

Network operating systems and security assignment 2

by Alexander Hall

FILE	2655_ALEXANDER_HALL_NETWORK_OPERATING_SYSTEMS_AND_SECURITY_ASSIGNMENT_2_113613_2051575469.DOCX		
TIME SUBMITTED	21-MAY-2018 03:48PM (UTC+0100)	WORD COUNT	2842
SUBMISSION ID	89667632	CHARACTER COUNT	16429



[2018]

Assignment Title: Security Measures Within Computer Network

Student Name: Alexander Hall

Student Number: P151746

Module Code: M2X8522

Module Lecturer: Dr Tim Bashford

Module Title: Network Operating Systems and Security

Table of Contents

Introduction	2
Background theories	2
Devices connected to a network.....	2
Security threats	2-4
Denial of services	3
Packet Sniffing.....	3
ARP Spoofing.....	3-4
Password Cracking	4
Recommendations/Data recovery	4-6
Data recovery-plan.....	4-5
Other Recommendations.....	5-6
Summary	6
References	6-7

Introduction

Within this essay there will be a detailed investigation into the many threats that could jeopardize the security of a computer network. Research will be carried out which will outline the descriptions of many different attacks that could occur, once these attacks have been identified and explained, recommendations will also be made on how each of the attacks can be eliminated or protected against, in extension there will also be a discussion on the recovery of data if or when a network has been compromised by any person or organization that means to harm a Computer network or computer system, this will be illustrated in the form of a data recovery plan.

Background theories

This section of the essay will be used to describe all the theories that are linked with the risks or threats that may affect the integrity of any given computer network, it will include the explanation of different computer network attacks and considerations of many devices that are connected to any given computer network.

Devices connected to a network

As by request of the assignment brief, the inclusion of the considerations of the devices connected to a network that could be potentially attacked during any of the attacks mentioned below, there are many devices that could be susceptible to networks attacks. Here are a few descriptions of the devices and their risk of being attacked: -

Personal Computer- peoples personal computers are highly vulnerable to hackers attacking mainly as there as usually a plethora of data to be stolen such as passwords, credit card details, details of their social networking accounts and other precious data such as documents they have created and photos, this can be done in many ways such as phishing emails(to gain information), purchase scamming or the owner of the computer unknowingly downloading infective software, the best way to solve any of these problems is to download anti-virus software that would pick up and eliminate any threats that the malware poses to the persons personal computer.[1]

USB-Sticks- USB's are not usually attacked by hackers, they are normally a clever way of infecting a large company, these attacks are usually called 'USB drop attacks' or lost and found USB attacks, this occurs when an attacker purposely places USB drives that are infected with malicious malware into the near vicinity of a large company with the sole purpose of infecting a company to either steal data or infect the companies computer system, an example of this was discussed in the book Seven Deadliest USB Attacks [2].

This type of attack can be devastating as an employee of a large company could pick up the infected drive thinking that it may be someone's personal USB flash drive, they may then insert it into their company computer to try and identify who the owner of the flash drive is, subsequently infecting the company's network with a malicious piece of software, this software may log all of the data and transfer it to the attacker's database, or after the data has been taken a ransom may be put on it, which would lead to a loss of the company's capital or lead to a loss of custom and revenue if the general public finds out about it.

Security threats

Below are a range of attacks that a computer network would be susceptible to, these attacks are usually concerned with the collection of a computer networks user's data as well as the halting of vital services for a computer user.

Denial of services

A denial of services(DoS) attack is an attack on the systems resources and is used so that a computer networking system is swamped or inundated with masses of many types of system requests that the network ceases to cope and then in turn leads to the network server becoming unresponsive.

Another method that the denial of services attack operates is that a substantial quantity of files could be sent to the systems storage causing there to be a lack in capacity in the systems storage[3].

This type of attack is implemented by the attacker installing the DoS software onto the victim's host computer/s, when this software is initiated it begins the barrage of communications against the computer to overwhelm it[3].The DoS can be broken down into a few types of attack these can include: -

Buffer overflow- This is used by the attacker to run modified code within the computer systems stack, they then send substantial amounts of data to the system stack, which means the processes controlled by the stack do not have a way of handling that amount of data, therefore the important processes cease to function[3] .

SYN Attack- A SYN attack is used during the processing of TCP(Transmission Control Protocol)/IP protocol authentication, the authentication process is normally carried out by two or more hosts sending and receiving SYN (Synchronise) packet messages and ACK (Acknowledge) packet messages, the bias of this attack is that the attacking host would transmit an immense amount of SYN packets to a target host, the target host would not be able to answer that many requests, in extension it would not be able to answer any genuine requests that it receives and so the target host would become inaccessible.[4]

Packet Sniffing

A Packet Sniffing attack utilizes software called sniffers, this software normally intercepts and then captures information that is sent as data 'packets' throughout a network, after the packets are captured by the attacker they are examined and analysed to figure out what types of data lie within them, the main reason this type of attack is carried out is to collect or steal a vast amount of data, attackers can also connect sniffers onto network routers through a WAP (wireless network point), this way a person trying to use the sniffer as an attack method can remotely and wirelessly be transferring the data back to the devices that are capturing the data to decrypt at a later date.[5]

There are many good tools that are used for both people who are trying to steal/analyse data maliciously and people who want to view the traffic through their own networks, here are two good examples used for windows products: -

Wireshark is probably the most popular tools made for windows to capture, decrypt and analyse the data going throughout a network, as well as the checking of protocols that are in a network.[6]

Smart Sniff is a free sniffing tool used for capturing and analysing TCP/IP packets that are going through a network's network adapter, the sniffing tool presents the data as communications between the networks clients and its server.[6]

ARP Spoofing

The ARP spoofing attack within a network is concerned with the spoofing or fooling of the Address Resolution Protocol (ARP) of a computer network, this type of attack is performed by an attacker that is attempting to steal data and involves the attacker intercepting and spoofing ARP messages going through the LAN (Local Area Connection).[7]

The attacker does this so that their MAC (media Access Control) address becomes linked with the network users IP (internet Protocol) address, this is done so that any data that is being sent through the Network users LAN can be gathered or stolen by the attacker, the data could also be modified before reaching the network user, in addition to the previous reasons the attacker could use the ARP spoofing attack to stop all traffic going into or coming out of the LAN.[7]

Furthermore, ARP spoofing can also be used to aid other types of attack including the previously explained DoS attacks, as well as man in the middle (MITM) network attacks.[7]

Password Cracking

Password Cracking is the act of cracking or deducing the password of a system to steal a person or company's personal data, there are a few methods of figuring out or 'cracking' a password, the main two that will be outlined will be brute forcing and social engineering, brute forcing is the act of attempting to solve a password by trying every combination of characters including letters, numbers and any symbol you can usually find on an everyday keyboard, brute forcing is carried out until a correct password is found, although this is an excellent method of solving a password it can be very time expensive as it may take months or years to crack a single password, this all depends on how many characters the password is consisted of and how many combinations are tested [8], here is a table showing how long it would take for a password to be cracked depending on different amounts of characters, being tested 10,000 times per second:-

Time to brute force password space, assuming 10,000 attempts per second			
	Lowercase (26 letters)	Uppercase, lowercase, digits (62 characters)	Uppercase, lowercase, digits, punctuation (94 characters)
Length = 5 characters	19 minutes	1 day	8 days
Length = 6 characters	8 hours	65 days	2 years
Length = 7 characters	9 days	11 years	200 years
Length = 8 characters	241 days	692 years	19,000 years
Length = 9 characters	17 years	42,000 years	1.8 million years

Table 1- table of how long it would take to brute force crack a password depending on amount of characters.[16]

The second method that could be used to crack a password is social engineering, social engineering is the act of obtaining information such as passwords by the attacker pretending to be someone they are not, they exploit this fact and usual techniques can include sending phishing emails or contacting a person by phone to gain information that could lead to the cracking of the password and in turn the person's valuable information[9].

Recommendations/Data recovery

In this section there will be recommendations about the procedures that can be used to combat the above-mentioned attacks on a given computer network, these recommendations will be followed by a data recovery plan.

Data recovery-plan

The data recovery plan displayed below is concerned with the data that may have been lost during an attack of the outlined attacks mentioned in the Security threats section of this essay, the plan will

contain techniques that could be put in place to minimise the amount of the user's data being lost, as well as the methods of recovering or restoring the data that may have been protected with the aforementioned techniques. Here is the data recovery plan: -

Where and how to back up Data?

Cloud Storage – Cloud storage is usually used as it is a very convenient way for large companies or the general public to backup many types of important data, cloud-based storage is used to keep copies of their data and is normally kept by a company who issues software or an online site that allows users to easily backup any of their data and when the data is given it is then managed by the company themselves generally within a cloud-based infrastructure [10].

If this is implemented correctly the data should be easy enough to restore if it is ever lost, the popular cloud based storage software includes Dropbox, Google Drive and Microsoft's OneDrive which for free will allow you to store between 5GB and 15GB [11].

RAID -RAID ((Redundant Array of Independent Disks) is a method within the area of data storage and the protection of personal data, the method consists of linking together either hard drives or SSD(solid state drives) to store any important data, the protection aspect being that depending on the number of RAID level (0,1,5,6,10 or any other combination of RAID levels), the numbers stand for a specific ways of splitting the data amongst a set of disks to either save an exact copy of the data or include the use of a parity piece of data to check the fault tolerance of the drive [12].

What data to back up?

There are many types of data that are important to a computer user such as their pictures, music, documents and accounts, there should also be considerations to what data a large company would need to back up, the data that a large company would need to be concerned with would be consumers accounts, sales, designs of products/services and any data connected to the workers of the company.

Other Recommendations

Protection against Password cracking attacks- The best way of protecting the personal data held on peoples accounts is to create a password that is strong, by that a strong password is a password that is unique and complex, do not write a Password down where it can be easily seen and change your password every 2-3 months, so that if an attacker was to be using any of the techniques mentioned above you have a new password before they have worked the old one out.[13]

Protections against DoS attacks include- A SYN DoS attack can be stopped by either employing a rule within the victim hosts firewall so that any connection messages that are pending on the host network are reset after specified timeout time, the SYN attack can also be thwarted using SYN cookies that would mean that when the victim host receives the mass of SYN messages, it replies with an SYN/ACK message, only when the victim host has the SYN/ACK response does it let the received host gain entry to its network.[4]

Protection against ARP Spoofing- ARP Spoofing can be protected against by using software to monitor the IP/MAC addresses and any ARP traffic of the network, there is software called arpwatch, this software records the IP/ MAC Addresses that are used within a network over a pre-determined amount of time, if it picks up any information that doesn't match the "usual" IP/MAC addresses within the systems ARP Table then it would send an alarm to the syslog of the network, this software is good for a singular device on the network, but if it is to be used for many devices, the software

must be downloaded onto every device on a switched network, this way the ARP spoofing attack can be picked up and dealt with.[14]

Saving Data from a Packet Sniffing attack- The best solution to make sure that important data cannot be stolen during data packet transfers is to encrypt the data using SSL(Secure Sockets Layer) or its successor TLS(Transport Layer Security) protocols, these protocols are put in place so that the data such as passwords or user data being sent is encrypted, so even if the data was to be stolen by an attacker they would not be able to understand what the information within the packets was and so it would be useless to them.[15]

Summary

Within this essay the area of network security has been spoken about and outlined within the essays sections were the descriptions of two low-level devices that may be affected by the attack of a given network system such as USB Flash drives or personal computers, also mentioned were the types of attacks that affect a networks security on many different levels some attacks mentioned were password cracking which is used to gain data or ARP spoofing which is used to intercept and log data meant for a designated computer system, this was followed up with recommendations and a data recovery plan which described valuable techniques used to thwart or minimise the many attacks on any given network's system.

References

- [1] R. A. Grimes, *Hacking the hacker : learn from the experts who take down hackers*. Indianapolis, IN: Wiley & Sons Inc, 2017.
- [2] B. (Brian J. Anderson and B. Anderson, "Brain Games," in *Seven Deadliest USB attacks*, Burlington: Syngress, 2010, pp. 178–179.
- [3] E. Cole, R. L. Krutz, and J. W. Conley, "Attacks and Threats," in *Network security bible*, 2nd ed., Indianapolis, IN: Wiley, 2009, pp. 129–130.
- [4] I. Dubrawsky, "General Security Concepts: Attacks," in *How to cheat at securing your network*, Burlington: Syngress, 2007, p. 409.
- [5] D. Gibson, "Sniffing Attack," in *Microsoft Windows security : essentials*, Indianapolis, IN: Wiley, 2011, pp. 149–150.
- [6] A. Gupta, "3 free Packet Sniffing Tools for Windows systems," *The Windows Club*, 2016. [Online]. Available: <http://www.thewindowsclub.com/free-packet-sniffing-tools>. [Accessed: 03-May-2018].
- [7] D. Kumar G., M. K. Singh, and M. K. Jayanthi, "ARP Spoofing Attacks," in *Network security attacks and countermeasures*, Pennsylvania: IGI Global, 2016, p. 140.
- [8] R. Svensson, "Password Attacks," in *From hacking to report writing : an introduction to security and penetration testing*, Berlin: Apress, 2016, p. 90.
- [9] K. Beaver, "Password," in *Hacking for dummies*, 5th ed., Hoboken, NJ: Wiley, 2015, p. 97.
- [10] A. Wheeler and M. Winburn, "Data in the cloud," in *Cloud storage security : a practical guide*, amsterdam: Elsevier, 2015, p. 2.
- [11] M. Muchmore, "The Best Cloud Storage and File-Sharing Services of 2018 - Storage Devices - Reviews and Price Comparisons from PC Magazine," *PCmag*, 2018. [Online]. Available: <http://uk.pcmag.com/storage-devices-reviews/3682/guide/the-best-cloud-storage-and-file->

sharing-services-of-2018. [Accessed: 21-May-2018].

- [12] K. Paulsen, "SATA, SAS, AND RAID," in *Moving media storage technologies : applications & workflows for video and media server platforms*, Burlington: Focal Press, 2011, pp. 139–140.
- [13] M. Burnett and D. Kleiman, *Perfect passwords : selection, protection, authentication*. Rockland, MA: Syngress, 2006.
- [14] A. Lockhart, "Network Security," in *Network security hacks*, 2nd ed., Sebastopol, CA: O'Reilly Media, 2007, p. 185.
- [15] A. O'Donnell, "What Are Packet Sniffers and How Do They Work?," *Lifewire*, 2018. [Online]. Available: <https://www.lifewire.com/what-is-a-packet-sniffer-2487312>. [Accessed: 21-May-2018].
- [16] Office Team and A. Myrvold, "Enabling password rules for Office 2010 – Microsoft Office 2010 Engineering," *Microsoft TechNet*, 2009. [Online]. Available: <https://blogs.technet.microsoft.com/office2010/2009/10/15/enabling-password-rules-for-office-2010/>. [Accessed: 01-May-2018].

Network operating systems and security assignment 2

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

57 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

GRADING FORM: SMU GENERIC_GJ

ALEXANDER HALL

57

RESEARCH-INFORMED LITERATURE



A good number of sources used correctly. Very good academic credibility, bar source 15.

19

KNOWLEDGE AND UNDERSTANDING



Good evidence of knowledge and understanding throughout the report. It'd be nice, however, to see some more discussion of lower-level devices.

14

ANALYSIS



Slightly weak synthesis in this report - try to use more than one source to make a point. Conclusion is also a tad short for the length of the report.

13

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



Reasonably good SPG - be careful with apostrophes. A nicely-presented report.

11