International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, Vol. 3(4), 2025
DOI: 10.61359/11.2206-2555

AI-based Deployment of Efficient Custom Backdoor in Virtual Environment

Dr. A. Ayyasamy*

Email Correspondence*: samy7771@gmail.com

*Department of Computer Engineering, Alagappa Government Polytechnic College, Karaikudi, Sivagangai District, Tamil Nadu, India.

Abstract:

The aim of this paper is to deploy a custom backdoor on to a target machine (Metasploit/Windows) from the source machine (Kali Linux) in a virtual environment (Hypervisor -Windows). For the Virtual system, a wired network is used. The overall goal of the project is to deploy malware such as a backdoor, on devices connected to the infected network, to highlight the threat posed by such malicious software. This work proposes a framework for the AI-based deployment of effective custom backdoors within a virtualized environment. The local virtualization platforms have leveraged to create scalable, isolated, and reproducible sandboxes for backdoor research. This is achieved by carrying out an ARP (Address Resolution Protocol) spoofing attack. It is followed by manipulation of DNS (Domain Name System) server response to redirect the victim to a malicious site or intercept HTTP (Hyper-Text Transfer Protocol) response to enable downloading of malicious files on the target system. Hence, the trojan downloaded can be of any form, like a key-logger or Backdoor. The Backdoor will help us get full system access to the target site and we will be able to download and upload files on or from the target machine, thus effectively creating a backdoor.

Keywords: HTTP, DNS, ARP, Kali Linux, AI, Virtual Environment.

1. Introduction

This paper addresses the security problem of the necessity of providing fundamental protection and security mechanisms against malwares that may attempt to hijack and take over a secure system. To this aim, we have tried to deploy malware such as a backdoor on devices connected to the infected network to show how easily users can be targeted by malicious hackers to achieve this by carrying out an ARP spoofing attack followed by manipulated DNS server response to redirect the victim to a malicious site or intercept HTTPS response to enable downloading of malicious files on the target system. The trojan hence downloaded can be of any form, like a key-logger or Backdoor. The Backdoor will help us get full system access to the target site and we will be able to download and upload files on / from it. The aim was to successfully implement these attacks and to analyse the possible prevention and detection techniques. The main objective of this project is to deploy malware such as a backdoor on devices connected to the infected network on a self-made local target machine by the attacking machine; to highlight the threat they pose [1]. ARP spoofing [2], also known as ARP cache poisoning or ARP poison routing, is a method wherein a hacker transmits (spoofed) Address Resolution Protocol (ARP) packets over a LAN. The goal is to link the hacker's MAC address to the IP address of some host, like the default gateway, and so any communications intended to and from the IP address is then delivered to the hacker. A hacker can gain access to data

*Department of Computer Engineering, Alagappa Government Polytechnic College, Karaikudi, Sivagangai District, Tamil Nadu, India.

Article Timeline: Received: Dec 09, 2025; **Revised:** Dec 14, 2025; **Accepted:** Dec 15, 2025; **Published:** Dec 15, 2025

packets on a connection, change network traffic, or block all transmission via ARP spoofing. Initially, we will send a falsified ARP to the victim, to masquerade as the router.

Packet sniffing [3] is an approach for identifying and observing packet data travelling over a network. Packet sniffing techniques are used by server admins to analyze and verify network activity, but malicious actors are using these techniques for malicious reasons. The attacking computer will be able to view incoming and outgoing packets from the victim device, enabling phishing. DNS spoofing, also known as DNS cache poisoning, is a type of digital network breach wherein malicious Domain Name System information is inserted inside the cache of a DNS resolver, leading the hostname to provide an inaccurate response report, such as an IP address. The attacker is now lodged in between the server and victim as a man-in-the-middle, thus enabling it to redirect the victim's legitimate queries to fraudulent websites.

Whenever Hypertext Transfer Protocol (HTTP) [4] headers get automatically created depending on user interaction, a type of web service security issue arises, which is known as HTTP header injection. Using HTTP File Injection, we will guide the user to download a malicious file to load a trojan onto the system. Once the backdoor is in place, files can be uploaded, downloaded, and manipulated as desired by the attacker.

2. Related Works

The backdoor exploits a vulnerability in the operating system and is implemented with the reverse TCP payload. The OS flaw that is exploited is that the system firewall only examines incoming traffic and not the outgoing traffic. The user initiates a connection in the reverse TCP payload. In the attack, the payload is uploaded by the attacker in the server and an email containing the link to the payload is sent to the user. Social engineering toolkit is used to make the email look legitimate. Once the payload is executed, the attacker can access files, sniff packets et cetera [5].

The most popular open-source tool for penetration testing and carrying out various exploitative simulated attacks is Kali Linux. The paper investigates the most frequent and popular security attacks including SQL injection, cross site scripting and WPA2, all of which were implemented using Kali Linux. The results showed that the attacks launched both on web and firewall were conducted successfully. The machine for the simulated attacks had the following specs – Intel core i5, 8GB RAM and Kali Linux was used through virtual machine [6].

The attacks studied war: USB malware attacks, drive-by download attacks and backdoor malware attacks. Backdoor attacks are undetected when the firewall was used with its default configuration settings [7]. Thousands of gadgets are linked to the Web every day. Personal information of individuals and large corporations, like customer financial transactions, health-related data, social media data, and so on, is available on the Web. Because anything is available over the internet, the security of electronic information has become a major problem. Malicious hackers use vulnerabilities to breach computers by targeting software weaknesses. Attack tactics, vulnerability concepts, and defensive strategies must all be thoroughly explored in order to create improved approaches to secure computerised systems [8]. Honeypots are commonly employed to improve the integrity of the organisational setup and will specifically monitor activity directed at themselves. Until it communicates directly with the other device, a honeypot would not be able to identify an attack [9].

TCP is a connection-oriented protocol that is used to send data over the Web. The use of reverse TCP attacks to target the connection mechanism is a fairly recent technique. The hacker attempts to get remote access to the network of the victim end user. To create the connection, this assault relies heavily on skilled

social engineering tactics to identify particular individuals [10]. Penetration testing helps to secure networks and highlights the security issues. In this paper, the authors investigate various aspects of penetration testing including tools, attack methodologies, and defense strategies. More specifically, we performed different penetration tests using a private networks, devices, and virtualized systems and tools. We used tools within the Kali Linux suite [11]. To help avoid APT attacks, the paper examines and analyses a substantial proportion of publicly published APT attack scenarios, as well as providing an outline of the APT attack process and assault strategies [12]. Smart edge computing solutions based on collaborative learning are extensively used in numerous contexts, thanks to the phenomenal growth of mobile Internet and deep learning (DL) [13].

3. Proposed Work

The proposed framework establishes an integrated, automated framework for the development, deployment, and analysis of effectual stealth backdoors in machine learning models, all within a secure and scalable virtualized environment. At its core, the system is orchestrated by an intelligent AI agent which manages a unified three-phase pipeline, transforming the complex process of backdoor engineering from a manual, ad-hoc endeavor into a reproducible and systematic security assessment tool. The steps that were followed are given below. They can be broken down into five key steps.

Step 1: ARP Spoofing

ARP spoofing, also known as ARP cache poisoning or ARP poison routing, is a method whereby a hacker transmits (spoofed) Address Resolution Protocol (ARP) packets over a LAN. The goal is to link the hacker's MAC address to the IP address of some host, like the default gateway, and so any communications intended to and from the IP address is then delivered to the hacker. A hacker can gain access to data packets on a connection, change network traffic, or block all transmission via ARP spoofing. The assault is frequently used as a springboard for other types of attacks, such as denial of service, man-in-the-middle, and session hijacking. Initially, we will send a falsified ARP to the victim, to masquerade as the router.

Step 2: Packet Sniffing

Packet sniffing is an approach for identifying and observing packet data travelling over a network. Packet sniffing techniques are used by server admins to analyze and verify network activity, but malicious actors are using these techniques for malicious reasons. The attacking computer will be able to view incoming and outgoing packets from the victim device, enabling phishing. The attacking computer will be able to view incoming and outgoing packets from the victim device, enabling phishing.

Step 3: DNS Spoofing

DNS spoofing, also known as DNS cache poisoning, is a type of digital network breach wherein malicious Domain Name System information is inserted inside the cache of a DNS resolver, leading the hostname to provide an inaccurate response report, such as an IP address. The attacker is now lodged in between the server and victim as a man-in-the-middle, thus enabling it to redirect the victim’s legitimate queries to fraudulent websites.

Step 4: HTTP File Injection Response

Whenever Hypertext Transfer Protocol (HTTP) headers get automatically created depending on user interaction, a type of web service security issue arises, which is known as HTTP header injection. HTTP response splitting, session fixation via the Set-Cookie header, cross-site scripting (XSS), and malicious

redirect attacks via the location header are all possible with header injection in HTTP replies. We will guide the user to download a malicious file to load a trojan onto the system.

Step 5: Backdoor Implemented

Once the backdoor is in place, files can be uploaded, downloaded, and manipulated as desired by the attacker.

The workflow provides a basic outline of the detailed steps that we undertook, to implement and deploy the backdoor. It starts from the beginning, with the first being ARP spoofing. Then, the Packet sniffer gains access to incoming and outgoing data. Thereafter, the DNS response is manipulated is demonstrated in Figure 1.

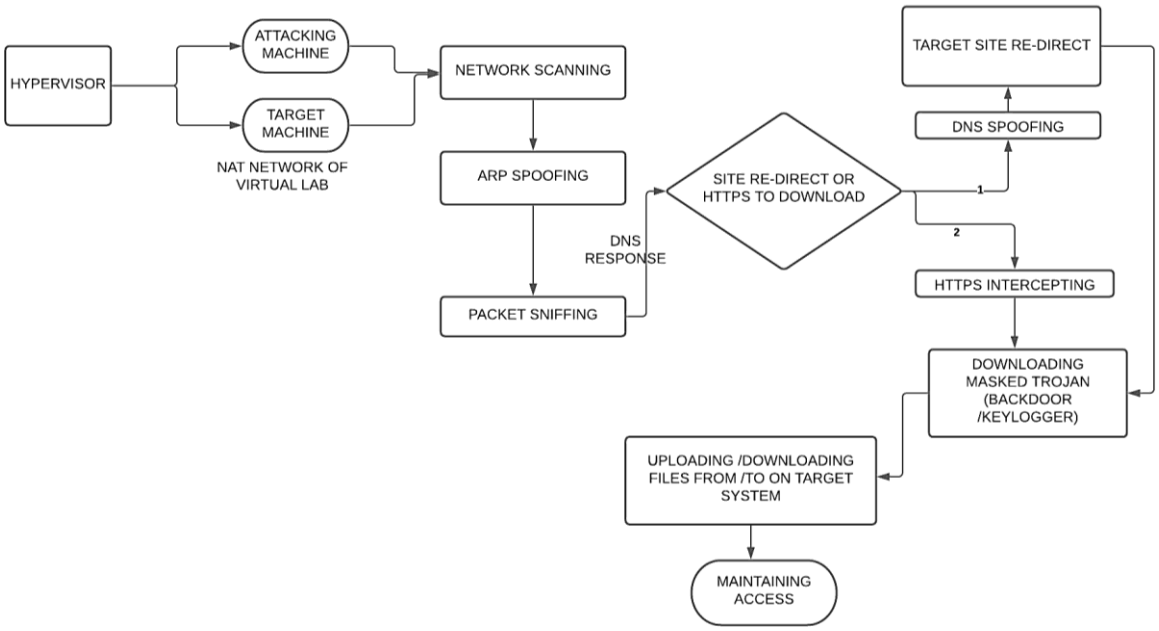

Figure 1. Workflow

4. Performance Evaluation

The Address Resolution Protocol (ARP) is a network communication protocol that allows network communications to reach a specific network device. ARP converts Internet Protocol (IP) addresses to Media Access Control (MAC) addresses and the other way around. ARP is most typically used by devices to communicate with the router or gateway that allows them to connect to the Internet. An ARP spoofing attack, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept network device communication. The constant ping spoofs the systems on both ends and makes them reset their IP tables. This is very provident in seeing the mac- address for the router change to the one on Kali, with "arp- a" command, reason being the IP-address is spoofed to be that of Router but in real the mac-address of the actual device will not change. This is the reason ARP is also really unreliable attack to gain access cause if there are programs on system to check for un-authorized devices or the new routers, then we can see that this attack might actually fail to work. The malicious website is frequently used to infect a user's computer with worms or viruses, granting the perpetrator long-term access to the computer and the data it stores. Attackers utilise DNS spoofing to carry out attacks, which usually involve stealing sensitive user data. Legitimate businesses, on the other hand, use DNS spoofing from time to time. Some internet

service providers (ISPs) have used DNS spoofing to enforce restrictions and for advertising purposes and the result is demonstrated in Figure 2. Creating customised backdoor executables often takes an extended period of time to do manually. When we say any executable, it means any executable file format of windows (.exe). In terms of malware, we have implemented a Backdoor which grants us access to the system , every time the system is connected to the web, and the Implemented attack is illustrated in Figure 3.

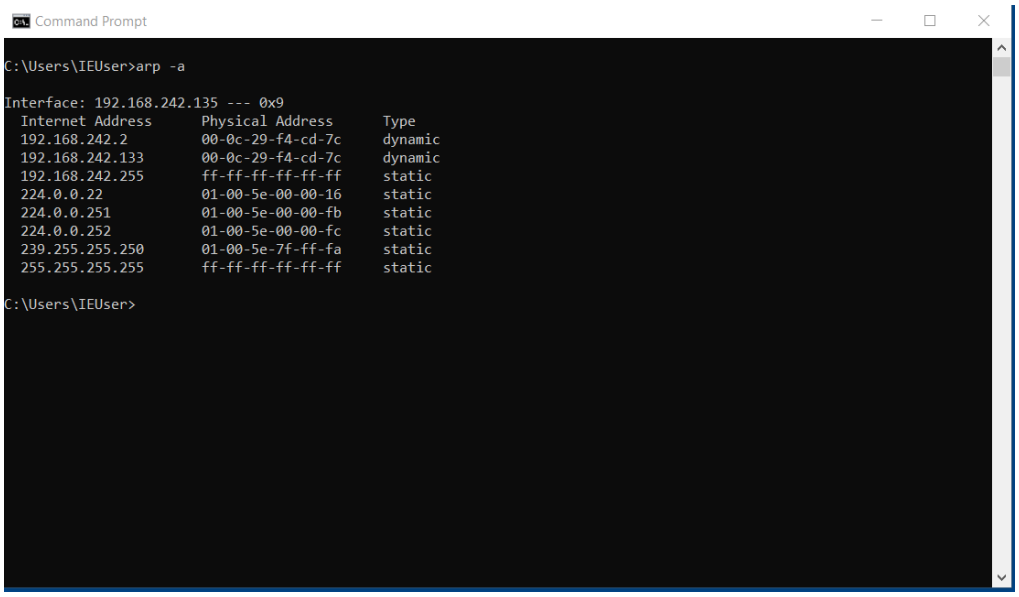

Figure 2. ARP- table of the Windows Machine after Attack

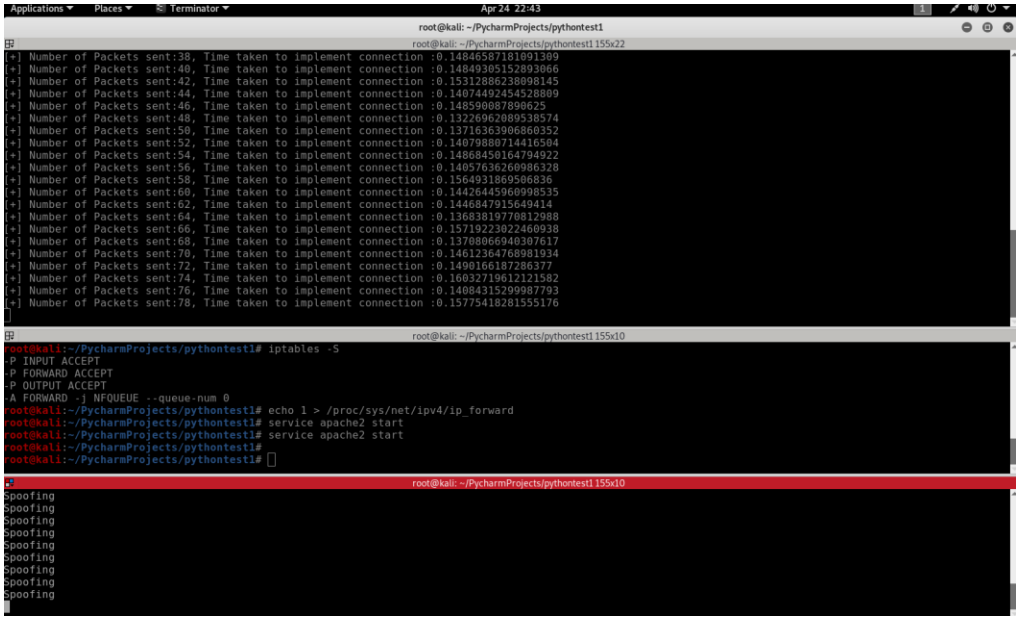

Figure 3. Implemented attack.

There are several methods and procedures one may adopt, to avoid having their wi-fi hijacked. This comprises the following:

1. If possible, utilise WPA2 (WPA2-AES).
2. Do not ever utilise WEP for wireless security since it is extremely unsafe.
3. Never make use of any existing terms as the wi-fi password.
4. Conceal the SSID, and wi-fi network's name, in the router's configuration.

Utilise the router's screening functionality, which enables users to specify which MAC addresses are permitted to join.

5. Conclusion

In conclusion, the web server has been penetrated by simulating the HTTP injection, ARP Spoofing etc. In the attack, the target machine was exploited with Metasploit. Our testing platform and payloads were able to effectively assume charge of the victim's machine. Even though anti-virus solutions might make a significant impact in the effectiveness of any system's protection against malicious hackers, no machine can outsmart the human mind, and human blunders must be at the root of how such sorts of attacks occur. IT executives ought to be conscious of the significance of penetration testing. With the rise of technology, cybersecurity is becoming a particularly tough subject, not just for businesses but also for consumers. It is time to acknowledge that simply having an antivirus is not enough to keep systems safe. Nowadays, a person is more likely to experience digital threats than any other physical threat. Taking the steps indicated in the protective measures is the ideal way to provide excellent defence against future threats. Future investigations will look into how this shift in security rules may evolve toward a society with less cybercrime as a consequence of human mistake and a failure to communicate for competitive advantage.

6. References

[1] Lai, T.-L., & Tsai, M.-H. (2021). Design and implementation of a DNS server with geolocation capability. In 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 370–373). IEEE.

[2] S. N., A. K. V., & Krishnakumar, S. (2023). Detection of ARP spoofing attacks in software defined networks. In 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS) (pp. 422–426). IEEE.

[3] Ali, M. L., Ismat, S., Thakur, K., Kamruzzaman, A., Lue, Z., & Thakur, H. N. (2023). Network packet sniffing and defense. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 499–503). IEEE.

[4] Calzarossa, M. C., & Massari, L. (2014). Analysis of header usage patterns of HTTP request messages. In 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS) (pp. 847–853). IEEE.

[5] Aslan, Ö. (2022). Computer system and third-parties vulnerabilities increases the risk of cyber attacks.

[6] Atwell, C., Blasi, T., & Hayajneh, T. (2016, April). Reverse TCP and social engineering attacks in the era of big data. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 90–95). IEEE.

[7] Denis, M., Zena, C., & Hayajneh, T. (2016, April). Penetration testing: Concepts, attack methods, and defense strategies. In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1–6). IEEE.

[8] Javid, F., & Lighvan, M. Z. (2021). Honeypots vulnerabilities to backdoor attack. In 2021 International Conference on Information Security and Cryptology (ISCTURKEY) (pp. 161–166). https://doi.org/10.1109/ISCTURKEY53027.2021.9654401.

[9] Gunawan, T. S., Lim, M. K., Kartiwi, M., Abdul Malik, N., & Ismail, N. (2018). Penetration testing using Kali Linux: SQL injection, XSS, WordPress, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science.

[10] Li, M., Huang, W., Wang, Y., Fan, W., & Li, J. (2016, June). The study of APT attack stage model. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS) (pp. 1–5). IEEE.

[11] Nicho, M., Oluwasegun, A., & Kamoun, F. (2018). Identifying vulnerabilities in APT attacks: A simulated approach. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1–4). https://doi.org/10.1109/NTMS.2018.8328696.

[12] Kolli, Y., Mohd, T. K., & Javaid, A. Y. (2018). Remote desktop backdoor implementation with reverse TCP payload using open source tools for instructional use. In 2018 IEEE International Conference on Electro/Information Technology (EIT) (pp. 249–254). https://doi.org/10.1109/EIT.2018.8500174.

[13] Zhao, Y., Xu, K., Wang, H., Li, B., & Jia, R. (2021). Stability-based analysis and defense against backdoor attacks on edge computing services. IEEE Network, 35(1), 163–169. https://doi.org/10.1109/MNET.011.2000265.

7.Conflict of Interest

The authors declare that there are no conflicts of interest associated with this article.

8.Funding

No funding was received to support this study.