PERFORMANCE ANALYSIS OF NETWORK PROTOCOL ATTACKS USING EVIL FOCA

***Zinmay Zaw*[1]*, Thiri Kyaw*[2]**

Mandalay Technological University, Lecturer, +095, Myanmar

Abstract

The world in today needs security in everywhere especially in communication. To make sure the network, a security engineer must know of a wide variety of attack types. There are so two types of attacks in communication such as layer protocol attacks and routing protocol attacks. Data Link layeris considered as the most fragile connection in a made sure about system. In the event that an underlying assault comes in at Layer 2, the entire system can be undermined. This paper analyses six attacks in Layer 2 protocol that are ARP (address resolution protocol) attack, CDP (Cisco Discovery protocol) attack, DHCP (Dynamic Host Configuration protocol) attack, DTP (Dynamic Trunking protocol) attack, STP (Spanning Tree protocol) and HSRP/VRRP (Host Standby Router Protocol/ Virtual Router Redundancy protocol). To represent the shortcoming of Layer 2 systems, assaulting tools for this layer are studied and examined in this paper. The principle elements of these tools and how they can be utilized to dispatch assaults are talked about. Although the authors of this paper strongly against malicious attacks to networks, it is a belief that the best way to protect a network is to know how it can be attacked. The system is implemented using Evil Foca tools. The tools drilled down in this paper can along these lines be utilized for doing assaults as a component of testing and learning.

Keyword: CDP, DHCP, STP and Evil Foca

1.INTRODUCTION

All attacks and moderation methods accept an exchanged Ethernet organize running IP. If it is a shared Ethernet as L2 protocol, some of these attacks may not work, but chances are, it is vulnerable to different ones. On the off chance that it is a mutual Ethernet as L2 convention, a portion of these assaults may not work, yet risks are, it is defenseless against various ones. New hypothetical attacks can move to practical in days. All testing was done on Cisco Ethernet switches. This is certifiably not an exhaustive chat on arranging Ethernet switches for security; the center is for the most part get to L2 attacks and their mitigation.

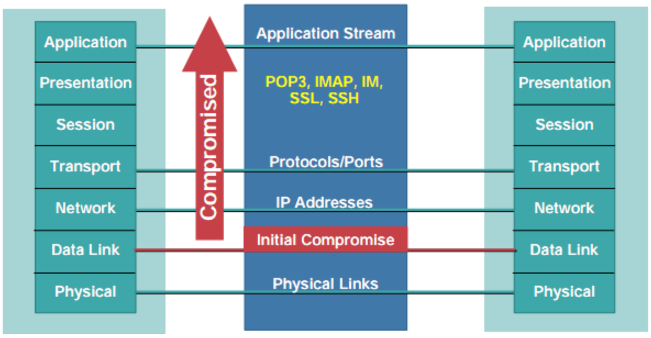


Figure 1. Lower Levels Affect Higher Levels

The proposed system is to analyze the attacks in layer 2 protocol. These attacks are vulnerable in communication. If the system maintains the data link layer attacks, the users can get the successful communication. The system considers six attacks in especially affecting the transmission channel. The system analyzes these six attacks for achieving good performance using Evil Foca

.

2. LITERATURE REVIEWS

Angelos D. Keromytis et al. in [1] proposed a Secure Overlay Services (SOS) architecture is associated with overlay tunneling, hashing routing and filtering. SOS carries out rigorous filtering at the edge routers and makes the attacker to move into the certain part of the network where the high speed routers considerably reduce the attack traffic. The attacker finds it difficult to attack the victim due to the introduction of uncertainty and security in the SOS architecture. The implementation of this architecture increases the delay latency by 2 and path reconstruction period is less than 10 seconds. Simple Object Access Protocol (SOAP) is the routing policy used to monitor the origin of traffic in the network.

Haining Wang et al. in [2] describes the Hop Count Filtering (HCF) is associated with the hop count information between the source and the destination. This HCF constructs a perfect IP-to-hop-count (IP2HC) mapping table and initialization and insertion of IP address into this mapping table requires equivalent pollution-proof method. Hop count value is not directly specified in the mapping table and the inspection and validation algorithm is associated with this mapping table. The main reason for selecting the hop count parameter to protect the victim from DDoS attack is that the hop count value is diverse in nature.

Angelos Stavrou et al. in [3] developed a Migrating Overlay (MOVE) is the Denial of Service prevention method that does not need any infrastructure support and filtering schemes. This method allots a new region for the valid users in the overlay networks to prove its efficacy. MOVE is an end to end solution or design for the DoS attack. In MOVE design, and overlay is combined with process migration settings.

Fanglu Guo et al. in [4] developed a Domain Name System (DNS) is one of the main components of the internet architecture. For a consistent internet system, all parts of the DNS organization must be filled and should not be left empty. When a small fraction of DNS becomes unavailable, it greatly affects internet connectivity. DNS requests and responses are more vulnerable to DDoS attack as they are base on UDP protocol. It is very difficult to protect the system against DDoS attacks. The attackers spoof the DNS request partially and they do not expose themselves and act as if they provide legitimate services.

The proposed system checks six attacks occurred in Data link layer. Then the system evaluates which attacks will be more vulnerable in communication system.

3. METHODOLOGY

This section may use some known form of attack and detect whether any traffic pattern matches the known pattern. Some of the prominent attacks based on Data Link layer are discussed in this section.

3.1. Working Principle of Attacks

The ARP (Address Resolution Protocol) is utilized to discover the MAC address that are attempting to reach on the nearby system, it's straightforward convention and helpless against an assault called ARP poisoning (or ARP spoofing).

There are three types of ARP attacks. These are ARP spoofing, ARP poisoning and MAC flooding. ARP spoofing is pretending to be something else. ARP poisoning is messing with ARP caches. MAC flooding is filling up CAM tables. This attack has no authentication in communication [5].

Address resolution protocol (ARP) is one of the important protocols in Transmission Control Protocol (TCP)/Internet protocol (IP) and is used to associate the IP address of the network layer to the MAC address of the data link layer3,4,5,6,12,17 18,21. Utilizing this protocol can recognize what numbers of hosts are associated in the LAN, and find the MAC address to IP address, in a LAN domain. ARP is finished by sending message request called broadcast to search the MAC address for the IP address. Subsequently, each device in the network receives the message and compares it with its IP address. If there is a match between IP's, then the generated ARP reply is called unicast. When other devices are identified which do not match the IP's, the packet will be dropped. After that, the IP-MAC addresses mapping is saved in the ARP cache table. ARP was designed without security features, so ARP doesn't support the authentication or integrity scheme, and thus can be easily spoofed. Therefore, ARP is highly susceptible to spoof and poison attacks.

The algorithm for ARP attacks in data link layer is as follows:

```
Step 1: Add static ARP entry for the server
Step 2: Automatically get user IP and MAC address
Step3: Formulate the Register Message
Step 4: Send the register message to the server
Step 5: Listen to updates from the server
Step 6: if message received from the server then
    Extract the source IP
    if source IP= Server IP then
        Extract the key, IP, MAC
        if received key is correct then
                if similar MAC in ARP Cache then
                        Delete this record
                else
                        Add static ARP entry using extracted IP and MAC address
                Return to step 5
        end if
    else
                Discard the message
                Return to Step 5
    end if
    else
                Discard the Message
                Return to step 5
    end if
    else
        Return to step 5
    end if
```

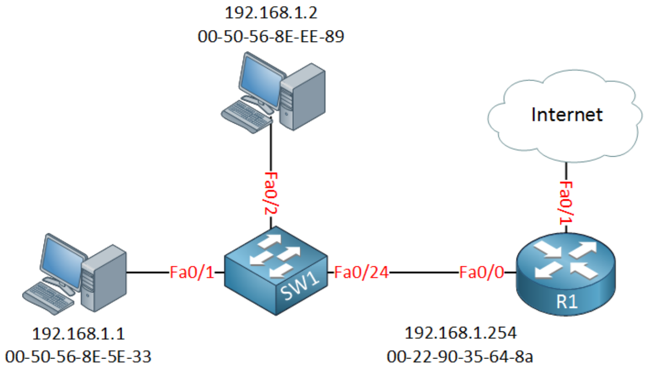


Figure 2. Flow of ARP Attacks in Communication

The Cisco Discovery Protocol (CDP) and the Link Layer Discovery Protocol (LLDP) are utilized for comparable purposes. Both offer an approach to see which sorts of gadgets are associated on a connection, just as a portion of the gadget setup (IP address, programming rendition, etc). Commonly this data is utilized by organize designers to improve investigating effectiveness on huge systems. Be that as it may, this data is likewise normally open to any individual who is "tuning in," which implies that an assailant simply needs to tune in on a similar connection so as to acquire a lot of data about the associated gadgets [6].

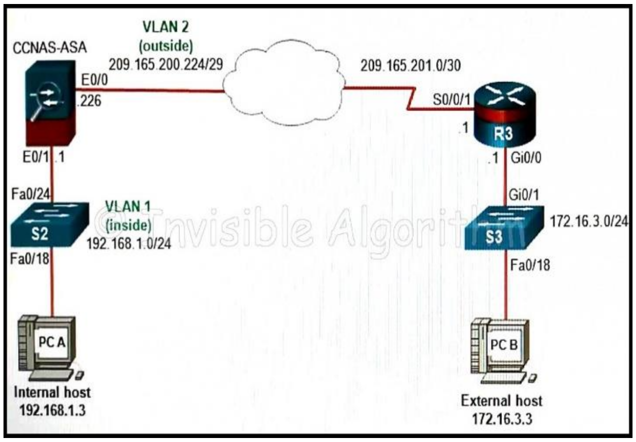


Figure 3. Flow of Attacks in CDP

Like different sorts of satirizing assaults, Dynamic Host Configuration Protocol (DHCP) ridiculing includes an assailant professing to be another person; for this situation, going about as the authentic DHCP server. Since DHCP is utilized on most systems to give tending to and other data to customers, losing control of this piece of the system can be perilous.

In DHCP ridiculing assaults, the aggressor puts a rebel DHCP server on the system. As customers are turned on and demand a location, the server with the quickest reaction is utilized. In the event that the gadget gets a reaction from the maverick server first, the rebel server can relegate any location just as control which gadget it utilizes as an entryway. An all around structured assault can channel traffic from nearby has to a rebel server that logs all traffic and afterward advances the traffic out to the "right" portal; to the gadget, this activity would be practically straightforward [7].

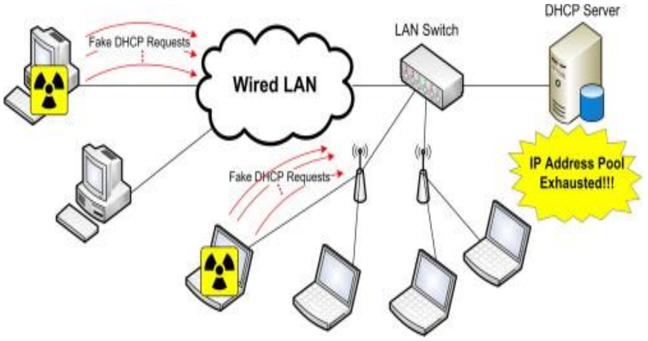


Figure 3. Flow of Attacks in DHCP

The Spanning Tree Protocol [8] is used on LAN-switched networks. It's essential capacity is expelling potential circles inside the system. Without STP, Layer 2 LANs just would quit working, in light of the fact that the circles made inside the system would flood the switches with traffic. The enhanced activity and setup of STP guarantees that the LAN stays stable and that traffic takes the most advanced way through the system. On the off chance that an aggressor embeds another STP gadget onto the system and endeavors to modify the activity of STP, this assault can possibly influence how traffic moves through the LAN.

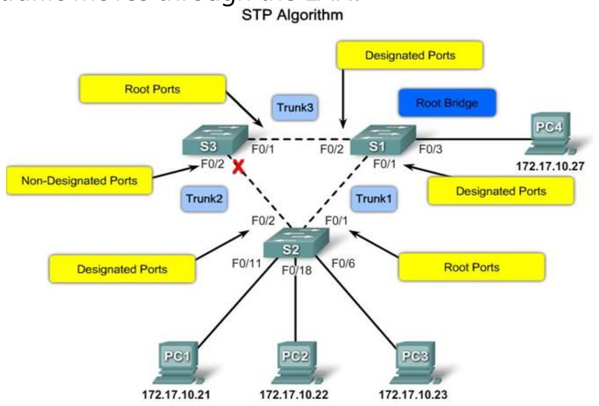


Figure 4. Flow of Attacks in STP

Utilizing HSRP, a lot of switches work in show to introduce the fantasy of a solitary virtual switch to the hosts on the LAN. This set is known as a HSRP gathering or a backup gathering. A solitary switch chose from the gathering is answerable for sending the bundles that hosts send to the virtual switch.

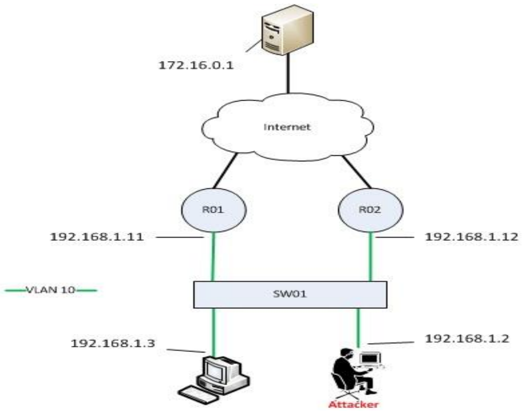
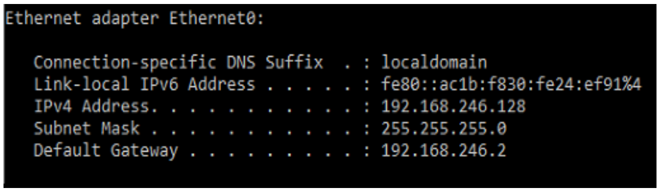


Figure 5. Flow of Attacks in HSRP

4. DESIGN AND IMPLEMENTATION PHASE

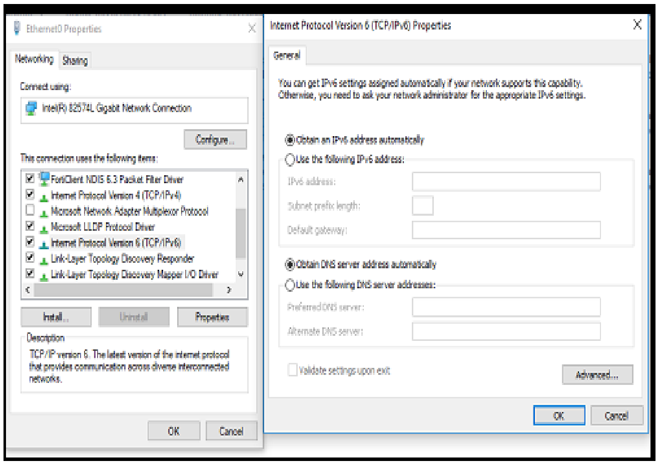
This paper discusses six attacks in Layer 2 protocol. These are ARP attack, CDP attack, STP attack, DTP attack, DHCP attack and HSRP attack. The proposed system tests these six attacks using Evil Foca Tools. After that the system concludes which one is most suitable in communication channel. The followings are the testing phase of attacks using Evil Foca.



```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::ac1b:f830:fe24:ef91%4
   IPv4 Address. . . . . . . . . . . : 192.168.246.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.246.2
```

Figure 6. Testing Connection using IPv4 address



Ethernet0 Properties

Networking | Sharing

Connect using:

Intel(R) 82574L Gigabit Network Connection

Configure...

This connection uses the following items:

☑ FortiClient NDIS 6.3 Packet Filter Driver
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Link-Layer Topology Discovery Responder
☑ Link-Layer Topology Discovery Mapper I/O Driver

Install... | Uninstall | Properties

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

OK | Cancel

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically
○ Use the following IPv6 address:

IPv6 address:
Subnet prefix length:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

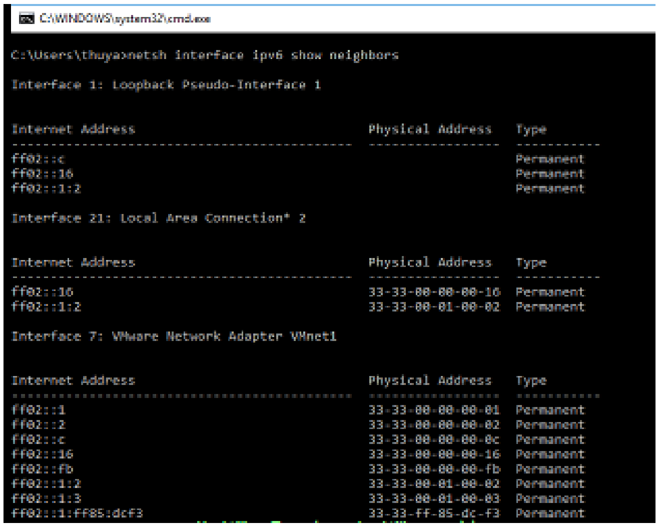
Preferred DNS server:
Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK | Cancel

Figure 7. IPv6is by Default Enable



C:\WINDOWS\system32\cmd.exe

```
C:\Users\thuya>netsh interface ipv6 show neighbors

Interface 1: Loopback Pseudo-Interface 1


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
ff02::c                                                          Permanent
ff02::16                                                         Permanent
ff02::1:2                                                        Permanent

Interface 21: Local Area Connection* 2


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
ff02::16                                      33-33-00-00-00-16  Permanent
ff02::1:2                                     33-33-00-01-00-02  Permanent

Interface 7: VMware Network Adapter VMnet1


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
ff02::1                                       33-33-00-00-00-01  Permanent
ff02::2                                       33-33-00-00-00-02  Permanent
ff02::c                                       33-33-00-00-00-0c  Permanent
ff02::16                                      33-33-00-00-00-16  Permanent
ff02::fb                                      33-33-00-00-00-fb  Permanent
ff02::1:2                                     33-33-00-01-00-02  Permanent
ff02::1:3                                     33-33-00-01-00-03  Permanent
ff02::1:ff85:dcf3                             33-33-ff-85-dc-f3  Permanent
```

Figure 8. Working with Neighbors

5. ANALYSIS OF COUNTERMEASURES

For accurate diagnosing, always accuracy performance metric is not sufficient to determine whether this is attack or not. And hence various performance metrics are used to measure the classifier's performance.

No	Attacks	Defense	Performance
1	ARP 1. spoofing 2. Poisoning 3. Flooding	1. port security and 802.1x 2. DAI 3. Static ARP entries	No authentication
2	CDP 1. DOS 2. Troll 3. Pwn	1. Turn of the CDP 2. Port security and 802.1x	No authentication
3	DHCP 1. DOS 2. Pwn - miTM attack -DNS spoofing -Boot from firmware and WiFi controller	1. Port security and 802.1x 2. DHCP snooping 3. IPS/IDS	No authentication
4	DTP 1. DOS 2. Pwn	1.Switchport nonnegotiate 2. Port security and 802.1x	No authentication
5	STP 1. DOS 2. Pwn	1. Stop using it 2. LACP + switch stack and virtualization 3. Disable STP on non-trunk ports 4. Enable BPDU Guard 5. Hope for no more bugs 6. Stay patched	No authentication
6	HSRP 1. DOS 2. Pwn • Act as MiMT for entries subnet • Easier than any other method • No need to brute force the password • Little/ no impact to users	1. MD5 for authentication string -Broken but better than nothing - Log failovers & treat as potential security events -Need to add more security 2. Get a better redundancy protocol -Common Address Redundancy Protocol -Form openBSD -Uses SHA1 & protects virtual IP	Get Authentication

Figure 9. Performance Evaluation of Attacks in Layer 2 Protocol

6. CONCLUSION

The proposed system mainly aims to evaluate which attack can get the most performance in data link layer (Layer 2) protocol. First the system designs the six attacks in layer 2. Then the system evaluates the level of attacks according to the testing results using Evil Foca. According to the evaluation, the users should use the HSRP attack in getting authentication. The proposed system analyses six attacks how to defense these attacks in layer 2.

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] W.-K. Chen, "Linear Networks and Systems" (Book style).Belmont, CA: Wadsworth, 1993, pp. 123–135.

[3] H. Poor, "An Introduction to Signal Detection and Estimation", New York: Springer-Verlag, 1985, ch. 4.

[4] B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[5] E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.

[6] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[7] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *WASET Trans. Neural Networks*, vol. 4, pp. 570–578, July 1993.

[8] R. W. Lucky, "Automatic equalization for digital communication," *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.