KALI TOOLS, 18 February 2014. [Online]. Available:
1 <https://tools.kali.org/password-attacks/john>. [Accessed 23 May 2018].

4
]

["How to crack Oracle Passwords : 5 best tools," Online Hash Crack, [Online]. Available:
1 <https://www.onlinehashcrack.com/how-to-crack-oracle-passwords.php>. [Accessed 24 May 2018].

5
]

["White Hat Hacker," techopedia, [Online]. Available:
1 <https://www.techopedia.com/definition/10349/white-hat-hacker>. [Accessed 23 May 2018].

6
]

["Emerging Threats," Norton by Symantec, 2018. [Online]. Available:
1 <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-7-white-and-grey-hat-hackers.html>. [Accessed 23 May 2018].

]

["What is a Black Hat?," secpoint, [Online]. Available: <https://www.secpoint.com/what-is-a-black-1-hat.html>. [Accessed 23 May 2018].

8
]

["7 practical tips to keep yourself from getting hacked," Business Insider UK, 10 February 2016.
1 [Online]. Available: <http://uk.businessinsider.com/7-hacking-protection-steps-2016-9-2?r=US&IR=T/#a-vpn-doesnt-necessarily-mean-that-all-your-web-traffic-is-in-safe-hands-so-exercise-caution-6>. [Accessed 23 May 2018].

["Cracker," techopedia, [Online]. Available:
2 <https://www.techopedia.com/definition/10257/cracker>. [Accessed 23 May 2018].

0
]

["PHISHING ATTACKS," Imperva Incapsula, [Online]. Available: <https://www.incapsula.com/web-application-security/phishing-attack-scam.html>. [Accessed 24 May 2018].

1
]

["10 Ways To Avoid Phishing Scams," Phishing.org, [Online]. Available:
2 <http://www.phishing.org/10-ways-to-avoid-phishing-scams>. [Accessed 24 May 2018].

2
]

["Why do I need an antivirus software for my computer?," F-PROT, 2014. [Online]. Available:
2 http://www.f-prot.com/support/customer_service/15.html. [Accessed 25 May 2018].

3
]

Assignment part 2

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

50/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

GRADING FORM: SMU GENERIC_GJ

ADAM SPENCER MCGOWAN

50

RESEARCH-INFORMED LITERATURE

-  A good number of sources used, though not all of great academic credibility. Try to rely more on journal articles and less on web sources. Endeavour, also, to use far fewer quotes. Quotes should be used only in cases where the precise phrasing is important, it's always better to paraphrase when you can. **10**

KNOWLEDGE AND UNDERSTANDING

-  Good knowledge and understanding evidenced in the report. Some areas where you're very close to the correct information, but just slightly off. **19**

ANALYSIS

-  Some analysis, though limited synthesis of sources - try to get away from the "say one thing, cite one source" approach. Some conclusions drawn. **14**

PRACTICAL APPLICATION AND DEP.

-  N/A - no marks assigned to this section.

SKILLS FOR PROFESSIONAL PRAC.

-  Be sure to proof read your work carefully - there are quite a few errors. Several errant apostrophes. Document is fairly-well presented. **7**