



**A Comprehensive Study on the Vulnerabilities and Mitigation Strategies on
Network Switches**

by

Rohan Ravindra Chavan
2212517

Supervisor: Kapilan Radhakrishnan

Second Marker: Munyaradzi Nicholas Murira

Project submitted as part of the requirements for the award of MSc Cyber
Security and Digital Forensics

February 2024

Abstract:

In the realm of digital communication, securing network infrastructure against a wide array of vulnerabilities and cyber threats is paramount for ensuring the integrity and confidentiality of data. This dissertation explores the intricate vulnerabilities present at the Data Link Layers of the Open Systems Interconnection (OSI) model, focusing on the impact and mitigation of network attacks such as MAC flooding, ARP spoofing, DHCP starvation, and VLAN hopping. Through a comprehensive analysis of these vulnerabilities, this study aims to shed light on the multifaceted nature of network security challenges and to propose effective strategies for enhancing network resilience.

Utilizing simulation tools like EVE-NG, this research conducts practical simulations of the network attacks, providing a vivid illustration of their mechanisms, impacts, and potential countermeasures. The simulations employ tools such as macof, ettercap, and yersinia to emulate attack scenarios in a controlled environment, thereby offering invaluable insights into the dynamics of network vulnerabilities and the effectiveness of various mitigation techniques.

The study proposes a suite of mitigation strategies, including the implementation of dynamic ARP inspection, port security, and DHCP snooping, aimed at fortifying the network against Layer 2 attacks. Furthermore, it emphasizes the importance of regular network audits, real-time monitoring, and the education and training of IT staff as crucial components of a comprehensive network security framework.

This dissertation contributes to the ongoing discourse on network security by providing a detailed examination of Layer 2 vulnerabilities and their implications for network integrity and performance. The findings highlight the necessity of adopting a proactive, informed, and multifaceted approach to network security. By offering practical insights and advanced security protocols, this research aims to assist network administrators, cybersecurity professionals, and policymakers in safeguarding digital networks against the evolving landscape of cyber threats, ensuring the security and integrity of digital communications in the contemporary digital era.

Table of Contents

Chapter 1:	4
1.1 Introduction	4
1.3 Relevance of Study:	5
1.4 Target Beneficiaries:	5
Chapter 2.0: Methodology	5
2.1 Literature Review	5
2.2 Simulation Environment Setup	5
2.3 Data Collection and Analysis	6
2.4 Ethical Considerations	6
2.5 Conclusion	6
3.1 Attack 1	7
3.3 Attack 3	13
3.4 Attack 4	17
3.5 Attack 5	21
Chapter 4:	30
4.1 Recommendations for Network Administrators:	30
Chapter 5:	31
Chapter 6:	31
References:	32

Chapter 1:

1.1 Introduction

In the evolving landscape of digital communication, the security of network infrastructure stands as a paramount concern for enterprises and individuals alike. The foundational architecture of these networks, governed by the Open Systems Interconnection (OSI) model, delineates a framework wherein each layer presents unique vulnerabilities and attack vectors. This dissertation delves into the intricacies of network security, with a particular focus on the vulnerabilities inherent to Layer 2 (Data Link Layer) in facilitating network interconnectivity.

The ubiquity of networking devices such as hubs and switches, which operate at the Physical and Data Link layers respectively, underscores the complexity of securing network traffic. Hubs, with their simplistic operation of broadcasting data packets to all connected devices, and switches, which intelligently direct packets using Media Access Control (MAC) addresses, illustrate the spectrum of network design philosophies from the minimalistic to the complex. However, the sophistication of switches does not exempt them from vulnerabilities, as evidenced by attacks like MAC flooding and ARP spoofing, which exploit the fundamental mechanisms of Layer 2 operations to disrupt network integrity and security.

Moreover, the dissertation explores the implications of such attacks, including Man-in-the-Middle (MITM) and Distributed Denial of Service (DDoS) attacks, which leverage the weaknesses at Layer 2 to intercept or disrupt the flow of information. These attacks not only compromise the confidentiality and integrity of data but also highlight the limitations of existing network security protocols, which often lack the robustness to withstand sophisticated cyber threats.

The transition from theoretical vulnerabilities to practical exploitation is demonstrated through the utilization of simulation environments such as EVE-NG, which facilitates the replication of complex network setups and the deployment of attack vectors in a controlled manner. Tools such as macof, ettercap, and yersinia become instrumental in this context, enabling the simulation of attacks like MAC flooding, ARP spoofing, and others, thereby providing valuable insights into their mechanics, impact, and mitigation strategies.

This comprehensive investigation into network vulnerabilities, particularly at Layers 2 of the OSI model, serves not only to highlight the critical need for security measures but also to propose strategic improvements in network security practices. Through a combination of simulation-based evaluations and theoretical analysis, this dissertation aims to bridge the gap between academic research and practical network security, offering a blueprint for enhancing the resilience of network infrastructures against an ever-evolving landscape of cyber threats.

In summary, this dissertation examines network security to illuminate digital communication's multiple issues. This study contributes to network security by dissecting the core OSI model weaknesses and using a comprehensive approach to mitigate them. In addition, it supports the concept that digital communications will be protected from the many cyber threats that are increasingly arriving in this digital age.

1.2 Dissertation Focus and Scope

Aim: A Comprehensive Study on the Vulnerabilities and Mitigation Strategies on Network Switches

Objectives:

1. To identify and analyze the vulnerabilities present on switches.
2. To explore and evaluate the impact of various network attacks, including MAC flooding, ARP spoofing, DHCP starvation, and VLAN hopping.
3. To simulate network attacks using tools like macof, ettercap, and yersinia in controlled environments to understand their mechanisms and impacts.
4. To review and propose effective mitigation strategies, such as dynamic ARP inspection, port security, and DHCP snooping, for enhancing network security.
5. To assess the effectiveness of these mitigation strategies through practical simulations.

1.3 Relevance of Study:

This study addresses the critical need for robust network security protocols in the digital age, where cyber threats are becoming increasingly sophisticated. By focusing on the vulnerabilities on switches, it provides a comprehensive understanding of potential attack vectors and offers practical solutions to safeguard digital communications.

1.4 Target Beneficiaries:

1. Network Administrators and IT Security Professionals: Who can apply the findings to enhance the security and integrity of their networks.
2. Cybersecurity Researchers: Who are interested in the detailed analysis of network vulnerabilities and the effectiveness of various mitigation strategies.
3. Academic Institutions and Students: Engaged in cybersecurity studies looking for comprehensive research on network security challenges and solutions.
4. Organizations and Enterprises: That depend on secure network infrastructures for their operations and are seeking ways to protect their data and services from cyber threats.
5. Policy Makers and Regulatory Bodies: Interested in understanding network vulnerabilities to develop better guidelines and standards for network security.

Chapter 2.0: Methodology

The methodology section of this dissertation outlines the systematic approach adopted to investigate the vulnerabilities present on switches, with a focus on Layers 2 and to evaluate the effectiveness of different mitigation strategies against network attacks such as MAC flooding, ARP spoofing, DHCP starvation, and VLAN hopping. This comprehensive study leverages both theoretical analysis and practical simulations to bridge the gap between academic research and real-world network security challenges.

2.1 Literature Review

A thorough literature review was conducted to establish a solid theoretical foundation for the study. This involved the examination of peer-reviewed articles, Conference papers, Journal proceedings, Industrial websites and textbooks that discuss the, network vulnerabilities, attack vectors, and mitigation techniques.

2.2 Simulation Environment Setup

The study utilized EVE-NG (Emulated Virtual Environment Next Generation) as the

primary tool

for creating a simulated network environment. This virtualization platform allowed for the replication of complex network configurations, enabling the testing of various attack scenarios and mitigation strategies under controlled conditions. The simulation environment included the following components:

- **Network Devices:** Cisco Router and Switches were used.
- **Attack Tools:** Tools such as macof (for MAC flooding attacks), Yersinia (for VLAN hopping attacks), and Ettercap (for ARP spoofing attacks) were employed to execute and analyze the impact of cyberattacks on network security.
- **Mitigation Techniques:** Security features such as port security, DHCP snooping, Dynamic ARP Inspection (DAI), and BPDU Guard were implemented and tested for their effectiveness in mitigating the identified attacks.

2.3 Data Collection and Analysis

Data was collected through the simulation of network attacks and the application of mitigation strategies. Key performance indicators (KPIs) such as CPU utilization, CAM table entries, network traffic patterns, and packet loss rates were monitored to assess the impact of attacks and the effectiveness of security measures. The analysis involved comparing network performance and security before and after the application of mitigation strategies to determine their efficacy.

2.4 Ethical Considerations

The study adhered to ethical guidelines to ensure that all simulations were conducted responsibly. Measures were taken to prevent any real-world implications or access to unauthorized networks. The research focused solely on simulated environments, and all findings were presented in a manner that promotes network security and awareness without enabling malicious activities.

2.5 Conclusion

This methodology enabled a comprehensive examination of network vulnerabilities and the assessment of mitigation strategies' effectiveness, contributing valuable insights to the field of network security. Through a combination of theoretical research and practical simulations, this study provides a holistic view of the challenges and solutions in protecting networks against cyber threats.

Chapter 3:

Literature Review:

At the physical layer (Layer 1) of the Open Systems Interconnection (OSI) model, a hub is a fundamental networking device that operates. It acts as a central connection point for devices that are part of a network, meaning that it broadcasts incoming data packets to all other devices that are connected to the network without making any distinctions. As a result of this lack of data filtering, several network inefficiencies may occur, including data collisions and security vulnerabilities. This is because every device that is connected to the hub is required to analyse each packet in order to know who the packet is meant for. [1]

On the other hand, switches are more sophisticated in terms of managing network traffic since they operate at the data link layer (Layer 2) of the Open Systems Interconnection (OSI) model. This allows them to handle more traffic than other types of switches. The devices that are part of a network are linked to it, and it makes use of media access control (MAC) addresses in order to intelligently

transport data packets only to the areas where they are meant to go. creating direct, point-to-point communication channels between devices enables switches to reduce irrelevant network traffic, minimise collision rates, and increase network performance and security. This is accomplished by creating communication channels between devices. Switches also reduce the amount of unnecessary network traffic that is sent across the network. [1]

Man-in-the-middle attacks: Sometimes known as MITM attacks , is a kind of cyberattack that may be carried out using mac flooding attack. The communication that is taking place between two parties that believe they are communicating directly with one other is subject to this form of attack, in which the attacker secretly intercepts and maybe modifies the communication that is taking place between them. An example of this kind of active eavesdropping is when an attacker intercepts command or measurement signals that are being sent across a communication channel that has been compromised, and then perhaps re-transmits them. The attacker now has the capacity to control the whole communication process they are attempting to manipulate. The attacker has the ability to introduce arbitrary instructions and falsify measurements without the system operators being able to trace them down. [2]

3.1 Attack 1

MAC Flooding Attacks: MAC flooding is a kind of cyberattack that is carried out with the intention of attacking the essential components of network switches. The Content Addressable Memory (CAM) table is an important component that can be found within network switches. It is responsible for mapping Media Access Control (MAC) addresses to the port numbers that correspond to those addresses. The primary objective of the attack is to take advantage of the limited capacity of the CAM table. By flooding the CAM table with a high number of false MAC addresses, the attackers encourage the table to exceed its maximum capacity and cause it to become overloaded. It is because of this that the table will be unable to contain any legitimate entries for network traffic. However, as a result of this saturation, the switch is compelled to revert to a fundamental mode of operation that is analogous to that of a hub. This mode allows the switch to broadcast incoming packets to all connected ports without making any distinctions between them. Instead of forwarding them to a specific destination based on the MAC address, the switch broadcasts them to all connected ports. This operational modification not only results in the security protocols of the network being compromised, but it also results in a significant fall in the performance of the network, which makes it susceptible to further exploitation. [3]

Consequences of MAC Flooding on Network Integrity and Performance: The consequences of a successful MAC flooding attack go well beyond the inconvenience it causes to operations. If it turns out that the attack is successful, the attack effectively manipulates the switch to permit the transmission of packets through every available port, thereby compromising the network's integrity. The advantages of segmentation that switches often provide in comparison to hubs are thus basically become null and invalid because of this. When this activity is carried out in broadcast mode, it makes it easier for people who are not permitted to access the flow of data. Because of this, attackers are given the ability to passively listen in on critical messages that are being sent across the network. Additionally, the effect of the attack is not restricted to a single virtual local area network (VLAN), but rather it is dispersed across the whole of the network, which increases the possibility that it may cause harm. This is because the attack is distributed throughout the entire network. It is possible that a denial of service (DoS) scenario will emerge as a consequence of the resultant congestion on the network and the high processing strain that is placed on the switch. This scenario would significantly

limit the availability and dependability of the network for users who are permitted to use it without interference. [4]

Utilization of Tools for Executing MAC Flooding Attacks: A well-known example of a tool that was developed particularly for the purpose of carrying out a MAC flooding attack is macof, which is a tool that is included in the dsniff package. macof is a tool that was built to carry out a MAC flooding attack. The execution of such an attack is made much less complicated by the use of these modern technology. This tool is engineered to generate and dispatch a flood of Ethernet frames, each frame with a unique, randomly generated MAC address . As a result of the massive amount of these frames, which are capable of producing up to 155,000 false MAC entries each minute, the CAM table will rapidly find itself flooded. This guarantees that the table will quickly get full with all of the items. Because this tool is able to overload both physical and virtualized network systems, it highlights the significant susceptibility of switches to MAC flooding . [4] [5]

Strategies for Mitigating MAC Flooding Attacks: The strategic installation of port security devices inside switches is an absolute need in order to reduce the risk of attacks that include multiple access control (MAC) floods. Port security effectively reduces the ability of an attacker to flood the CAM table with fake entries by putting a tight limitation on the number of MAC addresses that a port is authorised to learn. In order to achieve this goal, the number of MAC addresses that a port is allowed to learn is restricted. It is possible to configure this restriction in such a manner that it will automatically stop the port once it recognises unusual patterns of traffic, so eliminating the danger that was previously present. Furthermore, the network's defences against attacks of this kind have been significantly strengthened as a consequence of the installation of sticky MAC addresses and protection against packet storms. This has been accomplished by enhancing the network's vulnerability to attacks. In order to provide a powerful defence against the multiple dangers that are presented by MAC flooding, these measures, which guarantee that MAC addresses are securely associated to particular ports and control the traffic volume that is authorised via a port, respectively, are used. [3] [5] [6]

Simulation: EVE-NG was used to simulate mac-flooding attack, from attacker's machine (Kali Linux), vividly illustrates the disruptive potential of MAC flooding attacks. As there was no traffic on the switch, CPU usage was at 0% but switch stop responding on simulation upon the execution of the macof attack from eth0 port.

```
—(root@kali)-[~]
—# macof -i eth0 -n 209388488

Switch#show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 88%; five minutes: 91%
 PID Runtime(ms)      Invoked      uSecs      5Sec      1Min      5Min  TTY Process
-----
Mac Entries for Vlan 1:
-----
Dynamic Address Count   : 50265
Static Address Count    : 0
Total Mac Addresses     : 50265

Total Mac Address Space Available: 209388488
```

The switch's CPU utilization soared to 91%, and the CAM table was inundated with over 50,000 fake MAC addresses within a mere five-minute span as shown in above figures. Not only does this practical example provide evidence that the theoretical vulnerabilities that have been identified in

the literature are accurate, but it also highlights the crucial significance of employing complete mitigation methods in order to protect network infrastructure against MAC flooding attacks.

In summary A comprehensive investigation of MAC flooding attacks, including their operating mechanics, devastating impact on network security and performance, and practical insights from simulations, shows the need for alert defence measures. To prevent MAC flooding, this investigation was conducted. Finally, the investigation shows how crucial these measures are. [3] [4] [5] [6] [7]

3.2 Attack 2

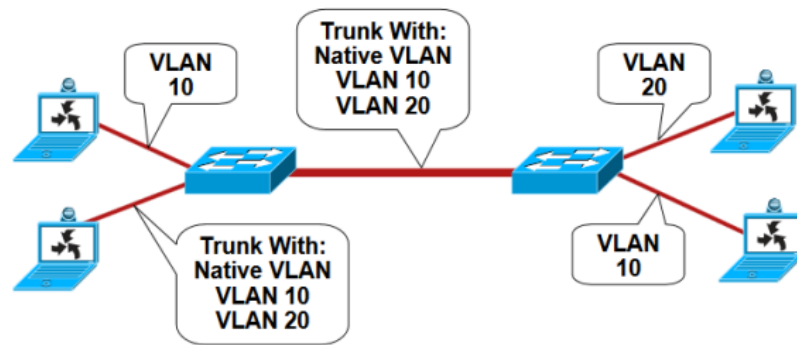
VLAN

Virtual Local Area Networks, more often referred to as VLANs, are networks that are logically break a physical network. The capacity to segment devices based on variables other than physical location, such as the department, the kind of user, or the application, is one of the capabilities of these networks. Virtual local area networks (VLANs) can increase the efficiency of networks as well as their security by segregating network traffic at the Ethernet switch level. [8] [9]

Dynamic Trunking Protocol (DTP): Data Transfer Protocol, sometimes known as DTP, is a proprietary protocol that was created by Cisco. Its purpose is to simplify the process of locating and creating trunk connections between switches. The capability of this device to negotiate trunk configurations and the encapsulation type (Cisco ISL or IEEE 802.1Q) that will be used makes it possible for it to assist the dynamic building of trunk connections in virtual local area networks (VLANs). This protocol is a key component of VLAN hopping attacks since it gives attackers the opportunity to adjust switch settings in order to obtain unauthorised access to traffic across a variety of VLANs for the purpose of gaining access to traffic that is not allowed. [10]

IEEE 802.1Q: In the realm of networking, IEEE 802.1Q is a standard that enables the tagging of virtual local area networks (VLANs) on Ethernet packets. In addition to being one of the kinds of encapsulation that DTP is able to negotiate for trunk lines, it also makes it possible for a large number of virtual local area networks (VLANs) to coexist on the same physical network. This particular standard, which is regarded as being of great significance for VLAN operations, is used by VLAN hopping attacks, which are employed to go over the confines of VLAN isolation. [9]

VLAN Hopping Attack: VLAN hopping is a kind of attack that enables unauthorised access to communication that is moving across many virtual local area networks (VLANs). This type of attack is known as "hopping." Attackers are able to send packets to a virtual local area network (VLAN) that the end system would normally be unable to access. This is accomplished by exploiting vulnerabilities in the configuration of the network, namely the automatic trunking capabilities of switches. One of the methods that might be used to carry out this attack is known as switch spoofing. Through the use of this technique, the adversary is able to get access to all of the virtual local area networks (VLANs) that are linked with a trunk by tricking a switch into making a trunk connection. [9] [11]



Switch Spoofing [12]

Effects on the Network: The core goal of virtual local area networks (VLANs), which is to segment a network for the purpose of increasing administration and security, is instantly undermined by attacks that hop over VLANs. VLANs are a kind of network that are used to separate networks. Due to the fact that it allows attackers to evade the logical separations that exist between the various segments of the network, the practice of VLAN hopping leaves all of the segments of the network vulnerable to the risk of eavesdropping and being accessed without authorization. When this occurs, not only does it violate the secrecy of the data that is going through the network, but it also puts the integrity of the data at jeopardy. This is because it indicates that attackers have the capacity to alter or inject harmful data into the traffic that is flowing through the network. [12]

Tools Used for the Attack: Using Yersinia, a powerful open-source security programme, it is feasible to automate DTP attacks against Cisco switched networks. Utilising the Dynamic Trunking Protocol makes it feasible to conduct out switch spoofing attacks, which in turn makes it easy for attackers to carry out VLAN hopping. [13]

Detection of VLAN Hopping: Detecting VLAN hopping attacks involves a strategic approach leveraging network monitoring tools and protocols to identify unauthorized traffic crossing VLAN boundaries. Key to this detection is the use of Syslog, SNMP (Simple Network Management Protocol), and SPAN (Switched Port Analyzer) to monitor and analyse network behaviour for anomalies indicative of VLAN hopping. Syslog serves to capture system messages and anomalies, while SNMP gathers metrics and logs from network devices, offering insights into unusual activities. SPAN, or port mirroring, duplicates network packets from one port or VLAN to another for analysis, enabling real-time traffic observation without disrupting network operations. [12]

Monitoring for unexpected traffic patterns, such as traffic on VLANs where it doesn't belong or abnormal volumes of traffic, is crucial. This includes scrutinizing DTP (Dynamic Trunking Protocol) messages and trunk port negotiations for signs of unauthorized attempts to establish trunk links, a common tactic in VLAN hopping attacks. [9]

Mitigation: If you want to keep the network's security and integrity intact, it is essential to prevent attacks that include VLAN hopping. To acquire unauthorised access to many virtual local area networks (VLANs), these attacks take use of weaknesses in network protocols and settings. As a result, the vulnerabilities compromise the confidentiality, integrity, and availability of network resources. By taking a holistic approach to mitigation, one may take several important actions that are targeted at strengthening the network against vulnerabilities of this kind. [10] [9]

The first thing that must be done is to deactivate Dynamic Trunking Protocol (DTP) on each switch port of the network. Given that DTP has the capability to facilitate the automatic negotiation of trunk connections, it is not impossible for attackers to take use of this capability. They can create unauthorised trunk connections because of this, which in turn enables them to get access to traffic that is not restricted by VLANs. To significantly lessen the risk of VLAN hopping attacks, managers of networks have the option to disable digital transmission protocol (DTP), which enables them to prevent automated trunk negotiation from taking place. [9]

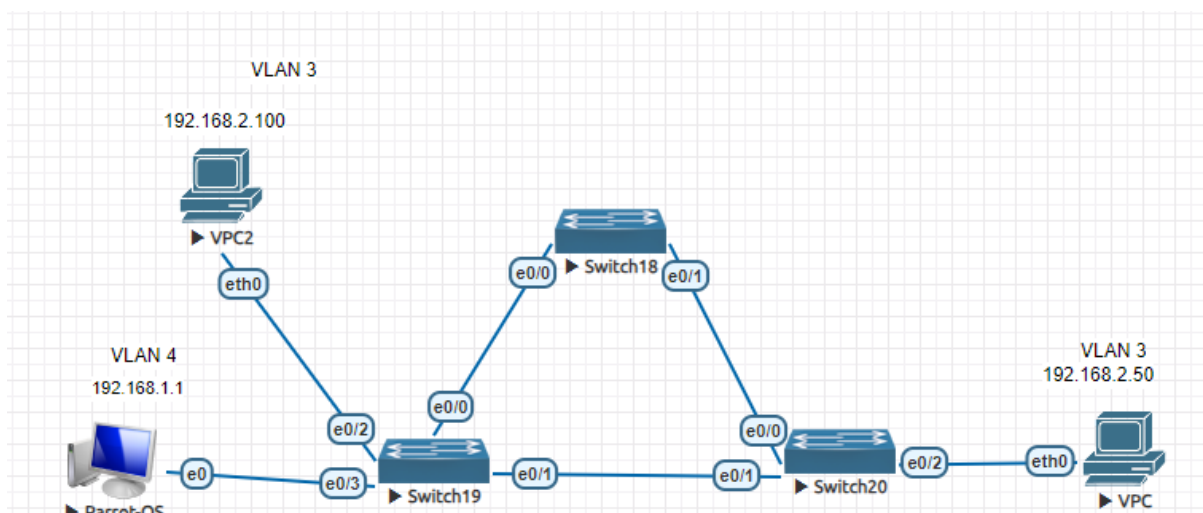
Secondly, when it comes to virtual local area networks (VLANs), it is essential to exercise diligence. One of the items that goes under this category is avoiding the use of VLAN 1, which is the default VLAN on many switches and is often targeted by attackers due to its widespread configuration and use. This is one of the elements that falls under this category. In order to avoid unauthorised access, it is possible to give a unique VLAN ID to trunk ports and ensure that important network traffic is divided into secure VLANs. This will allow for the prevention of unauthorised user access. [9]

Another essential tactic is to take a proactive approach to port management. To reduce the number of active entry points that are accessible to attackers, this entails closing unused ports and assigning them to a virtual local area network (VLAN) that is not being utilised. It is possible to further protect the network from efforts to get unauthorised access by specifically configuring switch ports as access ports and guaranteeing that they are unable to build trunk linkages by discarding DTP packets. [10] [9]

Another essential tactic is to take a proactive approach to port management. In order to reduce the number of active entry points that are accessible to attackers, this involves closing unused ports and assigning them to a virtual local area network (VLAN) that is not being utilised. It is possible to further protect the network from efforts to get unauthorised access by specifically configuring switch ports as access ports and guaranteeing that they are unable to build trunk linkages by discarding DTP packets. [10] [9]

In summary, a robust mitigation strategy against VLAN hopping attacks involves disabling unnecessary protocols, managing VLANs and port configurations carefully, and implementing security measures to detect and prevent unauthorized access. These strategies, are essential for protecting network resources from the security threats posed by VLAN hopping attacks, ensuring the network's security posture is both proactive and resilient. [10] [9] [13]

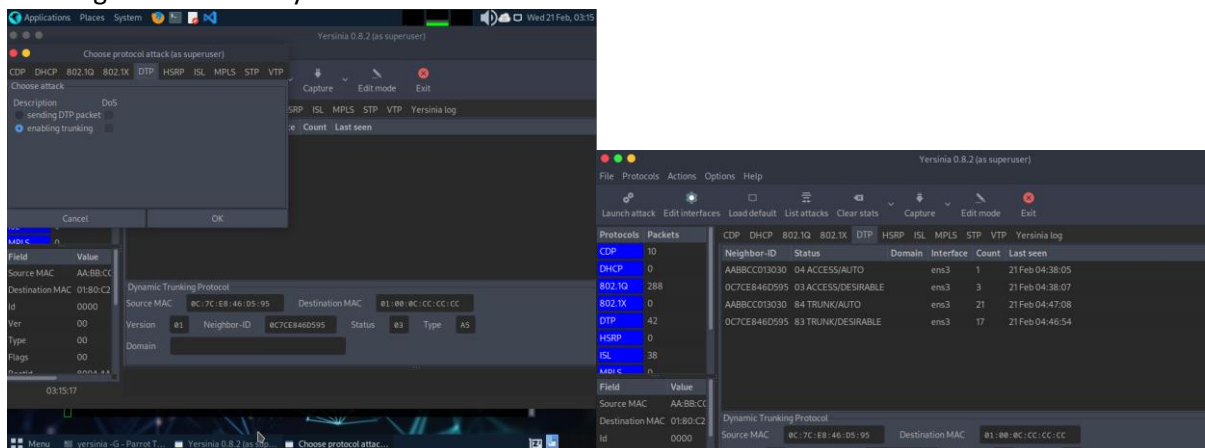
Simulation:



Lab Topology Overview: The above lab topology for the VLAN hopping attack simulation features a network setup with Parrot OS connected to Switch 19 (SW19) on VLAN 4 and Virtual PC 2 (VPC2) on VLAN 3. On Switch 20 (SW20), another Virtual PC (VPC) is configured on VLAN 3. A trunk link is established between SW19 and SW20 to facilitate inter-VLAN communication. This setup is crucial for demonstrating the VLAN hopping attack and its mitigation strategies.

```
[x]-[root@parrot]-[/home/parrot]
#ifconfig ens3.3 192.168.2.5 netmask 255.255.255.0 up
[root@parrot]-[/home/parrot]
#ifconfig ens3.4 192.168.1.5 netmask 255.255.255.0 up
[root@parrot]-[/home/parrot]
```

Configuration of Sub interfaces : As shown above, sub interfaces for VLAN 3 and VLAN 4 were created with assigning IP addresses on respective VLANs on the Parrot OS system, each assigned with an IP address. This configuration is a preparatory step for executing the VLAN hopping attack, allowing the Parrot OS system to communicate across both VLANs.



Launching the VLAN Hopping Attack : Yersinia, a network tool known for its capability to perform various network attacks including VLAN hopping, was used on the Parrot OS to initiate a DTP (Dynamic Trunking Protocol) trunking with the switch as shown in above figures. By exploiting DTP, the attack attempts to convert an access link into a trunk link, thereby gaining unauthorized access to traffic across multiple VLANs as shown in above figures.

```
[x]-[root@parrot]-[/home/parrot]
#ping 192.168.2.50
PING 192.168.2.50 (192.168.2.50) 56(84) bytes of data.
64 bytes from 192.168.2.50: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 192.168.2.50: icmp_seq=2 ttl=64 time=0.898 ms
64 bytes from 192.168.2.50: icmp_seq=3 ttl=64 time=0.782 ms
64 bytes from 192.168.2.50: icmp_seq=4 ttl=64 time=0.605 ms
64 bytes from 192.168.2.50: icmp_seq=5 ttl=64 time=0.806 ms
```

Successful VLAN Hopping : Following the attack, the Parrot OS system was able to ping VPC, which is located on a different VLAN. This successful communication across VLAN boundaries according to above confirms the effectiveness of the VLAN hopping attack, demonstrating the vulnerability of the

network to such exploits.

```
S19(config)#int e0/3
S19(config-if)#sw
S19(config-if)#switchport mo
S19(config-if)#switchport mode ac
S19(config-if)#switchport mode access
S19(config-if)#sw
S19(config-if)#switchport ne
S19(config-if)#switchport nen
S19(config-if)#switchport non
S19(config-if)#switchport nonegotiate
S19(config-if)#

S19#sh int e0/3 switchport
Name: Et0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 4 (VLAN0004)
Trunking Native Mode VLAN: 1 (default)
```

Mitigation Strategies : Mitigating the VLAN hopping attack involved configuring the network switches to treat ports as access ports and using the "nonegotiate" command to prevent DTP negotiation [10] [9] This strategy effectively blocks the VLAN hopping attack, enhancing network security against the vulnerabilities highlighted in [10] and [13]

Conclusion: This simulation underscores the importance of understanding network vulnerabilities to VLAN hopping attacks and the effectiveness of specific mitigation techniques. Proper network configuration and vigilance are crucial for protecting against such sophisticated attacks, as discussed in [10] [13] , [12] and [9]

3.3 Attack 3

Introduction to Spanning Tree Protocol (STP)

When it comes to removing network loops in circumstances that include duplicate connections, the Spanning Tree Protocol (STP), and more especially the IEEE 802.1w standard, becomes an incredibly significant component on the list of components to consider. By placing network switches in a hierarchical structure with a root bridge that is particularly intended for that purpose, STP ensures that Ethernet networks have a topology that is free of loops. This organisation is achieved via the exchange of Bridge Protocol Data Units (BPDUs), which, in addition to assisting in the selection of the root bridge, also help in determining the quickest path to reach that bridge. As a result, this helps to detect the active and blocking states of ports, which in turn helps to prevent loops from forming. [14] [9]

Vulnerabilities in STP

Although it performs an important function, the design of STP, which is based on a trust paradigm that does not need BPDU validation, leads in the development of various vulnerabilities. This is the case despite the fact that STP serves a vital purpose. In the event that a lower Root Path Cost (RPC) or Bridge ID (BID) is proposed, any switch has the capability to claim the root role. This might potentially lead to unauthorised access and manipulation of the network architecture. An example of an attack that takes use of this vulnerability is the STP Root-Takeover, in which the attackers fake BPDUs in order to make their malicious device seem to be the new root. This takes place in order to disrupt the operations of the network or to make future attacks, such as a denial of service (DoS) attack, easier to carry out via the use of BPDU flooding. [15] [16]

Mitigation Strategies [17]

Some of the approaches that have been developed to protect the STP topology include Root Guard, BPDU Guard, and BPDU Filtering. These methods were developed by Cisco and other organisations. These safety measures are implemented on a port-by-port basis in order to provide a counterbalance to the vulnerabilities that have been discovered. By placing ports that are receiving superior BPDUs into a root-inconsistent state.

Root Guard: It can prevent unauthorised switches from taking on the root role. This is accomplished by displaying a root-inconsistent state.

BPDU Guard: When a BPDU is received, BPDU Guard pauses ports to avoid topology modifications that may have been performed purposefully or accidentally. These changes might have been made in either direction.

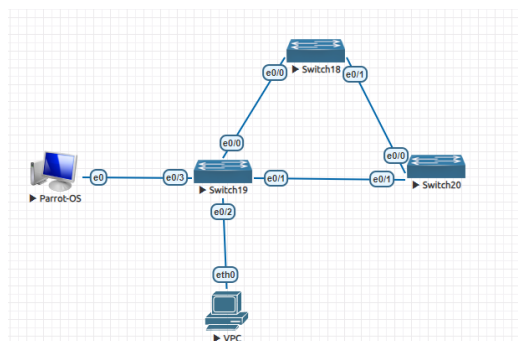
BPDU Filtering: It eliminates the potential of STP manipulation by preventing BPDUs from being transmitted or received on certain ports. This eliminates the possibility of STP manipulation.

Advanced Protection Techniques

Additional layers of security may be achieved using more complex strategies, such as Unidirectional Link Detection (UDLD) and Loop Guard, in addition to these core approaches. The issue of unidirectional connection failures, which would normally result in loops, is addressed by UDLD by the adoption of bidirectional communication technology. To prevent a switch from inadvertently switching a blocking port to a forwarding state due to the absence of BPDUs, Loop Guard sets such ports in a loop-inconsistent state. This stops the switch from making the adjustment. This helps to ensure that the switch does not make use of the incorrect transition. [17]

Practical Application and Simulation

Simulation Overview:



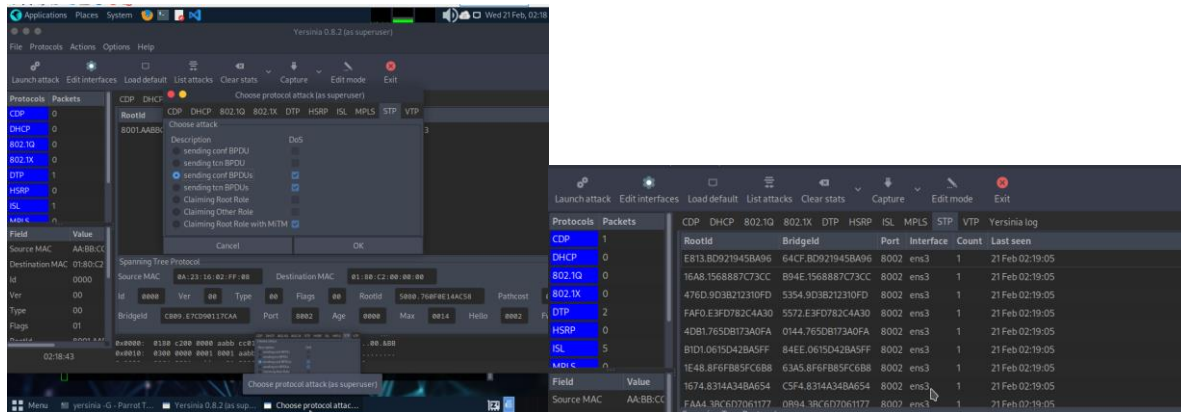
The goal of the simulation was to investigate the vulnerabilities that are present inside the Spanning Tree Protocol (STP), with a specific focus on the STP Root-Takeover attack, and to provide feasible approaches for mitigating these vulnerabilities. The simulation was constructed with the intention of presenting possible solutions to mitigate these vulnerabilities. There were three switches that comprised the topology of the network, and their names were S19, S18, and S20. There was a connection between the S19 network and a malicious actor who was operating from a device that was running Parrot OS. For the goal of demonstrating STP root-takeover vulnerability exploitation and the subsequent mitigation processes, this setup was not only essential but also absolutely vital.

STP Root-Takeover Attack Simulation:

```
s18#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     aabb.cc01.2000
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Initial Topology Observation: The simulation began with an examination of the current STP topology, identifying S18 as the root bridge. This setup was essential for understanding the network's baseline behaviour before the introduction of any malicious activity.



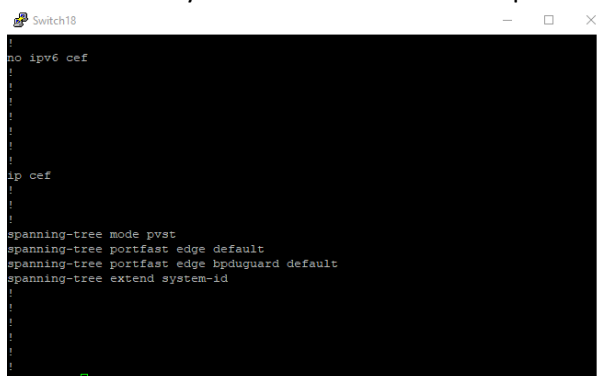
Launching the Attack : Utilizing Yersinia, a known tool for conducting Layer 2 attacks, the attacker initiated an STP Root-Takeover attack from the Parrot OS device. Yersinia was configured to send crafted Bridge Protocol Data Units (BPDUs) that falsely advertised the attacker's device as having a superior bridge ID, misleading the network into electing it as the new root bridge.

```
s18#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
             Address     a002.ad7f.44a0
             Cost        200
             Port        1 (Ethernet0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     aabb.cc01.2000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   15 sec
```

Observing the Topology Change: Following the attack, it was observed that S18 was no longer recognized as the root bridge. This change underscored the attack's effectiveness, demonstrating how maliciously crafted BPDUs could manipulate the network's topology.



Mitigation Implementation: To counteract the attack, mitigation strategies were employed. Specifically, BPDU Guard was activated on relevant switch ports to prevent unauthorized BPDU transmissions. This step was crucial in restoring the network's integrity and resilience against similar attacks.

Mitigation Effectiveness and Network Restoration:

```

s18(config)#
*Feb 21 02:27:31.827: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Etherne
t0/0 with BPDU Guard enabled. Disabling port.
s18(config)#
*Feb 21 02:27:31.827: %PM-4-ERR_DISABLE: bpduguard error detected on Et0/0, putt
ing Et0/0 in err-disable state
*Feb 21 02:27:32.801: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Etherne
t0/1 with BPDU Guard enabled. Disabling port.
*Feb 21 02:27:32.801: %PM-4-ERR_DISABLE: bpduguard error detected on Et0/1, putt
ing Et0/1 in err-disable state
s18(config)#
*Feb 21 02:27:32.834: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
*Feb 21 02:27:33.802: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
s18(config)#
*Feb 21 02:27:33.828: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to do
wn
*Feb 21 02:27:34.807: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to do
wn
s18(config)#

```

The activation of BPDU Guard effectively neutralized the threat, preventing the attacker from influencing the STP topology further. This mitigation strategy underscored the importance of proactive security measures in maintaining network stability and security. Following the mitigation steps, the network topology was restored to its original state, with S18 reassuming its role as the root bridge.

Conclusion and Insights on simulation:

This simulation highlighted the vulnerabilities inherent in the STP's trust-based mechanism, which can be exploited through STP Root-Takeover attacks. The successful execution of the attack demonstrated the potential for significant disruption within a network's topology, emphasizing the need for vigilant security practices.

Conclusion

In summary, while STP is indispensable for maintaining network stability and preventing loops, its inherent vulnerabilities pose significant security risks. Understanding these vulnerabilities and implementing a comprehensive set of mitigation strategies is crucial for network administrators to protect against unauthorized access and manipulation. The combination of STP's hierarchical organization, the potential for exploitation, and the available protective mechanisms forms a complex landscape that requires vigilant management and ongoing adaptation to emerging threats [14] [9] [15] [16] [17].

3.4 Attack 4

Introduction to DHCP

When it comes to network administration, the Dynamic Host Configuration Protocol (DHCP) is a protocol that is utilised on Internet Protocol (IP) networks, as stated in [18]. Every device that is connected to a network may have a dynamic Internet Protocol (IP) address and other network configuration settings assigned to it by a DHCP server thanks to this protocol, which enables the server to automatically provide these parameters. That the devices are able to connect with other IP networks is made possible by this. Client-server architecture serves as the basis for Dynamic Host Configuration Protocol (DHCP). A broadcast query is sent out by a device whenever it establishes a connection to the network. This inquiry makes a request for the information that is necessary. The DHCP server will then offer the appropriate settings in response. This configuration will contain the IP address, the subnet mask, the default gateway, and the information about the DNS server. [19]

DHCP Operation (DORA Process):

DHCP, which stands for Dynamic Host Configuration Protocol, is comprised of four important operations that are referred to as the DORA process. These processes are Discover, Offer, Request,

and Acknowledge. These actions are necessary in order to ensure that IP addresses are distributed in a network in a dynamic manner. In the course of this method, two well-known UDP port numbers are used for the purpose of communication between DHCP clients and servers. This communication is intended to take place. Within the context of the Dynamic Host Configuration Protocol (DHCP), the client communicates with the server by means of UDP port 67, while the server communicates with the client by means of UDP port 68. [19] [20] The Internet Assigned Numbers Authority (IANA) is responsible for standardising these port numbers in order to guarantee that DHCP connections are routed and received in the right manner between clients and servers that are part of a network. Additionally, they are necessary for the effective operation of the DHCP protocol, which is needed for the protocol to operate in the correct manner without any problems. The Dynamic Host setup Protocol (DHCP) server is able to dynamically distribute network setup settings to DHCP clients by providing port numbers. Internet Protocol (IP) addresses, subnet masks, and default gateway addresses are all included in these settings. The automation and simplification of procedures linked to the establishment of the network is made possible as a result of this. [20] [18]

DHCP Starvation Attack:

The malicious attack known as DHCP starvation is directed against the Dynamic Host Configuration Protocol (DHCP), which is the target of the attack. In this exploit, an attacker uses fabricated MAC addresses to send a huge number of DHCP DISCOVER packets to a DHCP server. This causes the server to become overwhelmed with traffic. This avalanche of requests is being made with the intention of lowering the total number of IP addresses that are available to be accessed by the server. In this way, legitimate users of the network will be prevented from gaining an IP address, which will ultimately result in their being refused access to the network. [19][20].

This attack takes advantage of the system by using the mechanism that the DHCP server employs in order to dynamically allocate IP addresses to devices that are connected to the network infrastructure. As a result of the attacker's ability to generate a large number of requests that include faked MAC addresses, they are able to effectively reserve all of the IP addresses that are accessible for these non-existent devices. Because of this, the Dynamic Host Configuration Protocol (DHCP) server is unable to process requests for IP addresses that are made by real devices that are seeking to join the network. These requests are made by the devices themselves. This is due to the fact that the address pool possessed by the DHCP server has been exhausted. [21] [22].

The DHCP starvation attack has the potential to cause significant disruption in environments where network connection is of utmost importance. Furthermore, it lays the groundwork for additional network-based attacks. An example of this would be an adversary bringing a rogue DHCP server into the network after the legitimate DHCP server had exhausted all of the IP addresses that were available in its pool. In the event that a device on the network is unable to get an IP address from the proper DHCP server, it is possible for that device to accept IP addresses from the malicious server. Consequently, this provides the attacker with the capability to redirect or monitor network traffic, which in turn makes it simpler for them to carry out Man-in-the-Middle attacks or other malicious actions. [23] [24]

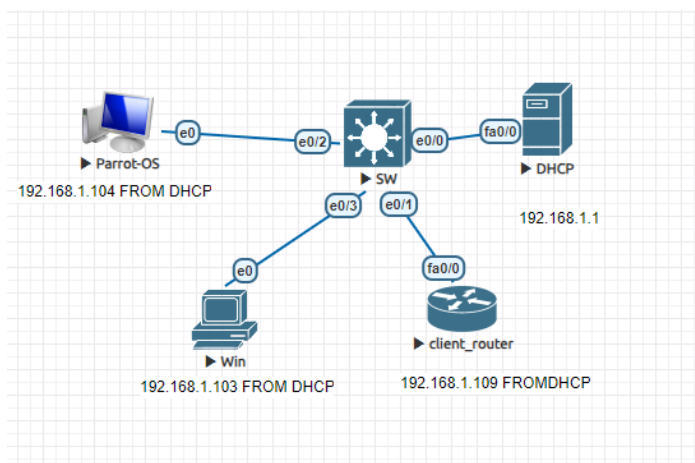
In essence, DHCP starvation represents a significant threat to network security, exploiting the DHCP service's inherent trust in client requests. It serves as a stark reminder of the need for comprehensive security measures to safeguard against such vulnerabilities and ensure the reliable operation of network services [22] [18]

Impact on the Network:

The DHCP starvation attack has a significant impact on the functioning of the network because it restricts access to new or existing devices as well as devices that need their IP configuration to be refreshed. In the event that it is combined with attacks that include a man in the middle, it has the potential to cause disruptions to the network, a reduction in productivity, and the possibility of data breaches. By using the fact that the DHCP protocol is stateless, which means that it does not have a method to authenticate DHCP requests, the attack is able to take advantage of this feature. The system is vulnerable to spoofing and impersonation if it does not have this technique of protection. [20]

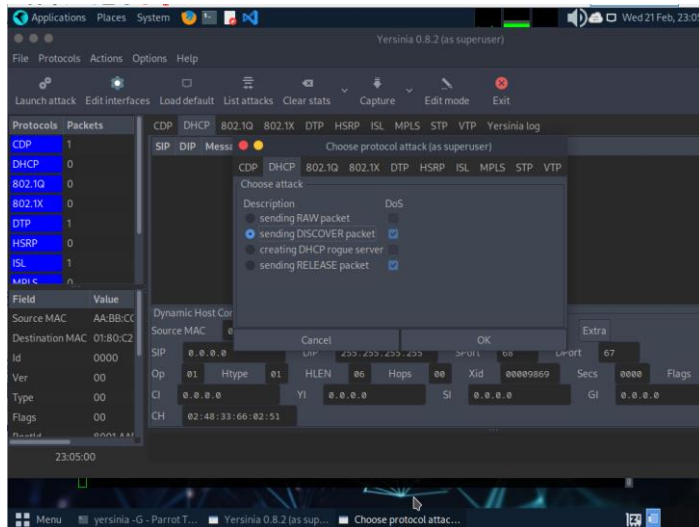
Simulation Overview:

The simulation provides a practical overview of a DHCP starvation attack and its mitigation within a network environment, illustrating the critical role of DHCP in dynamic IP allocation and the inherent vulnerabilities that can be exploited by attackers. By initiating a DHCP starvation attack using Yersinia from a Kali Linux machine, the simulation demonstrates how attackers can exhaust the IP address pool of a DHCP server, preventing legitimate devices from accessing the network. This attack underscores the trust-based vulnerabilities of the DHCP protocol, as highlighted in the literature. [23] [20] The subsequent implementation of port security as a mitigation strategy showcases an effective countermeasure by restricting the number of MAC addresses on a switch. port, thereby safeguarding the network against further spoofed DHCP Discover messages. [24] [22] This simulation, supported by academic and technical insights, emphasizes the importance of proactive security measures in maintaining network integrity and ensuring uninterrupted service to legitimate users.



Initial Network Setup: The simulation begins in a network environment where a DHCP server is operational on a router, serving IP addresses to various clients including a client router, a Windows PC, and an attacker's machine. This setup exemplifies a standard network configuration where DHCP plays a crucial role in dynamic IP allocation, facilitating seamless network management and

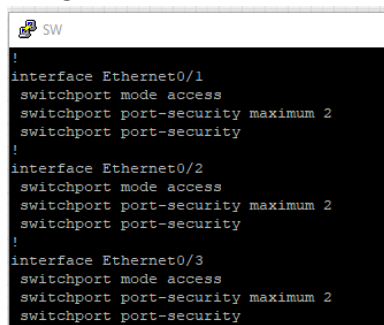
connectivity for devices.



Launching the DHCP Starvation Attack: The attacker initiates the DHCP starvation attack using Yersinia on a Kali Linux machine, sending a flood of DHCP Discover messages with spoofed MAC addresses to exhaust the DHCP server's IP pool. This step highlights the vulnerability of the DHCP protocol to exploitation due to its trust-based mechanism, allowing attackers to deplete available IP addresses without verification.

DHCP#sh ip dhcp binding							
Bindings from all pools not associated with VRF:							
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type				
192.168.1.101	0063.6973.636f.2d63. 6131.392e.3236.3734. 2e30.3030.302d.4661. 3026.30	Feb 22 2024 10:55 PM	Automatic				
192.168.1.102	01aa.aaaa.aaaa.88	Feb 22 2024 10:57 PM	Automatic	192.168.1.245	801a.1d16.f38f	Feb 21 2024 11:10 PM	Automatic
192.168.1.103	0150.0000.1a00.00	Feb 22 2024 10:57 PM	Automatic	192.168.1.246	88b3.ef7e.5ad4	Feb 21 2024 11:10 PM	Automatic
192.168.1.104	01aa.aaaa.aaaa.21	Feb 22 2024 11:03 PM	Automatic	192.168.1.247	9ab1.175a.49c8	Feb 21 2024 11:10 PM	Automatic
192.168.1.105	c8f8.237d.b41f	Feb 21 2024 11:10 PM	Automatic	192.168.1.248	7ee7.123a.bd31	Feb 21 2024 11:10 PM	Automatic
192.168.1.106	6aef.a97d.8d0a	Feb 21 2024 11:10 PM	Automatic	192.168.1.249	92b4.825a.0520	Feb 21 2024 11:10 PM	Automatic
192.168.1.107	8e96.0140.32a5	Feb 21 2024 11:10 PM	Automatic	192.168.1.250	0474.7f5a.2630	Feb 21 2024 11:10 PM	Automatic
192.168.1.108	82f6.232b.7fbb	Feb 21 2024 11:10 PM	Automatic	192.168.1.251	5cb6.4600.f98b	Feb 21 2024 11:10 PM	Automatic
192.168.1.109	7c96.a730.9b25	Feb 21 2024 11:10 PM	Automatic	192.168.1.252	d079.625f.8b56	Feb 21 2024 11:10 PM	Automatic
192.168.1.110	caeb.8005.d573	Feb 21 2024 11:10 PM	Automatic	192.168.1.253	82d5.d158.b6d0	Feb 21 2024 11:10 PM	Automatic
192.168.1.111	7e0b.2f43.afdd	Feb 21 2024 11:10 PM	Automatic	192.168.1.254	2ald.cf73.218c	Feb 21 2024 11:10 PM	Automatic
192.168.1.112	9244.5e76.34d3	Feb 21 2024 11:10 PM	Automatic				
192.168.1.113	d4ff.0f5a.1046	Feb 21 2024 11:10 PM	Automatic				
192.168.1.114	3629.0221.6f30	Feb 21 2024 11:10 PM	Automatic				
192.168.1.115	b4ce.9558.052a	Feb 21 2024 11:10 PM	Automatic				
192.168.1.116	de5f.950e.b2cb	Feb 21 2024 11:10 PM	Automatic				

Observing the Impact of the Attack: The DHCP server's depletion of IP addresses prevents legitimate devices from obtaining network access, effectively demonstrating the direct impact of a DHCP starvation attack. This scenario showcases the disruption caused by such attacks, emphasizing the critical nature of DHCP in network functionality and the ease with which attackers can deny service to legitimate users.



Mitigating the Attack with Port Security: To mitigate the attack, port security is implemented on the network switch, limiting the number of MAC addresses that can be learned on a switch port and preventing the attacker from sending additional spoofed DHCP Discover messages. This

countermeasure showcases the effectiveness of network security protocols in neutralizing threats and ensuring the DHCP server can resume normal operations.

Conclusion of the Simulation: The simulation, enriched literature, offers a comprehensive view of DHCP starvation attacks and the efficacy of mitigation strategies like port security. It underscores the importance of understanding DHCP vulnerabilities and implementing proactive security measures to safeguard network integrity and service availability.

Conclusion:

Dynamic Host Configuration Protocol (DHCP) is an important component in the management of networks because it allows for the dynamic assignment of Internet Protocol (IP) addresses and configuration settings to computers and other devices. On the other hand, the fact that it is vulnerable to DHCP starvation attacks poses significant threats to the network's ability to function properly and to maintain its security. For the aim of implementing efficient mitigation measures and maintaining the integrity and availability of the network, it is essential for network administrators to have a strong grasp of the mechanics of DHCP as well as the likelihood of exploitation. Without this understanding, it is impossible to apply effective mitigation techniques. [18]

3.5 Attack 5

Introduction DHCP rouge server

Following the discussion on DHCP starvation, the subsequent deployment of rogue DHCP servers represents a critical escalation in network security threats. After the official DHCP server's IP address pool has been exhausted as a consequence of starvation attacks, attackers are able to install a rogue DHCP server into the network. This allows them to take control of everything on the network. In the aftermath of this, the unauthorised server begins broadcasting its own IP addresses and network settings to the clients that it is connected to. Since it is pretending to be a legitimate network entity, the malicious server is able to redirect all client traffic via itself instead of going through the client. This provides the attacker with the capacity to carry out man-in-the-middle attacks, which are also referred to as MITM attacks. This circumstance not only results in interruptions in network connection, but it also puts the confidentiality and integrity of the data that is being sent over the network at danger. As a result, it poses a substantial threat to the security of the systems that are affected by this situation. [21] [26]

Rogue DHCP Server Threat

Using a rogue DHCP server, which is a server that is put within a network without authority and is often deployed deliberately, poses a significant danger of distributing incorrect network configuration settings. This is a major risk that may have catastrophic consequences. This might result in a number of undesirable results, including difficulties in gaining access to the network, inappropriate traffic routing, and the prospect of being susceptible to attacks that include a man in the middle. The malicious server is able to listen in on and alter the traffic that is being sent between legitimate users and services on the network with the ability to eavesdrop on and manipulate the traffic. As a result, the confidentiality, integrity, and availability of data and systems that are connected over a network are placed in jeopardy. [21]

Mechanisms of Rogue DHCP Server Attacks

DHCP Starvation and Rogue Server Deployment: Attackers use DHCP starvation attacks to deplete a valid DHCP server's IP address pool. A rogue DHCP server is then launched to assign clients IP

addresses and network configurations. The rogue DHCP server is then deployed. This server might configure its IP address as the default gateway, routing all client traffic via the attacker's device. This would allow data access and modification.[21] [26]

Man-in-the-Middle (MITM) Attacks: Malicious DHCP servers allow attackers to carry out man-in-the-middle attacks. These attacks are possible to be carried out. Clients and networks that provide actual services are connected via these servers, which serve as an intermediary between the two. They have the ability to sniff, change, or block the data that is being sent between clients and services, which may lead to data breaches and difficulties with service.[21] [26]

Detection and Mitigation Strategies

Detecting and neutralizing rogue DHCP servers is crucial for maintaining network security. Various techniques have been proposed:

Digital Certificates and DHCP Snooping: Digital certificates for DHCP server authentication may minimise malicious server risk. Rogue server attacks may be prevented using DHCP snooping, which filters unauthorised DHCP messages based on trusted switch ports. In addition, DHCP snooping may prevent unauthorised server attacks. Despite this, these systems have drawbacks. These include administrative burden and physical access attack risk. [21]

Whitelisting and Active Monitoring: Whitelisting the IP and MAC addresses of legitimate DHCP servers and keeping a constant watch for DHCP OFFER signals originating from unauthorised sources are two methods that may be used to achieve this goal. Both of these approaches have the potential to be useful in determining whether servers are malicious. On the other hand, these vulnerabilities may be circumvented by attackers via the use of IP spoofing, which underscores the need of detection systems that are more robust. [21]

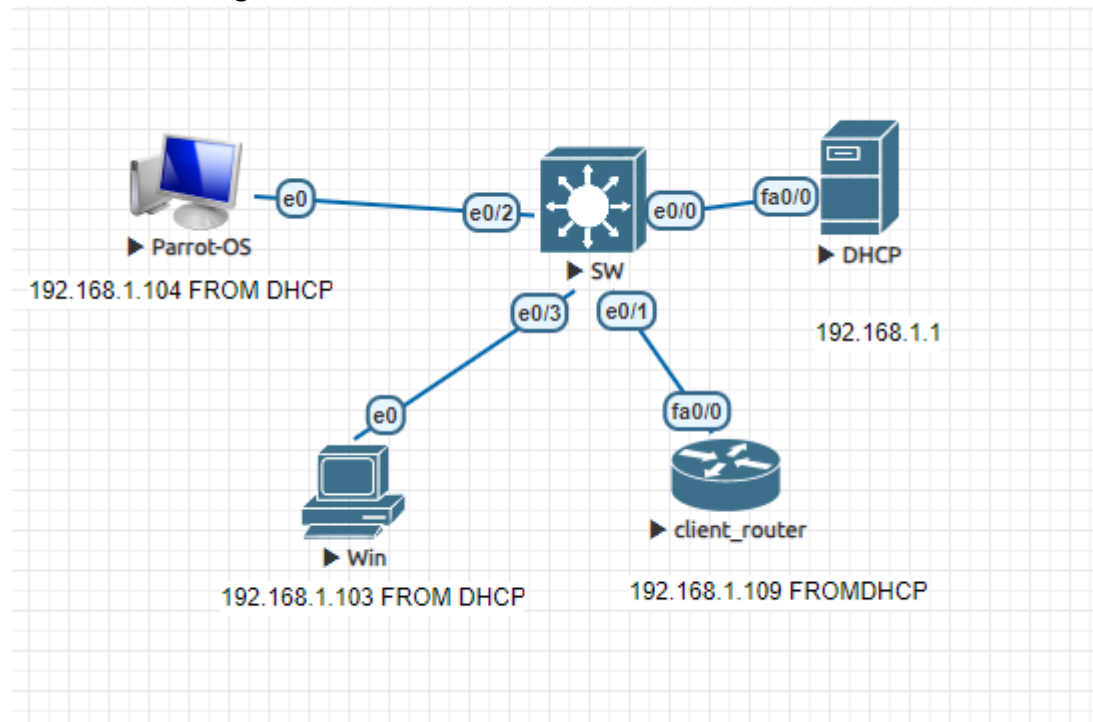
Automated Detection and NeutralizationThe creation of automated systems that are able to detect rogue DHCP servers by comparing incoming DHCP OFFER messages against a whitelist and then neutralising the rogue server via DHCP starvation attacks on its IP pool is an effective way for minimising the risk. This method is a strategy that has been shown to be effective. A little amount of hardware resources is required for the implementation of these sorts of systems, and they can be implemented on a wide range of various platforms. [21]

Simulation Environment Detail and Explanation of Screenshots

Introduction:

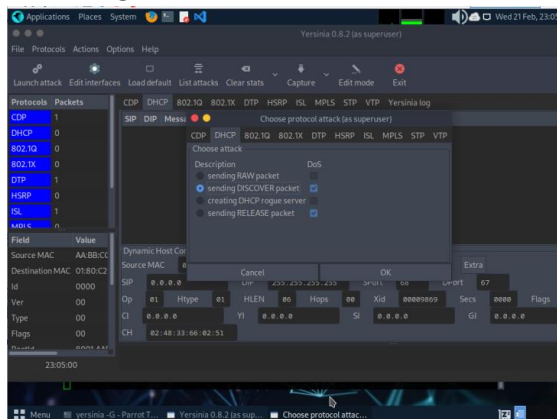
In the realm of network security, understanding the dynamics of DHCP servers and the potential for rogue server attacks is crucial. This simulation environment was meticulously set up to demonstrate how rogue DHCP servers can disrupt network operations by masquerading as legitimate DHCP servers, offering unauthorized IP addresses to unsuspecting clients. The environment includes a router acting as a DHCP server, a Parrot OS as the attacker's machine, a Windows machine, and a client router, all interconnected via a switch. The simulation walks through the process of launching a DHCP starvation attack followed by the creation of a rogue DHCP server, and concludes with the implementation of mitigation strategies.

DHCP Server Configuration:



The initial setup showcases a DHCP server configured on a router, successfully assigning IP addresses to various devices in the network, including the attacker's machine (Parrot OS), a Windows machine, and a client router. This setup establishes the baseline functionality of the network before the attack.

Launching DHCP Starvation Attack:



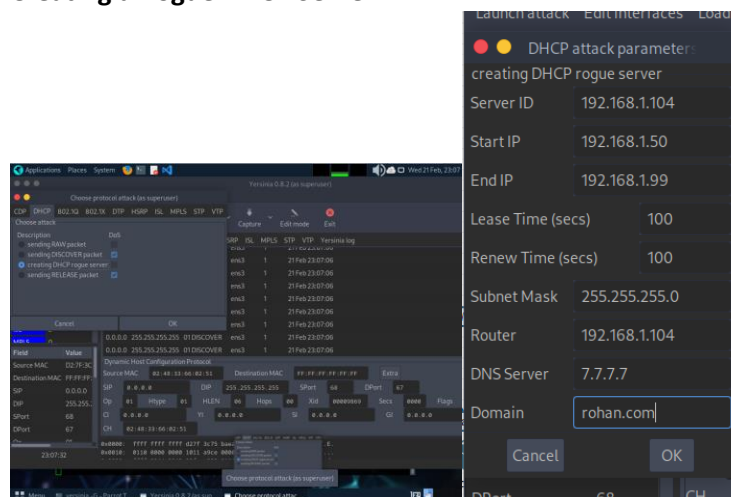
Utilizing Yersinia from the attacker's machine, a DHCP starvation attack is initiated by sending a flood of DHCPDISCOVER packets to the DHCP server. This attack aims to deplete the pool of available IP addresses, preventing legitimate clients from obtaining an IP address.

Depletion of DHCP IP Pool:

```
DHCP#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/
Hardware address/   Lease expiration    Type
User name
192.168.1.101       0063.6973.636f.2d63. Feb 22 2024 10:55 PM Automatic
6131.392e.3236.3734.
2e30.3030.302d.4661.
302f.30
192.168.1.102       01aa.aaaa.aaaa.88    Feb 22 2024 10:57 PM Automatic
192.168.1.103       0150.0000.1a00.00    Feb 22 2024 10:57 PM Automatic
192.168.1.104       01aa.aaaa.aaaa.21    Feb 22 2024 11:03 PM Automatic
192.168.1.105       c8f8.237d.b41f       Feb 21 2024 11:10 PM Automatic
192.168.1.106       6af1.a97d.8d0a       Feb 21 2024 11:10 PM Automatic
192.168.1.107       8c86.0140.32a5       Feb 21 2024 11:10 PM Automatic
192.168.1.108       82f6.232b.7fbb       Feb 21 2024 11:10 PM Automatic
192.168.1.109       7c95.a730.9b25       Feb 21 2024 11:10 PM Automatic
192.168.1.110       caeb.8005.d573       Feb 21 2024 11:10 PM Automatic
192.168.1.111       7e0b.2f49.a6dd       Feb 21 2024 11:10 PM Automatic
192.168.1.112       9244.5e76.34d3       Feb 21 2024 11:10 PM Automatic
192.168.1.113       d4ff.0f5a.1045       Feb 21 2024 11:10 PM Automatic
192.168.1.114       3623.0221.8f90       Feb 21 2024 11:10 PM Automatic
192.168.1.115       b4ce.9558.052a       Feb 21 2024 11:10 PM Automatic
192.168.1.116       de5f.950e.b2cb       Feb 21 2024 11:10 PM Automatic
```

This screenshot confirms the effectiveness of the DHCP starvation attack, showing that all available IP addresses in the DHCP server's pool have been consumed. This leaves the network in a vulnerable state, unable to assign IP addresses to legitimate clients.

Creating a Rogue DHCP Server:



Following the starvation attack, the attacker escalates the situation by creating a rogue DHCP server using Yersinia. This server was configured to set its own IP as default gateway and pool was set from 192.168.1.50 – 192.168.1.99.

Client_router Receives IP from Rogue DHCP Server:

```
client_router(config)#int f0/0
client_router(config-if)#ip add dhcp
client_router(config-if)#do sh ip int b
Interface      IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0 unassigned      YES DHCP    up           up
FastEthernet1/0 unassigned      YES unset   administratively down down

client_router(config-if)#
*Feb 21 23:18:17.751: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 192.168.1.50, mask 255.255.255.0, hostname client_router
do sh ip int b
Interface      IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0 192.168.1.50    YES DHCP    up           up
FastEthernet1/0 unassigned      YES unset   administratively down down
```

A client requesting an IP address post-attack receives an IP from the rogue DHCP server's pool (192.168.1.50), demonstrating the rogue server's ability to impersonate a legitimate DHCP server and manipulate network traffic.

Enabling DHCP Snooping:

```
!
no ipv6 cef
!
!
!
!
!
!
ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip cef
!
!
```

To mitigate the attack, DHCP snooping is enabled on vlan1. This security feature helps in distinguishing between legitimate and unauthorized DHCP messages, providing a layer of protection against such attacks.

Trusting the Legitimate DHCP Server:

```
!
!  
!  
!  
!  
!  
!  
!  
  
interface Ethernet0/0  
 ip dhcp snooping trust  
!
```

By applying the "ip dhcp snooping trust" command on the interface E0/0 where the actual DHCP server is connected to which the legitimate DHCP server is connected, the network is configured to trust DHCP responses only from this server, effectively blocking responses from the rogue server.

Enhancing Security with Port Security:

```
!
interface Ethernet0/1
  switchport mode access
  switchport port-security maximum 2
  switchport port-security
!
interface Ethernet0/2
  switchport mode access
  switchport port-security maximum 2
  switchport port-security
!
interface Ethernet0/3
  switchport mode access
  switchport port-security maximum 2
  switchport port-security
!
```

Further security measures include enabling access port security on other access ports to restrict the number of MAC addresses allowed per port, preventing unauthorized devices from connecting to the network. Additional settings like violation modes and aging timers can further tighten security.

Simulation Conclusion:

This simulation vividly demonstrates the threat posed by rogue DHCP servers and underscores the importance of implementing robust security measures like DHCP snooping and port security. By understanding the mechanics of these attacks and the effectiveness of mitigation strategies, network administrators can better protect their networks from such vulnerabilities.

Conclusion:

The presence of rogue DHCP servers poses a major security risk to networks because they have the potential to interfere with operations and make it easier for unauthorised users to access network data. When it comes to maintaining the integrity of a network, having effective detection and mitigation measures is very necessary. The development of automated detection and neutralisation systems provides a potential way to tackling the vulnerabilities posed by rogue DHCP servers. While the techniques that are now in use provide some degree of protection, this is not the only solution that is being considered. Continuous network monitoring, consistent upgrades to security protocols, and the installation of multi-layered defence tactics are all necessary components in order to guarantee the safety of a network against attacks of this kind.[21] [25] [26]

3.6 Attack 6

Understanding ARP and Its Operational Mechanism

When it comes to network communication inside a Local Area Network (LAN), the Address Resolution Protocol, which is sometimes referred to as ARP on occasion, is an exceptionally important component. The mapping of Internet Protocol (IP) addresses to the physical machine addresses, sometimes referred to as Media Access Control (MAC) addresses, that correspond to those IP addresses is the fundamental objective of this system. It is essential that this mapping be carried out in order to ensure that data packets may be transmitted between devices that are connected to the same network. It is possible for a source host to send out a request to the whole network in order to locate the MAC address that is associated with the IP address that is being requested. The host that has the IP address that corresponds to the request is the one that responds. This allows the host's MAC address to be saved for use in subsequent communication and, as a consequence, makes the flow of network data more efficient. [27]

The Vulnerability of ARP to Spoofing Attacks

However, due to the fact that the ARP protocol is stateless and does not have any authentication methods for ARP requests and responses, it is vulnerable to ARP spoofing attacks. This is because the protocol does not have any authentication mechanisms. For the purpose of carrying out attacks of this kind, a malicious actor will send fabricated ARP messages throughout the network. ARP cache poisoning, which occurs when devices store erroneous mappings of IP addresses to MAC addresses, is a potential consequence of this. It is probable that this phenomenon will occur. It is possible for the attacker to successfully conduct out man-in-the-middle attacks (MITM) or denial-of-service attacks (DoS) by intercepting, altering, or stopping data flows between hosts. This allows the attacker to successfully carry out these attacks. This vulnerability poses a significant threat to network

security since it has the potential to disrupt network operations and compromise essential data. Also, it has the potential to compromise sensitive information. [27]

Impact of ARP Spoofing on Network Security

substantial effect on the functioning of a network as well as its security. Through the technique of connecting the MAC address of the attacker with the IP address of another device, such as a gateway, the attacker is able to intercept all of the traffic that is intended for that appliance. This allows the attacker to cause disruptions in the network. The theft of data, the hijacking of sessions, and the suspension of services supplied by the network are all potential outcomes that might be brought about by this level of interception. On account of the lack of built-in security mechanisms within the ARP protocol, which are responsible for authenticating and verifying ARP messages, these attacks may be carried out with relative ease, hence revealing a fundamental opening in network security. [28]

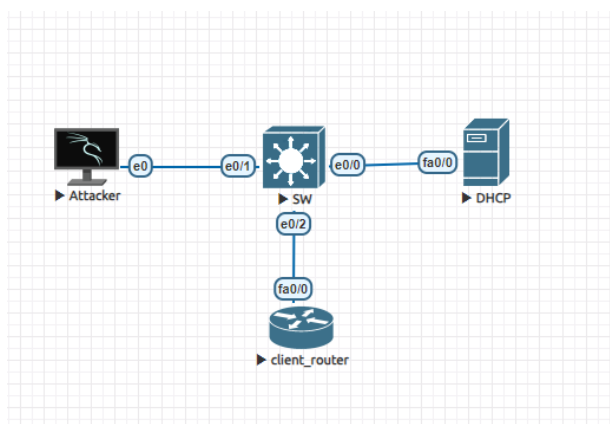
Strategies for Mitigating ARP Spoofing Attacks

When it comes to mitigating the effects of ARP spoofing attacks, it is essential to use a variety of strategies. When employing static ARP entries, which require manually inputting and locking IP-to-MAC address mappings, it is feasible to prevent spoofing. Enabling DHCP snooping on switch This is because static ARP entries are used. The utilisation of these entries, on the other hand, is not feasible when dealing with dynamic and vast networks. In addition, Dynamic ARP Inspection (DAI) on switches offers a solution that is more scalable. This is accomplished by examining ARP packets and prohibiting such packets from having inappropriate IP-to-MAC mappings. However, in order to put this idea into action, you will need hardware that is capable of DAI execution. The tools that are used for ARP monitoring are able to recognise unusual ARP traffic and alert administrators about the problem. [28]

Overview of ARP Spoofing Simulation

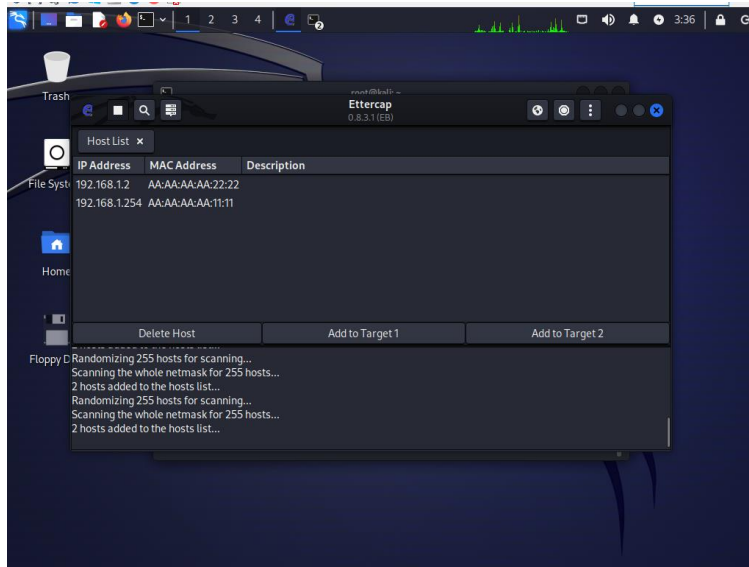
The simulation of an ARP spoofing attack and its mitigation provides a comprehensive understanding of the vulnerabilities within network communication and the effectiveness of countermeasures. This simulation involves a network topology consisting of an attacker, a DHCP server, and a client router connected via a switch, with the DHCP server running Telnet.

Simulation Steps and Screenshots Description

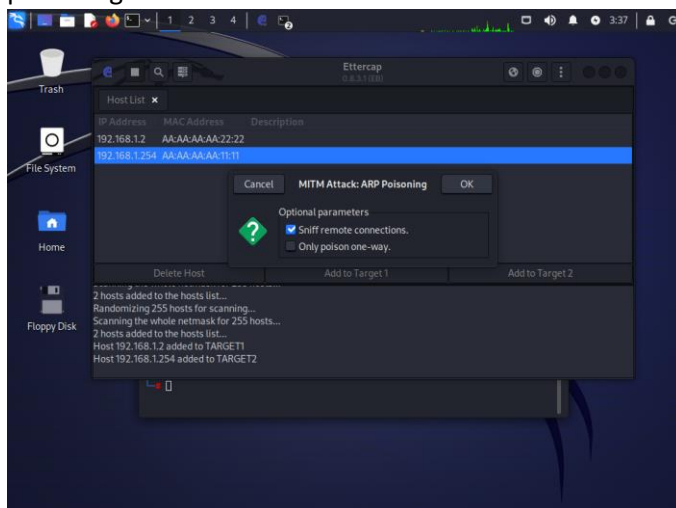


Network Topology Setup: The initial setup showcases the attacker, DHCP server, and client_router interconnected through a switch. This foundational setup is crucial for demonstrating the ARP

spoofing attack and subsequent mitigation strategies.



Packet Sniffing with Ettercap: Ettercap, a network security tool for packet sniffing and real-time monitoring of network traffic, is employed to capture packets within the network. This step is essential for identifying the communication between devices and selecting targets for the ARP poisoning attack.

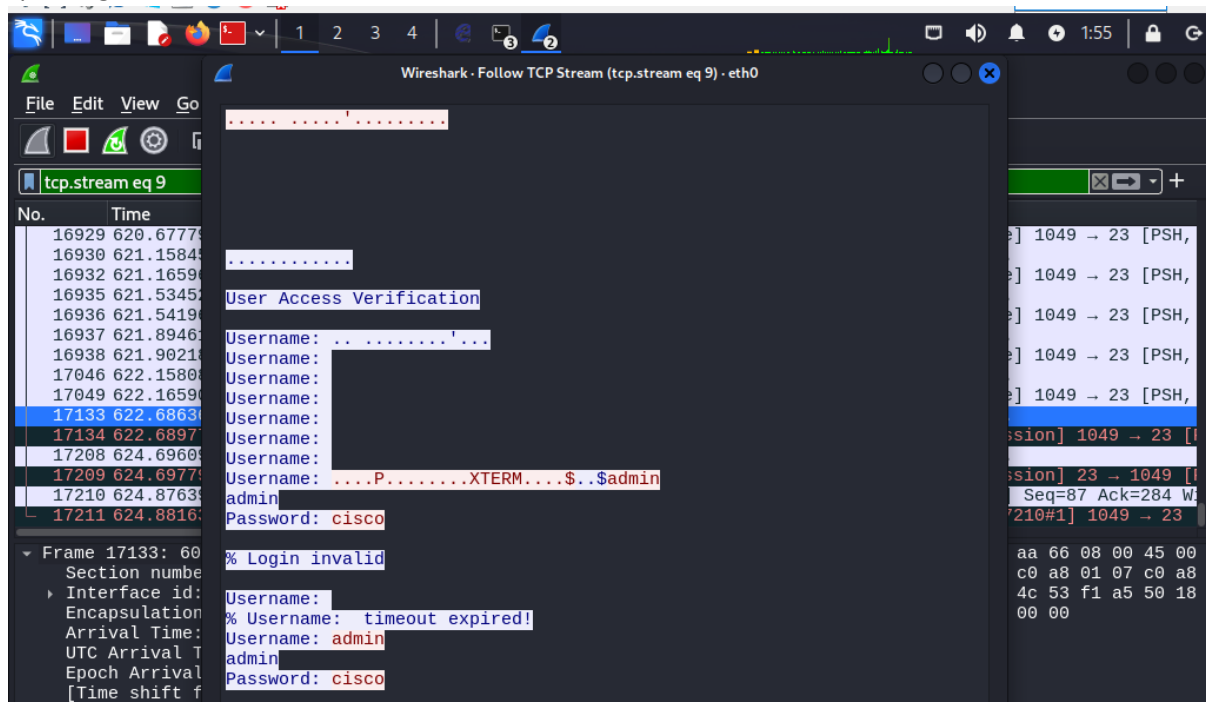


Target Selection for ARP Poisoning: The IP addresses 192.168.1.2 (client) and 192.168.1.254 (DHCP server) are chosen as targets for the ARP poisoning attack. This strategic selection aims to intercept and manipulate the traffic between these two devices.

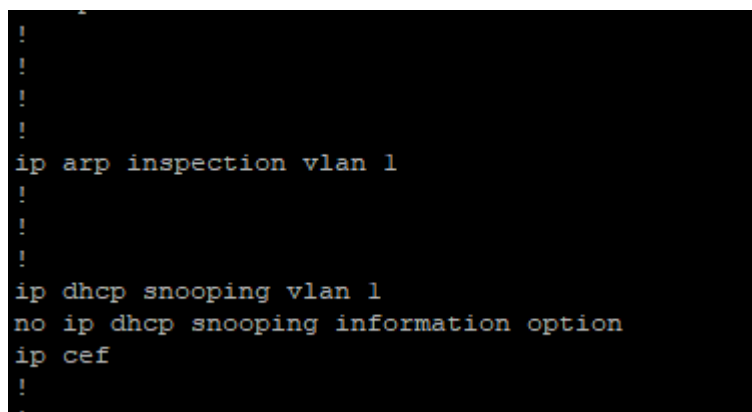
Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	1	aaaa.aaaa.3333	ARPA	FastEthernet0/0
Internet	192.168.1.2	0	aaaa.aaaa.3333	ARPA	FastEthernet0/0
Internet	192.168.1.8	3	aaaa.aaaa.3333	ARPA	FastEthernet0/0
Internet	192.168.1.254	-	aaaa.aaaa.1111	ARPA	FastEthernet0/0
DHCP_Server#					

Evidence of ARP Poisoning: The MAC addresses of the devices at IP addresses 192.168.1.1, 192.168.1.2, and 192.168.1.8 are manipulated to be the same, indicating a successful ARP poisoning attack. This manipulation allows the attacker to intercept the communication between the targeted devices.

Packet Inspection with Wireshark: Wireshark is utilized to inspect the packets within the network further. This tool provides detailed insights into the network traffic and the effects of the ARP spoofing attack.



Capturing Telnet Credentials: During the simulation, when the client attempts to establish a Telnet connection with the DHCP server, the attacker captures the username and password. This demonstrates the severe security implications of ARP spoofing, allowing attackers to intercept sensitive information.



Mitigation Strategy Implementation: To mitigate the ARP spoofing attack, IP ARP inspection and IP DHCP snooping are enabled on VLAN 1 of the switch. These measures are designed to validate ARP packets and DHCP responses, respectively, enhancing the network's security posture.

```
!
interface Ethernet0/0
 ip arp inspection trust
 duplex full
 ip dhcp snooping limit rate 60
 ip dhcp snooping trust
!
interface Ethernet0/1
 duplex full
!
interface Ethernet0/2
 duplex full
 ip dhcp snooping limit rate 20
!
```

Trusted Interface Configuration: On the trusted interface of the switch, IP ARP inspection trust and IP DHCP snooping are enabled. This configuration ensures that legitimate traffic from trusted sources is not inadvertently blocked by the mitigation strategies.

```
*Feb 21 09:07:19.954: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.([aaaa.aaaa.3333/192.168.1.8/0000.0000.0000/192.168.1.8/09:07:19
*Feb 21 09:07:19.954: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.([aaaa.aaaa.3333/192.168.1.1/0000.0000.0000/192.168.1.1/09:07:19
--More--
*Feb 21 09:07:21.959: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.([aaaa.aaaa.3333/192.168.1.8/0000.0000.0000/192.168.1.8/09:07:21
*Feb 21 09:07:21.959: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.([aaaa.aaaa.3333/192.168.1.1/0000.0000.0000/192.168.1.1/09:07:21
--More--
*Feb 21 09:07:23.968: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.([aaaa.aaaa.3333/192.168.1.8/0000.0000.0000/192.168.1.8/09:07:23
*Feb 21 09:07:23.968: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.([aaaa.aaaa.3333/192.168.1.1/0000.0000.0000/192.168.1.1/09:07:23
--More--
```

Blocking Unwanted ARP Traffic : Following the implementation of the mitigation strategies, any attempts to send spoofed ARP traffic to the switch are successfully dropped. This outcome validates the effectiveness of the countermeasures in preventing ARP spoofing attacks.

Conclusion

This simulation highlights the critical nature of ARP spoofing attacks and the importance of implementing robust security measures to protect network communications. By understanding the attack mechanisms and applying appropriate mitigation strategies, network administrators can significantly enhance the security and integrity of their networks.

Chapter 4:

Personal Recommendation

Given the comprehensive analysis and findings presented in this dissertation, it becomes evident that the security of network infrastructure at the data link layer is paramount to safeguarding digital communications against a myriad of vulnerabilities and cyber threats. The exploration of various attack vectors, such as MAC flooding, ARP spoofing, and VLAN hopping, alongside their respective mitigation strategies, underscores the critical need for a multifaceted approach to network security.

4.1 Recommendations for Network Administrators:

Enhanced Security Protocols: Putting in place strong security measures, such as the implementation of dynamic ARP inspection (DAI), port security, and DHCP snooping, is an absolute need for administrators of computer networks. Layer 2 attacks are substantially less likely to occur as a result of these protocols, which also guarantee a greater degree of network integrity and speed.

Regular Network Audits: Conducting network audits on a regular basis may assist in the early discovery of vulnerabilities and possible breaches, which enables prompt actions to be taken. Real-time insights into the behaviour of the network may be obtained by the use of network monitoring tools and protocols such as Syslog, SNMP, and SPAN, which can be of assistance in this process.

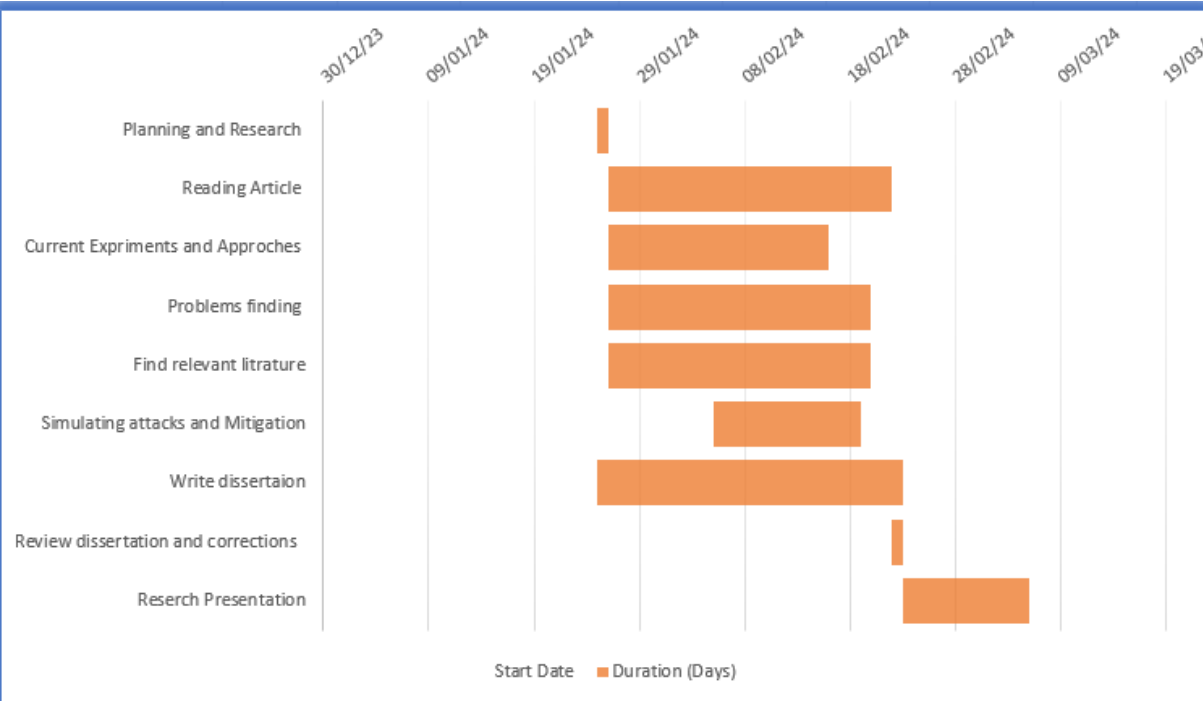
Education and Training: Improving the knowledge base and abilities of information technology staff in order to identify and mitigate network assaults is of the utmost importance. Increasing the overall resilience of network infrastructures may be accomplished via the implementation of regular training sessions on the most recent cyber threats and security measures.

Adoption of Simulation Tools: The use of network simulation tools like EVE-NG for testing and understanding the impact of various cyber attacks is highly recommended. These simulations provide invaluable insights into the dynamics of network vulnerabilities and the effectiveness of different mitigation strategies in a controlled environment.

Comprehensive Security Framework: Developing a comprehensive security framework that encompasses not only technical measures but also policy and procedure guidelines is essential. This framework should include strategies for both prevention and response, tailored to the specific needs and architecture of the network in question.

Chapter 5:

Gantt Chart



Chapter 6:

Conclusion

The digital era has ushered in unprecedented challenges in the realm of network security, making it a critical area of concern for organizations worldwide. This dissertation has highlighted the intricate vulnerabilities present at different layers of the OSI model, particularly on the data link layer. Through a detailed exploration of attack vectors such as MAC flooding, ARP spoofing, DHCP starvation, and VLAN hopping, this study has elucidated the multifaceted nature of network threats.

The practical simulations conducted using EVE-NG have demonstrated the disruptive potential of these attacks and the efficacy of various mitigation strategies. These simulations not only reinforce the theoretical underpinnings of network security but also offer practical insights into safeguarding digital communications against sophisticated cyber threats.

In summary, this dissertation contributes to the body of knowledge in network security by providing a detailed analysis of Layer 2 vulnerabilities, their implications for network integrity and performance, and a suite of mitigation strategies. The findings underscore the necessity of a proactive, informed, and multifaceted approach to network security, emphasizing the critical role of continuous monitoring, advanced security protocols, and comprehensive education and training programs. As cyber threats continue to evolve, so too must our strategies for defending against them, ensuring the security and integrity of digital networks now and into the future.

References

- [1] "www.cisco.com," cisco, [Online]. Available: <https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html>. . [Accessed 9 2 2023].
- [2] N. J. M. D. N. J. A. W. K. a. M. N. M. Qais Saif Qassim, "Compromising the Data Integrity of an Electrical Power Grid SCADA System," 2021.
- [3] S. N. Haroon Iqbal, "Wireshark as a Tool for Detection of Various LAN Attacks," *International Journal of Computer Sciences and Engineering*, vol. 7, pp. 833-837, 2019.
- [4] R. B. J. Matthews, "Exploring Layer 2 Network Security in Virtualized Environments," in *DEFCON 23*, Las Vegas, NV, 2015.
- [5] M. M. I. ., S. M Tanseer Ali, "A Practical Approach to Assess Fatal Attacks in Enterprise Networks to Identify Effective Mitigation Techniques," *International Journal of Computer Networks and Communications Security*, vol. 2, no. 9, pp. 298-307, 2014.
- [6] M. S. . a. J. M. Timo Kiravuo, "A Survey of Ethernet LAN Security," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 15, no. 3, pp. 1477-1491, 2013.
- [7] C. K. M. C. S. G. Biswajit Mondal, "Detection and Investigation of DDoS Attacks in Network Traffic using Machine Learning Algorithms," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 11, no. 6, pp. 2278-3075, 2022.
- [8] H. Team, "www.exploit-db.com," [Online]. Available: <https://www.exploit-db.com/docs/english/45050-vlan-hopping-attack.pdf>. [Accessed 9 2 2024].
- [9] S. M. M. M. Abrar Akber, "Network Security Issues of Data Link Layer: An Overview," 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2020.
- [10] H. Baum, "DETECTION OF VLAN HOPPING ATTACKS," *taltech digikogu*.
- [11] K. K. M. Lee, "SNMP-Based Detection of VLAN Hopping Attack Risk: ICISA 2018," in *Information Science and Applications 2018*, 2018.
- [12] H. Baum, "Taltech digikogu," [Online]. [Accessed 9 2 2024].

- [13] J. M. ., T. Ronny Bull, "VLAN hopping, ARP poisoning and Man-In-The-Middle Attacks in Virtualized Environments," in *DEF CON 24*, Las vegas,NV, 2016.
- [14] P. B. Rathod, "Comparative Analysis of Spanning Tree Protocol and Rapid Spanning Tree Protocol using Packet Tracer," in *International Conference on Science, Engineering & Technology*, 2022.
- [15] "Attacking the Spanning Tree Protocol," in *LAN Switch Security: What Hackers Know About Your Switches*, cisco press, 2008.
- [16] W. odom, *CCNA 200-301 Volume 1*, cisco press, 2020.
- [17] A. Balchunas, *Cisco CCNA Study Guide v2.71*, 2014.
- [18] A. K. S. & A. K. Misra, "Plugging DHCP Security Holes Using S-DHCP," in *Advances in Computing and Information Technology*, 1923.
- [19] Y. Dinç, "DHCP STARVATION".
- [20] N. T. Neminath Hubballi, "A Closer Look into DHCP Starvation Attack in Wireless Networks," *Computers & Security* , 2016.
- [21] A. S. M. M. A. J. Muhammad Nazrul Islam, "An Effective Method to Detect DHCP Starvation Attack using Port Scanning," in *2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM)*, 2023.
- [22] K. S. M. Youssef Iraqi, "Mitigation of DHCP starvation attack," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1115-1128, 2012.
- [23] N. T. Hubballi, "Detecting Stealth DHCP Starvation Attack using Machine Learning Approach," *J Comput Virol Hack Tech (2018)* , vol. 14, no. 2, pp. 233-44, 2018.
- [24] A. Nuhu, "Mitigating DHCP starvation attack using snooping technique," *FUDMA Journal of Sciences* , vol. 4, no. 1, p. 560, 2020.
- [25] A. R. . K. Elleithy, "Controlling Attacks of Rogue Dynamic Host Configuration Protocol (DHCP) to Improve Pedagogical Activities in Mobile Collaborative Learning (MCL) Environment," *J. of Commun. & Comput. Eng.*, vol. 3, no. 1, pp. 15-29, 2013.
- [26] F. A. B. Sameena Naaz, "Investigating DHCP and DNS Protocols Using Wireshark," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 18, no. 3, pp. 2278-0661, 2016.
- [27] S. M. M. N. Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing," *IEEE access*, 2022.
- [28] Z. T. E.-H. El-Hajj, "ARP spoofing: a comparative study for education purposes," 2009.
- [29] T. R. F. D. L. Nong Ye, "An attack-norm separation approach for detecting cyber attacks," *Information Systems Frontiers* , vol. 8, no. 3, pp. 163-177, 2006.

