

Vulnerability Exploitation in the Open Shortest Path First Protocol

Ahmed M. Faisal*, Dr. Nada Hussein M. Ali

University of Baghdad College of Science Computer Science Department

Abstract

Open Shortest Path First (OSPF) is one of the most popular interior gateway routing protocols. It uses a link state routing algorithm. OSPF neighbors need to be able to send and receive broadcast 'hello' packets to each other to begin establishing neighbor adjacency, OSPF is vulnerable to insider attacks. For this reason, the attacker within the network can collect the hello message and modify it before resending it to the target device and establishing a neighbor relationship with it, which will be sufficient to redirect traffic. This paper presents two types of attacks; a man-in-the-middle MIMD attack and a denial-of-service DOS attack against the OSPF protocol and studies the influence of these attacks on protocol performance. The experiment work was executed in a simulation environment for attacks against OSPF using a real-world experiment (hands-on lab). Besides, it has been used a network topology that is fully connected by OSPF configured on real Cisco IOS images via different hardware routers and firewalls has been used for that purpose.

The obtained results from the Experiment Hands-on lab show how the attacker inside the network can listen to and intercept messages that are related to the OSPF protocol and how sending these messages again can affect the direction of network traffic direction. This will make the attacker able to read the traffic that he was not able to read it before.

Keywords: OSPF Exploitation, Vulnerability, Attack experiment, Simulation, Cisco Attack

1. INTRODUCTION

Nowadays, computer network has been widely used in many aspects of human life and network security is becoming more essential to all companies and institutions using the Internet [1]. The transmission of information through networks has become very important due to its advantages in facilitating the demands of nowadays through improving methods of storing and distributing information. This, in turn, has resulted in a rise in information issues and threats that compromise the integrity of the information of the institution and can be implemented in distributed systems environments [2]. Network security is the set of policies and practices adopted by a network administrator to protect the network from unauthorized access, security breaches, and unauthorized network intrusion [3].

A network protocol is a routing protocol defines the way packets are forwarded in a network. Routing protocols are used by routers to communicate with their neighbors, then creating routing tables depending on the data they obtain. Every device in the network is involved in the routing protocols' operation. A huge number of devices will be affected once the protocol is exposed. Routing protocols such RIP, OSPF, IS-IS, and BGP are often used [16].

Interior Gateway Routing (IGP) Protocol (OSPF) is the most popular and widely used IGP protocol on the internet. IGP enables routers within an autonomous system (AS) to build their routing tables, while adapting to changes in the topology of the autonomous system. There are different types of OSPF packets. a router will use the "hello" packet to find out who its neighbors are. The database description packet and link state request packet synchronize two router's databases when initiating an adjacency. The link-state update packet updates two routers' link state database. The link state acknowledgment packet confirms a reliable transfer by acknowledging a flooded LSAs. [4][5][6][7][8]. Figure 1 clarifies how OSPF sets up adjacency between two routers in the network.

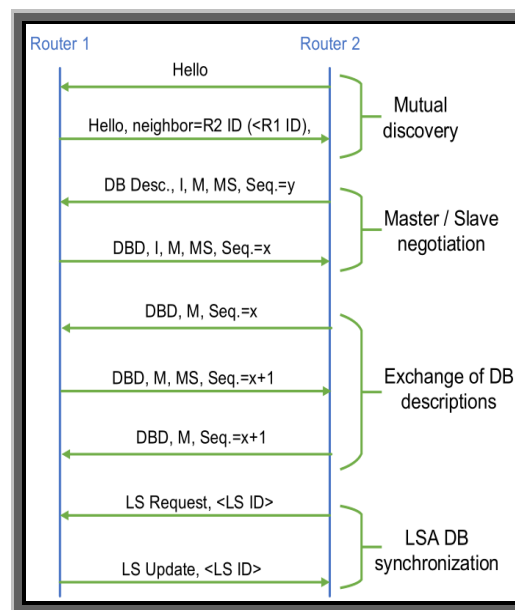


Figure 1. An example of setting up adjacencies between two OSPF routers [8].

Path spoofing constitutes a hazardous form of cyber-attack whereby an individual seeks to manipulate a computer or network to imitate other networks by assuming the identity of an authorized user and counterfeiting the Link State Advertisements (LSAs). The functionality of LSAs is predominantly reliant on the OSPF routing protocol, which utilizes a vulnerable protocol to alter tracking data and is frequently exploited for launching denial-of-service attacks [17].

The attacker manages to dispatch LSAs to the routers within the routing domain, with these routers erroneously recognizing them as authentic LSAs. In extensive scenarios encompassing service provider and enterprise networks, the subnet's gateway commonly operates as an OSPF node in core networks. Networks often possess roughly fifty percent of the broadcast "Hello" packets in a state of "passive disabled," effectively rendering them inactive. As a result, the host can capture the "hello" packets from these subsets, thereby extracting valuable network parameters from the adjacent routers. Armed with these network parameters, the attacker can fabricate counterfeit LSAs to deceitfully manipulate the routing tables across the entire OSPF network [9][10][12]. Among the most severe forms of attack is the manipulation of LSAs, where there exist two variants: self-LSA and other-LSA falsification. Self-LSA manipulation occurs when an attacker within a router fabricates an LSA connected to that specific router. Conversely, other-LSA falsification takes place when an attacker compels a target router to dispatch a fraudulent LSA on behalf of a victim router within the same Autonomous System (AS). To mitigate LSA attacks, OSPF incorporates several mechanisms, including flooding, a counter-response mechanism, link authentication, and employment of digital signatures. [8][11][18].

2. related works

Some of the related works that demonstrate the OSPF protocol vulnerability are shown as in the following:

Gabi Nakibly et al. (2014) [12], This work includes manual analysis and formal verification of OSPF specifications for additional vulnerabilities in the system's flight-back mechanism. The analysis showed that OSPF has a basic security flaw that makes it easy for a hacker to get around the flight-back mechanism. The vulnerability was confirmed by the majority of the leading router vendors. However, the findings of the analysis suggest that there are unlikely to be any other vulnerabilities with the flight-back mechanism.

Esmail Kaffashi et al. (2015) [13], Attacks on this protocol consist of LSA fake router that are controlled by the attacker. These attacks affect the routing domain portion of the protocol or cause serious harm based on the router's strategic location in the AS for bringing domain routing. The attacks that it's a type of attack that can cause a lot of damage to a network's security, and even though it has a fight-back feature, it won't have any effect on the routing domain. Basically, it's an attack that can change the routing domain's routing table with malicious threats without the fight back mechanism being turned on.

Yubo SONG et al. (2017) [14], The two most commonly used attacks to alter routing tables are adjacency spoofing and single path injection, which involve the injection of malicious (LSAs). Results from real-world experiments demonstrate

that these two attacks are capable of effectively altering routing tables of routers. This can result in DNS, spam, phishing website, interception, and man in the middle attacks. In addition, set up a vulnerability detection system to see if there are any existing vulnerabilities with the routing protocol used in the real-world routers.

Nan Li et al. (2018) [15], Conduct simulations involving the OSPF protocol to replicate instances of the Phantom Router's remote false adjacency attack and the concealed LSA attack. Evaluate the distinct traits exhibited by these attacks and subsequently assess their consequences through a comparative analysis. Drawing insights from the analysis outcomes, devise a detection mechanism grounded in the principles of a Finite State Machine. This mechanism is intended to accurately pinpoint the occurrences of the previously mentioned attacks. This undertaking contributes towards establishing an extensive comprehension of the attacks as well as the protective measures within the OSPF protocol.

3. Lab and Environment configuring

By using the EVE-NG platform as a lab simulation, the design of the proposed work simulates a private network that is fully connected and configured with OSPF as the main routing protocol. As depicted in Figure 2, the topology design of the lab consists of two parts (left and right). The left side part represents the headquarters (HQ) that provides and supports some of the services, such as DNS, mail service, and web service. All these services are installed on a Linux-Ubuntu server to simulate a real work environment and will help read different types of traffic. The right-side part denotes the client side, with the Windows 7 machine and two routers used and configured to provide a load balance in case one router are down. Moreover, two Cisco Adaptive Security Appliances (ASA) are used in the design as gateways for each side of the network.

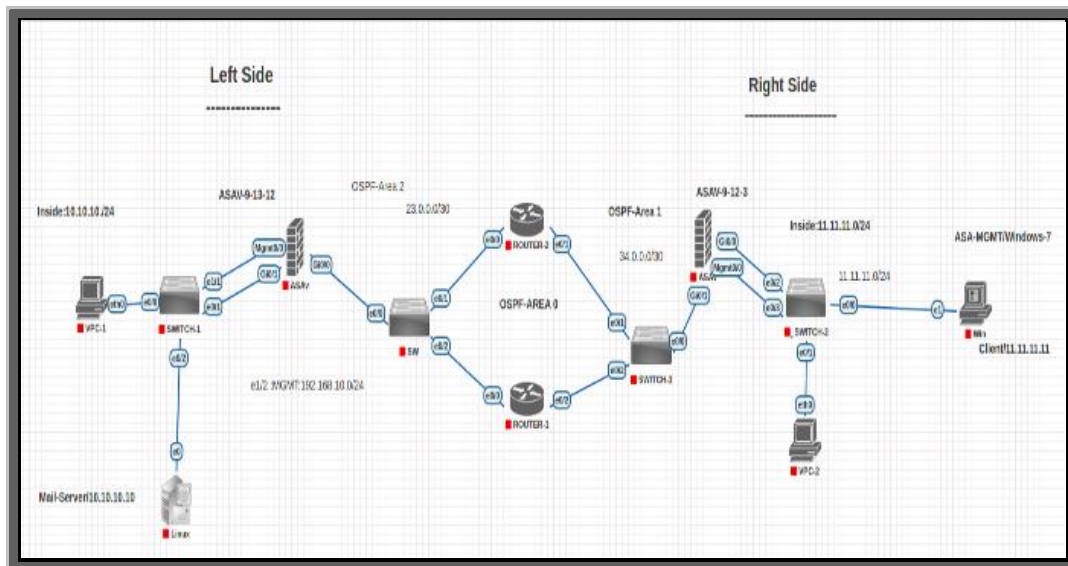


Figure 2. Network topology design.

3-1 Software to be required

Different types of software, operating systems, and simulation programs were being used in this work as described as follows:

- 1- VMware Workstation 16.1.2 build-17966106
- 2- PNET_4.2.10
- 3- Cisco Router image 7200
- 4- Cisco ASA image ASAV-9-12-3
- 5- Cisco ASA image ASA-9-13-12
- 6- Cisco Switch i86bi-Linux-L2
- 7- Windows 7 (As Client)
- 8- Linux-Ubuntu distribution (As a Server)

4. The Framework of the proposed work

To establish the attacks against OSPF, a number of steps need to be fulfilled. First step, the attacker machine needs to be inside the network to sense all the traffic passing through it. In the case of an attack on OSPF, it's easy to sniff the traffic because OSPF uses the multicast IP. After capturing the traffic, the second step is to choose the appropriate packet from that traffic or just can try to use a different number packet and then can choose the more appropriate one. The third step is to fuzz the packet and change some of the parameters. Using the Scapy tool to manipulate the OSPF parameters and propagate the fake packet to the target device and wait to build a neighbor relationship with it. Figure 3 clarifies the attacker's position in the network.

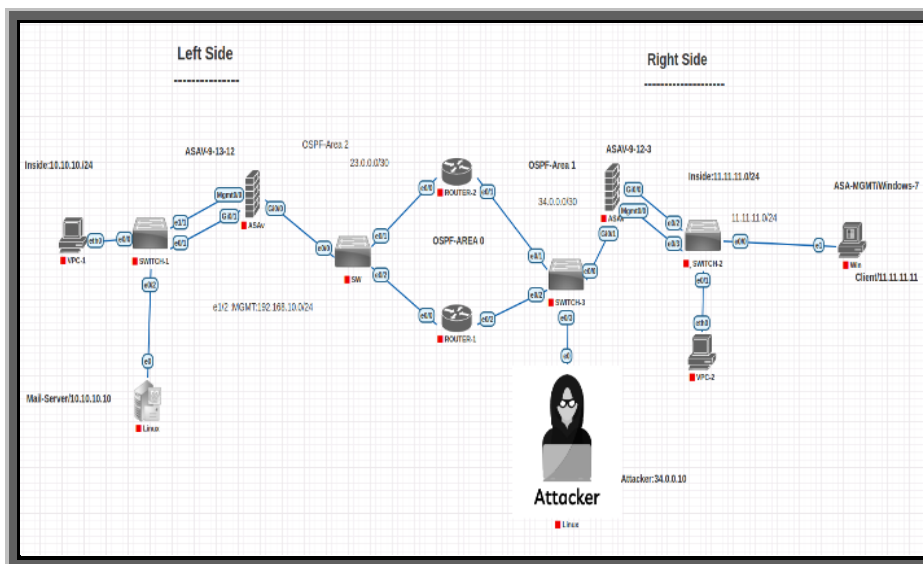


Figure 3. A network design clarifies attacker position.

Firstly, starting with capturing traffic that goes through the network and which is belonged to the OSPF protocol. Thereafter, the OSPF protocol starts it needs to negotiate with neighbor devices OSPF by sending Hello messages between each other to establish the neighbor relationship. Figure 4 clarifies the captured OSPF's messages.

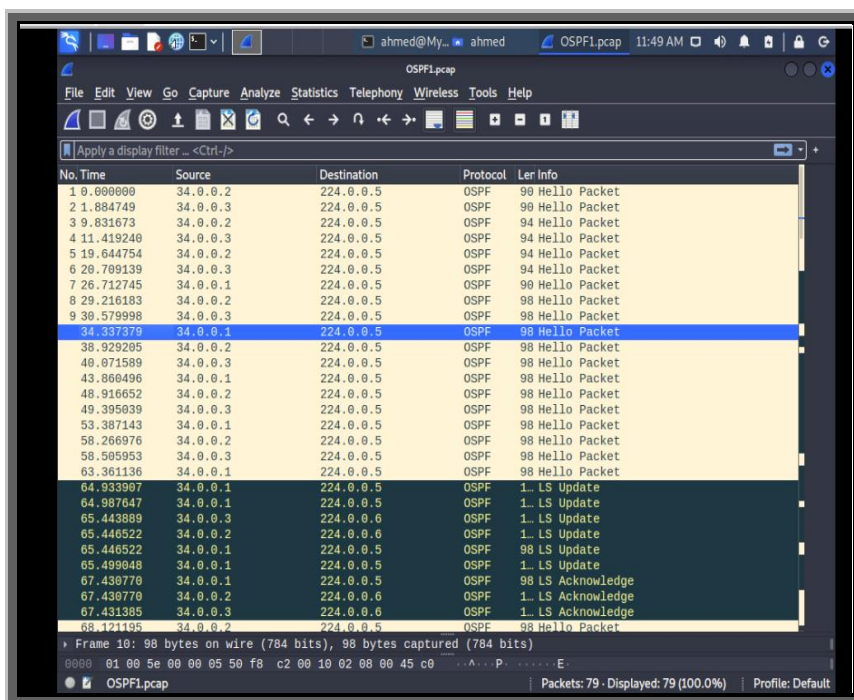


Figure 4. OSPF's messages captured.

At this time, after capturing the traffic and specifically traffic related to OSPF protocol there is a number of packets, only one packet is enough to implement this attack. In a random manner, one can choose the packet and make some of manipulating the parameters of that packet.

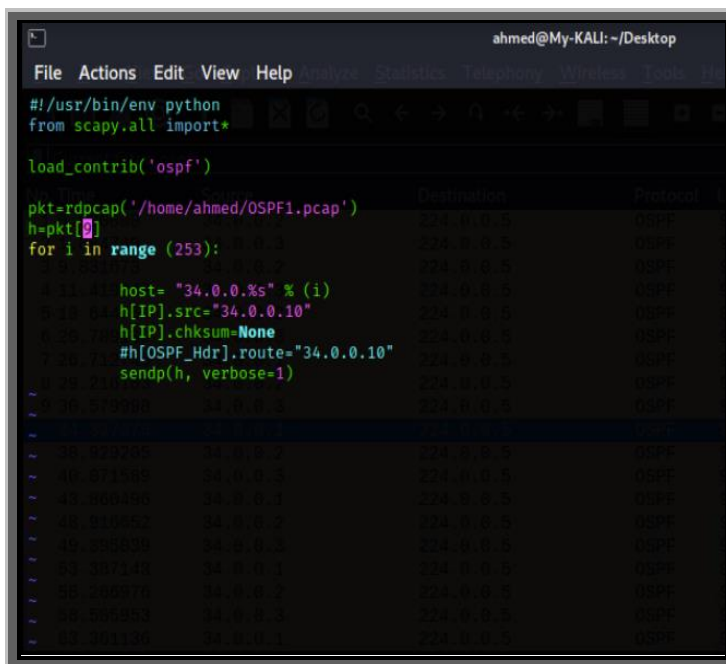
- *Attack Preforming*

Using the Python programming language and Scapy tool on a Kali-Linux machine would enable the user

To send a fake packet using the Scapy tool, the attacker will need to do the following steps:

- 1- The attacker will need to load the OSPF protocol contribution from Scapy's library.
- 2- Load the captured packet.
- 3- Change the parameters of the original packet, like the IP of the source's machine and others.
- 4- Send the fake packet.

After that, a new packet will be sent to the target device on the network. Figure 5 clarifies how to use the Scapy tool and manipulate packet parameters. Moreover, Figure 6 describes how to send fake packets to the target by using the Scapy tool.



```
ahmed@My-KALI: ~/Desktop
File Actions Edit View Help
#!/usr/bin/env python
from scapy.all import*

load_contrib('ospf')

pkt=rdpcap('/home/ahmed/OSPF1.pcap')
h=pkt[0]
for i in range (253):

    host= "34.0.0.%s" % (i)
    h[IP].src="34.0.0.10"
    h[IP].chksum=None
    #h[OSPF_Hdr].route="34.0.0.10"
    sendp(h, verbose=1)
```

Figure 5. Parameters modification by Scapy tool.

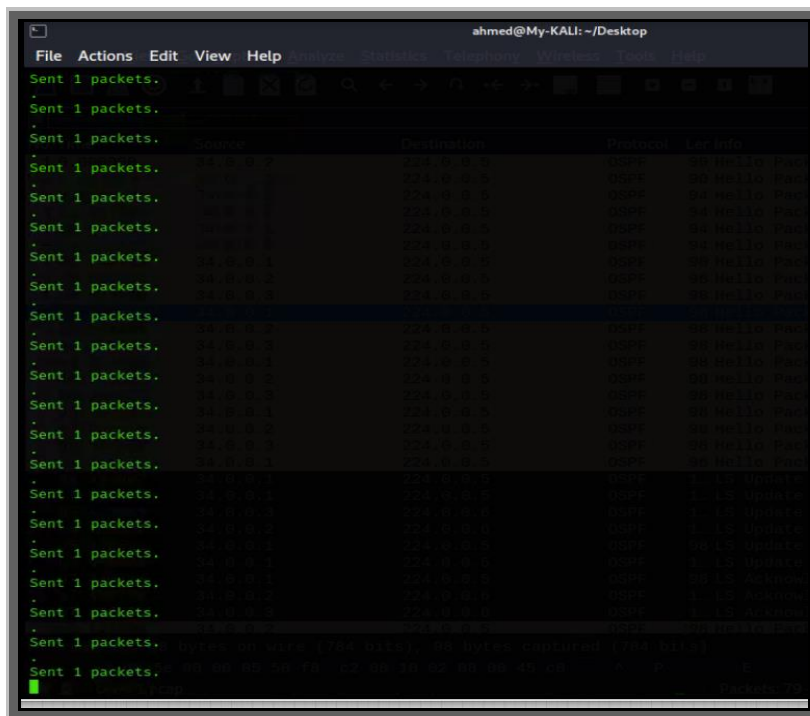


Figure 6. Fake packets sending.

5. Normal traffic Direction

To check the normal direction of traffic, it will use the client-side of the network and send Internet Control Message Protocol (ICMP) from the Windows client machine to the server destination. Figure 7 shows how to send ICMP traffic from client to server; the traffic would be moved through the interface e0/1 on Router-2. Although Figure 8 clarifies the normal traffic direction before the attack been occurred,

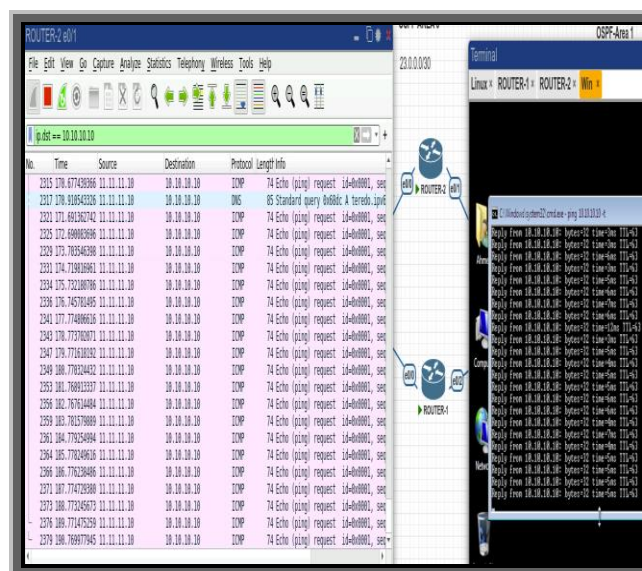


Figure 7. Normal traffic direction from client side to a destination.

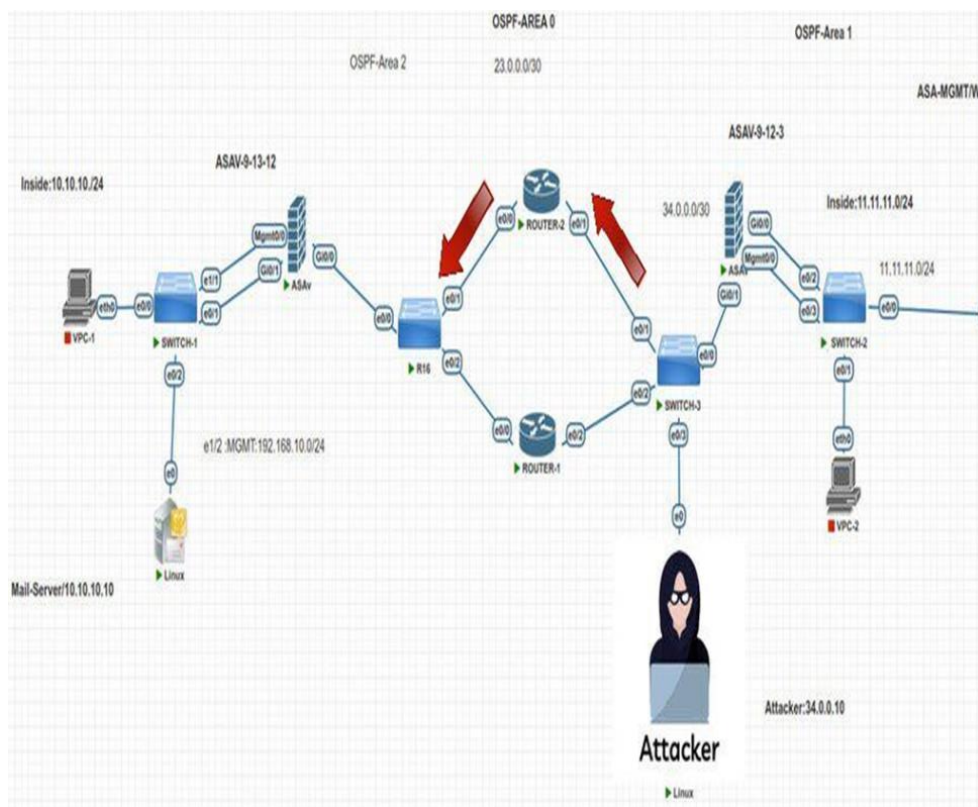


Figure 8. Normal traffic direction.

6. Establish the new neighbored relationship

To check the normal direction of traffic, it will use the client-side on the network and send Internet Control Message Protocol (ICMP) from the Windows-Client machine to the server destination. Figure 7 shows how to send ICMP traffic from client to server, the traffic would be moved through the interface e0/1 on Router-2. Although, Figure 8. Clarifies the normal traffic direction before the attack been occurred.

```

ROUTER-1#sh ip ospf neighbor
Neighbor ID  Pri  State           Dead Time   Address      Interface
34.0.0.2    1    FULL/DROTHER   00:00:39   34.0.0.2    Ethernet0/2
172.27.254.1 1    FULL/BDR      00:00:32   34.0.0.1    Ethernet0/2
172.27.254.1 1    EXSTART/DROTHER 00:00:20   34.0.0.10   Ethernet0/2
34.0.0.2    1    FULL/BDR      00:00:32   12.0.0.2    Ethernet0/0
192.168.10.1 1    FULL/DROTHER   00:00:31   12.0.0.1    Ethernet0/0
ROUTER-1#
    
```

Figure 9. The relationship with the attacker’s machine inside the Router-1.

7. Checking OSPF Neighbor relationship status on network’s devices

To confirm that the state of neighbor relations on devices has indeed been affected and that the attacker’s IP address has also been added to the target devices. If the attacker uses different sourced packets, like packet number 8, which is sourced from Router-1, the attacker will play the role of Router-1, which will create a neighbor relationship with both Router2 and ASA-2. Figure 10 clarifies the state relationship with the attacker’s machine inside the Router-2. In addition, Figure 11 shows the state relationship with the attacker’s machine inside Firewall 2.

```

Neighbor ID Pri State Dead Time Address Interface
34.0.0.3 1 FULL/DR 00:00:37 34.0.0.3 Ethernet0/1
34.0.0.3 1 EXSTART/DROTHER 00:00:33 34.0.0.10 Ethernet0/1
172.27.254.1 1 FULL/DROTHER 00:00:38 34.0.0.1 Ethernet0/1
34.0.0.3 1 FULL/DR 00:00:31 12.0.0.3 Ethernet0/0
192.168.10.1 1 FULL/BDR 00:00:31 12.0.0.1 Ethernet0/0
ROUTER-2#
    
```

Figure 10. Neighbor relationship on Router-2.

```

Neighbor ID Pri State Dead Time Address Interface
34.0.0.2 1 FULL/BDR 0:00:31 34.0.0.2 outside
34.0.0.3 1 FULL/DR 0:00:36 34.0.0.3 outside
34.0.0.3 1 2WAY/DROTHER 0:00:39 34.0.0.10 outside
FIREWALL-2#
    
```

Figure 11. Neighbor relationship on Firewall-2.

8. New Traffic Direction after Attack occurred

The new neighbor relationship between the attacker and target device can mainly affect the direction of traffic, the direction of traffic will change after the attacker adds himself inside the OSPF as a neighbor. The traffic will move through the attacker’s machine, from the inside of the attacker’s machine. Figure 12 describes the new direction of the traffic.

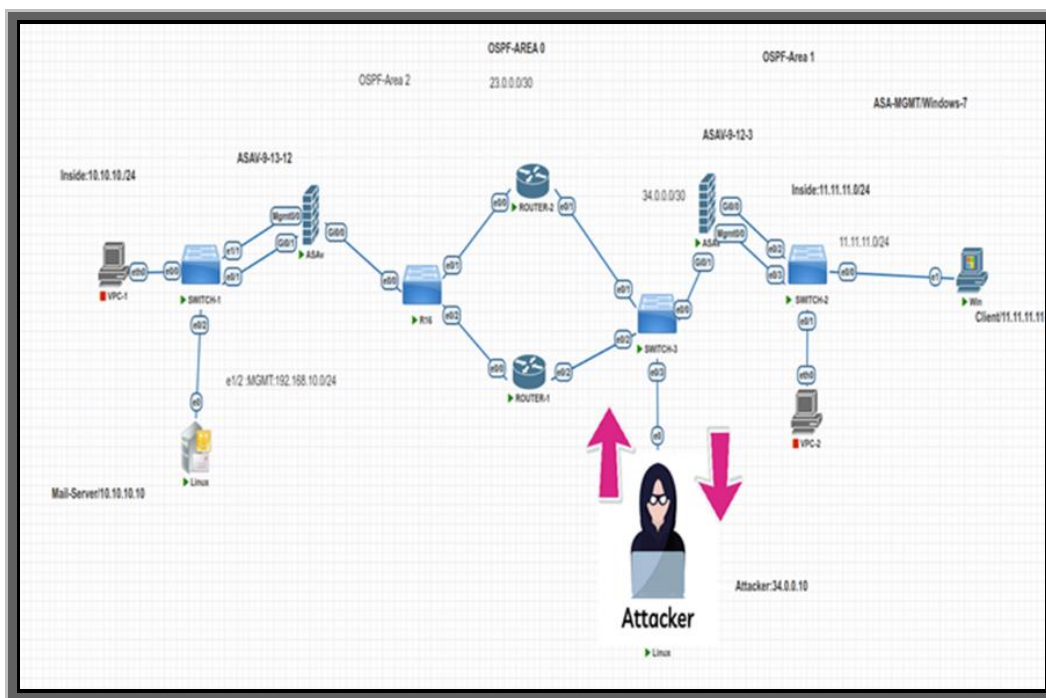


Figure 12. The new direction after attack.

As demonstrated in Figure 12, the attacker will be able to easily detect and sniff the traffic sourced from a client to a server after the new traffic direction using the Wireshark network sniffer. Figure 13 shows how the attacker can read and sniff the traffic.

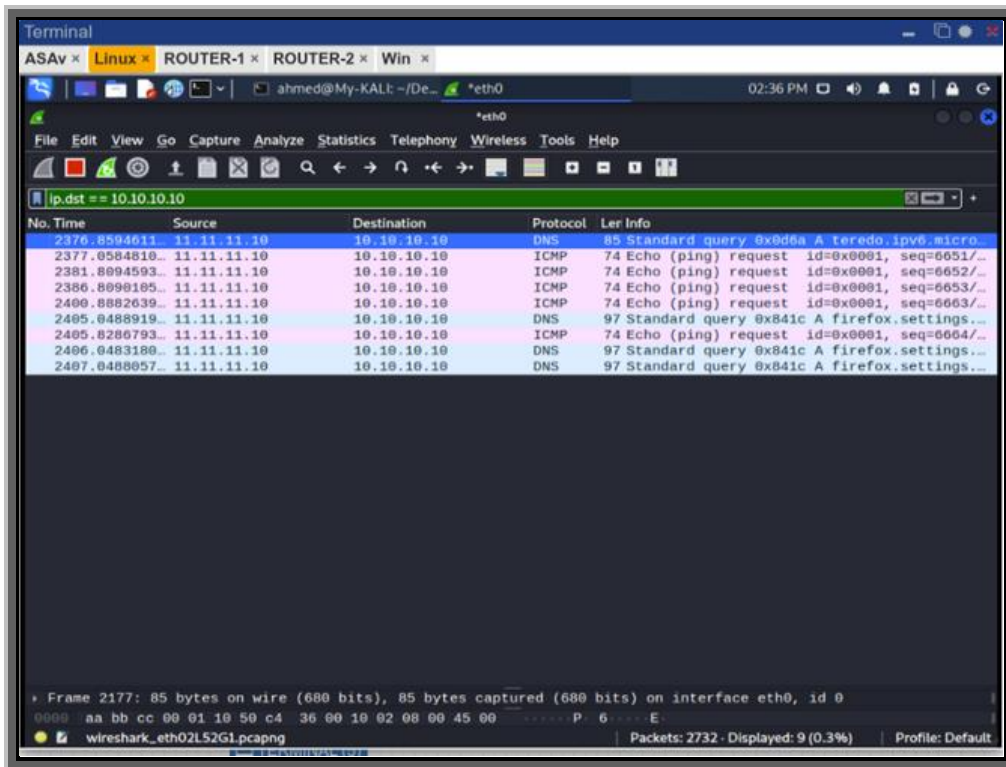


Figure 13. traffic redirection to Attacker’s machine.

8-1. DOS Attack

The change in traffic directly after the attack will affect the availability of the services since the number of packets will be dropped, causing a denial-of-service (DoS). Figure 14 clarifies the dropping of a number of packets after using PING to detect the destination.

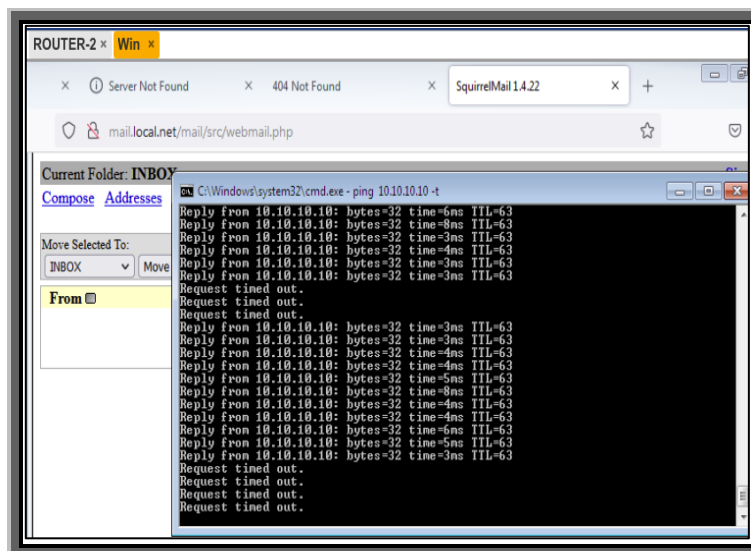


Figure 14. A Denial-of-Service after attack.

8-2 Captured Network Traffic

The change in traffic directly after the attack will affect the availability of the services since the number of packets will be dropped, causing a denial-of-service (DoS). Figure 14 clarifies the dropping of a number of packets after using PING to detect the destination.

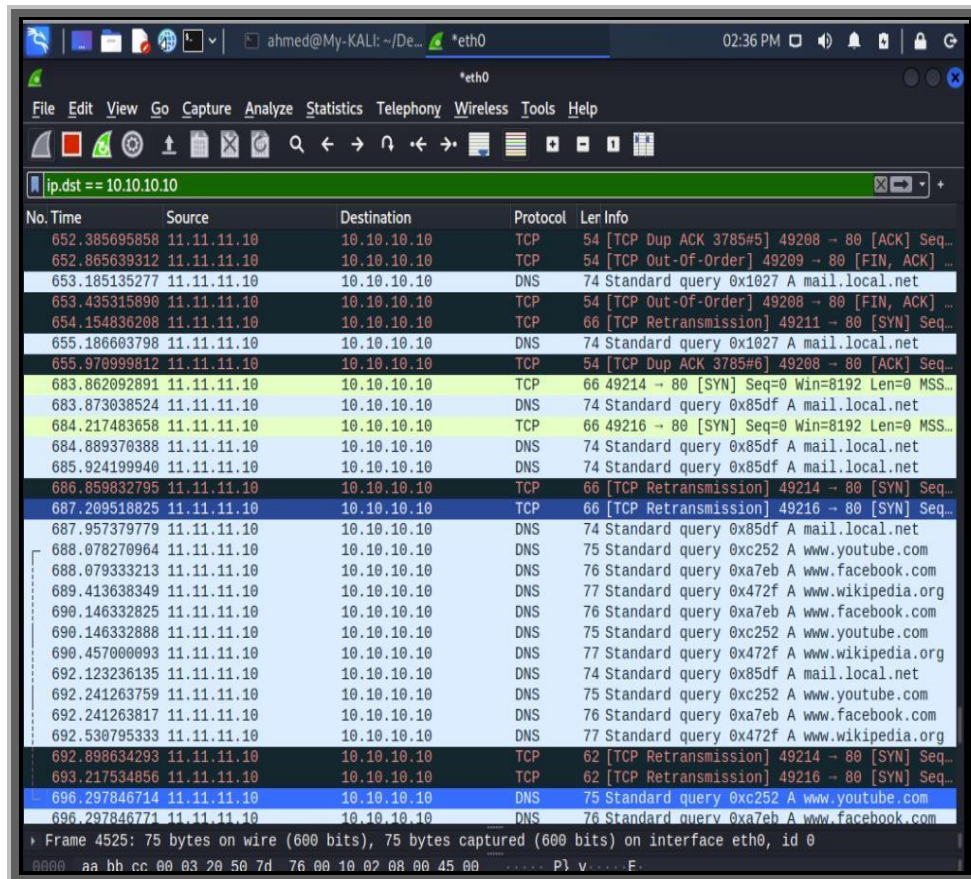


Figure 15. How the attacker can read different type of packets.

More details and information about packets can be gotten by choosing a specific one. Figure 15 clarifies the DNS packet that works on port 53 with the domain name (mail.local.net). whereas Figure 16 clarifies the DNS packet that works on port 53 with the domain name (mail.local.net).

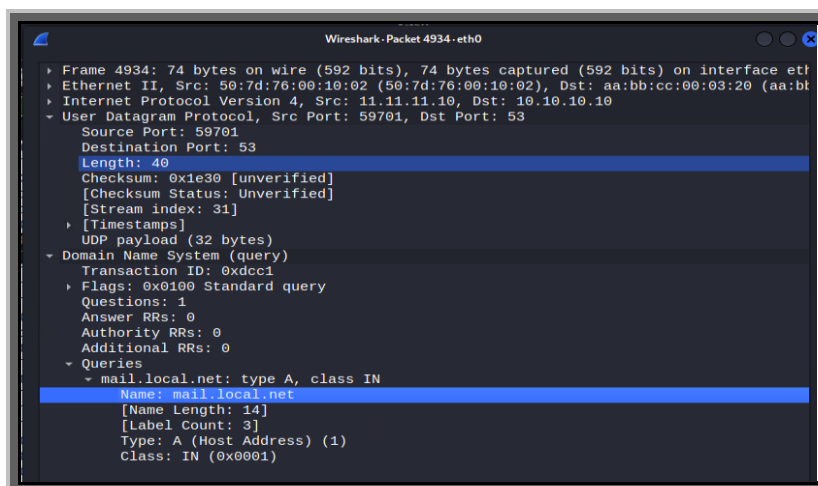


Figure 16. mail service from client.

Conclusions

The attack on the OSPF protocol would be achieved by a variety of techniques. This paper is based on one of these techniques, using a Python-based tool on Linux-Kali disruption. Any host inside the network is able to detect and sense the multicast broadcast of the OSPF packets.

An attacker could use one of the sniffing programs to read and try the most appropriate packet that could establish a neighbor relationship with the target device. After the neighbor relationship has been established between the target device and the attacker, the attacker will be able to add his device to the OSPF's state relationship. Not all OSPF parameters on the fake packet are able to be modified, the OSPF protocol that was configured on the network devices would be able to sense and detect the attack and the malformed packet. The fake packet needs to be sent within the interval of dead time; otherwise, the neighbor will be down. After neighbor relations have been established, a lot of packets will be able to be read and detected by the attacker. Based on traffic redirection a denial of service will take place, and the services on the server will be impossible to reach.

REFERENCES

- [1] D. I. Mahmood and S. M. Hameed, "A Multi-Objective Evolutionary Algorithm based Feature Selection for Intrusion Detection," *Iraqi Journal of Science*, vol. 58, no.1C, pp. 536-549, 2017. doi:10.24996/ij.s.2017.58.1C.16.
- [2] T. A. Khaleel and A. A. Al-Shumam, "A study of graph theory applications in it security," *Iraqi Journal of Science*, vol. 61, no.10, pp. 2705-2714, Oct. 2020. Doi: 10.24996/ij.s.2020.61.10.28.
- [3] M. Abdulkadhim and S. Hasan, "Boosting the Network Performance using Two Security Measure Scenarios for Service Provider Network," *Iraqi Journal of Science*, pp. 174-179, Jan. 2021. doi: 10.24996/ij.s.2021.SI.1.24.
- [4] F. Wang and S. F. Wu, " On the vulnerabilities and protection of OSPF routing protocol," *In Proceedings 7th International Conference on Computer Communications and Networks*, 1998.
- [5] A. Kirshon, D. Gonikman and G. Nakibly, " Owing the Routing Table New OSPF Attacks," *BlackHat Briefings and Trainings USA*, pp.1-18, Nov. 2011.
- [6] J. Deng, S. Wu and K. Sun, "Comparison of RIP, OSPF and EIGRP Routing Protocols based on OPNET," Simon Fraser University School of Engineering Science, 2014. Available: https://www.sfu.ca/~ljlja/ENSC427/Spring14/Projects/team9/ENSC427_team9_report.pdf
- [7] P. Anu, and S. Vimala, "Optimization of OSPF LSA flooding process using clustering technique," *in proceeding of the 2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 2016.
- [8] B. Al-Musawi, P. Bransh, M. F. Hassan and S. R. Pokhrel, "identifying OSPF LSA falsification attacks through non-linear analysis," *Computer Networks*, p.107031, Feb. 2020.
- [9] B. Vetter, F. Wang and S. F. WU, " An experimental study of insider attacks for OSPF routing protocol," *In Proceedings 1997 International Conference on Network Protocols*, pp. 293-300.
- [10] D. S. Robbins, " Using Protocol Redundancy to Enhance OSPF Network System Survivability," *in Southeast Conference*, pp. 1-7, Apr. 2018. doi: 10.1109/SECON.2018.8479134.
- [11] D. Sangroha, and V. Gupta, " An Approach to Detect and Recover from OSPF Attacks. *In Security in Computing and Communications*," *Second International Symposium, SSSC, Delhi, India*, 2014.
- [12] G. Nakibly, A. Sosnovich, E. Menahem, A. Waizel, and Y. Elovici, "OSPF vulnerability to persistent poisoning attacks: a systematic analysis," *In Proceedings of the 30th Annual Computer security applications Conference*, pp. 336-345, 2014. doi:10.1145/2664243.2664278.
- [13] E. Kaffashi, A. Mousavi, H. Rahvard, S. H. Bojnordi, F. Khademsadegh, and S. Amirian, " A new attack on link-state database in open shortest path first routing protocol," *Journal of Electrical and Electronic Engineering*, pp.39-45, 2015. doi: 10.11648/j.jeee.s.2015030201.19.
- [14] Y. Song, S. Gao, A. Hu and B. Xiao, "Novel attacks in OSPF networks to poison routing table," *IEEE International Conference on Communications (ICC)*, pp.1-6, 2017. doi: 10.1109/ICC.2017.7996829

- [15] N. Li, Y. Liu, and Z. Lu, "Research on Analysis and Detection Technology for Several Attacks of OSPF Vulnerability," *International Conference on Transportation & Logistics, Information & Communication, Smart City*, pp.299-303, 2018. doi: 10.2991/tlicsc-18.2018.48.
- [16]. C. Wen, Y. Liu S. Li, "A Routing Protocols Fuzzing Method based on MAN-IN-THE-MIDDLE," *In 2022 2nd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT)*, pp. 491-496, 2022. doi: 10.1109/ICFEICT57213.2022.00092.
- [17]. H. Sawalmeh, M. Malayshi, S. Ahmed, and A. Awad, "VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements," *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp.236-241, Sep. 2021. doi:10.1109/3ICT53449.2021.9581512.
- [18] R. Meredith, and R. Dutta, "Increasing Network Resilience to Persistent OSPF Attacks," *IEEE International Conference on Communications (ICC)*, pp. 1-7, May. 2019. doi:10.1109/ICC.2019.8761838.