Trust Evaluation of the Current Security Measures Against Key Network Attacks

Arya Sedigh, Kapilan Radhakrishnan, Carlene E-A Campbell, Dhananjay Singh*

School of Applied Computing, University of Wales Trinity Saint David, Swansea, UK
*Department of Electronics Engineering, Hankuk (Korea) University of Foreign studies,
Global Campus: Yongin, South Korea

Abstract: This paper security measures are implemented in enterprise network architecture and evaluated against current trend of network security as well as used various methods of penetration to confirm the vulnerabilities of the network within the confines of network security management. This was achieved by using a security distribution of Linux. The main focus of this paper is on Enumeration and Scanning of network devices and technologies. A general security model is generated to analyze the afore-mentioned scenario and to aid in better comprehending the concept of penetration testing and vulnerability assessment. This paper also contains information on common threats to Wide Area Networks (WANs) while analyzing their underlying structure.

Keywords: Enterprise WAN, Wireless Network Security, Penetration Testing, Intrusion Detection and Prevention

1. Introduction

With the daily increase of cyber-crimes, provision of appropriate network security has become necessary in order to protect the confidentiality, integrity and availability of intellectual property/data in organizations [1]. Also with the current pace of developments in computer networks and telecommunications industry, regular audits are necessary to assure each and every countermeasure's flawless functionality [2]. The prominent need for real-time communication in the current industry necessitates use of modern networking technology for all companies and especially large corporations, due to features such as scalability and Quality of Service (QoS) [3-4]. In order to assure high availability, integrity and confidentiality of vital data located on a network various security implementations could be devised. However, every measure comes with a known or an unknown vulnerability. Vulnerabilities are weak spots in a network where it is made possible for threats to occur in networking infrastructures [5]. These threats are usually aimed at valuable data or perhaps available resources of a target host. To maintain a stable and secure network, the administrator needs to ensure that all necessary measures have been implemented and that correct access rights have been put in place by defining boundaries and enforcing them by the aid of policies [6-9]. Also it is important that the routing protocols are configured to provide quick and sound convergence. Threats against inter-networks are about as old as the Internet itself. This clearly indicates that both computer networks and the threats against it have evolved significantly over the years. In terms of the rationale behind this paper, while considering the need for security, if looked from the attacker's side, it becomes clear that attackers are constantly researching to find new vulnerabilities in Internetworks' security architectures so that they can develop new attacking techniques to exploit the weak points of computer networks[10-11]. This argument on its own should be sufficient to satisfy the incentive behind the need for a sound network security [12-19]. There are so many measures being deployed in enterprise networks to prevent and mitigate various threats. These implementations often examine numerous characteristics of a network to determine its state of security. The experiment test-bed chosen for this paper allows the collection of comprehensive data on key characteristics of enterprise networks. These analyzed attributes, were carefully selected to respond to the effects an attack might have on a network [20-25].

The remaining of the paper is organized as follows. The Section 2 presents a brief discussion of IETF defines Denial-of-Service (DoS) and various methods security related issues. The Section 3 presents novel security model of logical topology and utilizes the hierarchical model in which redundancy, scalability and link aggregation are key. The Section 4 presents experimental results in a detailed analysis and a comparative study among the various communication vectors along with their performance efficiencies and finally we have concluded the paper in section 5.

2. Related Works and Security Issues

According to the report devised by Computer Emergency Response Team (CERT), nowadays no host is completely secure or immune to the threats over the Internet and this calls for a proper network security model and regular revisions on improvements to the mechanisms in use and development of new security measures to handle

today's technologies [2]. To achieve the highest level of network security, it is important that every entity in the network is secure and self-aware; this also applies to the user since he/she is also an entity in this system. Since, the serious attacks against the Internet's infrastructure conducted in 2000 [14]. The users have been warned and educated on network security. Based on the surveys undertaken by [17]. In 2004, 99% of the respondents used antivirus software, 98% used Firewalls, 68% implemented some Intrusion Prevention System (IPS) [16] and 64% used encryption for their data transits. Such information illuminates that devising sophisticated security measures on its own is not sufficient to secure a network, and that the user must be educated in matters related to network security in order to be able to deploy the correct detection and prevention methods to achieve an ideal fortification of their network.

IETF defines Denial-of-Service (DoS) [8-13] as attacks "in which one or more machines target a victim and attempt to prevent the victim from doing useful work" [14]. DoS is one of the oldest types of attacks used in telecommunication industry. So although the sophistication of attacks and the technology used to implement them has come a long way, their principle is still the same. Since this type of attack has been around the longest, many of the attacks launched on networks nowadays fall under this category. The following table includes the key DoS attacks and their year of origin. Morris worm was one of the most famous DoS attacks which occurred in 1988, when the Advanced Research Projects Agency Network (ARPANET) was being implemented in large scale. This worm was a self-replicating piece of code that caused overflow and disabled 1 in every 20 hosts connected to the network. The code would infect a system and take advantage of the resources available. By flooding all hosts in a network would then paralyse it. Although this worm caused considerable damage to ARPANET, many experts saw it as a wake-up call rather than a cold typical network attack. Worms had been around before this incident, but no one had succeeded in running the exploit in such large scope and complex topology [19]. Although DoS might sometimes be included in attacks, it doesn't necessarily mean that its structure should define its purpose; DoS could just be a small part of a bigger exotic attack. DoS attacks are not limited to wire-line networks. They are also considered a threat to Wireless Local Area Networks (WLAN) and Satellite Networking infrastructures. One of the key DoS attacks in satellite networks is disassociation [9]. Satellite networks are extremely vulnerable to DoS attacks since they rely on their highly dynamic broadcast nature [14]. It is also observed that in disassociation attacks the attacker sends forged disassociation requests to sever the communication link between the server and clients, hence denying service to legitimate end-users. Usually DoS attacks can be detected by analyzing the characteristics of the victim network. Regular updates and patches to the security programs running within the network, and regular analysis of the logs produced by packet capturing software's are two necessary requirements of a good DoS detection technique. For instance [6] argues that if the TCP or UDP data packets contain an unusually large amount of data, it is very probable that the network is under attack. The only way one could understand how to detect these attacks is if they were to analyse the attack's structure and procedure. As cited in [14], the stages below outline the necessary steps to conduct a Distributed Denial of Service (DDoS) attack.

- The real attacker host sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.
- In order to comprehend the underlying principle of DoS and DDoS one needs to understand the symptoms of such attacks. Authors of [12] identified such symptoms as:
- Unusual number of Address Resolution Protocol (ARP)1 arriving at the router.
- Large number of entries in network addresses translation tables.
- High router memory usage by attributes such as Internet Protocol (IP) entries, ARP inputs and IP Cache Ager.

Although there are no standard defense mechanisms available to deal with DDoS attacks, certain steps can be taken in order to decrease networks' vulnerabilities against DDoS attacks. The authors of [17] believed the following methods to be the most effective defences against current DDoS attacks [4].

- Filtering Routers
- Disabling IP Broadcasts
- Applying Security Patches
- Disabling Unused Services
- Performing Intrusion Detection

[1] ARP is the mapping of IP address to the subsequent MAC address of an entity within the network

When a DoS attack is detected certain steps can be taken to neutralize the problem. Firstly it is necessary to block the attacker's traffic to the network by implementation of Access Control Lists (ACLs)2 on the gateway router [21]. However, blocking the DoS traffic to the network doesn't rectify the issue as the DoS attack packets are still traversing within the Internet Service Provider's (ISP) links. In order to overcome this obstacle, ISPs usually activate temporary ACLs on their routers until the DoS traffic is dropped. As observed above, this is not a permanent measure and does not lead to sudden mitigation of the attack. ACLs are an essential implementation in DoS attack scenarios. They aid in both, detection and mitigation of DoS attaks. But since ACL logs are generated and stored on the routers, in heavy attacks they would require high processing power which could cause router failure due to memory overload. To overcome this issue, NetFlow is used which is a Cisco proprietary solution. NetFlow is defined in [22] as "a network-layer switching method that switches packets at high speeds and captures statistics for traffic analysis".

Table 1. Attack and Response

Packet Sent	Response from Victim
TCP SYN (open port)	TCP SYN/ACK
TCP SYN (closed port)	TCP RST (ACK)
TCP ACK	TCP RST (ACK)
TCP DATA	TCP RST (ACK)
TCP RST	No Response
TCP NULL	TCP RST (ACK)
ICMP ECHO Request	ICMP Echo Reply
ICMP ECHO Request	ICMP Echo Reply
ICMP TS Request	ICMP TS Reply
UDP pkt (open port)	protocol denpendent
UDP pkt (closed port)	ICMP Port Unreach

In terms of tracing the source of attacks where DoS is concerned, many face dead ends, since most likely the attacker's IP address is forged, therefore the only way to trace the attack traffic would be to analyze the network traffic hop-by-hop and in many cases the traffic might have been rerouted through various ISPs which makes the trace that much harder and might also raise legal issues [10]. Authors of [24] Classify DoS and DDoS attacks based on their target for depletion. According to [**Error! Reference source not found.**], the two main consequences of a DoS attack are targeted at network load and the Central Processing Unit (CPU) of the receiving host [**Error! Reference source not found.**]. Also presents a brief list of typical Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) attacks, shown in Table 1.

According to [26] most important classes of capacity depletion DoS are infrastructure layer and application layer. SYN flooding requires very little bandwidth and experience to execute. Essentially, the attacker sends SYN packets to a host in the network with a spoofed IP address. The receiving host sends out a SYN/ACK packet out the interface and waits for the RST but as there are no hosts present in the network with the spoofed IP address no RSTs are received. The attacker keeps sending SYN packets to the host in the hopes of receiving replies and this will cause backlog queue to be structured which will never clear out since spoofed SYN requests are constantly arriving. So by sending these SYN packets, all access to that certain port will be blocked. Authors of [13] Noted that the reason for such vulnerability in TCP is its inherent network structure which came from the idea of a safe environment where every user respects privacy of others. UDP is an unreliable protocol and therefore many organizations shut most if not all their UDP ports. In cases of open UDP ports, the network will be vulnerable to UDP flooding attacks. This attack's success is based on the number of packets that can be sent containing useless data [17], which could in turn paralyse the network. Authors recognized three necessary actors for success of amplification attacks.

- The attacker
- Amplifying network
- The victim

DDoS attacks rely on the nature of broadcast, in the sense that the attacker directs spoofed ICMP ECHO packets to the broadcast address of the amplifying network. So once the hosts receive the ping they all reply to the spoofed address which would be the victim's address. And since the victim host is overloaded with packets it won't be able to access its local interface.

In DDoS attacks, the attack traffic is generated from multiple sources. Initially the attacker would require sophisticated software which would then infect vulnerable systems in various geographical locations through un-secure protocols such as Internet Relay Chat (IRC). Then the software or bot will control these DDoS clients or Zombies [12].

[2] ACL is a list of permissions and rights for specific addresses (Hosts) on the network.

Now that the attacker has control of multiple sources launching an attack would bring devastating consequences and tracing back the original attacker is impossible. That is why to date; DDoS attacks are most effective against the security structure of Internet. In application layer DoS attacks, first the attacker identifies a service in the victim network that requires very low processing power to request but considerably large utilization to deliver. By sending a couple of requests per second this attack could overload the CPU of the server and bring it down. There have been cases where DDoS and Application Layer attacks have been integrated to achieve both amplification and depletion. Wireless networks [13-17] are becoming more and more popular in this age. The technologies and standards involved in such architectures have gone through significant advancements at a fast pace and that's why so many home broadband users now connect to the Internet through wireless hubs such as [26] states that routers of Wireless Mesh Networks can be equipped with multiple interfaces to achieve parallel communication sessions among nodes.

The fast growth of wireless networks has made it possible for vast developments in this area and therefore the quality and speed of wireless connections are increasing by every newly defined standard. This fast growing industry has some disadvantages too. Since wireless connections are made through a medium that every node in range has access to, is harder to protect these networks from intrusion and attacks. Jamming attacks are a type of DoS attacks which are conducted on wireless networks. They are also known as Wireless Denial of Service (WDoS) attacks. Jamming attacks are known to be the biggest DoS threat against Wireless networks.

3. Security Model Design

The network has been designed to accommodate common Enterprise Standards. Hence, utilizes the hierarchical model in which redundancy, scalability and link aggregation are key. There are two links between the Core and each distribution switch. Use of Virtual Local Area Networks (VLANs) in WANs of this scale is common. Implementation of VLANs significantly increases time efficiency and assists the in charge network manager in configuring remote devices via Telnet sessions. To ease the process of configuring VLANs and to centralize such task, Virtual Trunking Protocol (VTP) has been used at the core level as server and as client in the rest of the devices in the network. So VLANs are configured in the Core switch and the VTP server running on the Core sends regular updates over the network to ensure each device has ample information on VLAN settings. These updates contain a revision number, so when they get to the client, these revision numbers can be compared and the client will update its VLAN database information based on such process. The two links between the network Core and each distribution switch are set up as trunks to accommodate VLAN traffic. Also each connection supports the native VLAN to enable the transport of untagged VLAN traffic over the network, between different segments.

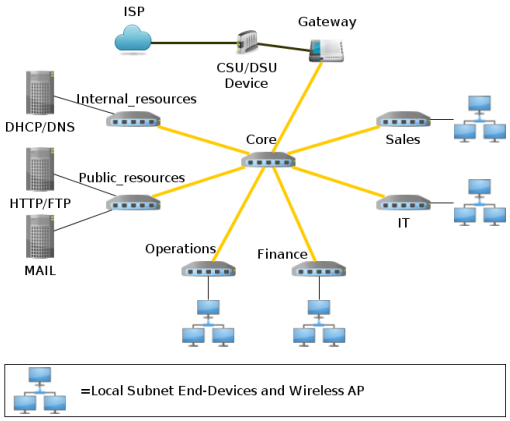

Fig.1. Logical Topology of the Test-bed.

Figure 1, is an illustration of the logical topology implemented in the test-bed. For testing purposes in this particular paper, two Access Points have been implemented in the enterprise on two separate distribution level switches. Network Address Translation (NAT) has been configured to secure inside local addresses and make sure they cannot be accessed via un-secured transport protocols such as ICMP. NAT has been configured to allow certain addresses to be visible to the outside world (i.e. Web and File Servers). For the router to be able to undertake the task of Inter-Vlan routing, Enhanced Interior Gateway Routing Protocol (EIGRP) is chosen. After researching on the relevant literature, according to [27], EIGRP is utilized better than OSPF for such implementation. The penetration test conducted in the course of this paper abides by the guidelines set out in the OSSTMM methodology produced by [28]. Firstly, some preliminary information about the network is gathered and the list of assets that are most valued to the company and are vital to everyday operations. The list has been appropriated according to highest priorities.

- Servers located in the company server farm
- Cisco gateway
- Core switch + 6 distribution level switches
- 2 wireless APs

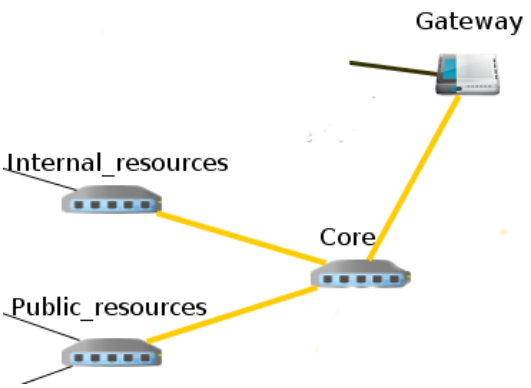

Fig. 2. Main Engagement Areas for Penetration Testing.

The controls in place for the above assets are to be tested to identify limitations. Engagement Zone is the perimeter in which assets are located and the security implementations present in such area are to protect the aforementioned assets, or as [15] puts it "This is where interaction with assets will take place". Figure 2 shows the main Engagement Zone defined for this paper in a logical topology format.

As mentioned earlier, the company relies on standard enterprise technologies and services to operate successfully. All these services and the protocols used to implement various methods of communication within this network are included in the scope of this penetration test. Communication vectors are the main links of communication between each department, also to and from the service provider's cloud. These Vectors have been graphically demonstrated in Figure 3.

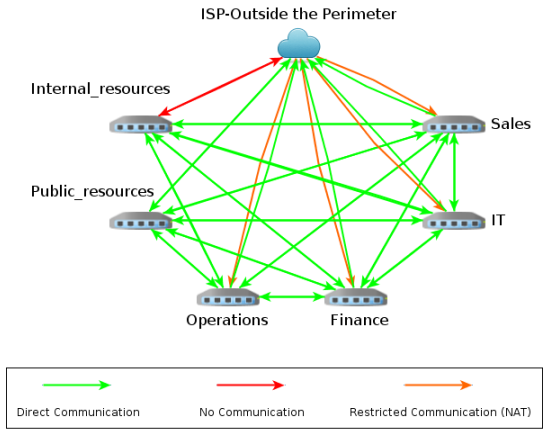

Fig.3. Communication Vectors.

Essentially, each of these vectors can correlate to a separate testing scenario. This allows for better results due to its compartmentalized structure, hence occurrence of too much change can be avoided. Above steps were taken to complete the Information Gathering and Planning phase of the test. The scanning process however was not conducted separately for each vector. This scanning and enumeration process produces general information about the visible technologies and services. Metasploit framework was the main software package used for information gathering and analysis.

4. Results and Discussion

To better understand the underlying causes of vulnerabilities in the implemented test-bed, Metasploit was used as the main information gathering and vulnerability assessment tool. This section exhibits the results collected from the Graphical User Interface (GUI) of Metasploit framework. The results gathered from Metasploit are in form of reports, but these reports have redundant information which will not all be used for evaluation and analysis in this paper. However, only the necessary information, relevant to this concept has been presented in this paper. To better distinguish the outputs, they have been categorized in Table 2 where active services and ports show the network services, discovered by Metasploit, which are relevant to this paper.

Table 2. Discovered ports and services

Address	Port	Service Name
172.31.70.2	80	Http
172.31.70.2	135	dcerpc
172.31.70.2	137	netbios
172.31.60.1	137	netbios
172.31.30.2	3389	ms-wbt-server
172.31.10.2	445	smb
172.31.40.1	3790	Https
172.31.50.1	80	Http
172.31.50.1	23	Telnet
172.31.50.3	1101	pt2-discover
172.31.50.3	3790	Https
172.31.50.4	80	Http
172.31.50.4	23	Telnet
172.31.70.254	80	Http
172.31.40.254	161	SNMP
172.31.10.254	161	SNMP
172.31.70.254	23	Telnet
172.31.40.254	23	Telnet
172.31.10.254	23	Telnet
172.31.50.254	80	Http
172.31.40.254	80	Http
172.31.10.254	80	Http

172.31.50.254	23	Telnet

Operating System Fingerprinting: Figure 4 is an overview of the information about Operating System Fingerprinting in the test-bed. Figure 5 on the other hand is a more detailed output generated by Metasploit.

Discovered Operating Systems

Operating System	Hosts	Services
Cisco IOS	6	16
Microsoft Windows	3	34
Netgear embedded	4	5
Unknown	1	1

Fig.4. OS Fingerprints Enumeration.

IP Address	Hostname	OS
172.31.70.254	172.31.70.254	Cisco IOS
172.31.70.2	SC-505-19	Microsoft Windows
172.31.70.3	SC-505-21	Microsoft Windows
172.31.70.4	172.31.70.4	Netgear embedded
172.31.40.254	172.31.40.254	Cisco IOS
172.31.40.1	172.31.40.1	Netgear embedded
172.31.10.2	SC-505-13	Microsoft Windows
172.31.10.254	172.31.10.254	Cisco IOS
172.31.10.4	172.31.10.4	Netgear embedded
172.31.60.1	sc-505-24	Unknown
172.31.50.4	172.31.50.4	Cisco IOS
172.31.50.1	172.31.50.1	Cisco IOS
172.31.50.254	172.31.50.254	Cisco IOS
172.31.50.3	172.31.50.3	Netgear embedded

Fig.5. Comprehensive Operating System Fingerprinting.

Compliance: Metasploit framework also enables the pentester to conduct certain tests to identify whether the target network complies with the guidelines provided by the following organizations:

Federal Information Security Management Act of 2002 (FISMA)[*Error! Reference source not found.****]*** : An act devised by the U.S. Department of Homeland Security, providing certain standards for issues in Cyber Security and Communications. Compliance with this act has has been tested and reported in Figure 6.

Payment Card Industry (PCI): [31] Security Standards: An open forum that defines guidelines for data security standards. Figure 7 shows the PCI compatibility of the target network.

FISMA Requirement	Result
AC-1	fail
AC-4	fail
AC-7	fail
AT-1	pass
AT-2	pass
CM-1	pass
CM-7	pass
RA-1	pass
RA-5	pass
IA-1	fail
IA-2	fail
IA-5	fail
IA-7	fail
IA-8	fail
SI-1	pass
SI-2	pass
SI-10	pass

Fig.7. FISMA Test.

Requirements Status Summary

PCI Requirement	Result
2.2.1	PASS
2.3	FAIL
6.1	PASS
8.2	PASS
8.4	FAIL
8.5	FAIL
8.5.8	PASS
8.5.10	FAIL
8.5.11	FAIL

Hosts Status Summary

Host	Test status
172.31.10.2 (SC-505-13)	FAIL
172.31.10.4 (172.31.10.4)	PASS
172.31.10.254 (172.31.10.254)	FAIL
172.31.40.1 (172.31.40.1)	PASS
172.31.40.254 (172.31.40.254)	FAIL
172.31.50.1 (172.31.50.1)	FAIL
172.31.50.3 (172.31.50.3)	PASS
172.31.50.4 (172.31.50.4)	FAIL
172.31.50.254 (172.31.50.254)	FAIL
172.31.60.1 (sc-505-24)	PASS
172.31.70.2 (SC-505-19)	PASS
172.31.70.3 (SC-505-21)	PASS
172.31.70.4 (172.31.70.4)	PASS
172.31.70.254 (172.31.70.254)	FAIL

Fig.7. PCI Compliance.

CDPSNARF is a linux based package that is used for sniffing Cisco Discovery Packets (CDPs) and gaining information about the devices in the network. Figure 8, is a screen-shot showing the output of such procedure regarding the network gateway. This information was gathered from outside the network.

Fig. 8. CDPSnarf Output.

CGE.pl is a purl module that operates linux environment. This packet has the capability of overloading ports on networking devices, hence deeming them unusable. Figure 9 shows the successful exploit that was conducted using this tool.

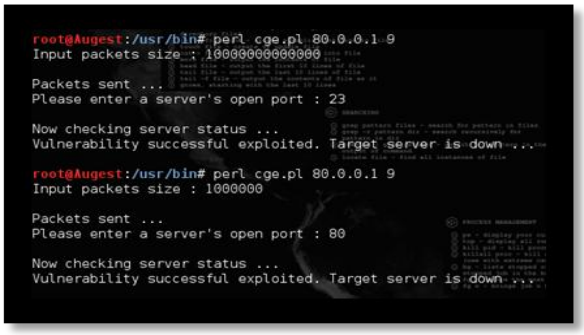

Fig.9. CGE.pl Output.

Zenmap is a powerful scanning tool. This is the same tool that metasploit utilizes for the purpose of network scanning and enumeration. Dmitry is used for information gathering from networking devices. The following output was gained by running Dmitry from outside the gateway. As seen in Figure 10, Dmitry has discovered two open ports on the router.

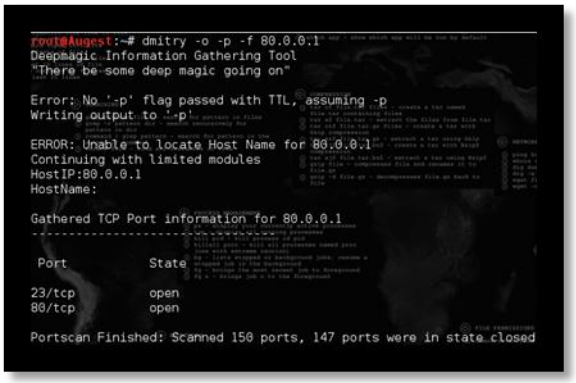

Fig.10. Dmitry Information Gathering output.

Fern WiFi Cracker is an automated tool which uses other packages such as aircrack-ng to crack wireless Access Points' passwords by using various methods like dictionary files. As an example one of the APs in the test-bed was successfully attacked in Figure 11.

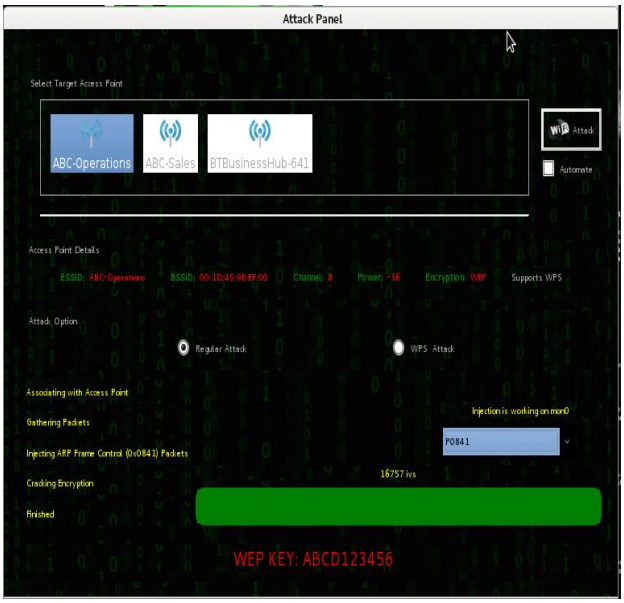

Fig.11. Fern-WiFi-Cracker Attack Successes.

Fern-Wifi-Cracker is a dangerous tool, since it supports multiple exploitation methods and uses updated dictionary files to crack the passwords on wireless APs. Zenmap is a very strong information gathering tool that can be used to gather a large volume of information about the target network. The intense scan in Zenmap can identify open ports, OS fingerprints and a partial topology map. But it is not a time efficient tool for network testing.

Finally, the strongest tool for penetrating a network is the Metasploit framework. Not only does this framework conduct attacks but also it provides reports for further evaluation and analysis. On top of

that, Compliance tests can be arranged to gain a better understanding of the status of the network.

5. Conclusion

In this paper it has become clear, that as technology grows so does the need for more advanced a security measure which is triggered by rise of vulnerabilities and evidently attack sophistication. On the plus side, the growth in technology has also had a negative impact from an attacker's point of view. Since the current architecture of WANs, is becoming more and more complicated with addition of new protocols, the attacks would require more knowledge and since not everyone can get educated in this field, a great number of attackers have been deploying attacks by aid of preprogrammed software patches. So the lack of knowledge on attacker's side can be exploited in the process of trace-back. There has always been a balance between security threats and their countermeasures, but these measures usually concentrate on detecting and blocking the threats rather than to hide important network resources from them.

Acknowledgement

In this work Dhananjay Singh was supported by Hankuk University of Foreign Studies research funds.

References

1. W. Chun-zi and H. Guang-qiu, "A new method for network threat quantification analysis," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 1, 2010, pp. V1–601–V1–605.
2. X. Liang and Y. Xiao, "Game theory for network security," Communications Surveys Tutorials, IEEE, vol. 15, no. 1, pp. 472–486, 2013.
3. M. Dekker, "Cert Coordination Center Reports on Security of the Internet," The Froehlich/Kent Encyclopedia of Telecommunications, 1997.
4. F. Lau, S. Rubin, M. Smith, and L. Trajkovic, "Distributed denial of service attacks," in Systems, Man, and Cybernetics, 2000 IEEE International Conference on, vol. 3, 2000, pp. 2275–2280 vol.3.
5. L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "2004 CSI/FBI Computer Crime and Security Survey," CSI/FBI, Tech. Rep., 2004.
6. A. Salah, M. Shouman, and H. Faheem, "Surviving cyber warfare with a hybrid multiagent-base intrusion prevention system," Potentials, IEEE, vol. 29, no. 1, pp. 32–40, 2010.
7. J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, and R. Thomas, "Accurately measuring denial of service in simulation and testbed experiments," Dependable and Secure Computing, IEEE Transactions on, vol. 6, no. 2, pp. 81–95, 2009.
8. J. Haggerty, Q. Shi, and M. Merabti, "Early detection and prevention of denial-of-service attacks: a novel mechanism with propagated traced-back attack blocking," Selected Areas in Communications, IEEE Journal on, vol. 23, no. 10, pp. 1994–2002, 2005.
9. A. Kuzmanovic and E. Knightly, "Low-rate tcp-targeted denial of service attacks and counter strategies," Networking, IEEE/ACM Transactions on, vol. 14, no. 4, pp. 683–696, 2006.
10. H. Huang, N. Ahmed, and P. Karthik, "On a new type of denial of service attack in wireless networks: The distributed jammer network," Wireless Communications, IEEE Transactions on, vol. 10, no. 7, pp. 2316–2324, 2011.
11. Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Analysis of coordinated denial-of-service attacks in ieee 802.22 networks," Selected Areas in Communications, IEEE Journal on, vol. 29, no. 4, pp. 890–902, 2011.
12. M. Handley and E. Rescorla, "Internet Denial-of-Service Considerations," Internet Engineering Task Force, Tech. Rep., 2006.
13. H. Orman, "The Morris Worm: a fifteen-year perspective," Security Privacy, IEEE, vol. 1, no. 5, pp. 35–43, 2003.
14. L. Wang and B. Srinivasan, "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard," in Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on, vol. 2, 2010, pp. 109–113.
15. T. Ma, Y.-H. Lee, and M. Ma, "Protecting satellite networks from disassociation dos attacks," in Communication Systems (ICCS), 2010 IEEE International Conference on, 2010, pp. 662–666.
16. W. Liu, "Research on dos attack and detection programming," in Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on, vol. 1, 2009, pp. 207–210.
17. R. A. Deal, "Cisco Router Firewall Security: DoS Protection," Cisco, Tech. Rep., 2004.
18. P. Kumar and S. Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms," in

Advance Computing Conference, 2009. IACC 2009. IEEE International, 2009, pp. 1275–1280.
19. D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006.
20. S. McClure, J. Scambray, and G. Kurtz, Hacking Exposed 5th Edition (Hacking Exposed). plus 0.5em minus 0.4emMcGraw-Hill Osborne Media, 2005.
21. I. Ahmed, A. James, D. Singh, "Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP", Security and Communication Networks, John Wiley & Sons, Ltd., March 2013.
22. E.-A. Campbell, I. A. Shah, and K.-K. Loo, "Medium Access Control and Transport protocol for Wireless Sensor Networks: An overview," International Journal of Applied Research on formation Technology and Computing, 2010.
23. C. E.-A. Campbell, K.-K. Loo, and R. Comley, "A new mac solution for multi-channel single radio in wireless sensor networks," in Wireless Communication Systems (ISWCS), 2010 7th International Symposium on, 2010, pp. 907–911.
24. D. Singh, H.J. Lee, W. Y. Chung, "Secure IP-Ubiquitous Sensor Network for Healthcare Applications Monitoring In-Home Area", The Second International Conference on the Applications of Digital Information and Web Technologies 2009, (ICADIWT 2009), London, Aug. 2009, pp. 335-337.
25. K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical Guide to Information Security Testing and Assessment," National Institute of Standards and Technology- US Department of Commerce, Tech. Rep., 2008.
26. A. Bechtsoudis and N. Sklavos, "Aiming at higher network security through extensive penetration tests," Latin America Transactions, IEEE (Revista IEEE America Latina), vol. 10, no. 3, pp. 1752–1756, 2012.
27. F. A. Alisherov and F. Y. Sattarova, "Methodology for penetration testing", International Journal of of Grid and Distributed Computing, vol. 2, no. 2, pp. 43–50, 2009.
28. ISECOM, "Open source security testing methodology manual," ISECOM, Tech. Rep., 2001.
29. C. Wijaya, "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network," in Informatics and Computational Intelligence (ICI), 2011 First International Conference on, 2011, pp. 355–360.
30. R. Ross, "Managing enterprise security risk with nist standards," Computer, vol. 40, no. 8, pp. 88–91, 2007.
31. J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, and V. Singh, "A survey of payment card industry data security standard," Communications Surveys Tutorials, IEEE, vol. 12, no. 3, pp. 287–303, 2010.