TO MITIGATE DNS CACHE POISONING USING ICMP PING

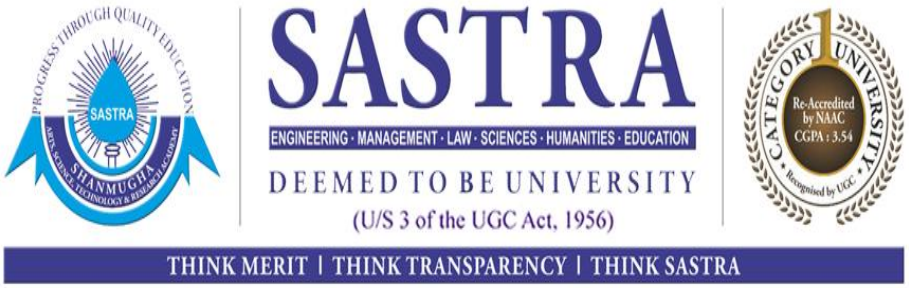
Report submitted to the SASTRA Deemed to be University
as the requirement for the course

CSE302: COMPUTER NETWORKS

Submitted by

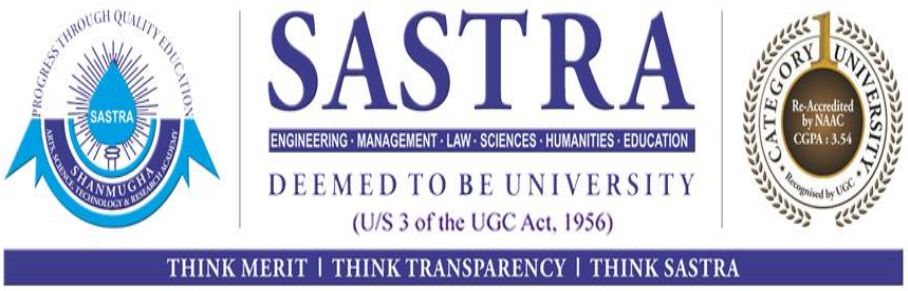
NAME (PUJITA V)
(Reg. No.: 123004189, ECE)

February 2021



SCHOOL OF COMPUTING

THANJAVUR, TAMIL NADU, INDIA – 613 401



SCHOOL OF COMPUTING

THANJAVUR – 613 401

Bonafide Certificate

This is to certify that the report titled "" submitted as a requirement for the course,

CSE302: COMPUTER NETWORKS for B.Tech. is a bonafide record of the work done by

Shri/Ms. Pujita V (Reg. No.123004189,ECE) during the academic year 2020-21, in the School of Computing

Project Based Work *Viva voc*e held on _____

Examiner 1 **Examiner 2**

List of Figures

List of Tables

Abbreviations

ICMP	Internet Control Message Protocol
DNS	Domain Name System
IP	Internet Protocol

Abstract

ICMP ping is used to prevent DNS cache poisoning. If we get ICMP ping reply, when DNS pings the IP address sent to it as a reply for DNS query, then the reply to the query is from legitimate server. The above model is stimulated using cisco packet tracer.

KEY WORDS: DNS cache poisoning, Cisco packet tracer, ICMP.

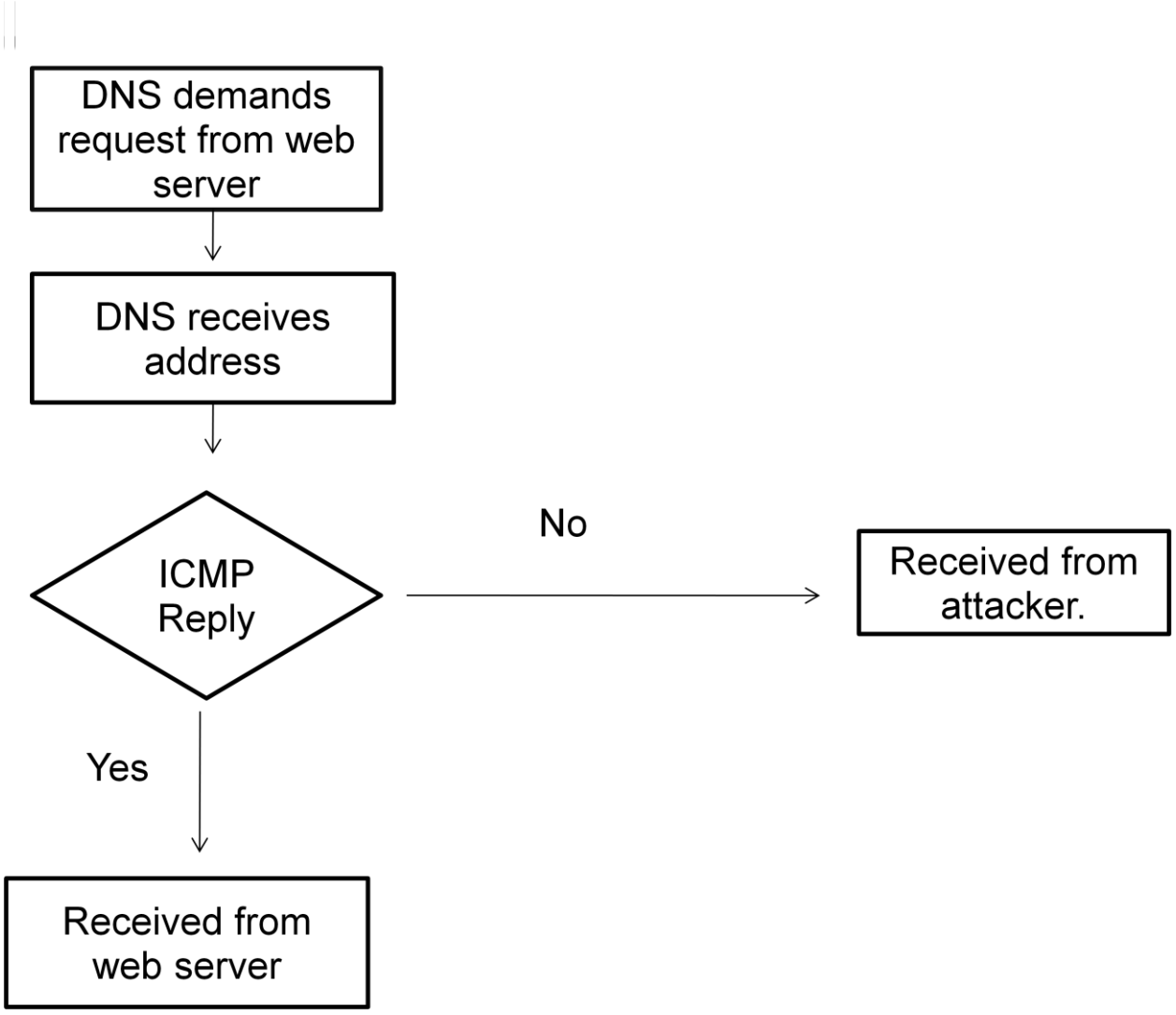
Table of Contents

INTRODUCTION

The operation of DNS is to provide the IP address of domain requested by the host.
DNS gets request from host demanding IP address of a domain.DNS sends message to say root server DNS demanding the IP address of the domain. Root DNS sends IP address to DNS. DNS sends IP address to host. If frequently a domain name's address is requested by hosts then DNS will not request the IP address from Root server each time .The IP address of the domain is stored in cache, but this IP address will not stay in cache forever. This is called cache aging. The amount of time, domain address remain in cache depends on TTL (time to live). After TTL, the domain address will removed from cache. DNS requests for domain address from web server at that time the request is answered by attacker with wrong domain address (for this the attacker must be faster than web server) and it will be stored in cache. Hence hosts asking for the domain address will be directed to wrong domain address. This is called DNS cache poisoning.

To mitigate DNS cache poisoning using ICMP ping .When ICMP ping message is sent to attacker we won't get reply back hence we can conclude the ip address is received from attacker.
Using the above model we can prevent cache poisoning. Using ICMP ping feature in cisco packet tracer the model is simulated.

METHODOLOGY



Network Topology

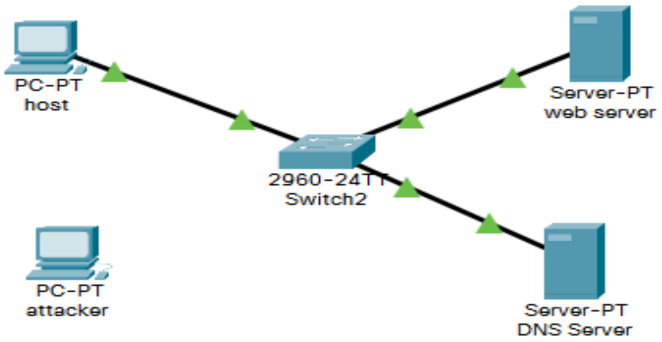


Fig -2

IP Address

Host	192.168.5.13
Web server	192.168.5.14
DNS	192.168.5.12
Attacker	192.168.5.17

Table 1

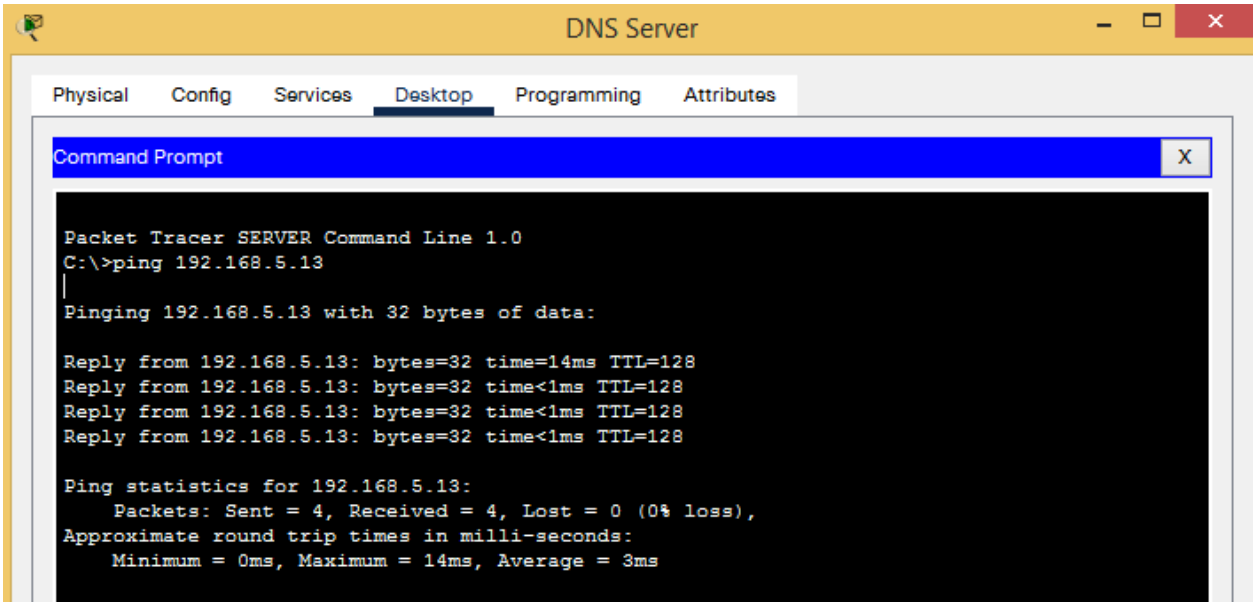

DNS Server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.5.13
Pinging 192.168.5.13 with 32 bytes of data:
Reply from 192.168.5.13: bytes=32 time=14ms TTL=128
Reply from 192.168.5.13: bytes=32 time<1ms TTL=128
Reply from 192.168.5.13: bytes=32 time<1ms TTL=128
Reply from 192.168.5.13: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.5.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 3ms

Fig -2

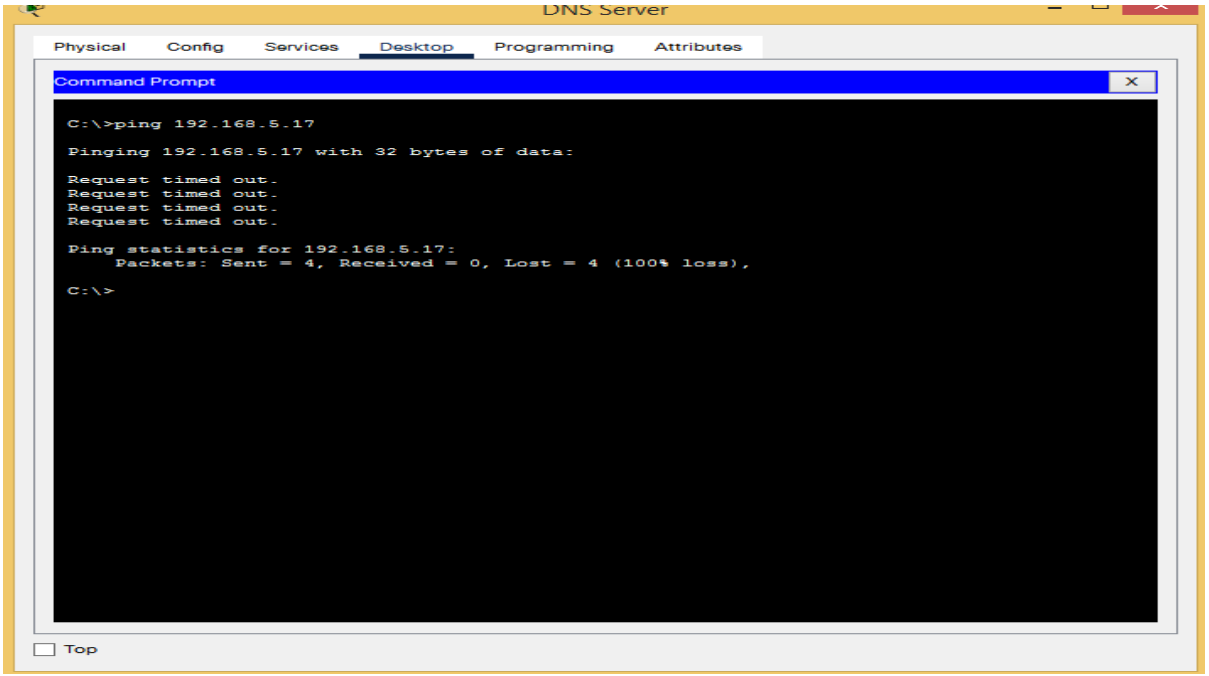

DNS Server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
C:\>ping 192.168.5.17
Pinging 192.168.5.17 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.5.17:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

Fig 3

Conclusion

From the output we can see that when we send ICMP ping message to reply from legitimate web server we get reply. But when ICMP reply is sent to attacker we didn't get reply back. Hence we can conclude ICMP ping can be used for finding malicious attacker. The above model can be used to overcome DNS spoofing as there is subtle difference among the two. The major demerit here is if web Browser is firewall configured then ICMP reply messages can't be sent and legitimate reply for the DNS query may considered as reply from attacker.

References

1) Yong Jin;Masahiko Tomoishi;Satoshi Matsuura 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)
2) Xi Yu;Xiaochen Chen;Fangqin Xu 2011 International Conference of Information Technology, Computer Engineering and Management Sciences
3) https://www.cloudflare.com