

Research and practice of DNS exploits

Mircea-Radu-Şerban Dobrău
P147987

M7X01702
Dr. Mabrouka Abuhmida

Abstract

More and more devices are getting connected as time goes on. As a result, cyber-security breaches are much more likely and may have far more dangerous consequences. As an example, DNS attacks have been getting more and more popular, as well as highly dangerous, as can be seen in the 2014 Dyn DNS DDoS attack. As such, knowledge of DNS operation as well as DNS attacks is essential with regards to expertise in the field of cyber-security. This report presents a project proposal with the topic of DNS exploit research. It starts with an introduction which details the important context of DNS exploit research. Following this, a literature review of the DNS protocol's operation, design, as well as a summary of some DNS exploits is presented. Next, the context and motivation for the chosen research topic is presented, as well as the project's aim and objectives. Finally, the following chapters detail the project's research and development methods, concluding with the resources and planning of the project.

Contents

1	Introduction	4
1.1	The “Internet of Things” as an emerging concept	4
1.2	Prevalence of DNS attacks	4
1.3	DNS DDoS attack using the Mirai botnet	5
1.4	End of introduction	5
2	Literature review	6
2.1	DNS design and operation	6
2.2	DNS exploits	7
3	Context and motivation for research	10
4	Aim and objectives	10
5	Expected outcomes and deliverables	11
6	Research Methods	11
6.1	Research Types	11
6.2	Philosophy	12
6.3	Approaches	12
6.4	Strategies	13
6.5	Data collection	13
7	Development Methods	13
7.1	Experiment	13
7.2	Software development	14
7.3	Risks and limitations	14
7.4	Data collection and evaluation	15
8	Resources and Planning	15
8.1	Resources required	15
8.2	Gantt chart	16
	References	17

List of Figures

1	DNS recursive look-up process	6
2	DNS MitM attack	9
3	Gantt chart	16

1 Introduction

1.1 The “Internet of Things” as an emerging concept

The level of connectedness between everyday objects and devices is steadily increasing. For example, there exist tens of billions of connected devices and increasing [3, p. v], with an expected number of 26 billion to be reached by 2020 [4, p. 114], as well as 7 billion devices connected over cellular networks by 2025. [5, p. 35]

Within this context, new concepts have emerged with the scope of dealing with small and large-scale connectivity issues, such as the “smart cities” and “Internet of Things” concepts.

For example, the “smart city” concept is gaining ground in urban areas [6, p. 29], which aims to implement ICTs (Information and Communication Technologies) towards the aim of improving the level of quality in urban life as well as the reduction of resource consumption. [5, p. ix]

On the other hand, the IoT (Internet of Things) concept is defined as the connection of physical devices through the Internet [5, p. 59], of which aim is to provide “smart” solutions to other issues [5, p. ix] such as:

- Governance
- Economic growth
- Environmental sustainability
- Transportation
- Power
- Water usage

As a result, cyber-security breaches happen more often and could have wider-reaching consequences. [7, p. 156] [8, p. 153] For example, cyber-security threats against mobile devices, such as Android-running smartphones, have been perpetually increasing. [9, p. xiii] Furthermore, breaches caused by vulnerabilities in computer networks were responsible for roughly 37% of all breaching incidents in US health-care facilities. [10, p. 274]

1.2 Prevalence of DNS attacks

A type of cyber-security attack is one which makes use of the DNS (Domain Name System) protocol. A network security newsletter [11, p. 1] cites a claim that “77% of organizations were hit with a DNS-related attack in the past year, with an average of seven attacks per organization.” As a result of these attacks, roughly a third of the organizations lost data worth 715,000 dollars.

Furthermore, it is noted [12, p. 17] that a Cisco security report from 2014 found that all of the examined corporate networks had DNS look-ups to malware-hosting sites, with 96% of traffic going to hijacked servers and 92% to sites hosting no content, which is typically thought as a sign of malware hosting web-sites.

DNS attacks may also be arguably targeted against end-user IoT devices as the majority of end-users are not familiar with DNS settings, thus facing the

risk of losing access to the Internet if their primarily used DNS server is taken down or not functioning properly. [13, p. 119]

Malicious users may often make use of the DNS protocol with the scope of conducting attacks. A simple and relatively easy to implement attack [14, p. 138] involves the hosting of a server with a domain-name/URL highly similar to that of a popular service, so that users may accidentally visit the malicious web-site by a typing accident and download malicious content.

1.3 DNS DDoS attack using the Mirai botnet

A particular example of the importance of DNS server stability is the 2016 Dyn DDoS attack. The DDoS (Distributed Denial of Service) attack [15, p. 5] took control of a very large number of IoT devices such as IP cameras and old routers with the help of the “Mirai” botnet program. The devices were then used to make a significant part of the Internet unavailable by sending a very large number of requests to the DNS servers of the “Dyn” DNS provider.

More concretely, the Mirai botnet process runs thus [16, p. 1]:

- Run a C2 (Command and Control) server that is connected to by infected devices
- Scan for other devices and test them for weak SSH/Telnet credentials
- If credentials are found, send them to a separate server which uses the said credentials to download malware on the vulnerable devices
- Once the device is infected, it waits for DDoS attack commands to be sent to it

Achieving a speed of up to 1 terabytes per second [17, p. 4], the Mirai botnet DNS DDoS attack [18] has disabled access to hundreds of services, such as Twitter, Netflix, Reddit, CNN and many other services found within Europe and the US. Furthermore, Dyn estimated that the attack involved up to 100,000 infected devices.

1.4 End of introduction

As such, it can be confidently asserted that DNS constitutes a critical part of the Internet’s infrastructure. For this reason, a knowledge of how DNS, DNS vulnerabilities and DNS exploits function is essential for a cyber-security expert with regards to expertise in securing networks of any size.

Within this context, this report presents a project proposal which involves the research and practice of DNS exploits. By improving the amount of research on this topic, a better knowledge with regards to DNS is to be attained by both the writer of this report. Furthermore, it could also benefit other individuals wishing to research the DNS protocol, so that networks will be more secure in the long run.

The following chapter details the design and operation of the DNS protocol, as well as several DNS attacks.

2 Literature review

2.1 DNS design and operation

DNS, or Domain Name system can be defined in various ways:

Database – Within the context of this definition, DNS is a database used for distributing domain-name information. As such, the DNS database is a hierarchical, redundant and distributed database. [19, p. 1]

Protocol – On the other hand, DNS may be more commonly referred to as the application protocol used for exchanging domain-name information between a DNS server and a DNS client or other DNS server. This function is achieved with the help of DNS “queries”. [20, p. 31]

As a definition of its primary function [21, p. 1], DNS helps end-users add a level of abstraction to IP addresses by mapping them to a host-name and/or domain-name label. As a result, end-users can refer to a web-site, for example, by its domain and/or host-name instead of its IP address.

As such, there exist multiple types [1, p. 8] of DNS servers:

Root DNS server – Root DNS servers are among the most critical resources with regards to the functioning of the Internet. As such, when a name server is queried for information with regards to a domain of which it currently does not have any information, it first queries one of the root DNS servers.

TLD DNS server – TLD name servers are operated by organizations called “Registry Operators” and are responsible for the right-most or TLD (top-level domain); for example, the “.com” TLD.

Domain (user) DNS server – Finally, the domain or user DNS server is responsible for providing an “authoritative” answer with regards to the secondary-level domain; for example, “example” in “example.com”.

Whenever a user wants to find the domain-to-IP mapping of a particular resource, the following steps are undertaken [1, p. 9], with a query for the “fred.example.com” domain-to-IP mapping as an example:

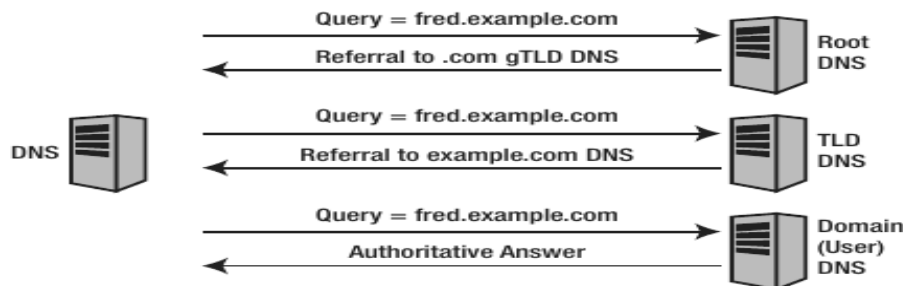


Figure 1: DNS recursive look-up process [1, p. 9]

- First of all, A query for the “fred.example.com” domain is sent to the root DNS server. As such, the root DNS server responds with a referral to the general TLD DNS server for the “.com” TLD.
- Next, the same query is sent to the TLD DNS server provided by the previously mentioned referral. Once the query is received by the TLD DNS server, the TLD DNS server sends back a referral to the SLD (Secondary-level domain) or domain/user DNS server for the “fred.example.com” domain.
- Finally, the same query is sent to the domain DNS server provided by the previous referral. The domain/user DNS server then sends the domain-to-IP mapping for the “fred.example.com” domain back to the client’s DNS server. As such, this answer is considered an “authoritative answer”.

DNS resource records, which are stored into the DNS server’s “forward look-up” zone or zone file [22, p. 389], hold information with regards to various aspects of the domain covered by the zone [22, p. 389-393], such as:

A record – Indicates the IPv4 address of a host in the domain.

AAAA record – Indicates the IPv6 address of a host in the domain.

SOA record – Indicates the primary DNS server with regards to the forward look-up zone.

NS record – Indicates the primary DNS server.

CNAME record – Indicates an alias for a host.

MX record – Indicates the mail server (if any) of the domain.

SRV record – Indicates non-mail servers of the domain.

TXT record – Contains any form of written content, can be used towards any kind of purpose.

The following chapter details several types of DNS exploits.

2.2 DNS exploits

DNS poisoning – There exist multiple methods [23, p. 3] of DNS poisoning:

Intranet DNS spoofing – Involves the poisoning of the end-user’s router at the LAN (Local Area Network) level. Afterwards, the legitimate DNS request is intercepted by the attacker and a fake response is sent back to the user, redirecting him/her to a fake web-site for malicious purposes.

Internet spoofing – Otherwise known as “remote DNS poisoning”, this attack involves sending a Trojan horse to the end-user with the scope of changing his/her main DNS server IP address to the attacker’s IP address. As a result, the attacker can now extract the end-user’s visited web-sites, as well as redirect him/her to malicious web-sites.

Proxy server DNS poisoning – Involves using a Trojan onto the end-user with the scope of changing the end-user’s proxy settings so that all his/her traffic goes through the attacker’s device.

DNS cache poisoning – Involves modifying the end-user’s DNS resolver settings/cache so that if a domain-to-IP mapping does not exist in the cache, then the end-user’s DNS query is sent to the attacker’s malicious server.

Alternatively, the attacker may impersonate as a genuine LLD (Low Level Domain) and/or SLD server, after which he/she sends a fake domain-to-IP mapping back to the end-user’s DNS resolver. [24, p. 1268] This can be accomplished by tricking the resolver into misjudging crafted DNS packets as being legitimate packets. [25, p. 3]

DNS spoofing – On the other hand, DNS spoofing can be done, for example, through a MitM (Man-in-the-Middle)-type attack. [2, p. 85] When the end-user attempts to visit a HTTPS web-site the following steps are undertaken:

- The attacker intercepts the server-to-client authorization request and replaces the original URL with a homo-graphically similar URL (for example, “accaunt.com” in the place of “account.com”) with a utility such as “SSLstrip+”.
- The end-user’s browser performs a DNS query for the non-existent domain “accaunt.example.com”; however, this request is then intercepted by the attacker using a tool such as “dns2proxy”, so that the domain-to-IP mapping sent back to the end-user contains the valid IP address of “account.example.com” but mapped to the domain-name of the non-existent “accaunt.example.com”.
- Next, the “accaunt.example.com” domain is checked against the end-user’s preinstalled HSTS (HTTP Strict Transport Security) list which helps web browsers automatically redirect visits to web-sites with the HTTP protocol to the more secure, encrypted HTTPS protocol. [2, p. 84]
- As the non-existent domain is not in the list, the web browser performs the connection to the web-site with the help of the unencrypted HTTP protocol. The attacker may now again intercept the end-user’s unencrypted traffic with the scope of extracting confidential data such as passwords.

Zone poisoning – Next, “zone poisoning” [26, p. 273] has been defined as an attack which involves the unauthorized modification of a domain’s authoritative DNS server’s zone file. For this process to work, two requirements must be met:

1. The domain’s authoritative name server must allow non-secure zone file updates from any host.
2. The attacker must know one of the names of that domain’s zones and its name server/s.

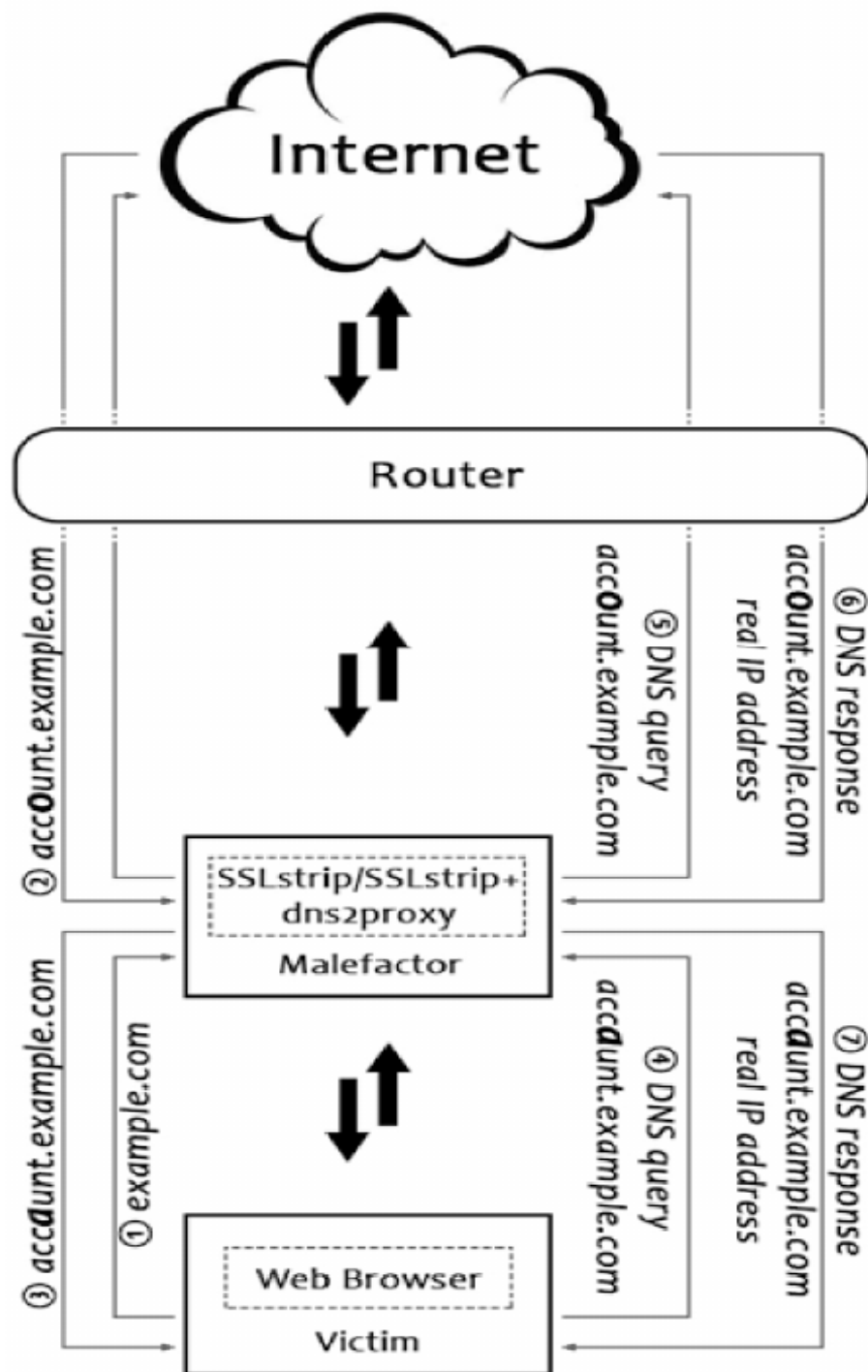


Figure 2: DNS MitM attack [2, p. 85]

As such, the attacker could, for example, update/modify the domain's "MX" (mail server) record/s, thus determining where the domain's end-users' mail is sent to.

Others – Other types of DNS attacks include domain hijacking [27] [28] [29], DNS amplification attacks [30] [31] and DNS tunneling and/or ex-filtration [32] [33] [34]. In addition to these, there exists a likely possibility for more DNS exploitation methodologies to be found, as well as more thorough research on the exploits previously mentioned, such as:

- The likelihood of such attacks to occur during the present period
- Defense and security methodologies; strategies which strive to minimize the risk and/or impact of said DNS attacks
- Tools used, if any, for both the accomplishment and defense of DNS attacks

The following chapter deals with the context and motivation for the chosen research topic.

3 Context and motivation for research

The subject of DNS exploits has been chosen for the following reasons:

- To broaden personal knowledge in the field of network security
- To attain a thorough understanding of DNS operation, as well as DNS attacks and mitigation against them
- To improve research on the subject by contributing with more up-to-date information with regards to DNS attacks and exploits

It is hoped that the writer of this report's subsequent research and contribution to the currently available knowledge of this topic will also help other individuals who wish to gain a more thorough understanding of DNS exploits.

4 Aim and objectives

The aim of this project is to research DNS exploits. As such, its objectives are to:

- Conduct and write a literature review, comprising of both old and new exploit research; including details such as their operation, defense against them and the mitigation of their impact
- Design and run a simulated live network consisting of VMs (Virtual Machines)
- Experiment and practice with DNS exploits and attacks with the help of the simulated network
- Analyze, evaluate and compare each exploit with regards to multiple factors
- Write either an original implementation of a DNS exploit or a DNS exploitation "toolkit"/wrapper program (Optional)

5 Expected outcomes and deliverables

The expected outcomes and deliverables of the project are the following. It is important to note that the level of output with regards to each deliverable may vary, depending on subsequent time constraints, or the lack thereof:

- A thorough research of DNS exploits, including information such as frequency, complexity, and effectiveness
- An implementation of a simulated, live network with the help of virtualization software and VM instances
- A practical presentation and application of the exploits, with the help of the previously mentioned live network
- An overview of the latest tools used for exploitation as well as defense and impact mitigation with regards to each attack
- An analysis, evaluation and comparison of each exploit, taking into account multiple factors
- A practical demonstration, as well as evaluation of methods of defending against each DNS attack
- (Optional) Either an originally written C implementation of an exploit, or a more basic “toolkit”/wrapper of various, already-existing DNS exploit programs

The following chapter deals with the research methodologies chosen with regards to the current project.

6 Research Methods

6.1 Research Types

The types of research to be undertaken for this project are as follows:

Descriptive – A part of the research will be of the descriptive type, as it will describe DNS and DNS exploits.

Explanatory – Next, some research will also be of the explanatory type, as it will involve the explanation of how DNS operates, as well as how DNS exploits work in practice.

Secondary – Furthermore, most of the research will be of a secondary level, as it will involve the extraction of knowledge with regards to already-documented exploits, as well as knowledge taken from current literature on DNS operation.

Primary – Finally, there will also be some primary level research, as it involves the extraction and presentation of information found from new/recent resources found outside of the traditional area of existing literature and research papers. Furthermore, it could involve research on entirely new, undocumented exploits and/or new defense strategies and software.

6.2 Philosophy

The philosophies chosen to be applied for this project are as follows:

Positivist – As positivism entails the “observation of real phenomena in an objective and real world”, the project will make use of the positivist philosophy, as it will involve the extraction and observation of specific, quantitative data (for example, packets found in network traffic).

Additionally, it will involve the performing of experiments, as well as the process of dealing with specific data, as the project will involve the practice and experimentation of DNS exploits with the help of a simulated network, as well as analysis and evaluation of the subsequent resulting data of the experiments.

Finally, the outcomes of the experiments present some level of reliability and validity, as the results of the experiments could be any time reproduced, under the condition that the experiments are run under the same technical circumstances. However, it can be argued that some of the outcomes of the experiment/s could be to some extent generalizable and encompass other circumstances, due to the broad and technical nature of cyber-security and computer network attacks.

Phenomenological – On the other hand, the project will also make use of the phenomenological philosophy, as it will attempt to collect, evaluate and present subjective and qualitative data, such as the frequency and effectiveness of DNS exploits.

Furthermore, the project will attempt to “generalize from one setting to another”; for example, it will attempt to conclude whether or not one or more exploits will function on specific platforms under specific circumstances etc.

Finally, the phenomenological part of the research presents a high level of validity and some level of reliability, as the more generalized conclusions will be valid with regards to a large number of computer networks. However, it can be argued that some of the validity and reliability may get lower over time, due to the rapidly-changing nature of the Information Technology and network security fields.

6.3 Approaches

The approaches chosen with regards to the project are as follows:

Inductive – Most of the approach for the project will be of an inductive nature, as it aims to develop a description of the “how” with regards to DNS operation, exploitation, and attack mitigation.

Deductive – On the other hand, a part of the project will also use the deductive approach, as it will hypothesize that DNS attacks are highly dangerous and effective within the current day and time.

6.4 Strategies

The strategies to be undertaken for this project are as follows:

Experiment – A part of the project will involve the experimental process, whereby a simulated live network will be created with the help of virtualization software and VMs (Virtual Machines). As such, the live network will function as the “test platform” onto which practice of DNS exploits, as well as DNS exploit mitigation, will be the main processes.

Document review – Next, the “document review” strategy will also be undertaken, which comprises of literature-based research on DNS operation, design and functionality, as well as DNS exploit operation and mitigation.

Software development (Optional) – Finally, depending on time-constraints, an attempt will be made of writing an original exploit implementation in the C language. Alternatively, a “wrapper” program will be created with the scope of grouping multiple, preexisting exploit programs into a single “DNS exploitation toolkit”.

6.5 Data collection

Finally, the following data will be collected using the following methods:

Packets – Packet activity will be collected using a packet capture program such as “wireshark”, “tshark” or “tcpdump”.

Screen – A video recording, consisting of the practical application and/or mitigation of the exploit/s, will be provided with the help of the “recordmy-desktop” program, or other similar screen-recording programs.

Logs – Finally, relevant data, such as server logs and/or computer network traffic, will be extracted and placed into the report whenever necessary.

The following chapter deals with the chosen development methods for this project.

7 Development Methods

7.1 Experiment

The principal development method is that of the experiment. The experiment consists of the following steps:

Live Network – The principal “test bed” for the experiment is the simulation of a real, live network. This network will consist of multiple nodes, each of which is represented by a VM (Virtual Machine).

The structure of the network and of what nodes it will consist will depend on each of the exploit’s network prerequisites. As such, it is expected that, at a minimum level, the nodes could represent:

- Root DNS server

- TLD DNS server
- SLD DNS server
- Recursive DNS client
- etc.

Experiment – Following this, the practical experimentation proper with DNS exploits will take place. As such, the exploits presented in the subsequent literature review will be put to practice in the simulated network if possible.

Record, Log – Finally, the exploitation process will be recorded, as well as its results extracted, with the scope of analysis and evaluation.

7.2 Software development

An attempt will be made to develop an original program, if lack of time constraints permits this objective. It would consist of either:

An original implementation of a DNS exploit made in the C language, or

A wrapper for multiple preexisting DNS exploit tools made in “Bash”, whose function would be of a simple and convenient “toolkit” for DNS exploitation.

7.3 Risks and limitations

During engagement with the project, there is a significant chance for one to run into the following risks and/or limitations:

- Lack of or difficulty finding resources necessary for the project;
- Time constraints which hamper the project’s level of quality;
- Difficulty in either the understanding of or the practice of DNS exploits;
- Difficulty or time constraints with regards to the implementation of the optional objective (the writing of an original C or Bash program).

As such, if one runs into these risks, one or more of the following steps will be undertaken with the scope of minimizing the risk of an only partial completion of the project:

- The abandonment of the C/Bash objective
- The reduction of the number of researched exploits
- The reduction of depth in exploit research

7.4 Data collection and evaluation

As research and practical experimentation will be undertaken with regards to each exploit, the data presentation format which take results into will be of the following form; the following format is not conclusive and may take a different form during the development of the project:

Attack name – Name of the attack

Tools used – Tools used for the attack

Demonstration video – A video recording whose purpose is to show the attack process in real-time

Explanation – An explanation of how the attack works

Results – The result/s of the attack

Observations – Other observations

Mitigation – How to mitigate the attack

Evaluation – Evaluation of the attack, which will comprise of a subjective rating (0 to 10 each) and discussion of the following factors:

Complexity – The level of complexity of the attack, taking into account both the likelihood of its success as well as the level of knowledge required with regards to successful implementation of the attack

Impact – The attack’s level of impact

Stealth level/Risk – The level of risk involved when deciding to use this particular attack towards the scope of malicious use

Ease of Mitigation/defense – The level of difficulty involved in mitigating the risk and impact of this exploit

The next and final chapter deals with the resources and planning of the project.

8 Resources and Planning

8.1 Resources required

The resources required for this project are the following:

- An internet connection for acquiring the necessary resources
- An operating system, or Linux distribution, with the necessary tools and setup for both simulating a network (using virtualization software) and DNS exploitation/analysis (for example, Kali Linux)
- Virtualization software such as “qemu” or “virt-manager”, whose scope is to help towards the creation of a simulated network using VM instances
- Knowledge of, and access to, online resources which function as repositories of cyber-security knowledge

8.2 Gantt chart

The Gantt chart, whose scope is to detail the proposed time-frame with regards to work on the project, is presented below:

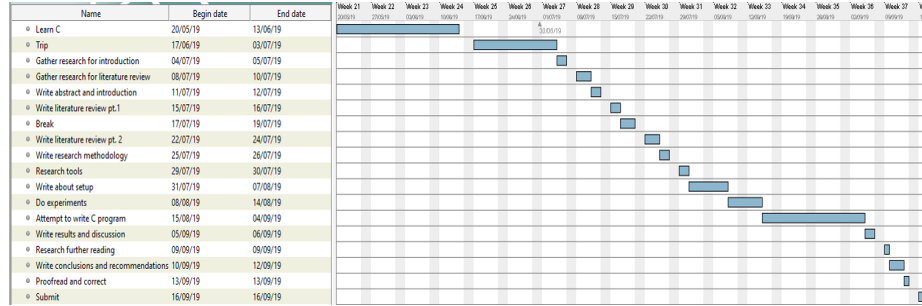


Figure 3: Gantt chart

It should be noted that the time-frame is of an estimative/inconclusive nature, and as such may not be rigidly followed or accurate, as was previously mentioned in the “Risks and Limitations” sub-section.

References

- [1] R. Aitchison, *Pro DNS and BIND 10*, 1st ed. Apress, 2011.
- [2] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, “Detection and prevention of dns spoofing attacks,” in *2017 Siberian Symposium on Data Science and Engineering (SSDSE)*. IEEE, 2017, pp. 84–87.
- [3] S. Ziegler, *Internet of Things Security and Data Protection*, ser. Internet of things. Springer Nature, 2019.
- [4] S. S. Ammar Rayes, *Internet of Things From Hype to Reality: The Road to Digitization*, 2nd ed. Springer International Publishing, 2019.
- [5] A. A. Waleed Ejaz, *Internet of Things for Smart Cities: Technologies, Big Data and Security*, 1st ed., ser. SpringerBriefs in Electrical and Computer Engineering. Springer International Publishing, 2019.
- [6] C. Dotson, *Practical Cloud Security*. O’Reilly Media, Inc., March 2019.
- [7] M. J. Carey, *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World*. Threatcare Press, 2019.
- [8] J. Warfare, *Journal of Law & Cyber Warfare Vol. 4:3 Winter 2015*. Lulu.com, 2016.
- [9] A. Misra and A. Dubey, *Android Security: Attacks and Defenses*, ser. An Auerbach book. CRC Press, 2016.
- [10] P. Kathryn A. Blair, *Advanced Practice Nursing Roles, Sixth Edition: Core Concepts for Professional Development*. Springer Publishing Company, 2018.
- [11] “Sharp rise in costs and damage from dns-related attacks.” *Network Security*, vol. 2018, no. 6, pp. 1–3, June 2018.
- [12] C. Marrison, “Understanding the threats to dns and how to secure it,” *Network Security*, vol. 2015, no. 10, pp. 8–10, 2015.
- [13] D. Winder, “So what should you be doing to mitigate the iot botnet threat? start with a network aud it,” *PC Pro*, no. 288, pp. 118–120, 2018.
- [14] D. Chiba, M. Akiyama, T. Yagi, K. Hato, T. Mori, and S. Goto, “Domainchroma: Building actionable threat intelligence from malicious domain names,” *Computers Security*, vol. 77, pp. 138–161, 2018.
- [15] S. Mohan, M. Asplund, G. Bloom, A.-R. Sadeghi, A. Ibrahim, N. Salajageh, P. Griffioen, and B. Sinopoli, “The future of iot security: Special session,” in *Proceedings of the International Conference on Embedded Software*, ser. EMSOFT ’18. Piscataway, NJ, USA: IEEE Press, 2018, pp. 16:1–16:7.
- [16] J. Margolis, T. T. Oh, S. Jadhav, J. P. Jeong, Y. H. Kim, and J. N. Kim, “Analysis and impact of iot malware,” in *Proceedings of the 18th Annual Conference on Information Technology Education*, ser. SIGITE ’17. New York, NY, USA: ACM, 2017, pp. 187–187.

- [17] R. Winward, *IoT Attack Handbook: A Field Guide to Understanding IoT Attacks from the Mirai Botnet to Its Modern Variants*. Radware, 2018.
- [18] N. Woolf, “Ddos attack that disrupted internet was largest of its kind in history, experts say,” *The Guardian*, vol. 26, 2016.
- [19] A. Liska and G. Stowe, *DNS Security: Defending the Domain Name System*. Elsevier Science, 2016.
- [20] M. D. T. Rooney, *DNS security management*, ser. Series on networks and services management. John Wiley and Sons; IEEE Press, 2017.
- [21] M. Jeftovic, *Managing Mission - Critical Domains and DNS: Demystifying nameservers, DNS, and domain names*. Packt Publishing, 2018.
- [22] M. Meyers, *CompTIA Network+ Certification All-in-One Exam Guide, Seventh Edition (Exam N10-007)*. McGraw-Hill Education, 2018.
- [23] P. Anu and S. Vimala, “A survey on sniffing attacks on computer networks,” in *2017 International Conference on Intelligent Computing and Control (I2C2)*. IEEE, 2017, pp. 1–5.
- [24] J. Cao, M. Ma, X. Wang, and H. Liu, “A selective re-query case sensitive encoding scheme against dns cache poisoning attacks,” *Wireless Personal Communications*, vol. 94, no. 3, pp. 1263–1279, 2017.
- [25] Z. Wang, S. Yu, and S. Rose, “An on-demand defense scheme against dns cache poisoning attacks,” in *International Conference on Security and Privacy in Communication Systems*. Springer, 2017, pp. 793–807.
- [26] M. Korczyński, M. Król, and M. van Eeten, “Zone poisoning: The how and where of non-secure dns dynamic updates,” in *Proceedings of the 2016 Internet Measurement Conference*. ACM, 2016, pp. 271–278.
- [27] T. Vissers, T. Barron, T. Van Goethem, W. Joosen, and N. Nikiforakis, “The wolf of name street: Hijacking domains through their nameservers,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 957–970.
- [28] Z. Wang, “An elastic and resiliency defense against ddos attacks on the critical dns authoritative infrastructure,” *Journal of Computer and System Sciences*, vol. 99, pp. 1–26, 2019.
- [29] B. Braun, “Investigating dns hijacking through high frequency measurements,” Ph.D. dissertation, UC San Diego, 2016.
- [30] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, “Dns amplification attack revisited,” *Computers & Security*, vol. 39, pp. 475–485, 2013.
- [31] D. C. MacFarland, C. A. Shue, and A. J. Kalafut, “The best bang for the byte: Characterizing the potential of dns amplification attacks,” *Computer Networks*, vol. 116, pp. 12–21, 2017.

- [32] A. Nadler, A. Aminov, and A. Shabtai, “Detection of malicious and low throughput data exfiltration over the dns protocol,” *Computers & Security*, vol. 80, pp. 36–53, 2019.
- [33] Z. Wang, “Combating malicious dns tunnel,” *arXiv preprint arXiv:1605.01401*, 2016.
- [34] D. Tatang, F. Quinkert, N. Dolecki, and T. Holz, “A study of newly observed hostnames and dns tunneling in the wild,” *arXiv preprint arXiv:1902.08454*, 2019.