Analysis of the Software Most Used by Hackers to Carry Out Penetration Testing in Public Organizations

Segundo Moisés Toapanta TOAPANTAa, Raúl Francisco Pérez GONZÁLEZa, Máximo Giovani Tandazo ESPINOZAb and Luis Enrique Mafla GALLEGOSb

aDepartment Computer Science, Salesian Polytechnic University of Ecuador (UPS), Chambers 227, Ecuador
bFaculty of Systems Engineering, National Polytechnic School (EPN), Ladrón the Guevara E11-253, Ecuador

Abstract. Currently, the software handled by hackers is the main one to tackle a series of empirical knowledge, with this software attacking and helping organizations. The main objective is to analyze and systematize the software that is detected by hackers and crackers, in order to prevent risks and study the tactical levels and strategies for a given process. The analytical method is used in this investigation, for the study or analysis of the offensive software structure in public organizations. The results obtained from this research were an attack launching algorithm, software prototype taken by hackers, massive obfuscation model, and quantitative encryption model. It was concluded that piracy tools are used for preventive prevention and systems aggression, that is, to be defensive or offensive for a period, throughout an attack cycle.

Keywords. hacker, hacking tools, hacking, malicious program, public organizations.

1. Introduction

Within the penetration processes towards organizations or establishments of each type are based on a consecutive row of manipulation techniques for each specific case, these courses have enlarged many organizations[1]. Organizations choose hackers to manipulate these events in neighboring establishments and thus begin a launch of competitions between organizations or companies, they are generally having a very high level of appointment, while hackers are the most benefited today for its great ability to manipulate technology[2]. Old penetration software has been very useful for attack situations, exploits in a more practical way for individuals who know about these techniques and their vulnerabilities[3]. The software may have poorly developed code, which will allow ineffective functionality within an attack process, it is recommended that a check be performed before starting or violating a system, this refers to the high vulnerability of mobile phones[4]. Tracking the signals by means of an attack between two distant nodes, it will be possible to carry out a respective analysis on the different

1Corresponding Author: Segundo Moisés Toapanta Toapanta, Department Computer Science, Salesian Polytechnic University of Ecuador (UPS), Chambers 227, Ecuador. Email: stoapanta@ups.edu.ec
types of software that come onto the market, due to automation and execution problems within a software, a large part of the structure will be found running on one level. low[5].

For the processes of a comparative evaluation to the tests that these software undergo, they have a lot to do with the hardware parts, as indicated by the strategies of the components retracted by the intangible processes of each stage in their permanence[6].

As a result of the above analysis, the following possible risks can be concluded within public organizations by each hacking software.

- Public institution provides access control at occupational levels.
- The security that is equated is extremely low, giving continuity to an incidence management.
- Physical preparation is mitigated by risk management presented in processes and activities of public services.

Why is it necessary to analyze penetration software in public organizations?

It is necessary to analyze the software, because there is a high risk of violation creating malicious functions that will reproduce and stagnate within a system.

The main objective is to analyze and systematize the software that is obtained by hackers and crackers, in order to prevent risks and study the tactical levels and strategies for a certain process.

The reviewed articles are: PsyBoG: A scalable botnet detection method for large-scale DNS traffic[1], An application of linear algebra theory in networked control systems: Stochastic cyber-attacks detection approach[2], Structural analysis of packing schemes for extracting hidden codes in mobile malware[3], An Empirical Evaluation of the Effectiveness of Attack Graphs and Fault Trees in Cyber-Attack Perception[4], Reinforcement learning for efficient network penetration testing[5], Hybrid detection of intermittent cyber-attacks in networked power systems[6], Effect of anti-malware software on infectious nodes in cloud environment[7], An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador[8], A Malicious Web Site Identification Technique Using Web Structure Clustering[9], Andro-Dumpsys: Anti-malware system based on the similarity of malware creator and malware centric information[10], Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions[11], Smart Contract: Attacks and Protections[12], Security Verification via Automatic Hardware-Aware Exploit Synthesis: The CheckMate Approach[13], Detection and elimination of spyware and ransomware by intercepting kernel-level system routines[14], A Comprehensive Overview of Government Hacking Worldwide[15], Definition of parameters to perform audit in cybersecurity for public one organization of ecuador[16], Creation of a DDOS attack using HTTP-GET Flood with the Cyber Kill Chain methodology[17].

The analytical method is used in this investigation, for the study or analysis of the offensive software structure in public organizations.

The results obtained from this research are disclosed in each structural phase that is developed with the hacking tools, these tools are expanded by each system that composes it.

It is concluded that the phases revealed with piracy software are part of a rigorous prevention and exploitation of computer processes in public organizations, as well as the security and management of a business structure.
2. Materials and Methods

The research resources and treatments are based on the scientific articles investigated, with a sequential aspect in their results.

2.1. Materials

It is considered a formal analysis taking into account the research references that are presented with the research material.

It was verified that for a meticulous penetration environment it is specified that, within the programming of the software, the implementation of a subsystem is necessary in order to integrate remote access within the social and strategic localities, such as public organizations[1]. Hackers evaluate their network before launching an attack, with the respective software they manipulate the functions of the public organization side, apart from quantitatively analyzing each and every risk within their own network, engineers continually determine the flaws of these software, starting from a structural analysis to give the appropriate answers to all the systems that surround the organization or institution[2]. Domain threats, it is required for most security within dynamic routes, improving the resistance of self-defense security is the most useful way for a static software course. Hackers run in parallel the critical analyzes your infrastructure needs when planning an assault on your public organization[3]. By performing different types of algorithms, it would help the software establish a design protocol for the analysis of vulnerabilities that have been run in the system, this helps not to decrease the development or progress that was established in the regulations[4]. The software and techniques that hackers have used in many public and private organizations. These have been very helpful for the security of the organization[5]. Indirect penetrations are observed indirectly, since their components are similar to the functions of attacks with defects to their launches[6]. It is analyzed that, with the technology and tools specified for a certain piracy purpose, it is advisable to study the receiving points[7]. Given that in a computer attack it is intentional and it is not possible to consider all the counter attack scenarios, as much as possible that the target is declaring a tracking attack in self-defense, as well as activating an alarming signal where it has defense support[8].

Social-engineer was used software with the participation of wireshark, an extended process of exploit launches occurs for full access of internal nodes through social engineering[9]. It should be recognized that the level of compatibility with the end user is unavoidable for this analysis, without this knowing what would happen within the source services in their environment[10]. The participation of tcp, http, udp and dns traffic is classified and detected, by identifying them within the network, producing better precision and the data transfer rate improving[11]. Using the Hoffman code, it will be possible to understand the valuation of the data received, if the strict way of the exact values of that information will be represented[12]. In itself, the use of software in a public organization is automated in its application profile since employees do not have the corresponding knowledge in coding[13]. The permanencies of the current states of the software operations are:

1. The probability of software decay with its encoding is low.
2. The standard that is set to the software has a length of responses the same as the arrival information.
3. Diagram the coding structure must be probable.
Also to the states, the servers and/or complete infrastructure of the public organization will be verified [14]. Sharing a remote connection to this destination, we proceed to investigate areas and check each point inside and outside the organization. [15]. A method that is very misleading for individuals with a lack of knowledge is analyzed when entering a website, which is classified as adware [16]. Therefore, this method is a considerable achievement for the general staff, the function of this method is to add badware while the person navigates and fulfills the needs that are within their reach [17].

2.2. Methods

In this study the analytical method was carried out, to make known the criteria that each software process analyzed by Institute for Security and Open Methodologies (ISECOM).

2.2.1. Manipulation of Hackers

To carry out the secret writing of a system or a file in general, one must focus on its encryption, developing an difficult function for the user in general, with this an initial space is made in the encoding of messages, where it requests the different characters for a secure structure within a system. In cryptographic systems the vast majority are made up of different settings, among them we have:

- Transmission of the encrypted message.
- Algorithms to decrypt the element.
- Data transmission rate combinations.

2.2.2. Systems with Gnu/Linux

Publicize this free system, which has allowed hackers to distribute distros in the development processes for each specific task, thus achieving the operation of generating different types of files, uniform to Table 1.

| Impact | Malicious Extensions |
|--------|----------------------|
| Low    | .exe                 |
| Low    | .pif                 |
| Half   | .com                 |
| Half   | .scr                 |
| Half   | .sys                 |
| Half   | .ovl                 |
| High   | .drv                 |
| High   | .bin                 |
| High   | .dll                 |
| High   | .bat                 |

Table 1. The impact of each file extension generated in the GNU/Linux system.
2.2.3. The Adware

Assimilating Table 2, the function for the structure of a malicious program is applied in the presence of browsing a website. This program can be hidden as a backdoor, without disclosing the structure to the end user.

| Level | Structure                  | Capacity |
|-------|----------------------------|----------|
| 1     | Directives                 | Very low |
| 2     | Main Features              | Low      |
| 3     | Coding                     | Low      |
| 4     | Instruction                | Half     |
| 5     | Organization Loops         | High     |
| 6     | Root Element               | Very High|
| 7     | Depuration                 | Critical |

Table 2. Ability level to denote the structure of a malicious program.

2.2.4. Using the Web Audit

To get vulnerabilities (XSS) complying with your command chain. On sites crossed with customer penetration on that website.

- Attack target vulnerable points of (DOM).
- Execution of the attacker script by the client.
- Theft of cookies.
- Inject (SCRIPTS JAVA, SCRIPTS CODE) into the website.

3. Results

Below are the phases acquired for the analysis of the software most used by hackers, these are:

- Attack Launch Algorithm.
- Prototype of Software taken by Hackers.
- Massive Obfuscation Model.
- Quantitative Encryption Model.

3.1. Attack Launch Algorithm

In the algorithm of Figure 1, the presence of attack launches to a given medium can be manifested, to intercept security rings and penetrate the secondary systems of public organizations and spread their coding in them.
3.2. **Software prototype taken by Hackers**

In this prototype the main computer security tools on the side of a hacker are enunciated, knowing the status of the Manual of the Open Method of Security Verification (OSSTMM) (Figure 2).

![Diagram of the algorithm for launching attacks on a secondary node.](image1)

**Figure 1:** Algorithm for launching attacks on a secondary node.

![Diagram of hacking tools.](image2)

**Figure 2:** Prototype of Software taken by hackers.
3.3. Massive Obfuscation Model

In this equation a data template is expressed, with which information can be hidden within a process without limits to the amount of creation, data and malicious information of the software, thus giving rise to the exploitation knowledge of the Method Penetration Test (ISSAF).

\[ x(C)r \approx \frac{x!}{(x-r)!r!} \in z...n \]  

(1)

**Where:** Desired number of data \((x)\), combinations of information taken from the data \((Cr)\).

3.4. Quantitative Encryption Model

In this quantitative encryption model, a process restart is performed for encrypted attacks, which occurs on an attack path between two nodes (primary, secondary).

\[ R_o \approx f(x_0) \in z_1 \rightarrow f(R_1)_2 \]  

(2)

**Where:** attack numbers \((R)\), Primary node \((f)\), Secondary node \((z)\), Denial processes.

4. Discussion

The triumphs achieved for this investigation are related to the means of software transmission through an attack zone, in such a way that they can obfuscate or carry out the respective assault launches, both to prevent and attack an organization and perform these acts on an impassive system[13].

The information in this research is not limited to learning actions or facts, generally based on computer attacks using cybersecurity software.

The results contracted by other authors and researchers in this research were pleased by techniques and tactics of software management and executions inside and outside public institutions or organizations.

It was concluded that any result obtained with piracy software can be attacked or prevented by an act of cybersecurity in a public organization.

5. Future work and conclusion

Given the bad information that is extracted by hackers, it is advisable to carry out an intense test on hacking software, it should be noted that the software can leave signs or can carry out searches in the primary software.

It is concluded that the dominated results are ways of preventing an unwanted act before an organization, placing yourself on the side of the individual who defends or mitigates the supernatural laws of technology.
6. Acknowledgments

The authors thank to Salesian Polytechnic University of Ecuador, to the research group of the Guayaquil Headquarters “Computing, Security and Information Technology for a Globalized World” (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior Ciencia, Technology e Innovation (Senescyt).

References

[1] Kwon J, Lee J, Lee H, Perrig A. PsyBoG: A scalable botnet detection method for large-scale DNS traffic. Comput. Networks, 2016, vol. 97, pp. 48–73.
[2] Li Y, Voos H, Darouach M, Hua C. An application of linear algebra theory in networked control systems: Stochastic cyber-attacks detection approach. IMA J. Math. Control Inf., 2016 33(4), 1081–1102.
[3] Liu J and Yi J H. Structural analysis of packing schemes for extracting hidden codes in mobile malware. EURASIP J. Wirel. Commun. Netw., 2016, 2016(1).
[4] Lallie H S, Debattista K, Bal J. An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception. IEEE Trans. Inf. Conf., Forensics Secur., 2018, 13(5): 1110–1122.
[5] Ghanem MC, Chen TM. Reinforcement learning for efficient network penetration testing. Proc 3rd Int. Conf., 2020, 11(1): 1–23.
[6] Kontouras E, Toes A, Dritsas L. Hybrid detection of intermittent cyber-attacks in networked power systems, Energies, 2019, 12(24): 1–29.
[7] Abazari F, Analoui M, Takabi H. Effect of anti-malware software on infectious nodes in cloud environment. 2016., Int. Conf. Comput. Secur., 58: 139–148.
[8] Moisés Toapanta Toapanta S, Enrique Mafla Gallegos L. An approach to optimize the management of information security in public organizations of Ecuador, CITS 2019-2019 Int. Conf. Comput Inf Telecomun, 2020.
[9] Nagai T, Kamizono M, Shiraishi Y, Member S. A malicious web site identification technique using web structure clustering. 9: 1665–1672, 2019.
[10] Jang JW, Kang H, Woo J, Mohaisen A, Kim HK. Andro-Dumpsys: Anti-malware system based on the similarity of malware creator and malware centric information, 2015 Int. Conf. Comput. Secur., 58: 125–138, 2016.
[11] Aldawood H, Skinner G. Analysis and findings of social engineering industry experts explorative interviews: perspectives on measures, tools, and solutions. IEEE Access, 2020, 8: 67321–67329.
[12] Sayeed S, Marco-Gisbert H, Caira T. Smart contract: attacks and protections. IEEE Access, 2020, 8: 24416–24427.
[13] Trippel C, Lustig D, Martonosi M. Security verification via automatic hardware-aware exploit synthesis: the checkmate approach. IEEE Micro, 2019, 39(3): 84–93.
[14] Javaheiri D, Hosseinzadeh M, Rahmani AM. Detection and elimination of spyware and ransomware by intercepting kernel-level system routines. IEEE Access, 2018, 6: 78321–78332.
[15] Li CY, Huang CC, Lai F, Lee SL, and Wu J. A comprehensive overview of government hacking worldwide. IEEE Access, Int. Conf. 2018, 6:55053–55073.
[16] Toapanta SMT, Peralta NA, Gallegos LEM. Definition of parameters to perform audit in cybersecurity for public one organization of ecuador, ACM Int. Conf. Proceeding Ser., no. 2019, pp. 91–96.
[17] Martínez-Lozano JE, Atencio-Oitziz PS. Creation of a DDOS attack using HTTP-GET Flood with the Cyber Kill Chain methodology, Iteckne, Int. Conf. 2019, 16(1): 41–47.