Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

A Study of Bypassing Security Control Methods in Kali Linux Environment

Prof. Vinit A. Sinha , Prof. Dr. Vilas M. Thakare
PRMITR Badnera, Amravati,
Maharashtra

Abstract:- In the very recent years, antivirus and similar kind advance security software has high peak value due to accurate detection of crucial malwares and occurrence of different security incidents. Usually whenever software testers and security specialist get root or network access at internal of system, they assume they done all type of security testing an possess all kind of knowledge, but they forget or neglect important thing during penetration test process i.e., bypassing security controls.

In this paper, we perform analysis of this bypass security methods and get out effective one. So that it cannot be neglected any more. We analysis four effective method as Bypassing network access control, Bypassing security software (antivirus) based on different framework, Bypassing windows OS-based security controls and Bypassing application-level control method. Throughput this paper we implement these different methods including their subdomain on Kali Linux platform as it supports different security tools and provide strong platform for advance penetration tester. Kali Linux provide security framework for hardening network security on prior basis for security vendors.

Keywords – Kali Linux, Penetration Testing, Antivirus, UAC, NAC, SSH

1. INTRODUCTION

This research paper focused on neglected issue by pen-tester or attacker, i.e., Bypassing security control methods, current scenario of penetration testing is shown as in **fig. 1.**

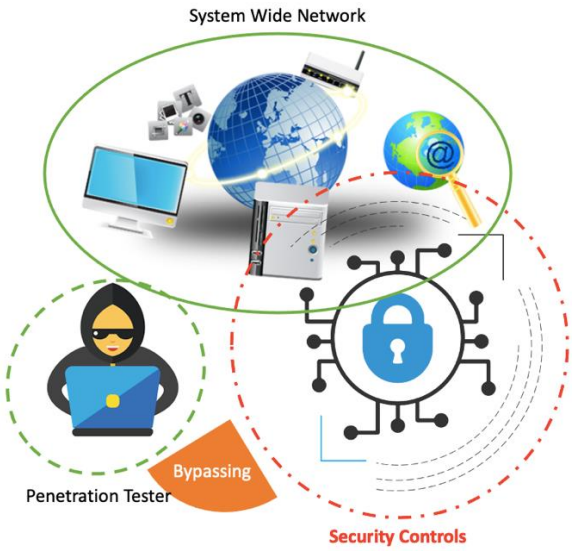

Fig.1 Current scenario of Penetration testing

We perform analysis on different Bypass methods on basis of network access control, application-level controls and operating system security control. During analysis we perform study on pre-admission NAC (Network Access Control) and post-admission NAC for maintaining all security control on basis of requirement, which include addition of new device (network basis). For this operation we used Kali linux platform, having shell access for newly added device. Next task is to implement Bypassing security software (Antivirus) method, this includes use of Veil framework[1] – Antivirus evasion framework, use of shelter[2] and effective method of going fileless for antivirus evasion. We then analyze Bypassing application-level method, which include tunneling client-side firewall by implementing SSH, Bypassing URL filtering technique for inbound and outbound rules. At last, we analyze Windows OS based Bypass control method. This includes UAC technique, fileless technique method using fodhelper to bypass user access control and disk cleanup technique in windows 10.

Research paper divides into six sections as section 2 describe about literature survey perform by various researchers, which include their distinct implementation of security technique. Section 3 briefs various methods use to bypass security controls. Section 4 explains implementation techniques that we use regarding bypass control methods. Section 5 describe result and

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

evaluation of different methods use in research with analysis report. Section 6 describe conclusion and future work related to research work for security measure.

2. RELATED WORK –

For analyzation of bypassing security control methods, we performed various literature surveys as, Junior et. al [2018][3] describe application of distributed firewall for managing firewall and their interactive rules. Ganji et. al [2018][4] explains new way to enhanced linux security in terms of vulnerability module, Log analysis module and security module. Khoumsi et. al [2018][5] describes automata-based method for analyzing firewall security policies. Their experiment includes design procedure for policy implication, detection of incompleteness in policy and detection of conflicts in the same policies. Mihalos et. al [2019][6] examines network security threats and mechanism, they implement Netfilter / Iptables as security techniques. Mclaren et. al [2019][7] develops MemDecrypt framework for providing security for live file transfer and file content. They include security to remote user credential. Li et al [2019][8] describes network security awareness mechanism, which involves different phases to provide effective cyber security awareness in cyber space. Mondejar et. al [2020][9] presents characterization of linux-based malwares. Their work include automated techniques for classifying malware into related threats. Pandi et al [2020][10] describe threat model called STRIDE for analyzing threat related activities and cyber-attack. Sudhakar et. al [2020][11] analyze fileless malware, they present a process model for fileless malware attack. They include modelling to handle lifecycle of fileless malware, which divides into three phases.

3. METHODOLOGY –

For analysis of Bypassing security control method, first we study each of them which are stated as,

- Bypassing Network Access Control (NAC)
- Bypassing Security software (Antivirus)
- Bypassing Windows OS based security control
- Bypassing Application-level controls

3.1. Bypassing NAC –

This is an old pattern method, introduced and worked on basis of 802.1x IEEE standard. A basic NAC technique acquire the control to place security at right place where it prevents intruder to enter into network. Some time it is hard for pent-tester or attacker to bypass this type of method as it more advances in two ways as,

3.1.1. Pre-admission NAC

3.1.2. Post-admission NAC

As shown in **fig.2**. All security controls, which are placed according to security requirement for addition of new network device. Here attacker always try and many times they become successful to add their own network device (element) to targeted network. So that they bypass restriction set by NAC on Kali linux environment.

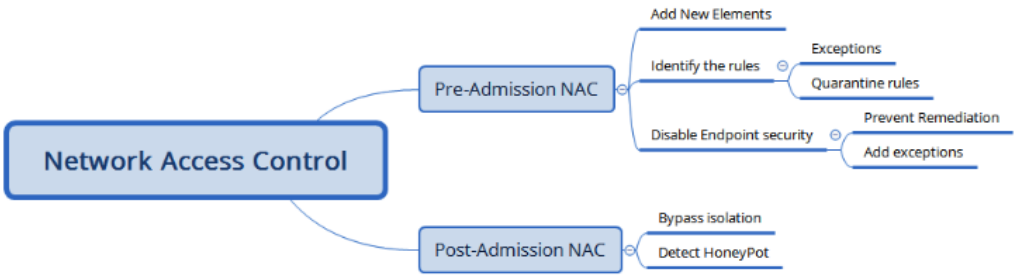

Fig. 2 Working of NAC

3.2. Bypassing security software (Antivirus) –

Security software is major obstacle for attacker as all activities can log by this software. Usual antivirus software are relies on various pattern of signature for matching with intrusion activity (like attacked by ransomware, viruses and trojan). Attacker identifies this pattern and use Metasploit framework that allows standalone executable files to bypass this type of detection. Pen-tester or attacker uses various kind of tools for antivirus evasion some of them are describes as,

3.2.1. Using Veil framework –

It provides effective protection for detection of any exploits for server and endpoints. As shown in **fig. 3.** Veil has main menu for selection and payload purpose.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

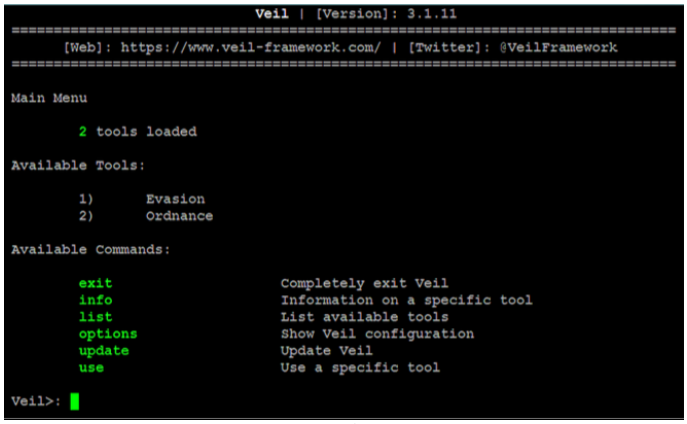

Fig. 3. Veil framework

3.2.2. Using Shellter tool –

This is another tool used by various attacker for antivirus evasion. It generally use to inject shell code into any windows application based on 32bit. Fig. 4. Shows Shellter operation mode.

Fig. 4. Modes of Shellter

3.2.3. Fileless techniques for antivirus evasion –

This type of bypass techniques is based on network port pattern. It depends on various maturate organization that provide firewall security basis on port number range, like traditional as 4444, 5444 or port number apart from 80 or 443. So, attacker bypass this traditional way and use simple technique to implement port number i.e., 80 or 443 for listening from all clients connected in network.

3.3. Bypassing Windows OS based security control –

It is common to use windows Operating system (OS) in day today life work. As it is common, pen-tester and attacker both targeting that system. So they uses different ways to bypass security controls some of them are discussed as,

3.3.1. User Access Control (UAC) –

In recent researches, it is found out that there are 52 different ways to bypass windows UAC. As windows administrator build their policy based on Always notify, notify me when program make changes, notify me when program make changes without notifying on desktop and last Never notify. To bypass this attacker just know that who is user identified by system and what types of rights that user have. Following fig. 5. Shows output of running whoami / groups on C:\>

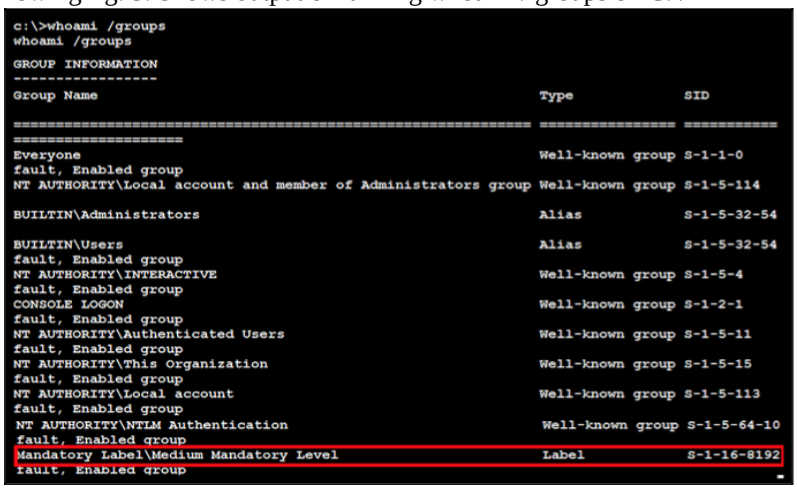

Fig. 5. Output of whoami

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

3.3.2. Using Fileless technique –

This technique use by attacker whenever windows is focused to scanning of all external files coming from outside of system network. This technique based on shell access attack, which include addition of malicious code in existing executable files for attack purpose. Details of shell attack is shown in following fig. 6.

```
meterpreter > upload /root/chap09/test.ps1 c:/windows/temp
[*] uploading  : /root/chap09/test.ps1 -> c:/windows/temp
[*] uploaded   : /root/chap09/test.ps1 -> c:/windows/temp\test.ps1
meterpreter > shell
Process 7316 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17134.472]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> powershell c:\windows\temp\test.ps1
powershell c:\windows\temp\test.ps1
```

Fig. 6. Use of PowerShell

3.3.3. Using fodhelper method –

This is executable file use by windows to managed windows features in setting option. Attacker use the same files to bypass UAC by manipulating the user roles in administrator group.

3.4. Bypassing application-level method –

After getting into system, attacker or pen-tester always use these techniques to get control over various application for this they use various techniques as,

3.4.1. Using SSH to get tunnel out firewall –

Attacker added themselves in internal network to hideout from firewall policies using tunnel past technique on implementation of SSH (Secure Shell).

3.4.2. Bypassing URL filter technique –

By using SSH or PowerShell, attacker can intermediate between network connection and port forwarding method. It is used to bypass any restriction applied by security policy. Following Fig. 7 shows implementation of PUTTY tool for the above mentioned task.

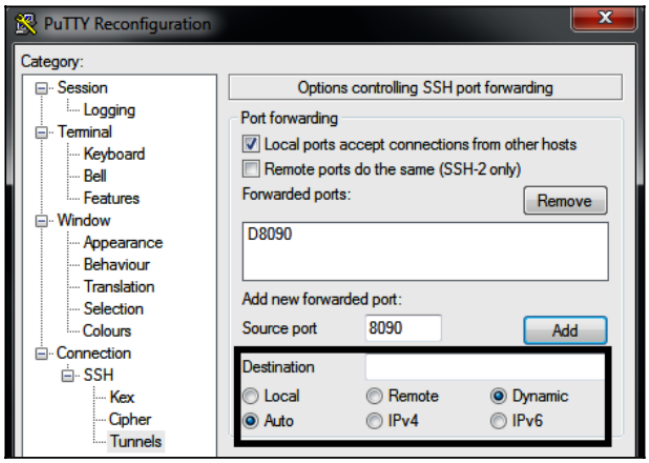

Fig. 7. PUTTY tool

4. IMPLEMENTATION –

After getting all this details about different methods of bypassing security controls. We initiated virtual environment using virtual box 6.2.0 having platform of Kali Linux 2020 as guest system. We install all mentioned tool in section 3 a start operating on that parameter. Following Fig. 8 shows virtual environment of kali linux using virtual box. We calculated different value based on parameters like using tunneling for bypass firewall, evasion of antivirus using Shellter in stealth mode. We tried fodhelper.exe file on Windows 10 platform. Finally, by manipulating inbound and outbound rules we tried bypass application-level controls.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

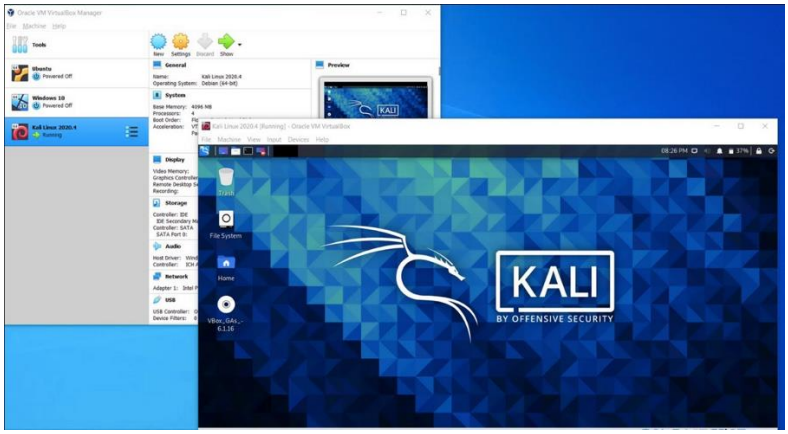

Fig. 8. Kali Linux in virtual environment

5. RESULT AND EVALUATION –

By studying various factors and implementation in section 4, we perform the effective analysis of all these four bypass methods on various factors shown in following fig.9

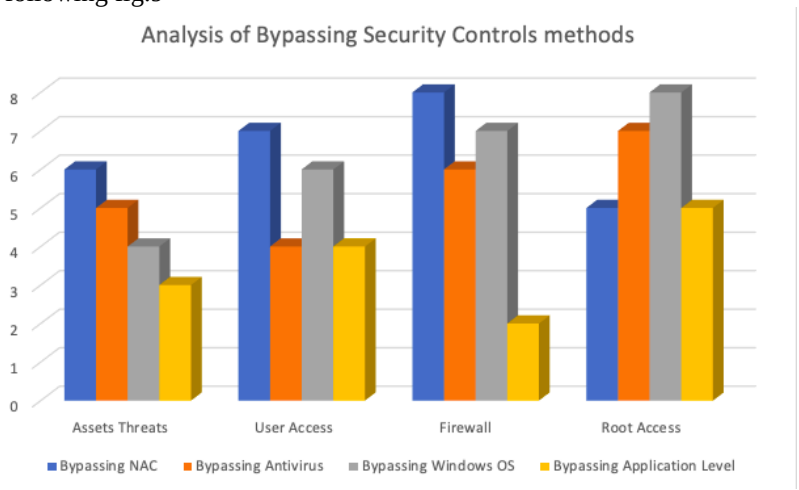

Fig. 9. Analysis of bypassing security controls

As shown in above fig. 9, it shows all methods are utilize on base of four factors i.e., Assets threats, user access, firewall and root access. Where Root access has top priority by all one to get administrator access of network-oriented system. Secondly firewall is most attacked factor in both Linux and Windows operating system. Application-level bypass need already penetrated system, so it had minimum bypass hits.

6. CONCLUSION AND FUTURE WORK –

We go through deep level into systematic way for overcoming techniques to bypass security controls. We described different way of bypassing NAC in both pre-admission and post-admission manner. We explained antivirus bypass techniques with two effective tool i.e., Veil and Shellter. Bypassing windows security tool is most common technique acquired by attacker or pen-tester that we focused in this study. Finally, we focus on application level bypass method, that is impressively used by attacker and for that already exploit system is needed. In future, we plan to implement a secure kernel for Linux to overcome bypass method as mentioned in research paper. With this we focused to upgrade firewall policy in view of bypassing itself by attacker.

REFERENCE:

[1]. Veil - Framework -. (2022). Retrieved 30 January 2022, from https://www.veil-framework.com/
[2]. Shellter | Shellter. (2022). Retrieved 30 January 2022, from https://www.shellterproject.com/introducing-shellter/
[3]. Costa Júnior, Edmilson P. da, Carlos Eduardo da Silva, Marcos Pinheiro, and Silvio Sampaio. 'A New Approach to Deploy a Self-Adaptive Distributed Firewall'. *Journal of Internet Services and Applications* 9, no. 1 (December 2018): 12. https://doi.org/10.1186/s13174-018-0083-6.
[4]. Ganji, Hamid Reza, and Kiarash Aghakhani. 'Provides a New Way to Enhance Security in the Linux Operating System'. *Emerging Science Journal* 2, no. 5 (4 November 2018): 295. https://doi.org/10.28991/esj-2018-01153.
[5]. Khoumsi, Ahmed, Mohammed Erradi, and Wadie Krombi. 'A Formal Basis for the Design and Analysis of Firewall Security Policies'. *Journal of King Saud University - Computer and Information Sciences* 30, no. 1 (January 2018): 51–66. https://doi.org/10.1016/j.jksuci.2016.11.008.
[6]. School of Social Sciences, Hellenic Open Unoversity, M. G. Mihalos, S. I. Nalmpantis, Dpt of Electrical Engineering, Eastern Macedonia and Thrace Institute of Technology, Kavala, Greece, K. Ovaliadis, and Dpt of Electrical Engineering, Eastern Macedonia and Thrace Institute of Technology, Kavala, Greece. 'Design and Implementation of Firewall Security Policies Using Linux Iptables'. *Journal of Engineering Science and Technology Review* 12, no. 1 (February 2019): 80–86. https://doi.org/10.25103/jestr.121.09.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

[7]. McLaren, Peter, Gordon Russell, William J. Buchanan, and Zhiyuan Tan. 'Decrypting Live SSH Traffic in Virtual Environments'. *Digital Investigation* 29 (June 2019): 109–17. https://doi.org/10.1016/j.diin.2019.03.010.
[8]. Li, Yan, Guang-qiu Huang, Chun-zi Wang, and Ying-chao Li. 'Analysis Framework of Network Security Situational Awareness and Comparison of Implementation Methods'. *EURASIP Journal on Wireless Communications and Networking* 2019, no. 1 (December 2019): 205. https://doi.org/10.1186/s13638-019-1506-1.
[9]. Carrillo-Mondéjar, J., J.L. Martínez, and G. Suarez-Tangil. 'Characterizing Linux-Based Malware: Findings and Recent Trends'. *Future Generation Computer Systems* 110 (September 2020): 267–81. https://doi.org/10.1016/j.future.2020.04.031.
[10]. Pandi (Jain), Gayatri S, Saurabh Shah, and K.H. Wandra. 'Exploration of Vulnerabilities, Threats and Forensic Issues and Its Impact on the Distributed Environment of Cloud and Its Mitigation'. *Procedia Computer Science* 167 (2020): 163–73. https://doi.org/10.1016/j.procs.2020.03.194.
[11]. Sudhakar, and Sushil Kumar. 'An Emerging Threat Fileless Malware: A Survey and Research Challenges'. *Cybersecurity* 3, no. 1 (December 2020): 1. https://doi.org/10.1186/s42400-019-0043-x.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)