Contemporary Engineering Sciences, Vol. 9, 2016, no. 13, 641 - 646
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2016.6452

A Study on the Kismet-Based Wireless Intrusion Prevention System

Chang-Su Kim, Chu Xun and Hoe-Kyung Jung*

Department of Computer Engineering, Pai Chai University, Daejeon, Korea
*Corresponding author

Abstract

Recently, the use of wireless networks that can be used conveniently increases due to the increasing number of people who are using internet and smart devices. Comparing with the wired network, the wireless network can be operated cheaper but it has weakness in security problems.

In this paper, we propose a system to detect and prevent security threats that occur in a wireless environment. The system detects security threats using the open source-based, Kismet and Wireshark and uses Iptable to prevent intrusion. We use a hacking tool that is used for the simulation in order to verify the compliance.

Keywords: Wireless Environment, Security, Iptable, Kismet, Wireshark

1 Introduction

Because of the advances in wireless communication technology and increasing use of smart devices, a number of users who use wireless network increases. Since the wireless network uses radio waves to send and receive data, it meets the network conditions required by the portable devices. In addition, the use of wireless network keeps increasing because of the convenient availability compared to wire network. However, wireless network has disadvantage in security compared to wire network. And wireless network users may use wireless network indiscreetly lacking both the security knowledge and the importance of security. Due to these problems, wireless network users can be exposed to the misuse crime [1, 2, 3].

In this paper, we suggest a system which can detect and then block security threats in wireless network environment by using kismet, wireshark and Iptable. In order to validate the performance of the suggested system, we reproduce attack conditions in a wireless network by employing tools used in hacking. And, by using kismet, we collect packets of hacking tools and analyze collected packets with wireshark. The analysed packets are applied to the Iptable rules and prevent system invasion by blocking corresponding packets and IP.

2 Related research

2.1 Vulnerabilities of wireless network security technologies

IEEE 802.1x is a standard technology that is being used in a Ethernet network environment, to authenticate the client. By referring the registered user information in RADIUS, server shall judge whether to allow network access by checking that the accessing AP user is registered in RADIUS server. And, in exchange of authentication message, EAP (Extensible Authentication Protocol) is used and data is being encrypted by using the WEP. The security vulnerability of IEEE 802.1x is the weakness of brute force and MITM (man in the middle attack). These causes are due to the vulnerable issues with EAP And WEP [4, 5].

2.2 Wireshark

Wireshark is a program developed to manage the network. Using wireshark enables to save network packets and to analyze the saved packets in detail. Wireshark can use the data in other packet programs and support a wide variety of operating systems with UNIX or Linux, widows, etc. And it also provides the ability to search for specific packet, which further enables one to effectively analyze the packets [6].

2.3 Iptable

Iptable is a processing system for network packet in Linux kernels, and it was developed from netfilter project. Iptable filters TCP and UDP, controls a specific port, and thus prevents intrusions by a malicious user. Iptable consists of table and chains, requiring root permission. Tables perform features such as packet filtering or network address translation and consist of the four tables like Filter, NAT, Magle, and Raw.

3 Wireless intrusion prevention system design and construction

3.1 Wireless intrusion prevention system design

In a wireless network environment, one can't detect security threats raised from system used in a wire firewall. To operate reliably on wireless network, one needs a wireless intrusion prevention system with a continuous monitoring function and integrated management. In this paper, suggested system configuration is shown in Fig. 1

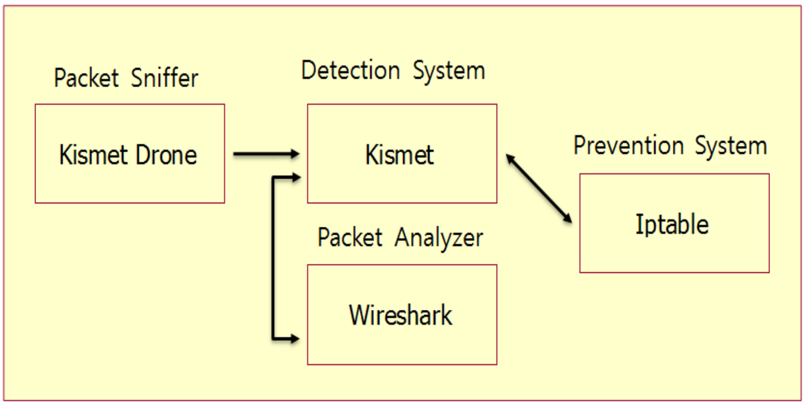


Fig. 1. Configuration of Wireless Intrusion prevention systems

By using Kismet, one collects packets in a wireless network, inspects AP, and detects trepass. The collected packets use Wireshark to analyze pattern of attack. And, based on the analysed patterns, Iptable's rules are created to prevent intrusion.

3.2 Wireless intrusion prevention system construction

Suggested wireless intrusion prevention system consists of a server and a client. The server of wireless intrusion prevention system consists of kismet and wireshark, Iptable to block intrusion. The client of wireless intrusion prevention systems consists of kismet, wireshark and hacking tools, which are used to inspect mock hacking and wireless network environment. The server construction order to build a wireless intrusion prevention system is as follows.

(1) Installation of linux operating system of CentOS 6.4
(2) Installation of Rpmforge package required for installing kismet
(3) Kismet installation and environment configuration
(4) Wireshark installation and environment configuration
(5) Iptable Installation

4 Experiments

4.1 Experimental environment

In this experimental environment, one uses PC used as a server in wireless intrusion prevention system and two laptops used as client. And, the experiment was conducted using one wired router and three wireless routers. The configuration of experimental environment is shown in Fig. 2.

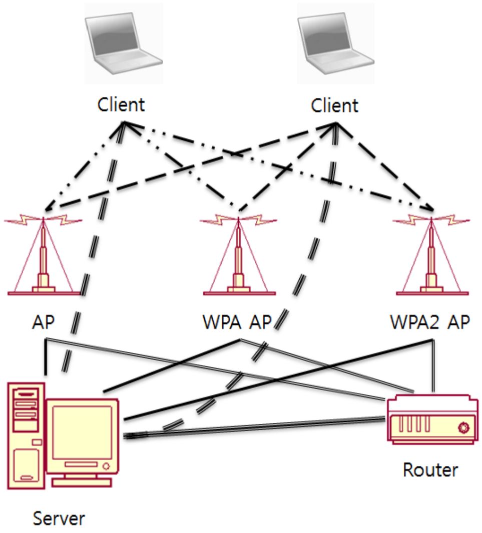


Fig. 2. Configuration of the experimental environment

4.2 Experimental method

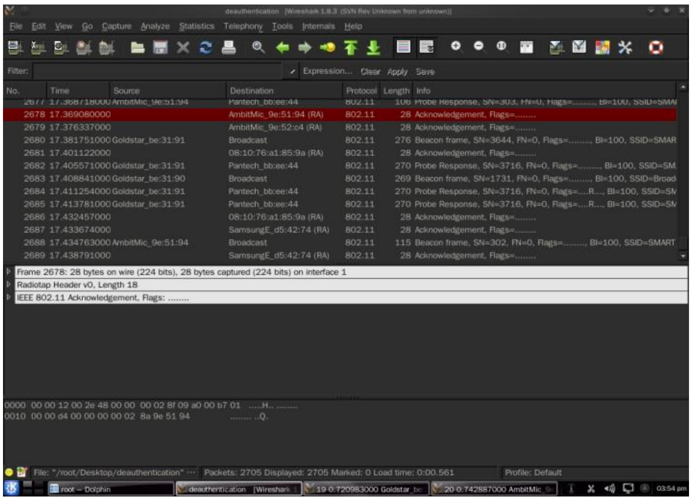
The experiment proceeds with WPA shared key crack, and MITM attack. A Details for each attack is as follows.

(1) WPA shared key crack
- Use Airmon-ng, Generate the monitor interface
- Use Airodump-ng, Gather information of the surrounding AP
- Use Airodump-ng, Collect information from target AP
- Use Aireplay-ng, Launch with replay attack
- Use Airodump-ng, Collect WPA handshake
- Use Aircrack-ng, Launch with dictionary attack

(2) MITM attack
- Use Airmon-ng, Generate the monitor interface
- Use Airbase-ng, Generate AP
- Generate a bridge consisting of wired and wireless

4.3 Experimental results

1) WPA shared key crack
Blocking the packets used in replay attack and complicating the password lead to a failure of dictionary attack. Replay attack is shown in Fig. 3, which is a screen analyzing the used packets with Wireshark.


deauthentication [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save

```
No.   Time        Source             Destination               Protocol Length Info
2677 17.368718000 AmbitMic_9e:51:94  Pantech_bb:ee:44          802.11   106 Probe Response, SN=303, FN=0, Flags=........, BI=100, SSID=SMA
2678 17.369080000                    AmbitMic_9e:51:94 (RA)    802.11    28 Acknowledgement, Flags=........
2679 17.376337000                    AmbitMic_9e:52:c4 (RA)    802.11    28 Acknowledgement, Flags=........
2680 17.381751000 Goldstar_be:31:91  Broadcast                 802.11   276 Beacon frame, SN=3644, FN=0, Flags=........, BI=100, SSID=SMAR
2681 17.401122000                    08:10:76:a1:85:9a (RA)    802.11    28 Acknowledgement, Flags=........
2682 17.405571000 Goldstar_be:31:91  Pantech_bb:ee:44          802.11   270 Probe Response, SN=3716, FN=0, Flags=........, BI=100, SSID=SM
2683 17.408841000 Goldstar_be:31:90  Broadcast                 802.11   269 Beacon frame, SN=1731, FN=0, Flags=........, BI=100, SSID=Broad
2684 17.411254000 Goldstar_be:31:91  Pantech_bb:ee:44          802.11   270 Probe Response, SN=3716, FN=0, Flags=....R..., BI=100, SSID=SM
2685 17.413781000 Goldstar_be:31:91  Pantech_bb:ee:44          802.11   270 Probe Response, SN=3716, FN=0, Flags=....R..., BI=100, SSID=SM
2686 17.432457000                    08:10:76:a1:85:9a (RA)    802.11    28 Acknowledgement, Flags=........
2687 17.433674000                    SamsungE_d5:42:74 (RA)    802.11    28 Acknowledgement, Flags=........
2688 17.434763000 AmbitMic_9e:51:94  Broadcast                 802.11   115 Beacon frame, SN=302, FN=0, Flags=........, BI=100, SSID=SMART
2689 17.438791000                    SamsungE_d5:42:74 (RA)    802.11    28 Acknowledgement, Flags=........

Frame 2678: 28 bytes on wire (224 bits), 28 bytes captured (224 bits) on interface 1
Radiotap Header v0, Length 18
IEEE 802.11 Acknowledgement, Flags: ........

0000  00 00 12 00 2e 48 00 00  00 02 8f 09 a0 00 b7 01   .....H.. ........
0010  00 00 d4 00 00 00 00 02  8a 9e 51 94               ........ ..Q.

File: "/root/Desktop/deauthentication" ···  Packets: 2705 Displayed: 2705 Marked: 0 Load time: 0:00.561  Profile: Default
```

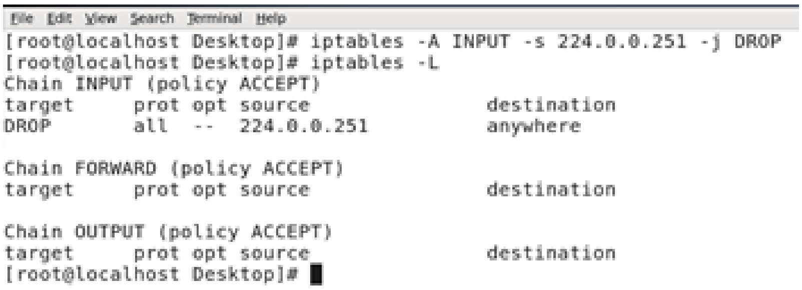
root – Dolphin
deauthentication [Wireshark
19 0.720983000 Goldstar_b
20 0.742887000 AmbitMic_9
03:54 pm

Fig. 3. Packet analysis of wireshark replay attack

2) MITM attack

AP used in MITM attack can detect the same way as honeypot AP attack is detected. In addition, using the packet information can detect MITM attack.

Packets of MITM attack analyzed with Wireshark are applied with the rule of Iptable as shown in Fig. 4.



```
[root@localhost Desktop]# iptables -A INPUT -s 224.0.0.251 -j DROP
[root@localhost Desktop]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  224.0.0.251          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost Desktop]# █
```

Fig. 4. Prevention of man-in-the-middle attacks with Iptable

5 Conclusion

In this paper, we suggested the system to prevent the security threats by detecting and blocking security threats on a wireless network. The server of wireless intrusion prevention system implements the system by using the kismet and wireshark, Iptable. And, client of wireless intrusion prevention system consists of kismet and wireshark, and hacking tools.

Wireless intrusion prevention systems collects the packets of wireless network as Drone of Kismet, and then Kismet saves the collected packets in files. And, the system uses kismet to inspect wireless network environment and detect illegally cloned AP or unauthorized AP. Wireshark is used to analyze the packet files, saved as kismet while those packets analyzed with Wireshark are transformed to the rules of Iptable. Once Iptable rules are generated, the system makes sure that invasion is blocked, and if the block is unsuccessful, Iptable rules are re-generated.

In this paper, in order to verify suitability of the suggested wireless intrusion prevention system, the system progresses mock hacking using hacking tools of client, analyzes the packets of mock hacking using wireless intrusion prevention system, and prevents trespass by adding rules. By using wireless intrusion prevention system suggested in this paper, one can expect an improved wireless network security in operating facilities using UNIX or Linux based server. Also, the system can be effectively used to users who intend to learn wireless network security.

For the future research, it is necessary to combine the suggested wireless intrusion prevention system and Snort in order to even detect a wired network.

References

[1] S. T. Joe, Research on the Editing Environment of Internet Portal News by the Increase of Smartifact Use, *Society of Korean Design Trend*, **35** (2012), no. 1, 441-450.

[2] I. Y. Hong, Spatial Distribution and Utilization Feature of WiFi, *The Korean Cartographic Association*, **10** (2010), no. 1, 55-64.

[3] G. S. Han, Threats Analysis and Solution of Security in Wireless LAN, *The Korea Entertainment Industry Association*, **2** (2008), no.1, 111-114.

[4] J. H. Kang, Y. S. Lee, J. Y. Kim, E. G. Kim, ARP Modification for Prevention of IP Spoofing, *Journal of Information and Communication Convergence Engineering*, **12** (2014), no. 3, 154-160. http://dx.doi.org/10.6109/jicce.2014.12.3.154

[5] Zi Gui Jiang, Study of Wi-Fi Security Basing on Wireless Security Standards (WEP, WPA and WPA2), *Advanced Materials Research*, **1049** (2014), no. 8, 1993-1996. http://dx.doi.org/10.4028/www.scientific.net/amr.1049-1050.1993

[6] Er. Narender Kumar Naryal, Er Satinderjit Kaur Gill, Security Issues in the Firewall Authentication caused by the Wireshark-A Protocol Analyzer Tool, *International Journal of Computer Science and Mobile Computing*, **3** (2014), no. 8, 18-23.

Received: May 19, 2015; Published: June 2, 2016