Information Privacy and Security on a Shared Resources Network: IP Spoofing Attacks

Pedro Graça[1]

[1] Lusofona University of Porto, Portugal
a21705454@mso365.ulp.pt

Abstract. In today's age, people consume and share information at an enormous rate. We live in a world where information is power and more importantly, money, lots of it. Companies are now increasingly requesting more sensitive information from their users, in order to provide better services to its customers. This paper focuses on underlining the importance of information privacy and security on a shared resources network, by analyzing the current level of awareness of the general population and of some of the most important governments around the world to such matters, discussing how the "benefits of the internet" and privacy issues are intertwined with each other, ways to achieve a good level of privacy and security while maintaining the same usability and comfort that people have grown accustomed to, explain how one's data can be important to many different entities such as companies and their advertising partners but also to ill-intentioned individuals wanting to profit from it or just intending to cause grief to others. The last section of this paper lists and describes the major threats to digital privacy and security, with special emphasis in one type of threat: IP Spoofing Attacks.

Keywords: Data, Confidentiality, Shared Resources Network, Privacy, Threats, Security, Availability, IP Spoofing.

1 Introduction

In the last decade, the bond between humanity and technology has only grown stronger. Our dependency on technology increases every year, as well as the benefits we get from it such as: the ability to talk to our friends, colleagues, family even a complete stranger, without any tariffs attached to it as long as we have an internet connection, the capacity of being able to acquire knowledge about any topic just by using a search engine and also, being able to share a photo or video with whoever we want whenever we want, instantaneously.

Despite the countless benefits technology brought us, it also brought us new dangers and ways of making us vulnerable to other entities, and these threats and vulnerabilities are increasing every year, as time passes by. [1]

Each time a person posts or shares an image, accesses a website, watches a video or buys something online, they leave behind a "digital trail" of themselves which can be used to analyze, track and identify an individual.

10.11228/dpsc.02.01.006

This "digital trace" is more commonly known as "digital footprint" [2], and unlike the snow or dirt footprints we see in real life, this type of trail cannot be erased just by simply throwing a dirt or snow on top of it. In fact, each footprint we leave behind in our "digital journey" is permanent, and some people are already realizing this when they are suddenly fired from their current job due to some tweet they wrote years ago, which was the case of James Gunn [3], a writer/director who worked for Disney and saw himself fired because of a series of tweets he wrote, some a decade old.

Section 2 of this paper talks about how important it is for people to be aware of the dangers of the internet and be more careful about what they share on places like social media, but also raise their awareness about how valuable their own data can be when it is available to everyone on the internet. Besides regular people, this section also emphasis the importance of the government on this matter, and how it should protect its citizens against evil entities and non-privacy respecting companies.

Section 3 shows how privacy and the internet are strongly connected, the various threats that exist and simple steps that help counter them, or at least diminishing the chances of being affected by one.

Section 4 presents a review of IP Spoofing attacks, the various forms an attack of this kind can take, an example of how one is performed and what results come from the success of one.

2 Social and Governmental Awareness on Online Privacy and Security

With how much impact the internet can have in everyone's life, we will now explore the current level of awareness, both social and governmental, on this subject and try to understand how governments are dealing with these digital threats, what measures are being taken to solve them or at least trying to diminishing them as much as possible and also, how much do ordinary people care about the safety and privacy of their digital information, what kind of precautions do they take when they access the internet, or if they just live their lives defenseless against any evil entity, hoping they never become victim of a cybercrime.

2.1 Social Awareness

An article published last year by the South African Journal of Science [4] analyzes and describes the importance of information privacy and online security by conducting a study using Facebook as the study's test environment, to evaluate how much of their personal lives people share on Facebook, and the results do not look good.

From a population of 357 users, the study found that 67% (n = 240) of Facebook users' personal data are partially available, while the remaining 33% (n = 117) have all of their personal details available to anyone (See figure 1).

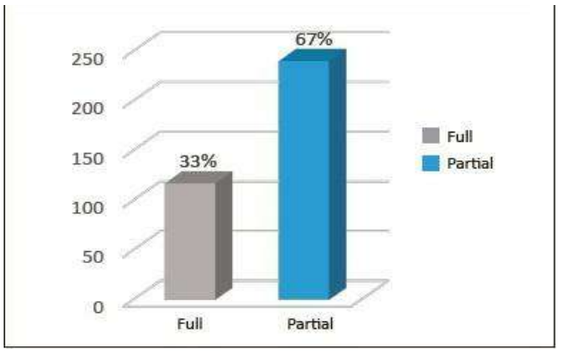

Fig. 1. Availability of users' data [4]

Another study, which also targets Facebook as their case study, wrote a paper in which it says that of the 210 respondents who participated in the study, only 2 of the 210 informed that they did not appear with their real names on Facebook [5]. Besides the astounding percentage of people who disclose their real name on Facebook (99%), the study dug deeper in what kind of information users share willingly on the social network and the results look very dim when it comes to privacy concerns.

Questionnaire item	n	%
Real name	208	99
Profile picture	206	98
Birthday	186	89
Home town	186	89
E-mail address	174	83
Education information	169	80
Photos of one's self	158	75
Photos of one's friends	130	62
Relationship status	124	59
Sexual orientation ("interested in")	103	49
Favorite music, movies, etc.	70	33
Contact phone number	69	33
Activities / interests	67	32
Partner's name	55	26
Street address	38	18
Website	25	12
Political views	20	10

Fig. 2. Personal information on profile [5]

Analyzing the table above, we can conclude that most respondents share a lot of their personal information on Facebook, making the process of gathering personal details of an individual, a simple and quick task for any interested party.

2.2 Government's Role

Despite information privacy and security being something that should be achieved mostly by each one of us, there are some things the average person can't control and should be taken care of by the government. For example, the situation of good companies becoming evil or too big, that they start thinking they can get away with anything, prevent data breaches, data mining and also the case of the government itself that should not abuse of the power it was bestowed with, as it is seen in some totalitarian countries [6], who use their powers to spy on their own citizens and citizens of other countries as well.

There's also a serious matter these entities should be paying attention to, and that is cybercrimes. There are many types of cybercrimes, and although some can be prevented by users, some can only be stopped and prevented by companies or governments.

Phishing emails, DoS attacks and Identity theft, are only a few types of cybercrimes [7] that can occur and should be fought against, now more than ever.

According to a news article [8], cybercrime is the fastest growing type of a crime in the U.S, and they are increasing in size, sophistication and cost. It is estimated that cybercrimes will cost $6 trillion annually by 2021, up from $3 trillion in 2015 [8].

After analyzing this data, it is evident that this is a problem that cannot be ignored either by us ordinary people or by governments, and should be payed attention to, before something serious happens, something that could be prevented if we had put a bit more effort in trying to comprehend and understand how this "digital world" works when there was still time to act.

3 Internet Benefits and How it Affects Privacy and Security

The internet today allows us to do many things, that we couldn't fully explore it in a single lifetime (Watching all YouTube videos would take more than that).

A few decades ago, if someone didn't know something about a specific theme, that person would have to go to a library and read a book about it or ask someone specialized in that specific area to explain it to them, but today you just insert your question on any available search engine and within a few seconds (or less), you have all kinds of information about the subject you were curious about, and all of this is available through a computer or a cellphone, millions and millions of documents, articles, news, all of it in the palm of your hand [9].

Amazon for example, allows us to read and choose from an enormous collection of online books, but this come with the cost of a portion of our online privacy, since amazon, as well as other companies, can track where someone started reading some-

thing, what was read/reread, what passages were marked or even if you finished reading that particular book. [10]

Additionally, if you open any social media website, you're flooded with all kinds of information: pictures and videos of your friends, "internet memes", news, there's just no end in sight.

These are only a few of the many things we can do by using the internet, but as mentioned before, every page you visit and all the "likes" you put on Facebook, are being tracked and not by the entities people commonly think about. It has become a norm, that every webpage we visit has some kind of advertising, and a large portion of these advertisement uses ads that have a strong possibility of being relevant to you [11]. This is what's called "targeted advertising" and although it can be beneficial to us, it comes with a cost, and that cost is our online privacy.

In order for "targeted advertising" to work, websites and companies have to collect has much data as they can about each one of us, in order to provide ads about things we like and might be interested in buying. This brings up the question of "how much can we trust in these companies" and "what do they do with their consumers personal information", we can only speculate, and so is up to governments to take a step forward and regulate what is allowed and not allowed to do done with our data.

Taking the United States as an example, there are virtually no government regulations on privacy policies and disclosure in e-commerce or on the Internet [12], this meaning that we are all at the mercy of a company's good will, and our data can be used in anyway they see fit.

3.1 Threats to Our Digital Privacy and Security

Unfortunately, the number of threats that exist nowadays is vast and is constantly increasing and stating and describing every one of them would lead to a whole other paper. Therefore, in this section, there are only going to be mentioned some of the most important threats that can affect network traffic, such as malwares.

Security Objectives

The classic model for information security defines three objectives of security: maintaining confidentiality, integrity, and availability [13].

- Confidentiality refers to protecting information from being accessed by unauthorized parties.
- Integrity focuses on ensuring the authenticity of information (that information is not altered, and that the source of the information is genuine).
- Lastly, availability means that information is accessible by authorized users.

List of Existing Threats

- Malware
- Phishing
- Trojans

- Ransomware
- The list goes on

In the case of Malwares, they are developed by cybercriminals and can be installed on all sorts of devices and operating systems, and this type of attack is increasing at a fast rate, growing by a third in 2018 when compared to the previous year. [14]

With so many threats, each of them growing in number and sophistication, its vital users protect themselves in every way they can.

3.2 How to Protect Ourselves

This section lists things we can do in order to enhance the level of privacy and security of our digital information and to reduce our "digital footprint" as much as possible. [15]

As discussed, there are things that affect our information security and privacy that we can't really control, but on the scope of things we can control, here are some small steps that can have a big impact on the process of hardening the privacy and security of our online data:

- Use of long passwords with strong encryption
- Use of password managers
- Enable automatic updates
- Avoid giving crucial information when signing up on a website (e.g. real name, address…)
- Avoid accessing websites that hold crucial data about you (such as banks) on a public network
- Always log out of your accounts on a public computer
- Deletion of "cookies" to reduce the risk of cross-website tracking
- For additional security, connect to websites which use encrypted DNS and HTTPS

These simple steps can greatly reduce the amount of information a person leaves behind when browsing the internet, either to evil individuals, advertising companies, a person's ISP (Internet Service Provider) or even governments in the most extreme cases. [16]

4 IP Spoofing Attacks

The last section talked about some types of attacks that we can be a target of, ways to reduce our digital footprint, and reduce the chances of having our digital information stolen or compromised.

This section will focus on a specific type of attack: IP Spoofing attacks, what they are, types of IP Spoofing, how to perform one, conducting an actual IP Spoofing attack. Lastly, we'll analyze the data obtained from the attack, with the aim of widening our knowledge about this subject.

4.1 Definition and Existing Types of IP Spoofing

Before diving into the actual testing and experimenting, let's first understand some key concepts about IP Spoofing attacks. To put it mildly, an IP spoofing attack is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. [17]

From a legal perspective, IP Spoofing is not a criminal activity since the act in itself (of spoofing an identity) is not illegal. It only becomes illegal when a threat of death or violence is involved, or personal data are stolen in order to commit fraud or identity theft. [18]

There are various types of IP Spoofing attacks namely "Distributed Denial of Service" more commonly known as DDoS, "Blind Spoofing", "Non-blind Spoofing", "Man in the Middle Attack", the list goes on.

4.2 Methodology and Testing

In this section, an IP Spoofing attack will be conducted between two machines, so that we can see how a typical IP Spoofing attack works and what kind of damage it can cause. Note that the attack was merely done for academic purposes and is done in a controlled environment, meaning that no entity or individual will be harmed.

Hardware and Software Used

- 1 machine with Windows 10 installed (The attacker)
- 1 machine with Linux installed (The target/victim)
- Wireshark - "Wireshark is the world's foremost and widely-used network protocol analyzer." [19]
- Colasoft Packet Builder – Enables the creation of custom network packets [20]

The Colasoft packet builder allows an entity to send ICMP (ICMP or "Internet Control Message Protocol", is a software component of the Internetworking layer of TCP/IP; essentially, it is a companion at that level to IP itself [21]) request with a spoofed IP address, create custom network packets (Custom TCP or UDP packets) and send them over a network as a valid request.

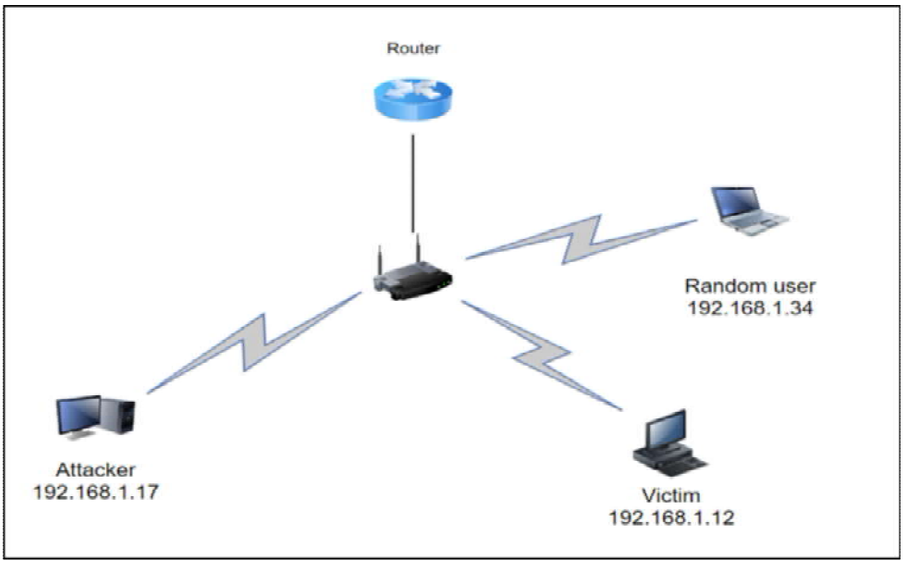

Fig. 3. Network constitution

Overview

As we can see, there are three hosts: the attacker, the host we want to target and a random authorized user in the network.

The test will consist in capturing ICMP packets that are heading towards the target machine (the machine with the IP address 192.168.1.12).

After grabbing the ICMP packets, we will modify the packet's source IP address by replacing it with a different IP address, for example with the random user's IP address (192.168.1.34). Lastly, we will verify if the target receives ICMP requests with the spoofed IP address.

Testing

To start the test, we must initialize "Wireshark" in order to start capturing packets.

Through the windows command line on the attacker machine, we will ping the victims IP address with 32 bytes of data.

```
C:\Windows\system32>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=182ms TTL=64
Reply from 192.168.1.12: bytes=32 time=404ms TTL=64
Reply from 192.168.1.12: bytes=32 time=323ms TTL=64
Reply from 192.168.1.12: bytes=32 time=242ms TTL=64

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 182ms, Maximum = 404ms, Average = 287ms
```

Fig. 4. Sending pings to target host

Now with the Wireshark software we will save the captured packets to a file, so we can modify them with the "Colasoft Packet Builder" software.

Loading the Captured Packets

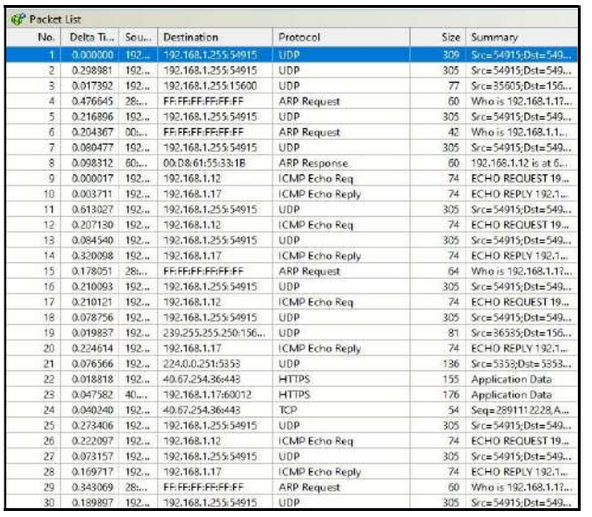

Fig. 5. List of captured packets

From the image above, we can see that there is a lot of data, but the data that interests us is the one where the protocols are labeled "ICMP Echo Req" and "ARP Request", hence we will remove everything else that falls out of this spectrum.

Removing Unnecessary Data

Packet List

No.	Delta Ti...	Sou...	Destination	Protocol	Size	Summary
1	0.000017	192...	192.168.1.12	ICMP Echo Req	78	ECHO REQUEST 19...
2	0.207130	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
3	0.210121	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
4	0.222097	192...	192.168.1.12	ICMP Echo Req	78	ECHO REQUEST 19...
5	0.269474	60:...	00:D8:61:55:33:1B	ARP Request	64	Who is 192.168.1.1...

Fig. 6. Filtered captured packets list

After removing the unnecessary data, we are left with only five packets (we are only going to need one of the ARP Request so no point in keeping more than one).

Each packet has a set of parameters we can edit using the "Colasoft Packet Builder" but for this test, we are only going to edit the field called "Source IP".

10

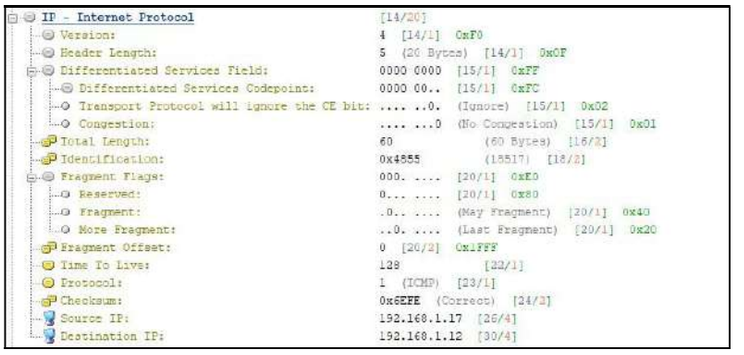

Fig. 7. Packet details

The “Source IP” field has the IP address of 192.168.1.17 (The IP address of the attacker machine). What we’re going to do is change this value to 192.168.1.34 (The same IP address of the “Random user” described earlier) in all the packets we captured. After that’s done, the last step is to send all the modified packets to the target host and analyze the results.

4.3 Results

To analyze the results, we’re going to open “Wireshark” on the target machine and start capturing packets, to see if one host replies to another with a spoofed IP address.

After sending all the modified packets, we can stop capturing incoming packets on the target machine and review the results.

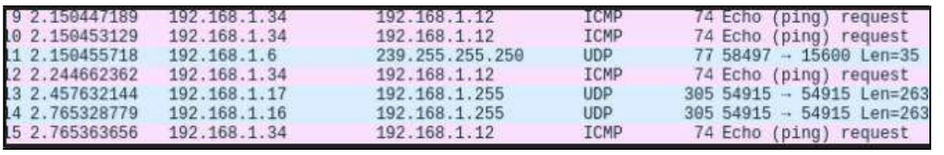

Fig. 8. Captured packets on the target host

As we can see, the host is replying to the other host with the IP address 192.168.1.34, making it look like it’s the random user in the network that is interacting with the victim’s machine, when in reality, the packets are being generated from the IP address 192.168.1.17 (The attacker’s machine).

This is a simple test and is meant to show how IP Spoofing can be done.

In a similar way, attackers can spoof custom packets to obtain information from the target host or target network. This shows how important it is for people and organizations to protect themselves, implementing security measures to counter these attacks and prevent bad situations from happening.

5 Conclusion

This paper was written with the objective of enlightening and raising the awareness to how important information has become in this technological age.

The paper covered many different subjects, all of them related to information privacy and security on a shared resources network, ranging from social and governmental awareness to threats and invasion of our digital privacy, what type of enemies and dangers we face and how we can protect ourselves against them, and lastly, an analysis of the matter of IP spoofing attacks.

The subject of social and governmental awareness is serious, and we can conclude from the data presented in this paper, that it still has a long way to go until we can say both users and governments, are taking all the necessary measures to protect themselves or their citizens against the many digital threats.

Consequently, the paper also covered the existing threats to information privacy and security, as well as measures to counter them in order to leave no stones unturned.

For the last section, the matter of IP Spoofing attack was heavily covered, giving a brief explanation of the concepts involved, types of IP Spoofing and also, an exploration of the process carried out in the execution of an actual IP Spoofing attack and what damage can be done if an attack of this sort is successful.

References

1. Shu, Q., Tu, Q., & Wang, K. The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective. International Journal of Human-Computer Interaction, 27(10),) 923–939 (2011)
2. Jessica Ching, Why does your digital footprint matter?; https://www.giveagradago.com/news/2018/01/why-does-your-digital-footprint-matter/261, consulted on 19-11-2019
3. Bryan Bishop, “Writer-director James Gunn fired from Guardians of the Galaxy Vol. 3 over offensive tweets”; https://www.theverge.com/2018/7/20/17596452/guardians-of-the-galaxy-marvel-james-gunn-fired-pedophile-tweets-mike-cernovich, consulted on 19-11-2019
4. South African Journal of Science, “Privacy and user awareness on Facebook” ISSN 1996-7489; S. Afr. j. sci. vol.114 n.5-6 Pretoria May./Jun. 2018
5. Tuunainen, Virpi Kristiina; Pitkänen, Olli; and Hovi, Marjaana, "Users’ Awareness of Privacy on Online Social Networking Sites – Case Facebook" (2009). BLED 2009 Proceedings. 42. Article title. Journal 2(5), 99–110 (2016).
6. DigitalPrivacyWise, “Security is everyone’s responsibility, Privacy is yours.” https://medium.com/digitalprivacywise/security-is-everyones-responsibility-privacy-is-yours-7a4e46398db7, consulted on 22-11-2019
7. Panda Security, “Types of Cybercrime” https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/ , August 2018, consulted on 23-11-2019
8. PR Newswire, “Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021”, https://www.prnewswire.com/news-releases/cyberattacks-

are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html, December 18, 2018, consulted on 23-11-2019
9. Tijssen, R. J.Science dependence of technologies: evidence from inventions and their inventors. Research Policy, 31(4), 509–526 (2002)
10. Landau, S. Control use of data to protect privacy. Science, 347(6221), 504–506. (2015)
11. Roosendaal, A. Facebook Tracks and Traces Everyone: Like This! SSRN Electronic Journal. (2015).
12. Norman E. Bowie and Karim Jamal. Privacy Rights on the Internet: SelfRegulation or Government Regulation?. Business Ethics Quarterly, 16, pp 323-342 (2006)
13. "Information Security Basics", MDN web docs, https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability, consulted on 28-11-2019
14. Jang-Jaccard, J., & Nepal, S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), pp 973–993 (2014)
15. Reeder, R. W., Ion, I., & Consolvo, S. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. IEEE Security & Privacy, 15(5), pp 55–64 (2017)
16. Bellare, M., Paterson, K. G., & Rogaway, P. Security of Symmetric Encryption against Mass Surveillance. Lecture Notes in Computer Science, pp 1–19 (2014)
17. Cloudflare, "IP Spoofing", https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/, consulted on 03-12-2019
18. Vlajic, N., Chowdhury, M., & Litoiu, M, IP Spoofing In and Out of the Public Cloud: From Policy to Practice. Computers, 8(4), pp 81 (2019)
19. Wireshark, "Wireshark User's Guide"; https://www.wireshark.org/docs/wsug_html_chunked/Preface.html, consulted on 08-12-2019
20. Colasoft, "Colasoft Packet Builder", https://www.colasoft.com/packet_builder/, consulted on 08-12-2019
21. George Mays, Global Knowledge Course Director, CCISP, CCNA, A+, Network+, Security+, I-Net+, "How Does Ping Really Work?", Galaxy Visions, (2006)
22. Breda F., Barbosa H., Morais T., Social engineering and cyber security, (2017)
23. Magalhães R., Barbosa H., International Journal of Scientific & Engineering Research, Cyber Espionage and Digital Privacy, Volume 8, Issue 1, pp 396 (2017)