Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 115 (2017) 674–682

Procedia Computer Science

www.elsevier.com/locate/procedia

7th International Conference on Advances in Computing & Communications, ICACC-2017, 22-24 August 2017, Cochin, India

Wireless Security Auditing: Attack Vectors and Mitigation Strategies

Aarthy Devi A[a,*], Ashok Kumar Mohan[a], Sethumadhavan M[a]

[a]*TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amrita University, Coimbatore-641112, India.*

Abstract

Wireless security is concise on protecting the resources connected to the wireless network from unauthorized access. Wi-Fi Protected Access II (WPA2) is a predominant variety of cryptography based wireless security protocol, which is crafted to be robust and can prevent all the wireless attacks. But numerous organizations explicitly like educational institutions remains vulnerable due to lack of security. By auditing the vulnerabilities and performing the penetration testing, it is possible to review the causes of the issues indicted over the network. Wireless security auditing is anticipated to be an exact blend of attack scenario and the well matched audit policy checklist provides a benchmark for a sheltered wireless network in safe hands.

Peer-review under responsibility of the scientific committee of the 7th International Conference on Advances in Computing & Communications.

Keywords: Wireless security; Zero day attacks; Audit policies

1. Introduction

In state of affairs, where wired security systems are not a feasible choice, wireless security devices are the most first-rated choice of an attacker to compromise. The dawn of wireless era based on cloud computing over IoT enabled devices has also set its security threats for a massive boost in enabling attack vectors. Security is now an essential element that forms the keystone of every corporate network and are considered for auditing. But educational institutions ignore the need for wireless security audit and it paves the way for leakage of humongous amount of sensitive and confidential data that are never noticed by the victim. So we have audited the wireless network of one

* Corresponding author. Tel.: +91 96262-62166.
E-mail address: aarthy.alagar@hotmail.com

1877-0509
Peer-review under responsibility of the scientific committee of the 7th International Conference on Advances in Computing & Communications
10.1016/j.procs.2017.09.153

such educational institution which spreads over 400 acre of university grounds and has roughly around 800 wireless access points connected to a radius server used by approximately 6000 individuals. This proposed model is an initial test run to deploy wireless security auditing to act as a point of reference for educational institutions which are not strictly bounded with IT audit polices. It is mysterious to watch the progression of wireless technology over the past decade. IEEE 802.11i for Wi-Fi offers strong authentication and encryption possibilities to protect networks and various enterprises have adopted this technology. At the same time, attackers are becoming more knowledgeable and significant system breaches are happening more often. Majority of payment cards attacks starts via POS terminals with a simple wireless exploit publicly available over the internet. Other wireless protocols have also contributed to wireless security namely WiMAX, DECT, Bluetooth, RFID, ZigBee and in recent times with NFC. Securing Wi-Fi connection is an important part of securing the sensitive user credentials.

Security over Wi-Fi is achieved via WEP, WPA and WPA2 protocol standards. Wired Equivalent Privacy (WEP) is the oldest protocol and are no more put into practice as they are proven to be broken.WEP keys does not avail an end-to-end encryption as they are not hashed, but simply concatenated to Initialization Vector (IV). RC4 encryption algorithm is used in WEP standard and several successful attacks has been discovered based on this algorithm. The flaws that are recognized in WEP such as lack of proper authentication, vulnerabilities in header and so on. Many obsolete wireless devices still uses WEP, but it is strongly suggested to avoid using WEP due to its open vulnerabilities. Several modifications are made to align WPA towards secure wireless communication. Temporal Key Integrity Protocol (TKIP) is used for encryption process. It requires a key to connect and access the network by authentication process of a typical four way handshake. Wi-Fi Alliance delivered this protocol as two variants, namely in WPA-PSK and WPA-Enterprise mode. WPA-PSK connects the access point by entering a password to be an authorized user. WPA Enterprise uses an additional Remote Authentication Dial-In-User Service (RADIUS) server for larger infrastructure. The Access Point (AP) and other authentication server authenticates end devices over this RADIUS protocol. 802.11 is developed to authenticate users wirelessly to connect to a wired network. It relies on the Extensible Authenticating Protocol (EAP) to send messages between the authenticated server and the client. There are different kinds of EAP which offers authentication options such as EAP-LEAP, EAP-FAST, PEAP, EAP-TLS, and EAP-TTLS. Among that, PEAP is the most recent and also the exceedingly used authentication protocol. It sets up TLS tunnel between client and server and then sends username and password through the tunnel. WPA is also proven to be vulnerable to some of the attacks. To overcome the flaws in WPA, an extension protocol was formulated in the name of WPA2. It works similar to WPA with modifications to patch the existing vulnerabilities. WPA is secure than employing WEP, but it is still vulnerable and are patched by WPA2. Currently WPA2 is considered as the most secure wireless authentication protocol put into practice and also commonly referred to as Robust Security Network (RSN). WPA2 comes in either with AES, TKIP and Counter mode/CBC MAC Protocol (CCMP) based encryption schemes. There are also proof of concept attacks reported against TKIP protocol used in WPA2. Wi-Fi network using WPA2 security integrates pair wise keys and group keys over a four way handshake mechanism to verify the participants. It enhances both security of the information passed through the channel and the privacy of the susceptible user credentials. WPA2 over Wi-Fi is a subset of 802.11i standard which operates commonly either in 2.4 GHz or in 5 GHz providing a Robust Secure Network. These packets are foot printed via four unique parameters by the attackers namely SSID, BSSID, channel which they operate and the IP addresses. Even after truthful implementation of WPA2 power-driven by early audit policies, sooner or later the end devices are forced to disclose their sensitive information to attacks.

Section 2 describes the various related works for detecting and performing wireless attacks. The methodology for conducting the attacks are described in section 3. The experimental outcomes are mentioned in section 4. Mitigation strategies with audit policy checklist are elaborated in Section 5. Section 6 concludes the paper.

2. Related Works

Wireless threats appears in all form, from some malicious clients attaching to the organizations legitimate AP without authorization, to sniffing all packets in promiscuous mode out of the air and performing a reconnaissance on them. These significant work done by our forerunners in wireless security analysis are taken into consideration as the rock-solid foundation for our proposed model.

Security threats in Wi-Fi networks by Masiukiewicz et al. [1], described the common threats in the wireless network and the security through obscurities with packet capturing, hidden SSID, MAC address filtering, evil twin attack and location based service attacks. A range of tools used for Wi-Fi security analysis such as ArcSight, Tripwire, Argus, Network Miner, Dsniff are rightly evaluated and compared. Beneficial security analysis can be achieved through certain hand crafted Linux distributions like Caine, Backtrack, Bugtraq, DEFT, and Kali Linux. Some of the predominant parameters that can be extracted during the analysis are SSID name, signal strength in dBm, encryption type, network throughput, geographical location (approximate up to 10 metres radius), channel of operation, wireless device manufacturer and physical address of the WLAN NIC (BSSID).

Concepts of penetration testing and its attack technique is discussed by Dennis M. et al., Penetration testing is a simulation of an attack which is used to validate the security of the system. It can be done using both hardware kits and software applications. Some of the tools such as Metasploit, W3af, Wireshark, Nessus, Dradis, Nmap and Kali Linux which is embedded with frameworks for performing penetration testing. Attacks like traffic sniffing, hacking Wi-Fi, gaining access of user machine and MITM can be performed with these frameworks. Mitigations of each attack is mentioned by the author, but real black hat attackers have already update themselves to bypass the proposed mitigation strategies [2].

Exploiting WPA2-Enterprise vendor implementation weakness through challenge response oracles proposed by Robyns et al., Demonstrated the steps to steal credentials from the user and gain access to the network by cracking MSCHAPv2 challenge response [3]. A proof of concept implementation has also been given to bypass the authentication and certificate validation in Apple iOS based wireless devices. Mitigation ways includes proper client certificate validation, cryptographic binding, enabling suitable iPhone configuration, using WIDS.

A comparison of wireless security procedure: Security coupled with ease of implementation of a college campus is discussed by Robyns P. and Bonne B. et al. The security of the network in the campus has been calculated by the researchers, it has been implemented different methods of user configuration and measured the suitable solution for securing the campus. Experimental setup was based on WPA2-Enterprise with RADIUS server in windows and Apple machines. Based up on the implementation and testing, they have concluded that WPA2- Personal suits more appropriate and recommended to deploy the same over the entire campus [4].

Audit for information security is described by Ana Maria *et al*. A risk based audit platform for developing the organization's security system is discussed in this paper. Access control, system activity monitoring and audit should be monitored in the enterprise on a regular basis. Audit standards like ISO 27001, NIST SP800-48, SP800-115 and SP800-153 will be used to improve the security of the organizational network.

Krekran Jan *et al.* proposed a statistical approach for password audit using probabilistic password generation. General attack of passwords can be done using pre computed lookup tables. i.e., rainbow tables. Tools like Cain and Abel, EWSA and Aircrack can be used for this purpose. But this will be a long time process [6]. GPU acceleration in the password recovery will increase the computational power of the graphics card. One professional graphics card can evaluate up to 1,00,000 passwords per second for that it will take only 160 minutes. If the password is not found in the dictionary, i.e., using dictionary attack, then by combining two words in the dictionary and concatenate the result. This is the statistical method followed here to solve the problem and increase the speed of password cracking. Finally, recommended to use strong password for the security purpose.

Most of the existing practices has been used in different ways to detect and prevent the attacks in the wireless network based on the algorithms, proof of concept techniques and solution with minimal level of security measures. Based on the size of the enterprise and use of the wireless network, standard compliance has been followed to secure their network environment [8]. To make the same process in the institutions, need to perform a suitable vulnerability assessment of wireless devices and appropriate penetration testing in the network environment. Finally, need to formulate the remedies to secure the network based on the proper audit policies which are performed at regular intervals in the campus network.

3. Proposed Methodology

Our main target is to focus on the mistaken belief about wireless security in the organizational environment, particularly in educational institutions. To avoid zero day attacks in the network [7], need to regularly audit and improve the security standards based on the audit policies which suits for the particular network environment. For experimental purpose, need to setup a virtual environment or a prototype of the actual infrastructure. Then, perform

the painstaking wireless attacks by spoofing the credentials of some of the legitimate users. In this experiment, considered the different sort of attacks such as wireless hosted network attack, WPA2 Enterprise challenge and response attack and network enumeration attack on router. Likely for a WPA2 Enterprise challenge and response attack, install and configure freeRADIUS server to authenticate the clients for cracking the PEAP. Create a fake AP that supports 802.1x authentication and redirect it to the freeRADIUS server. So that, all the users connected to that AP will be listened by the attacker and it facilitates in cracking the password with the gathered challenge and response of the user. For wireless hosted network attack, need to create a malicious payload executable file for it to automatically enable the hosted network in the victim's system. The attacker then connects to that hosted network by using the key which is already uploaded by the malicious file. It then performs the exploit with the help of Metasploit framework on the victim's machine. For network enumeration attack, we need to install and run SNMPcheck, SNMPEnum to gather the configuration and other information of the router to make use of. To avoid these kind of attacks [10], need to concentrate on the audit policies and other feasible techniques which are suitable for the campus network to enhance the security of the network.

4. Experimental Outcomes

4.1 Wireless hosted network attack

Windows Operating systems with version 7 and above are having a special feature called hosted network for creating software based access point by using the physical adapter. It is mainly used for Internet Connection Sharing (ICS) with other devices on the network and creating wireless Personal Area Network (PAN). That comes integrated with network shell (netsh) command line utility. Creating a virtual adaptor on top of the physical adapter can create software based AP. This feature in windows turned as an exploit. It is also effortless for a malware to create a backdoor that can abuse the hosted network. It is featured using the Metasploit framework to create a backdoor entry to get a meterpreter session entirely over a private network. The idea of this malware is to start the hosted network in the victim's system with a key known to the attacker and bind to a port to start a meterpreter session. The attacker uses the key, connects over the hosted network and finally connects to the victim machine using the session. The malicious payload will be send through an email or transmitted via the Wi-Fi networking devices. Advantages of this method is that they leave no trace of network logs like firewall, IDS, IPS making it impossible to trace back and hard to detect. It also does not give a change for any notifications by anti-virus and anti-malware software.

Once the malicious payload runs, it will create a hosted network and waits for meterpreter session on port 4444. Port number can be changed or set to take a random port depending upon the infrastructure. It has been normally visible when it listens to the available access points in the surroundings using airodump-ng and iwlist. Here, the SSID of the hosted network is named as Malw@re.

For example:

 # iwlist wlan0 scan | grep Malw@re

Output →ESSID: "Malw@re"

Configuration file of a key is explored as shown in the Fig. 1.

 # cat wi-fibackdoor.conf

```
{
 ssid="Malw@re"
 scan_ssid=1
 key_mgmt=WPA2-PSK
 psk="wi-fibackdoorkey"
 }
```

Fig. 1. Configuration file of a key.

Using the WPA2 supplicant utility, we connect it to that hosted network.

 # wpa_supplicant –Dnl80211 –iwlan0 –c/etc/wi-fibackdoor.conf

Now the attacker's machine over Wi-Fi is trying to connect to the victim through the created hosted network. Once the connection succeeds, it will be able to get the DHCP address of the victim. That is how the hosted network works and automatically has to give all the IP address and expose the devices behind it in the Personal Area Network. In

Metasploit, we set the RHOST and the IP address of the victim.

msf > use/exploit/multi/handler
msf > set PAYLOAD windows/meterpreter/bind_tcp
msf > set RHOST 192.168.137.1 →IP address of the victim
msf > exploit

Payload handler and bind handler starts and enters into the meterpreter session in the attacker machine.

meterpreter > ps

Now the attacker gains the access to the victim system over the hosted network. For example, through '*ps*' command, it is possible to see all the process running in the victim machine. It enables the attacker to type any command that has to been executed through this session as shown in the Fig. 2.

```
meterpreter > shell
Process 4000 created.
Channel created.
Microsoft Windows [Version 6.1 7601]

C :\>
```

Fig. 2. Remote access gained by the attacker via meterpreter.

4.2 WPA2 Enterprise's challenge and response attack

For this attack, D-link router which supports WPA/WPA2 Enterprise for creating rogue access point and Alfa adapter for professional pen testing to de-authenticate the legitimate clients are used. FreeRADIUS -WPE (Wireless Pwnage Edition) framework is used for setting up malicious radius server in Kali Linux. Set up for the FreeRADIUS server in lab environment as mentioned in the Fig. 3.

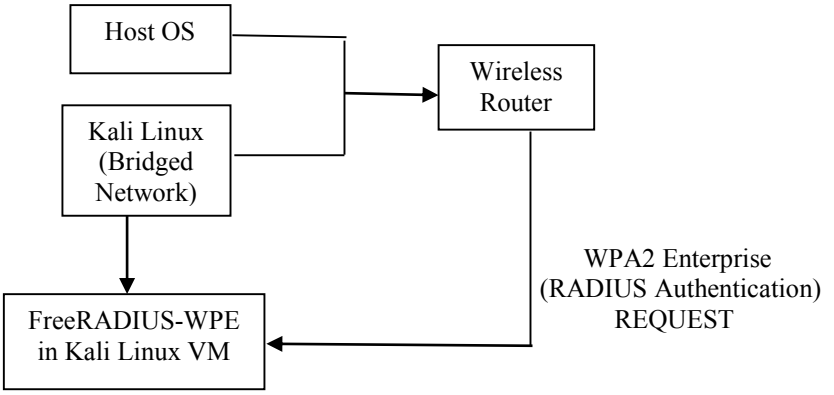

Fig. 3. FreeRADIUS-WPE server architecture.

Configuration for freeRADIUS server setup and cracking WPA2 Enterprise network:

 # radiusd –X

Configuration files is located in /usr/local/etc/raddb folder.

 # nano eap.conf

Change the EAP type into PEAP as it is currently the highly used and secured authentication protocol.

 # nano clients.conf

Then update the IP address, shared secret and password.

 # cd certs/
 # nano ca.cnf

Generate a certificate with certificate authority.

 # nano server.cnf

Configure the same details to the 'client.cnf' file as both the configuration should be the same.

```
CountryName            = In
StateOrProvinceName    = TN
OrganisationName       = Amrita
CommonName             = College Wireless LAN
EmailAddress           = admin@example.com
```

Fig. 4. Certifying Authority Credentials.

 # ./bootstrap

This command is used to create a valid certificate. Generate a fake certificate in the name of 'College wireless LAN' for authentication as shown in the Fig. 4. Finally copy the private keys stored in *'server.key'* and '*ca.key'* files. Then generating a 2048 bit RSA private key by writing new private key to '*ca.key'* file. Once the client accepts the self-signed certificate, TLS tunnel will be created between client and radius server to send the PEAP credentials. After the configurations of the malicious RADIUS server, create an access point with the same SSID as like in the college campus to advertise in the air using the router by configuring it with WPA2 Enterprise details and given the IP address of the freeRADIUS server configuration. Once the client is connected to the AP with the username and password, the details will be automatically updated in the freeRADIUS server database. The log details will be stored in '*freeradius-server-wpe.log*' file. The log file contains username, challenge and response, John NETNTLM hash values as shown in the Fig. 5. Crack the password by using john the ripper with NETNTLM hash value. It can also be extracted by using the utility called asleap with the help of saved challenge and response of the connected client. Here, asleap has been employed by using dictionary attack to break the challenge response pair of the credentials sent by the client to crack the password.

```
username :  admin
challenge :  da:c8:b4:34:db:45:ce:57
response :  d7:3e:ca:df:ba:a8:67:4f:93:b4:18:45:cd:5e:e4:81:26:2e:dc
John NETNTLM : admin : $NETNTLM$dc8b463ce353bef45dc8bc17f91bba2369cd75abef18ec45da327ef69
```

Fig. 5. Freeradius-server-wpe.log file with NTLM hash.

4.3 Network enumeration on the router

Network enumeration is used for gathering information about a particular network like the details of all the connected devices, hosts, usernames and other data by using the ICMP and SNMP protocols. SNMP is a simple protocol used by the network administrator to manage devices. So SNMP generally runs over UDP where the network administrator can have the network manager which queries the SNMP enabled network devices for various running configuration information.

By scanning the network using nmap for open ports, then gain the access of the router and its configurations

 # nmap –sS 192.168.1.1

SNMP enumerator tools such as SNMPcheck, SNMPEnum are used to compromise the router. Command for SNMPcheck is given below:

 # ./SNMPcheck.pl –t 192.168.1.1

Once the SNMPcheck connects to the router, it will get the information like hardware details, storage information, interfaces, number of processes running on the router, routing information, listening TCP and UDP ports as shown in the Fig. 6. Then, that information can be used for the attack purpose.

[*] Processes

Total Processes : -

Process id	Process name	Process type	process status	Process path
1	init	4	2	init [2]
1421	udevd	4	2	udevd
1750	rsyslogd	4	2	/usr/sbin/rsyslogd
1974	ospfd	4	2	/usr/sbin/ospfd
2290	getty	4	2	/sbin/getty
2562	sshd	4	2	/usr/sbin/sshd
3754	login	4	2	/bin/login

Fig. 6. Gathered information on network enumeration.

The above mentioned attacks are possible in the institution's network. Some common attacks such as DNS hijacking, router's firmware attack and other phishing attacks are also possible. To avoid these sort of attacks, regulate the newly formulated audit policies to secure the network.

5. Mitigation Strategies

Actual implementation of the security audits control policies in wireless networks in educational institutions are becoming vital nowadays, avoiding investments on security devices directly boosts up the profitability of institution to invest on other essential resources. But the authorities concern regret one fine day when all the wireless devices are compromised and subsequently results in the exposure of all confidential information and eventually the repudiation of the educational institution is blemished. Wireless security audit should be implemented regularly and monitored periodically to mitigate the newly discovered vulnerabilities. Good wireless security audit is not only performing practical testing and sorting out the faults, but it made complete with proper documentation, including recommendations of how to make the Wi-Fi networks more secure, isolate attack vectors, audit on them and remove if necessary and finally repeat the audit process on regular basis.

In the previous part, listed a set of attacks and the parameters to identify them. It can be carried out, in order to penetrate over the security of the infrastructure. Then put into practice the following formulated audit checklist, primarily by addressing why a particular audit is significant and secondarily, how one can perform an audit in a proper way.

5.1 Formulated audit policy checklist

Audit standards like ISO 27001, PCI DSS, HIPAA, NIST SP800-48, SP800-115 and SP800-153 are regularly used to improve the security of the enterprise network [5]. Here are the newly formulated audit policy checklist for securing the wireless network in the educational institutions which is inferred from the existing compliance.

5.1.1 According to ISO 27001 control A.13.1.3 – Network segregation, describes that groups of information services, users and information systems should be segregated on infrastructure to secure the network. Network segregation is the performance of splitting a network into smaller parts of sub networks [12].

5.1.2 IEEE 802.11w standard supports the protection of both de-authenticate and disassociation frames using a message integrity check to recognize the deceived frames. It is available only in WPA2 enabled wireless devices. Windows 8 and above clients supports this feature by default. But many AP will not allow this feature and are disabled as a factory configuration. Check the AP manufacturer for the firmware upgrade to overthrow de-authenticate and disassociation attack.

5.1.3 To secure the entities from the attacks against PEAP, the client should ensure legitimacy and validate the certificate. Because mostly in enterprises and organizations, the root certificate for their own institution's CA will be installed automatically. So the clients should check and verify the source of the new certificate before accepting them blankly.

5.1.4 To avoid Rogue DHCP server: Generally DHCP traffic is not authenticated, otherwise the network administrator would be prevent the attack. To avoid this kind of attack, the RADIUS server has to monitor the rogue DHCP server and disassociate and blacklist them quickly. Many open source based GNU GPL detection tools are publicly available for validation.

5.1.5 To avoid fake DNS server: Use a trusted third party like OpenDNS and Google public DNS service instead of the user crafted DNS to provide enhanced protection. Another solution is implementing DNSSEC, a DNS Security Extensions provides authority, data integrity and authenticated denial of existence by enabling DNS responses to be valid. F-secure router checker checks the router's connection settings and reports to the current DNS servers.

5.1.6 IPAM: All servers should be hard coded with a static IP address which needs to be maintained by a tool that manages all the IP addresses. It is beneficial to have an updated authoritative reference for each IP address on the network. IPAM services are available in Windows Server 2012 R2 and above to facilitate the reference. All management interfaces are assigned static IP addresses, an IP Address Management (IPAM) solution is used to log and trace every traffic and records are inserted into DNS.

5.1.7 Remote access: Stick with a comfortable remote access solution like SSH except built-in terminal services for windows client. It is advised to avoid remote access applications or remote additional features like PCAnywhere, RAdmin that can be enabled by any user. If mandated for remote access, enable a single interface and monitor them with red alert priority.

5.1.8 SNMP configured: To use SNMP, make sure to configure the community strings and restrict management access to individual systems.

5.1.9 Authentication: Use TACACS+ or any other remote management solution the institution supports, so as to allow only authorized users and authenticate with unique credentials based upon ACL formulated by the administrator.

5.1.10 Disable ports: To avoid accessing the internal network, ports that are not allocated to specific devices should be disabled or set to a default guest network. This avoids external devices from being able to penetrate the internal network.

5.1.11 Port blocking: Block outbound traffic used to bypass the Internet monitoring solution such that if users are tempted to violate policy, then the admin will be alerted. Remember, not every browser will honour Group Policy Auditing (GPO) settings and not every application will process what is in a Proxy Auto-Config (PAC) standards or Web Proxy Auto-Discovery (WPAD) protocols. We should not leave any element without being properly patched in our defence mechanisms.

5.1.12 OpenFlow technique: It is the leading architecture of Software Defined Networking (SDN), which is determined to be the forthcoming feature of deeply programmable networks. It is added as a feature to commercial Ethernet switches, routers and wireless access points. It provides a standardized hook to allow researchers to run experiments without requiring vendors to expose the internal workings of their network devices. Real time incursion threat detection [11], flexible and reliable network access security, virtualization of network are the advantages of using these SDN based technique. Enterprise network device manufacturers such as Cisco, Juniper, HP, DELL, Arista and Ceina by default provides OpenFlow complaint switches. Nine universities in U.S have implemented these sort of network based auditing in their campus. Top companies like Google, Facebook, Microsoft, Verizon and Yahoo are funding and encouraging predominant institutions all around the globe to implement this technology [9].

As cited earlier, can be formulate and audit such a setup only in a typical educational institution and not on any level of enterprise environments as it desires to act in accordance with several IT policies. Also in smaller infrastructure or small home atmosphere, would not need such a wireless security auditing. Our inferences are tabulated in Table 1. Below for a crispy replay of our findings to accomplish wireless security auditing.

Table 1. Wireless Security Auditing: susceptible attacks and anticipated audit policies.

Attack	Security	Impact	Mitigation	Audit Policy
Evil twin and rogue access point attack	WPA2 Enterprise with AES-CCMP	Loss of user sessions, phishing, unauthorized user access	Double up on firewalls such as SPI or NAT and use VPN	Refer Policy 5.1.2, 5.1.3, 5.1.4, 5.1.12
Firmware attack	Update the router firmware on regular basis	Gain router access, possibility of changing router settings, DNS hijacking, ARP spoofing	Change default network or router name and password, disable DHCP, turn off WPS, change router's LAN IP address	Refer Policy 5.1.1, 5.1.5, 5.1.10, 5.1.11, 5.1.12 for more secure environment
Malware attack	Wireless Intrusion Prevention System	Persuade the user to open malicious site or file, gain remote access	Check before opening a file or mail.	Refer Policy 5.1.5, 5.1.11, 5.1.12

6. Conclusion

The way this audit policies are implemented is fairly simple and if all the audits are passed every time, the wireless network infrastructure is proven secure. This means wireless audit policies are used to regulate the integrity of the Wi-Fi enabled networks. So the future audits can aim at automating and updating old policies, adding new policies, reviewing based upon user behaviour and other zero day attacks. It paves way for a huge chance that the attacks do not work on a network anymore or they are caught red-handed and proper disciplinary actions taken by the authorities concern. However, if an attack works within the audit team and most of them are compromised, then the state of affairs need to be handled and audit policies have to be redrafted based upon the infection mode of the individual entities.

References

[1] Masiukiewicz A, *et al*. Security Threats in Wi-Fi Networks. *Engineering and Science* 2016; **1(3)**: 6–11.
[2] Denis M, Zena C, Hayajneh T. Penetration testing: concepts, attack methods, and defense strategies. *In Long Island Systems Applications and Technology Conference (LISAT)* 2016; 1–6.
[3] Robyns P, *et al*. Short Paper: Exploiting WPA2-Enterprise Vendor Implementation Weaknesses through Challenge Response Oracles. *ACM Conference on Security and privacy in wireless & mobile networks* 2014; 189–194.
[4] Slack RD, Marshall B. A comparison of wireless security procedures: security coupled with ease of implementation for a college campus 2012; **13(1)**: 209–214.
[5] Suduc AM, Bîzoi M. Audit for information systems security. *Informatica Economica* 2010; **14(1)**: 43.
[6] Krekan J, *et al*. Accelerated GPU powered methods for auditing security of wireless networks using probabilistic password generation. *Journal of Electrical and Electronics Engineering* 2012; **5(1)**: 111.
[7] Noor MM, Hassan WH. Current Threats of Wireless Networks. *In The Third International Conference on Digital Information Processing and Communications* 2013; 704-713.
[8] Branch JW, *et al.* Autonomic 802.11 wireless LAN security auditing. *IEEE Security & Privacy* 2004; **2(3)**: 56–65.
[9] McKeown N, *et al*. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review* 2008; **38(2)**: 69–74.
[10] Sheldon FT, *et al*. The insecurity of wireless networks. *IEEE Security & Privacy* 2012; **10(4)**: 54–61.
[11] Ramesh MV, *et al.* Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks. *In Computational Intelligence and Communication Networks (CICN*) 2012; 783–787.
[12] K. M. Shivakumar, *et al*. Secured data aggregation in wireless sensor network. *International Journal of Applied Engineering Research* 2015; **10:** 26761–26768.