ATLANTIS PRESS
Advances in Intelligent Systems Research, volume 161
International Conference on Transportation & Logistics, Information & Communication, Smart City (TLICSC 2018)

Research on Analysis and Detection Technology for Several Attacks of OSPF Vulnerability

Nan Li*, Yujing Liu and Zexin Lu
College of Computer, National University of Defense Technology, Changsha 410073, China
*huanghelou2015@139.com

Abstract. OSPF is the most widely deployed intra-domain routing protocol within an autonomous system. Although there are several mechanisms, such as flooding and fight-back, strengthening the security of OSPF, some serious vulnerabilities of the protocol are newly exploited. In this paper, we perform simulations of Phantom Router Remote False Adjacency Attack and Disguised LSA Attack against OSPF protocol, analyze their characteristics and compare their effects. According to the analysis results, we propose a Finite State Machine Based detection mechanism to detect the above attacks. Our work shed light on a deep understanding of the attacks and defense of OSPF protocol.

Keywords: Vulnerability; Simulation; Detection.

1. Introduction

OSPF (Open Shortest Path First) protocol is the most widely used intra-domain routing protocol, providing dynamic routing for hosts within an autonomous system. There are several security strengths of OSPF to prevent attackers from disturbing the routing state, such as flooding and fight-back. However, in recent years, many serious vulnerabilities of the protocol have been discovered to bypass the fight-back mechanism. Furthermore, several attacks which exploit the vulnerabilities can persistently and stealthily change the routing table of OSPF, causing a serious security threat such as routing hijacking or routing blackhole. These new types of attacks includes the Phantom Router Remote False Adjacency Attack, the Disguised LSA Attack [1] [2], and the Partition Attack[3]. Except for the very first disclosure research of these attacks, there is few work for further understanding and defense against them.

In this paper, firstly, we perform simulations of Phantom Router Remote False Adjacency Attack and Disguised LSA Attack in GNS3 environment. Secondly, we analyze their characteristics and compare their effects. Finally, according to the analysis results, we propose a Finite State Machine Based detection mechanism to detect the attacks.

The structure of this paper is as follows: The second section introduces the principle of OSPF vulnerability utilization technology; the third section analyzes the characteristics of OSPF vulnerability utilization technology in detail; the fourth section details the OSPF attack detection scheme.

2. Introduction to OSPF Vulnerability Utilization Technology

2.1 Phantom Router Remote False Adjacency Attack

In the process of establishing an OSPF adjacency relationship, there is a vulnerability that the authentication is not strict. The attacker can establish an adjacency relationship between the target router and the phantom router that does not exist by constructing an OSPF packet with a malicious value. Then the attacker can continue forging LSAs and arbitrarily claiming network notifications directly connected to the Phantom Router, and achieve traffic transfer and even the effect of routing blackhole [2].

2.2 Disguised LSA Attack

When the normal router receives a LSA, the value of the ADVRouter field is used as the basic for the fight-back mechanism[1]. In the period of routing table calculation, the value of LinkState ID field in the LSA packet is used. The values of the above two fields are the same for the Router-LSA

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

packets sent by the normal router, however, an attacker can disguise a Router-LSA with inconsistent values in the above two fields, to bypass the fight-back mechanism and tamper the routing table, causing traffic transfer [3].

3. Analysis and Comparison of OSPF Vulnerability Utilization Technology Features

3.1 Phantom Router Remote False Adjacency Attack

The experiment uses GNS3 and kali virtual machine (Fig.1), and uses wireshark for packet capture analysis. The network type uses a peer-to-peer network. The target router is R2 and Tthe Scapy program running on kali virtual machine C1 is used to forge the LSA.

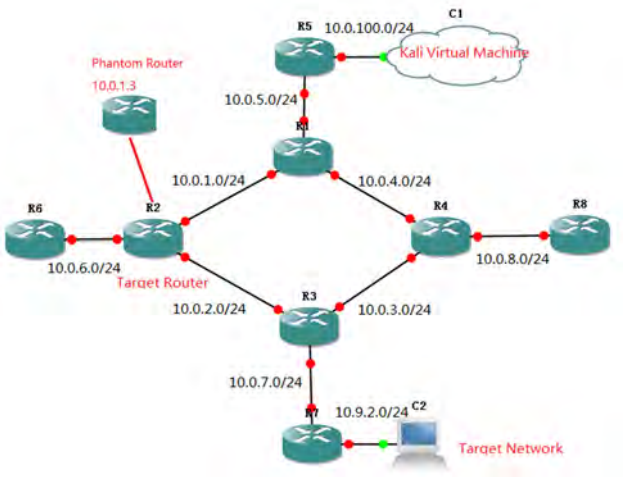

Figure 1. Phantom Router Remote False Adjacency Attack topology

In normal state, the next hop of R2 to the network of 10.9.2.0 is R3 (10.0.2.2). After C1 sending a sequence of attack messages, there shows up a phantom neighbor router (10.0.1.3) in R2's routing table. Moreover, after C1 sending forged LSAs that announce the network of 10.9.2.0 is adjacent to the phantom router, the next hop of R2 to the network of 10.9.2.0 has been falsified from 10.0.2.2 to 10.0.1.3 (Fig.2.). As a result, the route from R2 to 10.9.2.0 becomes a blackhole. This forged routing message propagates in the network. Therefore, routes from R5, R1, R6 to 10.9.2.0 become blackhole, too.

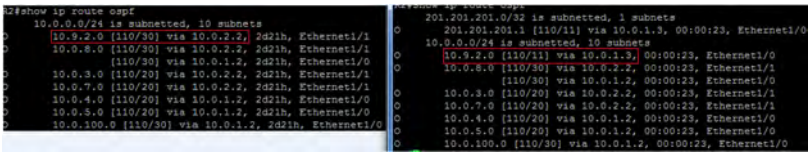

Figure 2. The routing table of Target Router R2

The premise of the Phantom Router Remote False Adjacency Attack is to control at least one router within the target network in order to propagate forged LSAs. Because the attacker can propagate the forged LSAs without the LAN of the target router, this attack is hard to be found. At the side of the effect of the attack, the Phantom Router Remote False Adjacency Attack may lead to routing black holes. Considering the duration of the attack, because the Phantom Router cannot reply LSACK to the target router in real time, the attack duration is not long. The attack has features that there will appears some OSPF packets with a blank DBD content in the OSPF network when the Phantom Router Remote False Adjacency Attack happened. Besides, the target router continuously sends a large number of ARP request packets, which will not be responded to the Phantom Router.

3.2 Disguised LSA Attack

The experiment uses GNS3 combined with kali virtual machine to build the simulation environment (Fig.3), and uses wireshark for packet capture analysis. The network type uses a peer-to-peer network. Disguised LSA will be constructed by scapy. The red arrow line in Fig.3 is the routing path from host C3 to host C2 before the attack occurs. Then, C1 sends a disguised LSA packet to R2, announcing that the network of 10.9.2.0/24 is directly linked to R1. Therefore, the routing table of R2 is changed. The next hop of R2 targeted to C2 has been falsified from R3 (10.0.5.2) to R1 (10.0.1.1) (Fig.4.). The green arrow line is the routing path from C3 to C2 after the attack occurs.

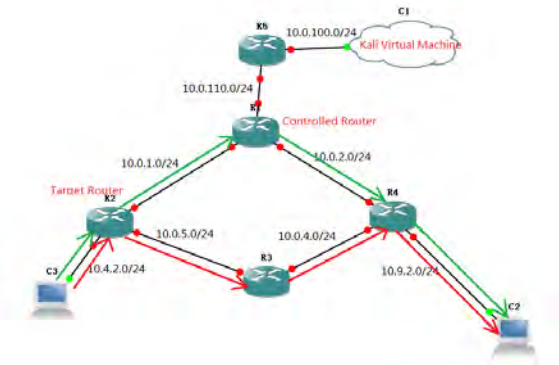

Figure 3. Disguised LSA attack experimental topology

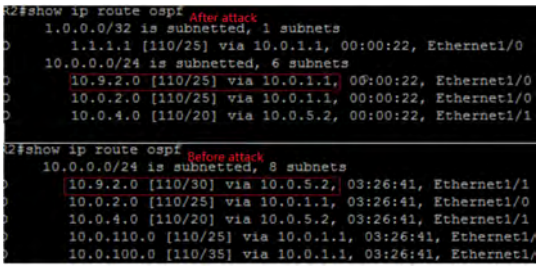

Figure 4. The routing table of Target Router R2.

The premise of Disguised LSA Attack is that the attacker has controlled at least one PC in the target network. Since the attacker just need one disguised LSA to have the effect, this attack is easy to implement. The Disguised LSA Attack can garble the routing table of target router in a long time. After the attack occurs, the effect of transferring traffic can be generated. For Cisco series routers, after the Disguised LSA Attack occurs, the obvious feature is that the routing table of some routers will be emptied, which may cause the attention of the network administrator.

4. OSPF Attack Detection Scheme

From the above analysis we can see that malicious attacks of OSPF often result in a set of possible alarm event sequences or some abnormal packets in the network, which can be described as input strings in the Finite State Machine. Previous researches succeed in detection of Seq++ attack, Maxseq attack and Maxage attack of OSPF based on the idea of Finite State Machine [4]. In this paper, we propose Finite State Machine based detection scheme for the two new attacks.

For the Phantom Router Remote False Adjacency Attack, the Finite State Machine is constructed by means of message content detection (Fig.5, IP(x) is the IP of phantom router.). When a large number of ARP request packets for an IP address appear but no response are generated in the OSPF network, and the LSA packets whose ADVRouter is equal to the IP of Phantom Router are propagated in the OSPF network, the Phantom Router Remote False Adjacency Attack may be happened in the OSPF network.

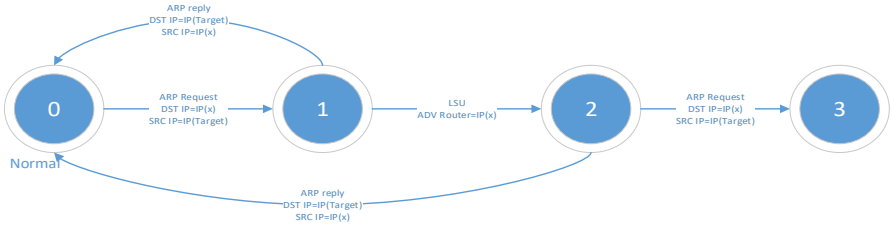

Figure 5. Finite State Machine for Phantom Router Remote False Ajacency Attack

For the detection of Disguised LSA Attack, there may be Disguised LSA Attack if two Router-LSAs whose LinkStateID field are the same but ADVRouter field are different(Fig.6, LinkStateID(x) and ADVRouter(x) may be the field in the Disguised LSAs.), because maybe one of the Router-LSA is from the original router, which is the correct LSA, and the other Router-LSA is from the attacker, which is the disguised LSA. If there are Router-LSAs whose value of LinkStateID field is different with its value of ADVRouter, the LSAs may be sent by the attacker. And the state will be record. In the next step, once there are Router-LSAs in the OSPF network, whose value of LinkStateID field are the same with LinkStateID(x) while different value of ADVRouter field from ADVRouter(x), the LSAs before whose value of LinkStateID is different with ADVRouter may be sent by the attacker.

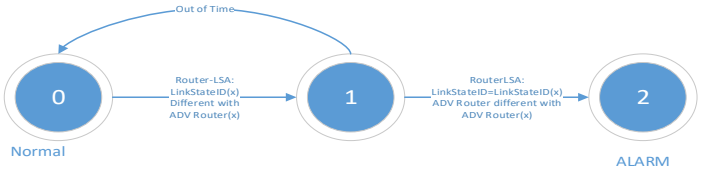

Figure 6. Finite State Machine for Disguised LSA Attack

5. Conclusion

Through the above several attacks' simulations for OSPF networks, it can be compared from the aspects of attack premise, attack difficulty, feature difference, attack effect and duration (Table 1).

Table 1. Comparison of Different Attacks

	Premise	Difficulty	Feature	Effect	Duration
Phantom Router Remote False Adjacency Attack	Routers controlled	8 OSPF forged packets	Empty DBD;Unreacted ARP requests	Routing blackhole	Short
Disguised LSA Attack	PC controlled	1 OSPF forged packet	Cleared routing tables	Data bypass	Long

This paper analyses the Phantom Router Remote False Adjacency Attack and the Disguised LSA Attack. From the theoretical level, the principle and possible effects of several OSPF vulnerability utilization technologies are analyzed. The OSPF network simulation experiment environment was built by the GNS3 simulation platform, and the specific analysis and comparison were made from the aspects of attack premise, attack difficulty, feature difference, attack effect and duration of different vulnerability utilization technologies. Finally, based on the above-mentioned different types of vulnerability utilization technologies, the research is carried out from the perspective of attack detection schemes, and the Finite State Machine is constructed for different types of OSPF attacks.

Acknowledgments

This work is supported by the National Natural Science Foundation of China, under Grant No. 61602503.

References

[1]. Nakibly G, Kirshon A, Gonikman D, et al. Persistent OSPF Attacks[J]. 2013.

[2]. Nakibly G, Sosnovich A, Menahem E, et al. OSPF vulnerability to persistent poisoning attacks: a systematic analysis[C]// Computer Security Applications Conference. ACM, 2014:336-345.

[3]. Cohen R, Hess-Green R, Nakibly G. Small lies, lots of damage: a partition attack on link-state routing protocols[C]// Communications and Network Security. IEEE, 2015:397-405.

[4]. Chang H Y, Wu S F, Jou Y F. Real-time protocol analysis for detecting link-state routing protocol attacks[J]. Acm Transactions on Information & System Security, 2001, 4(1):1-36.

[5]. Sosnovich A, Grumberg O, Nakibly G. Finding Security Vulnerabilities in a Network Protocol Using Parameterized Systems[M]// Computer Aided Verification. Springer Berlin Heidelberg, 2013:724-739.

[6]. Spring N, Mahajan R, Wetherall D. Measuring ISP topologies with rocketfuel[C]// Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. ACM, 2002:133-145.