Journal of Advances in Computing, Communications and Information Technology (JACCIT)

Journal homepage: www.sciengtexopen.org/index.php/jaccit

A Bit of Hacking Techniques for Vulnerable Subdomain

Maxwell Scale Uwadia Osagie *, Amenze Joy Osagie

Department of Physical Sciences, Faculty of Science, Benson Idahosa University, P.M.B 1100, GRA, Benin City, Edo State, Nigeria.

ARTICLE INFO

Article history:

Received 11 October 2020

Received in revised form
28 October 2020

Accepted 24 December 2020

Available online
25 April 2021

Keywords:

Application
Data
Domain
Hacking
Networks
Vulnerability

ABSTRACT

Hacking as it is popularly called is an official phrase for unauthorised access to a network/data. However, there are different methods used in gaining access to a designated network; hence, this paper explained a few hacker's intent using classified commercially available tools and techniques to expose the vulnerability of data and applications within networks. It also explained few simple ways of gaining access to a network without really having the key technical ability.

1. Introduction

Internet has become a world on its own, hence, offers several opportunities to end users [1]. As it is with human, the challenges associated with the security of lives and properties can be seen as the same with the internet world as revealed from the analysis [2], which bothers on the difficulty associated with the identification of real from fake end users. While some network providers pay serious attention to the security apparatus of the network infrastructures, others pay little or no attention and this is often seen from the ravaging effect of different threats that have affected the networking environment over the years [3]. Internet standardisation ensures information confidentiality and data integrity for every internet user [4]-[5]. Hacking a system or network can be interesting and fun catching but most importantly, it is the desire to try new thing that seems invisible and trying new things like new hacking techniques could be abstract to those without the desire to gather and analyse data [6].

Internet is a platform that allows different networks share similar or dissimilar resources. Thus, results as the bridging hub of all networks scattered worldwide. Networks of different kinds have different configurations with its operational scope based on the fundamental principle of the intended user [7]. The internal mechanism of the design structure of a network is usually not for public consumption and this is because there are inherent attributes of the security apparatus that prevent it from been hacked or accessed by unauthorised user [8]. Notwithstanding, as internet provides access to network of different kinds through authentication it also provides several opportunities to accessing network without following the structural rules of the security architecture [8]. Practical studies have shown serious vulnerability of some network infrastructures and the unwillingness on the part of the affected

* Corresponding author
E-mail address: msuosagie@gmail.com
https://doi.org/10.37121/jaccit.v1.133

networks to disclose these information(s) gave rise to thousands of illicit acts within and outside the cyberspace (network). The gravity of crime committed within a network is unquantifiable because there are no accurate measuring tools for determining the level of crime committed within network space. Crime such as Identity Theft, Tax-Refund Fraud, Cooperate Account Takeover, Sensitive Data Theft, Intellectual Property Theft, Username and Password Hijacking, Network Terrorism and Bio-Computing Missile have in one way or the other created serious setbacks to the safety operation of a network. Many of these crimes committed are linked/associated to software tools with high proficiency in network navigation [9]-[10]. Base on this premise, the study unveiled the underlying operation of some hacking tools and proffer a scientific recommendation to end users and network operators on how to avoid them [9]-[10].

2. Related Work

A lot of researches have been carried out on network security with the aim of unravelling the threat as well as safeguarding the network. In the work conducted by [11], explained that industries now utilise enterprise-wide and virtual private network (VPN) in bridging their systems across network. Organisations have left the traditional method of bridging network to more sophisticated approach aimed at preventing the hacker's business. Researches have showed that hackers innovate tools to gain access into networks [11]-[12]. [6] considered security as a complicated subject and it is only understood by a well-trained expert. Indeed, the act of securing system is far beyond simple approach and to understand how it works, proper understanding must be given to the system operational modules. [12] pointed out virtualised computing environment, which offers improved technology to the method of computing environment. However, it was opined from the research that one of the major obstacles to the widespread utilisation of virtualised technology was the issue of security. [13] captured five top cybercrimes and explained that the crime is part of the measure taken by AICPA in addressing cybercrime related issues. This was further buttress in a paper published by [14] on five top cyber fraud, they emphasised that the last three decades have witnessed frequent, and wide spread sophisticated attack against the personal information, social information and financial information. [15] unveiled a network threat called botnet. The threat had in recent times been seen as one of the most dangerous attacks on the network and has an exponential growth of about 170,000 within network server and client infrastructures per day. [16] exposed how hacking are carried out using three essential steps of which one of them is "foot printing". [17] analysed computer security to be a crossroad owning to the fact that its security architecture is failing regularly due to increase in attack. The researchers postulated that security issue is far beyond architectural solution rather a business problem and must be solved through policy adjustment. [18] pointed out that cybercrime and its laws for combating crimes are inversely proportional. This was established by an extensive survey conducted to ascertain the relevant laws for cyber-security. Also, recommendations to incorporate technical measures, cyber related legislation and Institutional measures into cyber security policies to compliment government's effort in securing, protecting the underlying Information and Communication Technology (ICT) infrastructures and boost Internet consumers' confidence.

3. Foot Printing Approach

The first approach to becoming a hacker or learning how to hack a system is foot printing. Foot printing is a systematic approach that allows the synchronisation of information required for hacking. In computing, it involves gathering relevant information concerning a network environment (network types). The hackers study the network architecture and other associated information(s) within and outside the environment and Just like any other systems, Computer network is also bounded by some drawbacks, these drawbacks in-turn becomes the vulnerability of the network, which the hacker unravels to intrude the network.

No hacker can gain access to network without proper guide or information. Some of the steps involve finding out location and reason for doing so. When accomplished, further steps are taken to finding critical information about the organisation. Usually, this is carried out through the traditional method of data gathering that could aid understanding. For instance, several organisations have information centre (a kind of repository/directory) of staff members. This information could be their emails, date of birth, state of origin etc., and a little query will show clearly the sub-domain names and domain of such network. Once this is done, a further look is achieved by knowing

the architectural dynamics, Operating System (OS) used, protocols involved and other relevant network information(s) such as the kernel of the OS. When the network type is known different approaches are used. For example, if the infrastructure is internet, things to identify are Internet Protocol (IP) address of the system used, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), the system structure, domain name (example: jek.com) Access Control Lists (ACLs), Intrusion Detection Mechanism System (IDMS) etc. In the case of intranet, network protocol such as IP address, Internetwork Packet Exchange (IPX) and Digital Equipment Corporation Network (DecNET) are identified along with the aforementioned in the internet technology. For remote access, Virtual Private Network (VPN), Internet Protocol Security (IPSEC), Point-to-Point Tunnelling Protocol (PPTP), Phone number, defensive mechanism system type, etc are identified. The extranet is a bit less complex because attentions are geared towards the receiving and sending end, access control type as well as the connection style [16].

4. Website Mirror

One of the biggest challenges that organisation face is their lack of knowledge to erroneously leave some tracks that aid hackers in achieving their target. Some websites have their security architecture/configuration and other information such as emails, phone numbers, names, security guidelines etc on their server. This act prompts a way forward for hacker. The hacker mirrors the website to give room for further exploit offline. Mirroring a web site is the act of using technological tool to download the entire site and the information to a local directory. Tool such as HTTrack, Teleport Pro, Portable offline Browser, Website Ripper copier, Pagenest, Blackwidow, backstreet Browser, Wget.html for UNIX are all used to mirror entire websites. One of the techniques aside the aforementioned tools used by hackers are useful information(s) about the targeted organization or staff. So, using open-source search engine give added advantage to hackers in finding information that may have been published on the websites over the years. Information such as the organisation allies can be the path way for further exploitation. There are websites that provide handful information about different organisations past experiences. Examples are finance.yahoo.com, companysleuth.com, nigerianstat.gov.ng etc. Furthermore, there are other advanced search engines such as Google hacking for engine queries and add to hacker's information on mirroring a website as shown in Table 1.

Table 1 Advanced Search Engine.

http://sites.google.com/site/gwebsearcheducitation//advanced-operator
. If "advance operator" is to be search for on ben.com website the construct will be: http://www.google.com/search? hi= en&1r=&ie=UTF-8&oe=UTF=8&q=intext: "advanced operators" site:ben.com For security related, search such as this can be constructed: http://www.google.com/search? hi= en&1r=&ie=UTF-8&oe=UTF=8&q=intext: "enable secret 5$"

Table 1 is a classic example of a configured file on Cisco device with encrypted and decrypted administrative password searched. Other information that will be available when Table 1 is activated is the IP address to which the configuration resides. FerrePRO suite which is a tool from FerretSoft (http://www.ferretsoft.com) also provides additional clue to searching for information from various search engines.

The website is a useful tool for accomplishing certain task of information gathering. The www.dogpile.com has some available search for multiple engines search [16]. Search Engine provides endless access to data on website. Search engine such as Alta Vista, hotbot, Excite, Ask Jeeves, google, Northern, Search Adobe PDF online, dogpile, profusion, SearchBug, yahoo, etc are designed to fetch information from website.

5. Finding Sub-Domain

Naturally, no organisation wants to be associated with the unclean nature of sub-root domain because it tries to ensure that the root domain is secured but developer usually create sub domain for so many reasons, one of the reasons is to test some features of the website independently with aim of implementing feature in the parent domain on later date. On a real note, the sub-domain contributes nothing to the website, hence are usually not part of the agreement reached before the development and at such most website owners are not aware of these embedded sub-roots within the website. Other reasons developers create sub-domains which is unknown to the client could be to keep untested features within the website. It is expected that sub-domain designed by developers is hidden from end users. Example: *http://www.Winpiesite.com* could be designed as the parent domain (root domain) but there could *be http://www.tag.Winpiesite.com* as the sub-domain name and when the firewall of the parent domain (root domain) is weak, it gives better chance for hackers to gain access through the subdomain. Finding subdomain in a website has become fun owing to different automated tool for exploiting them. It goes beyond just typing the root domain on searching tool. To be specific, for the desired target, the type of registrar of the domain name must be verified for accurate search. There are lists of registrars that go along with domain names. They are .com, .org, .edu, .ng, .net. Some sites like *(http://www.internic.net)* also provide useful information on all accredited registrar.

5.1. Subdomain Enumeration Tools

Rather than manually search for subdomain and other vulnerability within network infrastructure, there are handful tools that provides reliable search for finding subdomain as well as other vulnerabilities associated with the root domain but for the purpose of this research two will be discussed.

(a) *Pentest-tools*: Pentest-tools are automated applications that developers use to test the website vulnerability. The Pentest-tools does this by passively scanning the website in order to see vulnerability issue such as server software that is seen to be outdated, Hyper Text Transfer Protocol (HTTP) headers that are vulnerable as well as subdomain names. Fig. 1 shows the front end of the tool with three key features (Website scan module, Network and attack surface) for execution.

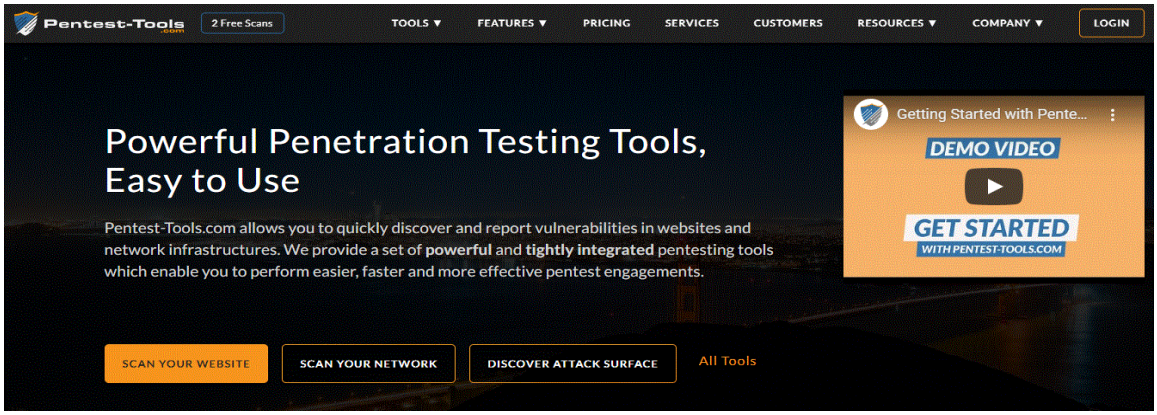

Fig. 1 Pentest-tools.

(b) *Censys.io*: As shown in Fig. 2, Censys.io is one of the recent search engines that allow hackers to investigate and analyse network infrastructure. Its approach is quite unique because it returns the configuration details of the devices, website or certificate.

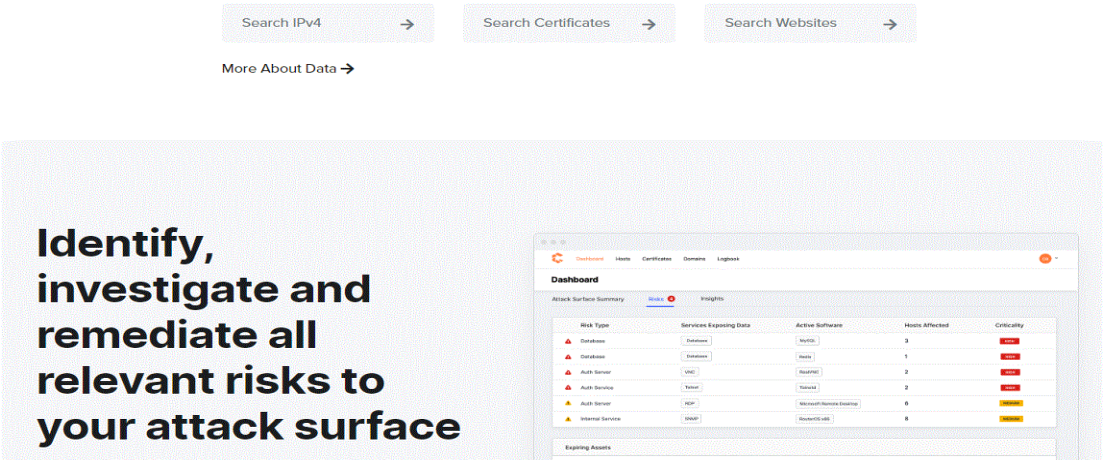

Fig. 2 Censys.io tool.

5.2. Domain Name System Server (DNS)

One key factor to understanding what the targeted network might look like is to know how to query the DNS for available information. Mapping a server helps to show some hidden features that would naturally not be available at the front end of the network. DNS is a server database known to be distributed and also assigns or maps internet protocol (IP) address to hostname. Many host companies pay little attention to the configuration of their DNS thereby resulting to zone transfer by third party or network malicious user. Zone transfer allows a secondary master server to update its zone database from the primary master [16]. A poorly configured DNS would automatically provide internal information about the organisation during zone transfer.

6. Mapping A Connected System

Vulnerability Mapping is a classical mapping operation of the security features of a system [19]. It involves breaking down the network associated attributes within a given system thereby exposing the systems drawbacks. This aspect is seen as the main function of system vulnerability exploration. Several literatures such as [12],[16]-[20] have exposed the actual act of this phase in system vulnerability. Its role is critical for further understanding of the functionalities and its connected devices/apparatus. Mapping elaborates the operational mode of the following attributes:

(a) Number of running servers and versions (it could be any version of Apache such as 1.3.9 for HTTP and 8.9.10 for Small Mail Transport Protocol (SMTP))
(b) The various services running via Hypertext Transfer Protocol (HTTP)
(c) The dynamic structure of the system (i.e., the technology used which could be ASP.Net etc.).
(d) User's information which could form a major path to more exploitations.

7. Method of Malicious Operation

There are really no specific method hackers used in gaining access to a systems network. They can employ different strategies to a single network or different network. Hence, there is need for constant updating of the requisite knowledge for the current techniques used in preventing and preserving network fraud or attack. It is quite difficult to compare operational method of hackers' techniques. However, the following are different methods used:

Physical mapping: this aspect involves mapping some attributed features of a specific system that is connected within a dynamic network infrastructure to source for vulnerabilities. Some classified Mapping operation includes Bugtraq, vendor security alert, computer emergency advisories (www.cert.org) and Seclists.org.

Another method employed by hackers is the use of *market available code* for unveiling vulnerable network. These codes are usually found within various security mailing lists as well as some websites. Some good hackers who are knowledgeable in programming developed codes for mapping systems network but this can only be done when the hacker is above ninety percent sure of a possible vulnerability within a given system. Various scanning tools that are commercially available allow hackers to scan for vulnerable systems within a network infrastructure.

tools shown in Figs. 1 and 2 as well as others such as www.iss.net, CyberCop Scanner from www.nai.com, Nessus (www.nessus.org) and SAINT (www.wwdsi.com/saint/) are dynamic tools that have shown positive results in network navigation [19]-[20]. Just like a real-life scenario, these tools as explained above have some positive and negative attributes but in a simple approach, focus should be geared towards fetching the required result from the key area rather than mapping the entire system infrastructure. Key focus should be:

(a) Holistic network survey/investigation on the expected system
(b) Mapping should focus on certain attributes such as the System structure, OS, and services
(c) Mapping to gain access for the identification of specific systems
(d) Prioritised potential access point

8. Conclusion and Recommendations

Network and other internet infrastructures have helped in the enhancement of knowledge in the 21st century and in-turn increased the economy fortune of both developed and developing countries. The network infrastructures designed to be human friendly have transformed the ways and manners knowledge are shared and used. The anxiety within network is as a result of the divergent views of end users. Today, several crimes occur on cyber-space thereby making it unreceptive for some users. It is understood that crime is dynamic, however, the criminals are also vulnerable unknowingly but this is sole dependent on the computer user. From the study review such as [15] the criminal's systems could as well be vulnerable. So, they are not totally protected. Every system within the internet has a unique identity and this identity is regarded as the "gateway" to which those with the technical ability can take advantage of. Crime within system's network is not novel but the approaches used by criminals have changed overtime. As the technological industries' quest for sophisticated infrastructures increases crime within network space would follow the same trend and as a result, different unauthorised tools used in gaining access to network will continue to emerge in the open market. To discourage or mitigate hacker's threat within network infrastructure strategy such as research into how the business of hackers is carried out should be encouraged and funded by relevant stakeholders. The unveiling of hacker's business and threats should not stop at research level; further strategies such as disseminating research findings to network users should also be encouraged and done periodically. Articles such as this should be given the need awareness as well as training and retraining of network infrastructure stakeholders. Strategy such as expository programmes designed especially for cyberspace security awareness in local broadcasting stations is considered a necessity in this regard. It should be a matter of policy for educational institutions to educate students on how cybercrime can be mitigated within network infrastructures. Predicting the operational outcome of students within network infrastructures could be difficult. However, the gain of such training should be the focus. This work, aside showing the tools and some of the steps required to hacking network infrastructures, it also explained how end users can practice the work of a hacker so as to mitigate its effect. [18] explained that there are no clear-cut policies and laws that compared cyber criminals. Hence, the knowledge of hacker's exploits within network infrastructures will go a long way in reducing the activities of network criminals. [21] created an approach that detect threats within network and also prevent unauthorised outbound traffic within network infrastructures. In this case, further input that can trace and probably denial the intruder access would be a welcome development.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

ORCID

M. S. U. Osagie https://orcid.org/0000-0002-0307-7025

References

[1] M. S. U. Osagie, K. O. Obahiagbon, and O. J. Amenze, "5PEN Technology: A new dawn in homogeneous and heterogeneous computing," arXiv preprint, 2018; arXiv:1804.10651

[2] M. S. U. Osagie & A. J. Osagie, "Internet penetration forecast and threats mitigation for Nigeria," *Benin Journal of Advances in Computer Science*, vol. 4. no. 1, pp. 20-29, 2019.

[3] M. S. U. Osagie, O. Enagbonma, & A. I. Inyang, "The historical perspective of botnet tools," 2019, *arXiv preprint arXiv:1904.00948*.

[4] M. S. U. Osagie, O. Glory, O. B. Obehi, I. A. John, E. J. Osarenkhoe, A. A. Shirley, et al. "Tendency of ICT usage among adolescent in Oredo local government primary schools, Benin City, Edo State-Nigeria," *Asian Journal of Probability and Statistics*, vol. 5, no. 2, pp. 1-10, 2019.

[5] M. S. U. Osagie, K. O. Obahiagbon, A. I. Inyang, & J. A. Osagie, "Digitalized responsive logical interface application," 2018, *arXiv preprint arXiv:1805.05846*

[6] M. Curtin, *Introduction to Network Security*, LaTeX2HTML translator Version 97.1, Leeds, UK, 1997.

[7] M. S. U. Osagie, D. E. Ajayi, O. Okoye, E. O. Faith, E. Anwuli, E. Osian, et al. "The role of information and communication technology (ICT) in the academic performance of the University of Benin Post Graduate Students," *Asian Journal of Probability and Statistics*, vol. 5, no. 2, pp. 1-9, 2019.

[8] M. S. U. Osagie & A. J. Osagie, "The architectural dynamics of encapsulated botnet detection (EDM)," 2019, *arXiv preprint arXiv:1904.07145*

[9] M. Uma, & G. Padmavathi, "A survey on various cyber-attacks and their classification," *IJ Network Security*, vol. 15, no. 5, pp. 390-396, 2013.

[10] M. Jouini, L. B. A. Rabai, & A. B. Aissa, "Classification of security threats in information systems," *Procedia Computer Science*, vol. 32, pp. 489-496, 2014.

[11] J. R. Vacca, (Ed.) *Network and System Security*. Second Edition, Elsevier, USA, 2014.

[12] T. T. Brooks, C. Caicedo, & J. S. Park, "Security vulnerability analysis in virtualized computing environments," *International Journal of Intelligent Computing Research*, vol. 3, no. (1/2), pp. 277-291, 2012.

[13] T. Singleton, "The five top cybercrimes," American Institute of CPAs, Durhan, North Carolina, 2013.

[14] R. K. Goutam, & D. K. Verma, "Top five cyber frauds," *International Journal of Computer Applications*, vol. 119, no. 7, pp. 22-25, 2015.

[15] M. S. U. Osagie, C. I. Okoye, & A. J. Osagie, "Mitigating botnet attack using encapsulated detection mechanism (EDM)," 2018, *arXiv preprint arXiv:1806.06275*

[16] S. McClure, J. Scambray, & G. Kurtz, "Hacking exposed: network security secrets and solutions," Sixth Edition, Corel VENTURA™ Publisher, California, USA, 2009.

[17] B. Schneier, "Hacking the business climate for network security," *Computer*, vol. 37, no. 4, pp. 87-89, 2004.

[18] S. Konyeha, "Evaluating hacking and cyber-security issues in Nigeria," *Benin Journal of Advances in Computer Science*, vol. 4, no. 1, pp. 39-47, 2019.

[19] K. Coffey, R. Smith, L. Maglaras, & H. Janicke, "Vulnerability analysis of network scanning on SCADA systems," *Security and Communication Networks Journal*, vol. 2018, doi.org/10.1155/2018/3794603

[20] R. J. Barnett, & B. Irwin, "Towards a taxonomy of network scanning techniques," In *Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries: Riding the Wave of Technology*, pp. 1-7. October 2008, https://doi.org/10.1145/1456659.1456660

[21] B. Wippich, "Detecting and preventing unauthorized outbound traffic," White Paper, SANS Institute-Infosec Reading Room, Boston, USA, 2007.