Opinion

BIOMEDICAL
Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2020.29.004736

Genetic Shackles of Intrusion: Put to an End

Usman Ali Dar* and Arsalan Iqbal

Georgian College, IT Department, Barrie, L4M3X9, Canada

***Corresponding author:** Usman Ali Dar, Georgian College, IT Department, Barrie, L4M3X9, Canada

ARTICLE INFO

Received: July 13, 2020

Published: July 20, 2020

Citation: Usman Ali Dar, Arsalan Iqbal. Genetic Shackles of Intrusion: Put to an End. Biomed J Sci & Tech Res 29(1)-2020. BJSTR. MS.ID.004736.

ABSTRACT

Today we all live and work in a partaking information superhighway. Almost every type of Machines, the Interconnecting communication networks, and the services available over the networks make up this cyberspace highway. As cyberspace conquers almost all areas of modern day existing, playing, and working, it is becoming more momentous that we recognize its technical nitty-gritties, threads and procedures, as well as its aptitudes, threats, and feebleness. This paper explores different kind of Intrusions threats and detection that are and can be used for and against target.

Keywords: Intrusion; Cyberspace; Attacks; Hacking; Information; Interconnecting Communication Network (ICT)

Introduction

The process of Intrusion is to find weaknesses and possible ways to break the security of any system, machine or communication network system or causing it to enter into an uncertain state. The act of intruding or acquisition unlawful access to a system typically leaves hints that can be revealed by Intrusion Detection Systems. We all live in the same neighborhood and within that neighborhood there are is one attacker beside each one of us, this result in never ending game of cat and mouse either it's home public or a workplace. There is abundance of research available on internet about the intrusion and its detection with different perspective from analysis of classification to traffic analysis and mining of information data. Apparently, a very little information has been published on a precise method of how this data is being manipulated and gathered in the network [1].

Today's world is all about ones and zeros a binary notation of any information, where any information is available in various forms and is ready to be used in any way, with the bit of luck and privilege. The very step of forming a strong attack on any target is scouting or it can be called reconnaissance. The attackers are very well equipped with unique skill sets and they not only walk into targets doorsteps and will gather all the possible information and will leave no traces that leads back to them [2]. The process of the cyber shackles is a combination of series of process which are discussed.

Scouting

The process of scouting, revolve around one simple idea "Information Gathering". By using different tool sets, techniques or methods for important information gathering and use for building a robust attack against the target. Reconnaissance has two main vectors: active and passive [3].

Invasion

On the bases of target scouting all the prior information is gathered using different tools and techniques to build a surface for a strong and robust attack against target [4].

Manipulation

After scouting and invasion of the target system the attacker can easily manipulate the system as required to explore further. The attacker will use multiple tools for gathering information and weaknesses of the system and the network its connected to and deliver malicious programs or executable set of processes to imprint its strong foothold.

Privilege Escalation

Once the target machine is accessed by the attacker. The very dire need is now to control the target completely and that only can be done with the master account. The attacker will use different ways with own 3rd party or own developed apparatuses to escalate his role to the master level. Some of the examples are cookies, brute force, zero-day or attacker can access group policy object, customize settings or acquired the credentials.

Cross Movement

Getting into the target and acquired complete control would only be the start, attacker will start cross bifurcation of traffic and learn more about the environment. The attacker starts the scouting process for mainstream assets like storage, servers to get sensitive and critical information [5].

Mystification

Anonymous is a privilege that is used very wisely by attacker. The attacker will not only avoid any footprints on the target machines; moreover, to avoid any noise or spike that can depict any alarm for examination. The attacker will use different methodologies to wipe out the points that could lead back that means scrubbing out any material, logs, false timestamping or embed abstruse information so that it looks like it was never happened.

Denial of Service

The denial of service attack is one of the worst nightmares for any service provider. Such attack not only block all the access of services for the clients; moreover, it will open more doors for them to find other weaknesses of the system and cause interference. These attacks are being planned and executed on larger scale with the help of group of nodes and multiple points to cause more damage, such segment of attack called as Distributed Denial of Service Attack [6].

Exfiltration

The extraction stage is basically exporting information of target. Once the attacker gets required information: they'll will move to further step ahead and get that information out to a meticulous location, where they will use that information according to what suited them best or let's say serve them best in terms of financially, politically, socially or even they will use it as bribery to get closer their other targets. There is no ETA or time to get such information out of any target, it depends on one skills and target (Figure 1).

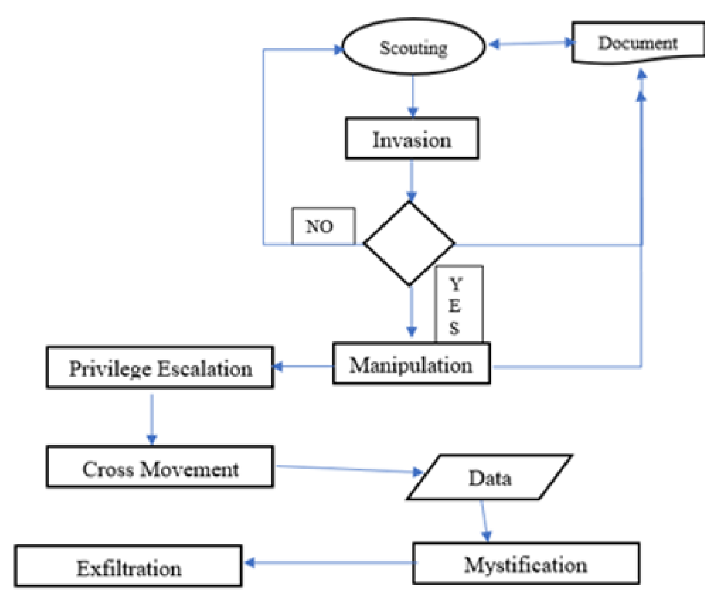

Figure 1: Process of Intrusion.

Conclusion

This paper outlines the stages and life cycle of computer systems or network intrusion. This paper further explains how each of the stage supports and provide information to gain stronger foothold on target machine. For any successful intrusion into any target, single tool may not give us all the required information for a successful cyber intrusion attack. Therefore, a combination of tools with methodologies and techniques are required to be incorporated together to get all the required information.

References

1. Purvag Patel, Chet Langin, Feng Yu (2012) Network Intrusion Detection Types and Computation. Shahram Rahimi (IJCSIS) International Journal of Computer Science and Information Security 10(1).
2. HP Sanghvi (2013) Cyber Reconnaissance in IJCA. (0975-8887) 63(6).
3. Usman Ali Dar, Arsalan Iqbal (2018) The Silent Art of Reconnaissance: The Other Side of the Hill. International Journal of Computer Networks and Communications Security 6(12): 250-263.
4. Airull Azizi, Marwan Hadri bin Azmi, Rudzida Akmam (2018) Proposed Framework for Network Lateral Movement Detection Based on User Risk Scoring in SIEM.
5. Saravanan kumarasamy, R Asokan (2011) Distributed Denial of Service (DDOS) Attacks Detection Mechanism International Journal of Computer Science, Engineering and Information Technology (IJCSEIT) 1(5).

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2020.29.004736

Usman Ali Dar. Biomed J Sci & Tech Res