

Networking Assignment R Lucas

by Robert James Lucas

FILE	2935_ROBERT_JAMES_LUCAS_NETWORKING_ASSIGNMENT_R_LUCAS_113613_214106149.DOCX		
TIME SUBMITTED	23-MAY-2018 02:21PM (UTC+0100)	WORD COUNT	2810
SUBMISSION ID	89791774	CHARACTER COUNT	16831

NETWORK SECURITY THREATS

07.04.2018

Robert Lucas

Contents

Introduction	2
Denial of Service	2
Rogue DHCP Servers	2
ARP Spoofing.....	3
Packet Sniffers.....	3
Password Cracking	4
Method 1: Obtaining the Passwords	4
Method 2: Guessing/Brute Forcing.....	4
Method 3: Rainbow Tables	5
Method 4: Phishing.....	5
Works Cited.....	7

Introduction

The objective of this assignment is to identify potential network security threats and provide solutions on how to fix said threats or prevent them from happening entirely.

Denial of Service

Denial of service attacks are security threats that involve denying access to a server by flooding it with traffic, halting other users from accessing it [1] [2]. This denial can go from certain websites, email accounts or any accounts you have online [3]. The most common DoS attack method is the SYN Flood, targeting the TCP connection. Under normal circumstances when one wants to open a network conversation, they send a SYN packet to the server, which then sends a SYN-ACK back and gets an ACK back from the person that sent the SYN, which opens a TCP connection. The SYN Flood interferes by flooding the server with multiple SYN packages, which the server will try to process one by one. This causes the system to grind to a halt [3].

The good thing about this particular threat is that it doesn't actually hack into anything and steal data, it just interferes with the system by causing a lot of traffic, however it was used as a distraction method by a hacker group named Anonymous in 2011, they hacked into Sony and took the credit card data of over 12 million customers while the DoS attack was still going on [4].

Of course this all leads to the question: is it possible to stop DoS attacks. The short answer is no, it isn't if there's one underway [5]. DoS attacks are a bit like plane crashes in that you will have fail safes to prevent it from happening but if it does happen the best you can manage is to limit the damage as much as possible and hope things go your way. There are two different types of DoS, one is where the attack comes from one direction, called Single-Origin, and the other where it comes from multiple sources, called a Distributed DoS. Single-Origin methods are limited in their methods, and easier to deal with. Blocking the IP address the signal is coming from is the simplest route, and there are security tools out there that can detect these attacks [4], such as SonicWall UDP.

Rogue DHCP Servers

A rogue DHCP server is an active DHCP server that hasn't been approved by the University Information Technology Services [6]. When this occurs computers on a network will obtain new IP addresses and will experience errors on their networks, such as being unable to access the internet.

The way this threat works is by waiting for a network computer to request for a new IP from a nearby legal DHCP server, however the rogue server will react first, and send its illegal IP address to the server. The computer will send its MAC address to the rogue server, getting an acknowledgment in return, thus the rogue server becomes the computer's default gateway [7]. Afterwards the one responsible for the attack is then capable of looking into the infected computer's contents, anything from files, browser history and any other personal data. These attacks are known as man-in-the-middle attacks [8]. It should be noted that there are two types of rogue DHCP servers, although the difference is extremely subtle: one is known as an evil rogue DHCP, which mimics the address of the server, and a simple rogue DHCP, which does not [9].

There are software programs that are capable of detecting rogue DHCP servers, limiting the damage done. One example of said software is DHCP Snooping, which is a protective layer of security that prevents DHCP malware from getting any access [10], however it research indicates that it may not be as good as it was advertised to be [9].

ARP Spoofing

ARP spoofing possesses several similarities with the rogue DHCP server hacking method, namely in its method of using fake data to gain access to networks. Spoofing works by setting their tool's IP address to match with the subnet of their target, which will allow the hacker who sent the false IP address to either steal data from the victim, or establish a foothold to launch further attacks [11]. Spoofing can be easy to do, on account that—unless a specific software is in place to counter it—it is simple to send a fake ARP response to a host, this is because ARP protocols are stateless, meaning they will accept any reply they receive [12].

The simplest way of dealing with a spoof attack, at least without using some form of spoof preventing software is to create a static ARP table, which involves manually programming the computer to only accept a single IP address and nothing else [13]. Of course this is only a delaying tactic, as the spoof might have the matching IP address and gain access anyway. The other method is to use anti ARP spoofing software such as AntiARP, remarp and Antidote.

Another couple of methods are cryptographic network protocols and packet filtering. According to Professor Georg Carle, cryptographic protocols are 'a series of steps and message exchanges between multiple entities in order to achieve a specific security objective' [14], essentially they are methods of making sure that the server connections are going where they should be. The method works around sequences of numbers called keys, which are used to encrypt programs [15]. One such method is the Secure Sockets Layer encryption method. It is mainly used for the internet and email, getting a secure connection between two separate machines [16]. Another example of key using cryptography is the Data Encryption Standard Algorithm, which uses a 56 bit long key, however it is not the most effective method because it can be hacked by brute force methods [17].

Packet filtering, also known as static filtering, is a firewall method that checks incoming packets and either grants or denies entry depending on if the source and destination of the IP address are correct [18].

Packet Sniffers

Contrary to most of the aforementioned attack methods above, packet sniffing wasn't initially designed to be a method of hacking, instead it was designed to spot network problems instead, finding out issues to ensure that the network is still running at peak capacity [19]. However despite its initial design purpose, hackers can still use the packet sniffers for less than laudable purposes.

Packet sniffers are designed to intercept data packets that are running through a network system, usually to detect messages, finding errors in the system or checking the statistics of the local network's traffic. There are also methods where packets can be further analysed and displayed in a readable form [20]. This particular feature is where the issues start cropping up. Anyone who wants to listen in on an email conversation between two people using the network can slip a packet sniffer

inside and read the conversation. They can also grab a hold of personal details, such as passwords, bank account details and security token details [21].

The way to stop packet sniffers is actually pretty simple: encryption. While it does not stop the sniffers from snatching the packets it does prevent the people trying to look at the packet's contents. If the packet is encrypted then the hacker won't see anything of value, merely nonsensical text. Another method of encryption is something that most people take for granted. Anyone who accesses the internet will look up to the top left and see 'https' in their web address, that is what stops sniffers from accessing people's web history and such [22].

For more specific purposes, it is possible to use something called a virtual private network. This will allow someone to encrypt the path between their computer and whatever said computer is accessing, for example someone else's computer for emailing, but this can apply to any other online feature. Any packet sniffers that try to access the data that is being sent will see nothing but absolute gibberish.

Password Cracking

Password cracking is an unusual method, mainly because it does not just use software oriented methods in order to attain the information the hacker desires. The first thing to point out is that password cracking is not what one would expect, mainly it is not like it is presented in movies.

Considering that cracking is a broader subject that covers many different methods of hacking, each method will be explained individually.

Method 1: Obtaining the Passwords

While this method is considered archaic compared to the other, more technological ways of hacking a network, simply retrieving the password is still an efficient way of doing just that. This method is more nuanced and unique than one would think, because it becomes a matter of psychological analysis and social engineering. The first way would be to steal the password itself, if someone has their password written down on a notepad for example, and this has been known to happen, then copying that will work [23]. Passwords can also be stolen by sniffing.

Another aspect of this psychological method is to look for clues by assessing the individual's hobbies. People tend to base their passwords on subjects within said hobbies, be it a football team, a certain game or another recreational activity. However this is guesswork and can be inefficient.

The method of dealing with these issues is rather simple: do not be careless. Do not put passwords on sticky notepads, do not give any indication or hint about your password, and if one is going to base the password off a subject, be sure to make it obscure enough not to be guessed by someone else.

Method 2: Guessing/Brute Forcing

Admittedly at first glance this seems like a slightly ridiculous method. Guessing is a fairly risky method, and can take a while to get the correct password. On a very general level this method involves typing in a certain password and hoping it works, in detail however the methods begin to make some sense. For instance the dictionary attack is a method by which the hacker uses words

that are more likely to be in the password to try and get the correct answer [24]. The way to deal with this hacking strategy is to ensure that the password that is being used will take days to be cracked open.

Method 3: Rainbow Tables

Another brute force method is called the rainbow table. Despite its generally non-threatening name this method can cause some issues, especially for passwords. To understand this some background theory needs to be known, specifically the concept of hashing. Hashing is when a password is inputted and the enter button is triggered. When a password is hashed it turns the password itself into something more like 'wdvwcgefy7y2e3r9ry3f' or something to that effect. So in truth it isn't the password that allows access, but the hashed version of it.

This is where the rainbow tables come into effect. Rainbow tables are essentially long lists of hashes. It skips past learning the passwords and goes straight to the important part. This form of hacking is a lot more effective, because it will allow the user to hack someone's password a lot faster than any brute force hacking tool can achieve [25].

Defending against this hacking method is a lot more difficult than standard brute force attacks, simply extending one's password will not grant absolute protection, and at best it will only cause a mild delay. The best way to stop the rainbow table attack is to use Salt. Before the password is turned into its hash value, a Salt program will place a random string of characters to the password, therefore making its hash state significantly more complicated and thus much harder to breach [26].

Method 4: Phishing

The general tactic of phishing attacks is to pose as a legitimate and trusted company of some description in order to trick people into giving away private details. This form of attack is extremely widespread, as to increase chances of someone taking the bait. This form of deception is incredibly varied in its methods. Such methods include:

- Phoning someone, stating they are a password protecting company
- Sending an email or text saying that someone has won a prize
- Unexpected email attachments
- Hyperlinks (specifically the URLs of said hyperlinks [27])
- Spear phishing: attacking more specific targets compared to normal phishing
- Trojan methods involve tricking web users into thinking they are something legitimate, before stealing their details [28]

Any form of ransomware or malware attacks usually start with a phishing attack [29]. There are in fact devices called phishing kits which can be bought on the dark web, which will allow even amateur hackers to create false websites, and the links to these websites will be sent to other web users via email [30]. This method can have one of the two purposes:

- Steal private information
- Download a virus contained in a zip file [30]

The best way to stop phishing is relatively simple: vigilance. Being careful has its benefits, think before clicking. Check the links to strange websites, as the links will undoubtedly have some strange

anomaly. It may even be recommended to study the phishing techniques, so that if any attempts of this form of hacking will be recognized.

Works Cited

- [1] N. Muraleedharan, "Behaviour Analysis of HTTP Based Slow Denial of Service Attack," in *Centre for Development of Advanced Computing*, Bangalore, 2017.
- [2] Tech Target, "denial-of-service attack," [Online]. Available: <https://searchsecurity.techtarget.com/definition/denial-of-service>. [Accessed 07 April 2018].
- [3] The Windows Club, "Denial of Service Attack: What it is and how to prevent it," [Online]. Available: <http://www.thewindowsclub.com/dos-denial-of-service-attack>. [Accessed 07 April 2018].
- [4] A. Weiss, "How to Prevent DoS Attacks," 02 July 2012. [Online]. Available: <https://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html>. [Accessed 13 April 2018].
- [5] M. Chapple, "How to prevent DoS attacks in the enterprise," [Online]. Available: <https://searchsecurity.techtarget.com/answer/How-to-prevent-a-denial-of-service-DoS-attack>. [Accessed 13 April 2018].
- [6] Indiana University, "What is a rogue DHCP server, and how can I tell when one exists on the IU network?," [Online]. Available: <https://kb.iu.edu/d/akpy>. [Accessed 21 May 2018].
- [7] R. Slosser, "How a Rogue DHCP Server Works," 17 December 2014. [Online]. Available: <https://www.plixer.com/blog/detect-network-threats/how-a-rogue-dhcp-server-works/>. [Accessed 21 May 2018].
- [8] N. Agrawal, B. Pradeepkumar and S. Tapaswi, "Preventing ARP Spoofing in WLAN using SHA-512," in *International Conference on Computational Intelligence and Computing Research*, Gwalior, 2013.
- [9] M. Agarwal, S. Biswas and S. Nandi, "Discrete Event System Framework for Fault Diagnosis with Measurement Inconsistency: Case," pp. 9-15, 2017.
- [10] E. Banks, "Five Things To Know About DHCP Snooping," 25 September 2012. [Online]. Available: <http://packetpushers.net/five-things-to-know-about-dhcp-snooping/>. [Accessed 21 May 2018].
- [11] Veracode, "What Is ARP Spoofing?," [Online]. Available: <https://www.veracode.com/security/arp-spoofing>. [Accessed 21 May 2018].
- [12] S. Jadodia, "Detecting ARP Spoofing: An Active Technique," Kolkata, 2005, pp. 239-241.
- [13] A. Lockhart, "Network Security Hacks: Tips & Tools for Protecting Your Privacy," Sebastopol, 2006, p. 186.

- [14] G. Carle, *Network Security*, Tubingen, 2003.
- [15] M. Rouse, "public key," [Online]. Available: <https://searchsecurity.techtarget.com/definition/public-key>. [Accessed 21 May 2018].
- [16] R. Margaret, "Secure Sockets Layer (SSL)," [Online]. Available: <https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL>. [Accessed 18 May 2018].
- [17] P. Semwal, "Comparative study of different cryptographic algorithms for data security in cloud computing," Uttarakhand, 2017.
- [18] H. Mohammed, "Design of Secured WLAN by Using "Packet Filtering Firewall"," in *IEEE WiSPNET*, Bucharest, 2017.
- [19] M. A. Qadeer, A. Iqbal, M. Zahid and M. R. Siddiqui, "Network Traffic Analysis and Intrusion Detection using Packet Sniffer," in *2010 Second International Conference on Communication Software and Networks*, 2010.
- [20] S.-Y. Phang, H. J. Lee and H. Lim, "Design and Implementation of V6SNIFF: an Efficient IPv6 Packet Sniffer," in *International Conference on Convergence and Hybrid Information Technology*, 2018.
- [21] A. O'Donnel, "What Are Packet Sniffers and How Do They Work?," 23 March 2018. [Online]. Available: <https://www.lifewire.com/what-is-a-packet-sniffer-2487312>. [Accessed 22 May 2018].
- [22] Flashrouters, "HOW TO PROTECT A HOME NETWORK FROM PACKET SNIFFERS," [Online]. Available: <https://www.flashrouters.com/blog/2017/10/31/how-to-protect-yourself-from-packet-sniffers/>. [Accessed 22 May 2018].
- [23] A. Han, D. Wong and L. Chao, "Advances of Password Cracking and Countermeasures in Computer Security," Macau, 2014.
- [24] V. Beal, "dictionary attack," [Online]. Available: https://www.webopedia.com/TERM/D/dictionary_attack.html. [Accessed 22 May 2018].
- [25] A. O'Donnell, "Rainbow Tables: Your Password's Worst Nightmare," 2 January 2018. [Online]. Available: <https://www.lifewire.com/rainbow-tables-your-passwords-worst-nightmare-2487288>. [Accessed 22 May 2018].
- [26] sqlity.net, "Salt – Preventing Rainbow Attacks against Password Stores," 31 March 2014. [Online]. Available: <https://sqlity.net/en/2309/salt/>. [Accessed 22 May 2018].
- [27] phishing.org, "What Is Phishing?," [Online]. Available: <http://www.phishing.org/what-is-phishing>. [Accessed 23 May 2018].

- [28] Phishing.org, "Phishing techniques," [Online]. Available: <http://www.phishing.org/phishing-techniques>. [Accessed 23 May 2018].
- [29] M. A. Qbeitah and M. Aldwairi, "Dynamic Malware Analysis of Phishing Emails," in *International Conference on Information and Communication Systems (ICICS)*, 2018.
- [30] J. Fruhlinger, "What is phishing? How this cyber attack works and how to prevent it," 8 December 2017. [Online]. Available: <https://www.csoononline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>. [Accessed 23 May 2018].

Networking Assignment R Lucas

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

47 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

GRADING FORM: SMU GENERIC_GJ

ROBERT JAMES LUCAS

47

RESEARCH-INFORMED LITERATURE



A very good number of sources, but a lot of them are really of quite poor academic credibility. As you move into level 6, please do consider the credibility

13

of the material you use and cite.

KNOWLEDGE AND UNDERSTANDING



Fairly good evidence of knowledge and understanding - as per the brief, it'd be nice to see a bit more mention of low-level devices.

14

ANALYSIS



There's a lack of synthesis of material in this work - try to use multiple citations to back up things you say. A conclusion/summary, with a bit more narrative would help too.

9

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



A well-written report, with good SPG. Fairly well-presented, though some of the content you've described could've been tabulated or provided as an image to break the report up a tad.

11