DNS Security Using Cryptography

Prof. Vaishali Gupta, Mr. Samay Kumar Singh
School of Computer Science Engineering , Galgotias University , Greater Noida ,U.P. , India

Abstract- **DNS, name System, is one in every of the foundational protocols for net to figure. It resolves hostnames to scientific disciplined addresses called informatics addresses that permits applications like net browsers and humans to use net or alternative networks simply. owing to its restricted practicality, it's wide open in several enterprise firewalls with a really less attention from enterprise security observation. because of of these factors, several tools have evolved to line up covert info tunneling channels through DNS which matches unobserved inflicting vital info exfiltration risks to organizations and money losses to ISPs. Hence, it is important to analyze and stop DNS tunneling. during this paper we tend to rehearse DNS summary, completely different DNS tunneling tools and techniques to dam it. thus DNS provides a mechanism to try to to mapping between hostnames and informatics address employing a distributed gradable info of system/service names and informatics addresses. A supply trying to find informatics address of any remote system or service is understood as DNS consumer**

Index Terms- **DNS Tunneling, IP addresses, hostnames, firewalls**

I. INTRODUCTION

Humans can’t assume like computers. they solely can’t keep in mind dozens of information science addresses. they have easy-to-remember names to find their mail server or their favorite sites. to create our lives on the net straightforward, DNS was thus fictional. And with it came a replacement place for hackers of all kinds to own fun. Moreover, the aim of DNS makes it a awfully sensitive area; for this is often the place the shopper association is oriented. the probabilities a black-hat will have by succeeding in hacking DNS area unit tremendous (a user will be directed to a bunch controlled by a hacker, no matter service he could be using: communications protocol, ftp, telnet ...). something is possible! The name System distributes the responsibility of assignment domain names and mapping those names to information science addresses by designatingauthoritative name servers for every domain. Authoritative name servers area unit assigned to be accountable for their supported domains, and will delegate authority over sub- domains to alternative name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the requirement for one central info. The name System conjointly specifies the technical practicality of the info service that is at its core. t defines the DNS protocol, a close specification of the info structures and electronic communication exchanges utilized in DNS, as a part of the net Protocol Suite. traditionally, alternative directory services preceding DNS weren't scalable to massive or international directories as they were originally supported text files, conspicuously the HOSTS.TXT resolver. DNS has been in wide use since the Nineteen Eighties. The DNS plays a essential role in supporting the net infrastructure by providing a distributed and fairly strong mechanism that resolves web host names into IP addresses and IP addresses back to host names. The DNS additionally supports different web directory-like search capabilities to retrieve info referring to DNS Name Servers, Canonical Names, Mail Exchangers, etc. sadly several security weaknesses surround IP and therefore the protocols carried by IP. The DNS isn't proof against these security weaknesses. The accuracy of the data contained at intervals the DNS is important to several aspects of IP primarily based communications.

The threats that surround the DNS square measure due partly to the dearth of credibleness ANd integrity checking of the info command at intervals the DNS and partly to different protocols that use host names as an access management mechanism. In response to the current, the IETF fashioned a social unit to feature DNS Security (DNSSEC) extensions to the prevailing DNS protocol.

The name System (DNS) may be a stratified distributed naming system for computers, services, or any resource connected to the net or a non-public network. It associates numerous info with domain names appointed to every of the collaborating entities. Most conspicuously, it interprets domain names, which might be simply memorized by humans, to the numerical IP addresses required for the aim of pc services and devices worldwide. The name System is a vital element of the practicality of most web services as a result of it's the Internet's primary directory service.

The DNS plays a essential role in supporting the net infrastructure by providing a distributed and fairly strong mechanism that resolves web host names into IP addresses and IP addresses back to host names. The DNS additionally supports different web directory-like search capabilities to retrieve info referring to DNS Name Servers, Canonical Names, Mail Exchangers, etc. sadly several security weaknesses surround IP and therefore the protocols carried by IP. The DNS isn't proof against these security weaknesses. The accuracy of the data contained at intervals the DNS is important to several aspects of IP primarily based communications.

The name System distributes the responsibility of assignment domain names and mapping those names to IP addresses by designatingauthoritative name servers for every domain. Authoritative name servers square measure appointed to be accountable for their supported domains, and should delegate authority over sub-domains to different name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the necessity for one central info.

The name System additionally specifies the technical practicality of the info service that is at its core. It defines the DNS protocol, a close specification of the info structures and electronic communication exchanges utilized in DNS,as a part of the net Protocol Suite. traditionally, different directory services preceding DNS weren't climbable to giant or world directories as they were originally supported text files, conspicuously the HOSTS.TXT resolver. DNS has been in wide use since the Nineteen Eighties. The DNS plays a essential role in supporting the net infrastructure by providing a distributed and fairly strong mechanism that resolves web host names into IP addresses and IP addresses back to host names. The DNS additionally supports different web directory-like search capabilities to retrieve info referring to DNS Name Servers, Canonical Names, Mail Exchangers, etc. sadly several security weaknesses surround IP and therefore the protocols carried by IP. The DNS isn't proof against these security weaknesses. The accuracy of the data contained at intervals the DNS is important to several aspects of IP primarily based communications. the net maintains 2 principal namespaces, the name hierarchy and therefore the web Protocol (IP) address areas. The name System maintains the name hierarchy and provides translation services between it and therefore the address areas. web name servers and a communication protocol implement the name System. A DNS name server may be a server that stores the DNS records for a website name; a DNS name server responds with answers to queries against its info. the foremost common sorts of records keep within the DNS info square measure for DNS zone authority (SOA), IP addresses (A and AAAA), SMTP mail exchangers (MX), name servers (NS), pointers for reverse DNS lookups (PTR), and name aliases (CNAME). though not meant to be a general purpose info, DNS will store records for different sorts of knowledge for either automatic machine lookups, like DNSSEC records, or for human queries like accountable person (RP) records. As a general purpose info, DNS has additionally seen use in combating uninvited email (spam) by employing a period of time part list keep within the DNS. whether or not for web naming or for general purpose uses, the DNS info is historically keep in a very structured zone file.

II. LITERATURE REVIEW

- In the within the Pharming attacks Detection mistreatment Authoritative mistreatment authors demonstrate regarding the detections of Pharming attack Associate in Nursingd planned an approach to guard user at client- side from Pharming attacks. Pharming attacks are often performed at the client-side or into the net. In pharming attack, attackers needn't targeting individual user. If pharming is performed by modifying the DNS entries, than it'll be moving to any or all users UN agency is accessing the net page through that DNS. we tend to propose Associate in Nursing approach to guard user at client-side from pharming attacks by comparison information science addresses, mistreatment info provided by native DNS server and an inventory of IP's provided by the domain's echt Name Servers that square measure the foremost trusty DNS servers for a website. it absolutely was chiefly done by comparison information science addresses, mistreatment info provided by native DNS server and an inventory of IP’s provided by the domain’s echt Name Services that square measure the foremost trusty DNS serve [2].
- Also within the paper conjointly and interference Algorithms of DDOS Attack in MANETs‖ authors demonstrate regarding the detections and interference of DDoS attack. we tend to introduce bottom-up approach, New Cracking algorithmic program, interference algorithmic program mistreatment IDS node for detection and dominant DDoS attack.Security could be a weak link of network systems. The malicious usage and attacks have caused

tremendous loss by impairing the functionalities of the pc networks.. In a trial to boost security in MANETs several researchers have recommended and enforced new enhancements to the protocols and a few of them have recommended new protocols. Existing Edouard Manet routing protocols, like spontanepous On-Demand Distance Vector Routing Protocol (AODV), don't give enough security defense capability. Distributed Denial of Service (DDoS) attack has become a serious drawback to networks. during this paper, we tend to introduce bottom-up approach, New Cracking algorithmic program, interference algorithmic program mistreatment IDS node for detection and dominant DDoS attack [4].

- In the paper ―Addressing complexness in DNS Security: A Case for Improved Security standing Indication supported a Trust Model‖ more and more complicated factors for DNS name resolution mean that users square measure unable to form enlightened choices of the risks they face on the net. we tend to conclude that there's no straightforward means that of assessing the trust users may place in DNS responses, which there's presently no effective means of interactively representing this within the browser UI. during this paper we tend to propose more work to develop a trust model for DNS name resolution, taking under consideration the numerous complicated eventualities users encounter. Building on such a trust model, a brand new means that of representing security risk to users in an exceedingly application ought to be developed. while not an easy illustration to convey the standing of the varied complicated factors mentioned here, it's impractical for user to form enlightened security choices once mistreatment the net. Another future step is to deal with the special wants that cloud computing can have in terms of DNS. this might embrace the management of inter-cloud resources to explore further options of past works concerning to effective programing or electronic messaging [5].

III. METHODOLOGY

We need create|to form} BIND DNS that make DNS Security mistreatment Cryptography. Enhance Open supply DNS server supply so as to support conditional parsing algorithms for machine-driven detection and interference against each, the attacks on DNS Associate in Nursingd wherever DNS is exploited as an attack vector. Develop a trade normal however Open supply net Interface for straightforward administration, management and news of DNS Server. It ought to facilitate with granular DNS configuration, rule definition (as a part of above), security feed assortment, custom news and knowledge export in numerous formats like CSV and PDF.

3.1 SOFTWARE_REQUIREMENTS SPECIFICATION

A computer code necessities specification (SRS) could be a description of a software to be developed. It lays out practical and non-functional necessities, and should embrace a group of use cases that describe user interactions that the computer code should give.

Hardware Requirements:
• System : Intel Core i3
• hard disc : forty GB.
• Monitor : fifteen VGA Color.
• RAM : 4GB

Software Requirements:
• package : Windows Server 2012
• DNS computer code : BIND
• different Application needed : net and Host Server, VM Ware

Database Support:
While earlier versions of BIND offered no mechanism to store and retrieve zone knowledge in something aside from flat text files, in 2007 BIND nine.4 DLZ provided a compile-time possibility for zone storage in an exceedingly kind of information formats together with LDAP, Berkeley decibel, PostgreSQL, MySQL, and ODBC.BIND ten planned to form the information store standard, in order that a range of databases could also be connected.

IV. RSA ALGORITHM

RSA is one in all the primary sensible public-key cryptosystems and is wide used for secure knowledge transmission. In such a cryptosystem, theencryption secret is public and differs from the coding key that is unbroken secret. In RSA, this spatial property is predicated on the sensible problem of resolution the merchandise of 2 giant prime numbers, the resolution downside. RSA is created of the initial letters of the surnames of Bokkos Rivest, Adi Shamir, and Elmore John Leonard Adleman, UN agency 1st publically delineate the rule in 1977. A user of RSA creates so publishes a public key supported 2 giant prime numbers, at the side of AN auxiliary price. The prime numbers should be unbroken secret. Anyone will use the general public key to inscribe a message, however with presently printed strategies, if the general public secret is giant enough, solely somebody with data of the prime numbers will feasibly rewrite the message. Breaking RSAencryption is thought because the RSA downside; whether or not it's as exhausting because the resolution problem remains AN open question. RSA could be a comparatively slow rule, and since of this it's less usually wont to directly inscribe user knowledge. More often, RSA passes encrypted shared keys for centrosymmetric key cryptography that successively will perform bulk encryption- coding operations at abundant higher speed

RSA Steps

Step one : choose 2 prime nos. – p& letter like p!=q
Step two : Calculate n as product of p & letter, i.e. n=pq
Step three : Calculate m as product of (p-1) & (q-1)
i.e. m = (p-1)(q-1)
Step four : choose any whole number esuch it's co-prime to m, co-prime suggests that gcd(e,m)=1
Step five : Calculate d such American state mod m = one , i.e. d = e^-1 mod m
Step 6: the general public secret is personal secret is, So these square measure the keys, currently if you would like to preform some encoding operation mistreatment these keys here square measure the steps, if you've got a text P..its encrypted version(cipher text C is)
C = P^e mod n
To decode it back to plain text use P = C^d mod n

V. RESULT AND DISCUSSION

- misprint Squatting: In misprint squatting, additionally known as URL hijacking, could be a style of cybersquatting that depends on mistakes like typographic errors created by web users once inputting an internet site address into an internet browser. Server can send to actual web site.
- Session Hijacking: In session hijacking or cookie hijacking is that the exploitation of a sound laptop session to achieve unauthorized access to data or services during a automatic data processing system. Server won't permit to transfer session.
- DDoS / DoS attacks: during this once offensive mistreatment unlimited ping, the server can avoid such pings by block that specific port.
- Cache Poisoning attacks: this kind of attack are avoided by mistreatment public and personal keys.
- Zone Transferring attacks: once assaulter tries to transfer zones files the server won't permit such activity thanks to security mistreatment RSA-256.
- Port Security: If there's malicious activity from any port or thanks to any program we will block it mistreatment firewall.
- Secure Sockets Layer: during this we've establishing AN encrypted link between an internet server and a browser. This link ensures that every one knowledge passed between the net server and browsers stay personal and integral.

VI. CONCLUSION AND FUTURE SCOPE

Now when this whole study of DNS and also the half that we've enforced you will talk over with your servers' personal network interfaces by name, instead of by information processing address. This makes configuration of services and applications easier as a result of you now not got to bear in mind the personal information processing addresses, and also the files are easier to browse and perceive. Also, currently you'll modification your configurations to purpose to new servers during a single place, your primary DNS server, rather than having to edit a spread of distributed configuration files, that eases maintenance. Once you've got your internal DNS came upon, and your configuration files square measure mistreatment personal FQDNs to specify network connections, it's essential that your DNS servers square measure properly maintained. If they each become unobtainable, your services and applications that believe them can stop to perform properly. this is often why it's counseled to line up your DNS with a minimum of one secondary server, and to keep up operating backups of all of them. we have a tendency to could use the conception of Active Directories and DHCP at distributed networking through name System so as to boost its practicality and dealing.

REFERENCES

[1] Naveen Kumar and Kamal Kumar Ranga, , June 2015, ―A Framework for mistreatment Cryptography for DNS Security‖, IJCSMC Vol. 4.

[2] Abraham S. Alfayoumi ,Tawgiq S. Barhoom, March 2015, ―Client-Side Pharming Attacks Detection mistreatment Authoritative mistreatment Volume 113- No. 10.

[3] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin and Nikita Somaiya, 2015,
―Connection-Oriented DNS to boost Privacy and

Security‖, IEEE.

[4] Geetika, Naveen Kumari, August 2013, additionally & bar Algorithms of DDoS Attack in MANETs‖ Volume three.