International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 3 Issue 6, June – 2019, Pages: 57-61

The Art of Anonymity: Traces Detection

Mourad Henchiri

Lecturer, Universty of Nizwa, Nizwa, Sultanate of Oman

[a]mourad@unizwa.edu.om

Abstract *-- Hijack the identity on a network is a vital penetration testing behavior, yet, such a task must be done in a legal, before being ethical, scenario.[1] as per the mind of a hacker, being anonymous in an attack is a priority, thus, the obscurity and the obfuscation are habitual tactics each hacker start with when in action. In this research we are highlighting the famous; exposed and hidden methodologies hackers do to succeed in being anonymous. In addition to that we are able through this study to present new tactics to use as ethical hackers and crackers for your journey as penetration testers. [1, 3, 5]*

Keywords-- Hijack, spoofing, sniffing, intranet, extranet, penetration testing, threat, anonymity.

I. INTRODUCTION

The art of being anonymous, nowadays, is a tradition between security experts and digital security breakers. Thus, it is proved that spoofed security reside on facing a data packet coming from a destination that you trust, while you cannot prove this destination authenticity, nor can you affirm its falseness. Spoofed security is the usage and the referral to this weak logical access point to the targeted host (victim). [2]

One of the very famous attack techniques is the spoofing of identity; where the technical tools for spoofing authenticity over networks are a successful approach to trespass security layers; such a fire wall, solving restrictions, scanning networks, and so many cases and scenarios. This is an effective way when approaching a different network segments.

Applying this technology needs a proficiency level and a well understanding in networks topology and network protocols. So here, and in the network context, the spoofing is the unauthenticated access. Yet, in network security context, spoofing is an unauthenticated attack.[3]

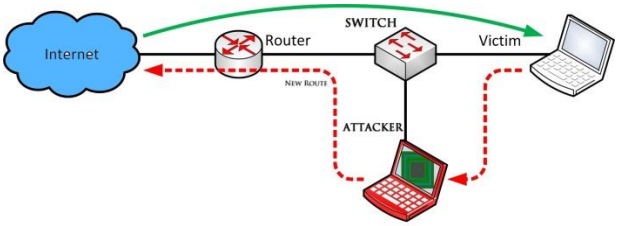

Figure I:-spoofed attack through internet[2]

The main actors that would benefit from the spoofing, and reach a high invisibility state, are the ones playing the role of a MitM (Man in the Middle). To accomplish the spoofed access, an attacker has to have an infiltration point to the communication medium which would give the starting key for retrieving the sender's email and replacing it within the current communication; and here the all the potential has moved to the hacker to present as the real node within the same network.[4, 5]

II. EVADING NET PROTOCOLS

It is trivial that remote activities need to be done in total obscurity once attacking a victim; thus, still the spoofing is considered to be a solution. The IP Spoofing technique is recognized as a network hacking tool. Thus, the protocols implemented in ensuring the usage of the spoofing technique are to be selected carefully, the NTLM (NT LAN Manager) could be a high level secure authentication process adopted along with your scan and checkup techniques.[4, 5]

The main purpose of this research not to limit the obfuscation techniques, yet, it is to prove the severity of the act of being anonymous and how to detect an intrusion trial. And, since everybody are talking security and cyber security, we conclude that the default hack approaches would fail anyway due to the security set on environment. Yet, here, we present the still alive security

breach that hardly to be said is secured and treated. Even, if the victim is an experience party, it would be a victim of the social engineering.

Not only automated activities to be evaded, yet, we reached to surround ten (10) common mistakes that administrators do and it leads to a vulnerability.

The first mistake administrators do is the misconfiguration of the rules behind passwords within an environment.

Right after unleashing the secret behind misunderstanding the passwords secrets, the second security sin exposed through this research paper is also a tool that might be referred to as a solution injecting backdoors and enlarging the vulnerability exploring the password as a sin. This is the off line access which allows an access to a deep level within the OS architecture. Deterring with an impersonated session as a local administrator. Adding a registry key like the Utilman, adding a .dll file in the right system location like the password filter... The actions here are as per the intruder imagination and willing. The off line access is to be implemented upon variety of scenarios. For the sane and sake of all, we introduce you, after a long research activities in the security field, the ethical and most stable attack technique for an off line access.
It is a must to check the signature of all software we download from a remote source; the internet, thus, we need a genuine OS that we can count on to be trusted by the machine in question, the machine to attack and hack. This OS is a MS windows OS that we are using and is the MS windows 10 Enterprise edition. To get it genuine and use it ethically at a free of cost we need to follow the instructions:

1- We visit the Microsoft evaluation center
2- From the tools and products menu we choose the MS windows 10 Enterprise
3- A iso file would be downloaded
4- Burn it to a dvd disc
5- Insert it into the dvd player of the victim machine, then boot from it
6- From the first window choose the default language then Next
7- From the second window choose Repair system
8- Troubleshoot
9- Command prompt
10- copy sethc.exe sethc_old.exe
11- copy cmd.exe sethc.exe
12- Reboot normally
13- At the windows access screen press the keyboard shift button five (5) times
14- net user mourad pa$$w0rd /add
15- net user mourad localgroup administrators /add

Enjoy the impersonated admin access to the machine. We reached to hack this machine because of a security missconfiguration that led to a successful boot from an external dvd.

A clear explanation to the hack steps and commands used in the above scenario is found at the Annex 1.

The third sin is SDDL (Security Descriptor Definition Language) misconfiguration that leads to processes to be injected and utilized as backdoors.

Then, the fourth sin is the Incorrect Access Control, manifested in bad services rights and permissions and also at the backupRead and backupWrite. This means “Lack of” Permissions in the Operating System.

The fifth sin is the usage of Old Technology. And this is because that Old Technology a Little Bit Too… Old.

The sixth security sin is the lack of encryption. At the time New Security Motto: Encrypt when you can!

At the seventh order, we define the sin that administrators do, which is Installing Pirated Software. This is because that malformed installation files are not necessary recognized by antivirus software.

The eighth sin is the Lack of Network Monitoring. Because this is a violation of the one well known rule: Do not allow traffic that you do not know.

The sin number nine is What You See Is NOT What You Get. Means that an admin has to have more than one troubleshooting technique for each case treated. Because lack of NTFS permission does not mean it is inaccessible.

The tenth sin is a Too Much Trust In People. Here, never to forget that insiders are a big threat to an organization, especially when they are non-skilled insiders.

III. STAY ANONYMOUS

Being anonymous is a step to be activated and set easily by referring to dedicated and third party solutions; amongst of them the famous TOR network browser, which is a peer-t-o-peer software that provides exit nodes to the external environments, and the destination would get served usually with a complete anonymity.

For such p2p software the real threat is usually a process that tries to communicate with the external environment. Here, the firewalls are useful to protect this obscure p2p network.

The proxy servers and NAT addressing are another type of utilities that help in being anonymous.

IV. STAY UNDETECTED

A deeper and more complex scenario via which to gain the state of being anonymous, is the steganography.

To be undetected is a scenario via which the doer would hide a process from the running processes list. It would be successful if a backdoor is running in background such the Advanced Persistent Threat (APT). Yet, the specialized analysis would expose and detect the malware activity with the help of the handles provided by the OS to control each running process.

V. IP SPOOFING ATTACKS

Each spoofing project starts at testing the ability of each host in a network of sending fake and spoofed packets, besides the test of ingress and egress filtering of packets from those hosts; here, usually we would like to keep the mind on that the routes has been deviated and changed.[6, 7]
The wide range of data resources available in the public networks gives the chances to new attack techniques; the IP spoofing is a crucial malicious attack used within all the new technological targets. Raising the status of a targeted machine or an application to a non-responding is the secret behind the DoS or DDoS attack.
Taking the identity of a node in a detected communication on a given network medium is the spoofing act; which is the success of taking the a real node role in a communication over a network, then getting and sending messages with the fake ID.
Here, and in a practical and real plane, every and each web site uploaded and published for a public use and distribution, is highly presented to an unwanted attack like so; the DoS or DDos attack. Thus, the presented attack and malicious infiltration has to be fought took into high consideration at each level and when needed. [2]

VI. REALIZATION

Proving that anonymity is a key solution for different security scenarios pushed us at the time of the research to generate different tests and schemas to accomplish and achieve our findings. The JEA [3], is a good automation solution of security purposes but it proved its limitation due the complex customization of the processes settings. A customized PowerShell skeleton has been identified for a better control of the undesirable anonymous behavioral approaches.
A survey was communicated with 44 different interviewees asking them about their anonymity experience on the internet.
The interview concluded to describe a myriad of unique anonymous activities on the Internet. A retired teacher created an anonymous online community for English learners to practice their language skills with each other. A Chinese student used anonymous social networking profiles to play good-natured tricks on his friends. Some interviewees used anonymity as a general online practice, but most used it judiciously, for particular kinds of online interactions.
About half of the interviewees (53%) used anonymity for illegal or malicious activities such as attacking or hacking others, or they engaged in socially undesirable activities like browsing sites depicting violence or pornography. Other socially undesirable activities included downloading files illegally, flaming others, ‘peeping’ others, or searching for others’ personal information

online. The line between illegality and undesirability was sometimes fuzzy, and many whose behavior was acceptable in some situations, as an example, within a discussion forum, were fearful it would be unacceptable in others, like at work. It was also impossible to cleanly separate "bad guys" from "good guys" in our data because many of those who reported antisocial behaviors (e.g., behaviors that are unfriendly, antagonistic, or detrimental to social order) also reported pro-social behaviors (e.g., behaviors that are altruistic, or intended to help others).

Adopted Working Solution Architecture

#Libraries
#Global declarations
Triggers
Packet Reception Check Up Function
Main Calls
Exceptions
#Rewind

Shared survey Analysis

Type of anonymous activity	Number of interviewees (N = 44)
Instrumental Anonymous Activities (75% of interviewees)	
File sharing and downloading	33 (75%)
Browsing and searching for information	33 (75%)
Social Anonymous Activities (95% of interviewees)	
Participating in special interest groups	35 (79.5%)
Social networking	24 (55%)
Sharing art or work	20 (45%)
Exchanging help and support	16 (36%)
Buying and selling	13 (30%)
Politics (Discussing or being involved in)	9 (20%)
Resourcing (Reviewing and recommending)	4 (9%)

Table 1. Anonymous activities types

Conclusion

After a deep study and a network traffic analyses, the findings are to be considered at each communication channel. Based on the target the option is control all communication channels. A pre-approved communication token is advised, yet, not usually implemented due to network circumstances. The PowerShell skeleton implemented within this research is to be customized at each time planted within an environment.

References

[1]. On investigating ARP spoofing security solutions Int. J. Internet Protocol Technology, Vol. 5, Nos. 1/2, 2010 ISSN 1743-8217

[2]. LOAD BALANCING ALGORITHM (LBA) AS A LOCAL SPOOFING THREATS & PREVENTION SOLUTION FOR DoS AND DDoS PAQUETS ***International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016*** ISSN: 2395-3470

[3]. JUST ENOUGH ADMINISTRATION (JEA) VIA SYSINTERNALS MICROSOFT SECURED INFRASTRUCTURE Indian J.Sci.Res. 17(2): 9 - 12, 2018 ISSN: 2250-0138

[4]. Learning PowerShell available at: https://riptutorial.com/Download/powershell.pdf

[5]. iTAP: In-network Traffic Analysis Prevention using Software-Defined Networks ACM SOSR 2017. Santa Clara, CA, USA (April 2017).