

An Enhanced Approach for DNS Pharming Detection

A thesis submitted in partial fulfilment of the requirements for the degree of
Master of Science in Network Security

By:

Fahad Badi Abdulmohassen Al-Dossary

Student Number# 4370806

Naif Arab University for Security Sciences 2019

Under Supervision of:

Dr. Ahmed Elsherif

Submitted to:

Department of Network Security
Information Security College and Computer,
Naif Arab University for Security Sciences

May 2019

Table of Contents

Abstract	ii
Statement of Original Authorship	iii
Table of figures.....	v
List of Abbreviations.....	vi
Chapter 1: Introduction	1
1.1 Introduction.....	1
1.2 Related works.....	2
1.3 Problem	4
1.4 Questions.....	5
1.5 Objectives.....	5
Chapter 2: Background and Literature Review	7
2.1 DNS attack.....	7
2.1.1: The concept of DNS.	7
2.1.2: Mechanism of DNS.	8
2.1.3: Detect and prevention DNS attacks.	9
2.2 Pharming and phishing attacks.....	10
2.2.1: The concept of phishing attack.	10
2.2.2: The types of phishing attacks:	11
2.2.3: Pharming attack.	12
2.2.4: The approaches to detect and prevent pharming attacks.	13
2.3 Previous studies.....	14
Chapter 3: Methodology	17
3.1 Introduction.....	17
3.2 Proposed framework	17
3.3 Discussion of proposed framework.....	21
3.3.1 VMs Configuration:.....	22
Chapter 4: Results and Discussions	31
4.1 Experimental Results and Evaluation	31
4.1.1 Attack 1: Attackers have already compromised the victim's machine	31
4.1.2 Attack2: Directly Spoof Response to User	34
4.1.3 Attack3: DNS Server Cache Poisoning	38
4.1.4 Attack 4: An Advanced DNS Cache Poisoning (Remote Attack)	47
Chapter 5: Conclusion.....	55
5.1 Conclusion.....	55
5.2 Recommendations	56
References.....	59
Arabic Title Page.....	Error! Bookmark not defined.

Table of figures

Figure [1]: description of pharming attacks.	13
Figure [2]: Flow chart of proposed framework.	19
Figure [3]: screenshot of Configure the DNS Server	23
Figure [4]: running of DNS Server configuration.	23
Figure [5]: Confirmed DNS settings	26
Figure [6]: Configure User PC	27
Figure [7]: running of User PC configuration.	28
Figure [8]: examble.com domain.	31
Figure [9]: attacker PC running.	32
Figure [10]: attacker PC running.	33
Figure [11]: hackthissite screenshot	34
Figure [12]: attack configuration.	36
Figure [13]: information of spoofed DNS response.	37
Figure [14]: change IP address.	38
Figure [15]: DNS Server Cache Poisoning attacks.	39
Figure [16]: configure Bind server as caching or forwarding DNS server.	40
Figure [17]: resolv.conf and add DNS server IP.	41
Figure [18]: In terminal type ping www.google.com.	42
Figure [19]: In terminal type ping www.google.com.	42
Figure [20]: using sudo netwag and set parameters.	44
Figure [21]: ping on www.lums.edu.pk.	45
Figure [22]: ping on www.google.com.	45
Figure [23]: spoofed responses.	46
Figure [24]: traced the attack in Wireshark	47
Figure [25]: attack is successful.	53
Figure [26]: successfully attacks.	53