Article **Journal Computer Technology**
June 2023, Vol.7 No.18 32-39

Importance of the analysis of computer attacks on a LAN network applying the predictive-quantitative method

Importancia del análisis de los ataques informáticos sobre una red LAN aplicando el método predictivo-cuantitativo

SAUCEDO-LEÓN, Daniel†, SAMPAYO-RODRÍGUEZ, Carmen Jeannette*, GONZÁLEZ-AMBRIZ, Rosalba and MORALES-OLIVARES, Rosibel

Tecnológico Nacional de México, Instituto Tecnológico Superior de Huauchinango, Ingeniería en Sistemas Computacionales, México.

ID 1st Author: *Daniel, Saucedo-León* / **ORC ID:** 0000-0003-2302-7233, **CVU CONAHCYT ID:** 1264052

ID 1st Co-author: *Carmen Jeannette, Sampayo-Rodriguez* / **ORC ID:** 0000-0001-8844-6055, **CVU CONAHCYT ID:** 951529

ID 2nd Co-author: *Rosalba, González-Ambriz* / **ORC ID:** 0000-0001-5400-9754, **CVU CONAHCYT ID:** 368433

ID 3rd Co-author: *Rosibel, Morales-Olivares* / **ORC ID:** 0009-0008-7151-5761, **CVU CONAHCYT ID:** 1296958

DOI: 10.35429/JCT.2023.18.7.32.39 Received: January 25, 2023; Accepted June 30, 2023

Abstract

In a global scenario, the amount of equipment exposed, the defense tools installed, the user culture and the subculture of information theft and damage to assets, it is necessary to create predictive stochastic models that can create a quantitative simulation about of a possible attack, and where appropriate the spread of it in an environment.

Security, Models, Predictive

Resumen

En un escenario mundial, la cantidad de equipos expuesta, las herramientas de defensa instaladas, la cultura del usuario y la subcultura de robo de información y daño en activos, se hace necesario la creación de modelos estocásticos predictivos que puedan crear una simulación cuantitativa acerca de un posible ataque, y en su caso la propagación del mismo en un entorno.

Seguridad, Modelos, Predictivos

Citation: SAUCEDO-LEÓN, Daniel, SAMPAYO-RODRÍGUEZ, Carmen Jeannette, GONZÁLEZ-AMBRIZ, Rosalba and MORALES-OLIVARES, Rosibel. Importance of the analysis of computer attacks on a LAN network applying the predictive-quantitative method. Journal Computer Technology. 2023. 7-18:32-39.

* Correspondence to the author (E-mail: carmen.sr@huauchinang.tecnm.mx).
† Researcher contributing as first author.

Introduction

With the continuous expansion of global network communications, the combination of traditional industries and the Internet is becoming more and more extensive. Network attacks are becoming more and more frequent, resulting in more and more threats and network losses.

Network security situational analysis (NSA) technology [I] incorporates data from intrusion detection system (IDS), firewall, virus detection system (VDS) and other network security protection devices. Essentially, it is an overall reflection of network security status and trends and can further serve as important evidence for early warning, network hardening and attack responses.

DBAG situation awareness or situational awareness [II] (SA) is a mental representation and understanding of objects, events, people, system states, interactions, environmental conditions, and any other factors in a specific situation that may affect the performance of complex or dynamic human tasks.

CVSS. The vulnerability measurement and scoring system, which allows to translate an arithmetic score into a qualitative representation of attack risk (low, medium, high and critical) [III]. This model, together with what is used in statistics and econometrics, in particular in time series, an autoregressive integrated moving average model or ARIMA methodology (autoregressive integrated moving average) is a statistical model that uses variations and regressions of statistical data in order to find patterns for a prediction into the future. It is a dynamic time series model, i.e. future estimates are explained by past data and not by independent variables. It was developed in the late 1960s. Box and Jenkins (1976) systematized it [IV] to achieve predictive models based on historical variables.

SNORT IDS. [V] It is an intrusion detection system, which for this research will be used in its intrusion prevention mode.

Micro Focus ArcSight is a cyber security product, first launched in 2000, that provides big data security intelligence and analytics software for security information and event management and log management.

MULVAL. It is a network security analyzer based on logical concepts, developed by Kansas State University. https://github.com/risksense/mulval.

The situation prediction technology includes two steps:

1. The first is the recognition of the situation. It refers to understanding the factors of the overall situation in the current network. The factors include the information of the network environment, attack strategies and defense strategies. The object is the current security state.

2. The second is situation prediction. Based on the previous step, it analyzed the regularity of the security situation and predicted the future trend in advance.

The exponential smoothing method is a way of forecasting the demand for a product over a given period. It estimates that demand will be equal to, for example, the average of historical consumption for a given period, giving greater weighting to values closer in time. It is optimal for random demand patterns where it is relevant to eliminate the impact of historical irregular elements by focusing on recent or targeted demand periods. [VI]

The 3 methods of predicting the network security situation by category are:

1. Methods based on time-space sequence (STS). The assumption of this method is that the change of the safety situation is regular and periodic. Suitable for short-term forecasting, time prediction is the next phase, and the value is fuzzy. [VII]

2. Methods based on graph theory (GRT). The GRT method uses vulnerability information in the network environment to generate the state transition diagram. In addition, it is designed from the intruder's perspective. The future situation is predicted based on the current network situation. [VIII]

3. Method based on game theory (GAT). Game theory is the study of mathematical models of conflict and cooperation between intelligent rational prediction of decisions. [IX][X]

ISSN: 2531-2197

Other necessary studies are required to solve the following problems:

1. General situational factors. STS and GRT methods primarily analyze attacker and environment information while ignoring defense information.

2. Accurate and complete prediction of the situation. Current research focuses on discovering the attack target, recognizing the attack path and predicting the probability of success.

In this document, a quantitative network situation prediction method that unifies the dynamic Bayesian attack graph (DBAG) is demonstrated.

The contributions of this document are as follows:

4. 1.- More complete prognostic information is obtained. The highlight is that not only can we predict common behaviors such as attack focus, attack path and probability of exploitation. In addition, the specific time to compromise the network can be calculated.

5. 2.- We design the risk quantification method for the security situation based on attack prediction. We provide a complete solution for the administrator to understand the security situation by quantitative value. One innovation is that we combine the common vulnerability scoring system (CVSS) [XI] with the information of predicted attack behaviors to quantify the possible risk from two angles of host and network.

Methodology to be developed

1. Network security situation prediction model. Predictions depend on the assessment of the adversary's attack capability, the effects of the defender's strategy, and information from the dynamically changing environment. Consequently, any change in the network security situation will lead to more or less changes.

Framework for quantifying the security situation based on attack predictions. The core idea is through collecting various information from running states of network devices to be aware of the "current situation" of the network, including network topology and connectivity, attack capability, observed attack events and defense strategies. Then, the above sample data is encoded into the DBAG to predict the possible attack.

Based on the attack prediction results and CVSS, we can further quantify the "future state" through security risk metrics. The feature of the framework is that the "future situation" can be adjusted in real time along with the "current situation" flexibly at any time. [XII]

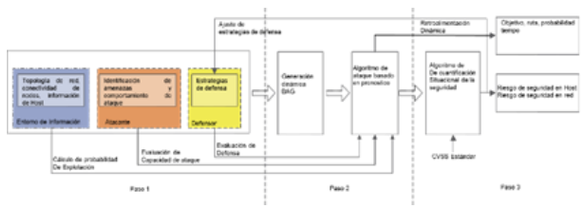

Figure 1 Predictive network security framework
Source: [XIII]

According to the framework, the specific steps are summarized as follows:

Step 1 Compilation of network security status factors.

Step 2 Network attack behavior prediction.

Step 3 Prediction of the network security situation.

2. Attack prediction algorithm

In this section, we first evaluated the attack capability of the adversary, then we calculated the vulnerability and the probability of exploitation of such vulnerability, as well as the expected time cost of future attacks, finally we calculated the prediction algorithm based on the DBAG and the complexity of the algorithm.

Attack Capability Metric. Assume that the attacker's ASLK attack capability is equal to the highest ever exploited ACPX of ASLK can be formulated as follows:

$$\mathrm{ASLK} = \max\big(\mathrm{ACPX}\ (\mathrm{Vuln})\big) \qquad (1)$$

ISSN: 2531-2197

Vulnerability exploitability probability metric. The relative vulnerability exploitability probability under different ACPX and ASLK is shown in Table 1.

ACPX	p(ACPX,ASLK) ASLK=LOW	ASLK=MEDIUM	ASLK=HIGH
Low	0.56	0.69	0.89
Medium	0.3	0.51	0.75
High	0.1	0.3	0.4

Table 1 Assessment of the probability of vulnerability exploitability
Source: Information processed with data obtained from the measurement of a network of 300 computers, between March 10 and March 23, 2023.

The probability of exploitability at the age or exposure time of the vulnerability (v), is as follows:

$$p(v) = \frac{p(ACPX,ASLK)}{F(t)} \quad (2)$$

Expected Attack Time-Cost Metric. The expected exploitation time with an unknown vulnerability cost V denoted as $ASLTexpcted$ is as follows:

$$ASLT_{Esperado} = \frac{ASLT_{prior}}{p(v)} \quad (3)$$

DBAG-based attack prediction algorithm. In this subsection, we encode the above information into the DBAG. In addition, by calculating the state transition equilibrium, the possible follow-up attack information can be predicted according to the equilibrium state.

Performance análisis of algorithms.

The complexity is:

$$O(nk) \quad (4)$$

The complexity of the space is:

$$O(4n2 + 2n) \quad (5)$$

3. Method of quantification of the security situation.

The impact metric of a vulnerability v is as follows:

$$Impact(V) = 10 \times (1 - (1 - C) \times (1 - I) \times (1 - A)) \quad (6)$$

Where C, I and A are the confidentiality, integrity and availability impact sub-scores respectively, and the score is obtained by querying the U.S. government's National Vulnerability Database (NVD) (NIST, 2023). [XIV]. The quantification of the security situation can be measured by the different types of attack and the severity of the threat.

Algorithm for quantifying the security situation. Input. Input matrices (SP, AT, DT, QD), vectors (T, P) and information (x, y, V, Weight). Output. Output $NSAr$ ($hostx$) and $NSAr$ ($network$).

Results

For method verification, SNORT IDS is used to collect the raw alert data during the test. Subsequently, two prediction experiments are conducted to verify the validity and rationality of our methods. Finally, the advantages of our methods are compared and discussed.

Network environment information. Small-scale experiment, the network is built and its topology is shown in Figure 2.

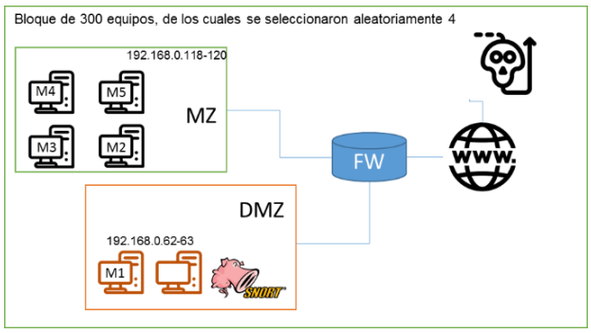

Figure 2 Test or experimental network topology determined for the research.
Source: Own elaboration

The network includes the firewall, intrusion detection system, five victim hosts and one attack host through the firewall with preset policies, the network is divided into two subnets.

Host M1 and IDS are deployed in the DMZ zone, and victim hosts M2, M3, M4 and M5 are deployed in the trusted zone. In addition, external hosts are prohibited from accessing hosts in the trusted zone and the adversary (connected to the Internet) can only communicate with host M1 (in the DMZ zone) via HTTP protocol (port 80).

ISSN: 2531-2197

Through scanning and querying network vulnerabilities on NVD public sites, we can obtain detailed information about vulnerabilities as shown in Figure 3 and Table 2.

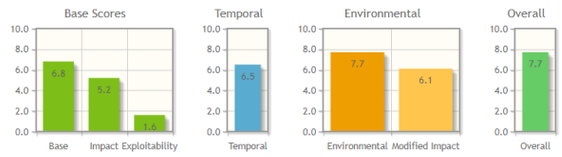

Figure 3 Predictive Network Security Framework
Source: Own elaboration

Whose attack vector is: CVSS v3.1 Vector AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H/E:H /RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC: H/MPR:L/MUI:R/MS:C/MC:H/MI:H/MA:H

Host	Service	Impact	CVE Code
M1	Apache	2.9	CVE-2020-1954
M2	DNS	6.4	CVE-2008-4126
	Linux cfingerd	10	CVE-1999-0243
M3	Windows Network File System	10	CVE-2020-17051
M4	DNS	10	CVE-2020-1350
M5	MYSQL	2.9	CVE-2014-0420

Table 2 Vulnerability information
Source: Own elaboration

Six vulnerabilities are discovered in the five internal hosts, each of the six vulnerabilities is unique, publicly known and denoted by a CVE identifier.

According to the network topological structure and vulnerability information, the MULVAL tool is employed to generate the network attack graph as shown in Figure 4.

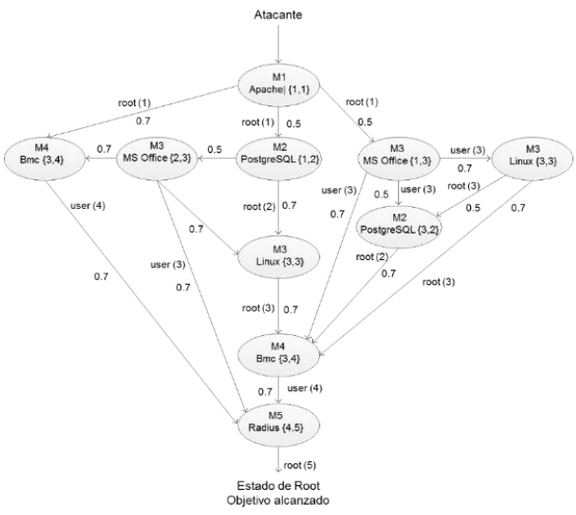

Figure 4 Experimental network attack graph
Source: Own elaboration

The granularity of the generated attack graph is the polynomial level, meanwhile, the generated graph is a directed acyclic graph.

Data collection test. To obtain from the real world experimental data, two skillful users of our network attack and defense scenario were selected and simulated, playing the roles of adversary and defender, respectively, and performing the experiment on the test network.

Experiment 1. In the first experiment, the raw alert sample data was selected from 9:00 am -11:00 am and analyzed through the ArCSight attack detection tool, finding the Exploit Vulnerability Probability Assessments and Expected Attack Time Cost shown in Table 3.

CVE #	Probability of success	Attack expectation in time/cost (h)
CVE-2020-1954	0.7230	0.2746
CVE-2008-4126	0.5163	0.3845
CVE-1999-0243	0.3097	0.6409
CVE-2020-17051	0.7222	0.2749
CVE-2020-1350	0.7215	0.2751
CVE-2014-0420	0.7229	0.274 6

Table 3 Experiment 1
Source: Own elaboration

The attacker has executed vulnerability exploitation on hosts M1 and M2 at 9:18 a.m. and 9:42 a.m. To forecast the subsequent attack behavior and security situation, the predictive algorithm and threat quantification method implemented together, the following steps were carried out and shown in Figure 5:

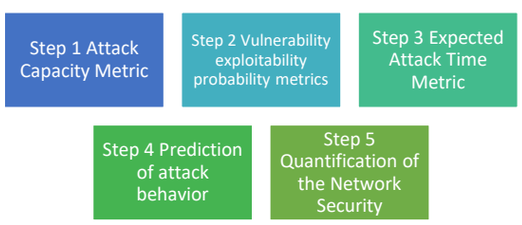

Figure 5 Steps of the predictive algorithm and quantitative threat method
Source: Own elaboration

ISSN: 2531-2197

Transition	CVE#	Probability	Time/Cost Expectation
S1→S2	CVE-2020-1954	0.7230	0.2746
S2→S3	CVE-2008-4126	0.5163	0.3845
S2→S4	CVE-2020-17051	0.7222	0.2749
S2→S6	CVE-2020-1350	0.7215	0.2751
S3→S4	CVE-2020-17051	0.7222	0.2749
S3→S5	CVE-1999-0243	0.3097	0.6409
S3→S6	CVE-2020-1350	0.7215	0.2751
S4→S3	CVE-2008-4126	0.5163	0.3845
S4→S5	CVE-1999-0243	0.3097	0.6409
S4→S6	CVE-2020-1350	0.7215	0.2751
S4→S7	CVE 2014-1878	0.7229	0.2746
S5→S3	CVE-2008-4126	0.5163	0.3845
S5→S6	CVE-2020-1350	0.7215	0.2751
S6→S7	CVE 2014-1878	0.7229	0.2746

Table 4 Description of attack behavior
Source: Own elaboration

According to Table 4, there are 14 different types of transition states/behaviors in the target network based on the primary attack sequence extracted from the observed sample alert.

All 9 possible attack paths from $S1$ to $S7$ are depicted in Table 5.

Number	Attack Route
Ruta 1	S1→S2→S6→S7
Ruta 2	S1→S2→S3→S4→S7
Ruta 3	S1→S2→S3→S6→S7
Ruta 4	S1→S2→S3→S4→S5→S6→S7
Ruta 5	S1→S2→S3→S5→S6→S7
Ruta 6	S1→S2→S4→S6→S7
Ruta 7	S1→S2→S4→S3→S6→S7
Ruta 8	S1→S2→S4→S5→S3→S6→S7
Ruta 9	S1→S2→S4→S4→S6→S7

Table 5 Possible attack routes
Source: Own elaboration

Quantification of the security situation occurs in two situations described below:

1. Host security status. We use the security situation quantification algorithm to calculate The security situation of hosts and network as detailed in Table 6.

Iterations	M1	M2	M3	M4	M5	Web
0	2.26	3.97	0	0	0	1.02
1	2.26	3.97	6.44	4.47	0	3.20
2	2.26	3.97	6.75	5.32	0.63	3.62
3	2.26	3.97	6.75	6.04	1.76	4.11
4	2.26	3.97	6.75	6.70	2.12	4.35
5	2.26	3.97	6.75	6.70	2.44	4.44

Table 6 Security predictions
Source: Own elaboration

Based on the predictions of attack behaviors obtained in step 4, the security situation of the host network is visualized illustrated in Figure 6, in which the horizontal axis is the cycle and the vertical axis is the NSA value [XV]. The higher value indicates the higher risk level at that time.

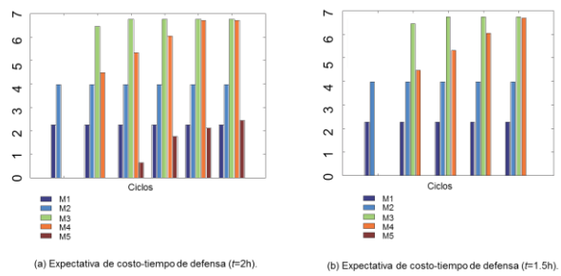

Figure 6 Host security status
Source: Own elaboration

By using the quantification of the host security situation, the administrator can recognize the threat of hosts, severity and further control the security risk of critical assets in a timely manner.

2. Network security situation. Considering two cases in Figure 7, the cost of defense time $t = 2$ and $t = 1.5$. the changes in the network security situation are illustrated in Figure 5, where the horizontal axis indicates the completion time of each attack step and the vertical axis indicates the security with its risk value, the higher value means the higher network risk, combined with Figure 5, we can obtain the following:

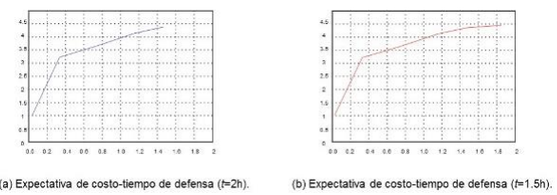

Figure 7 Network security status
Source: Own elaboration

- **Similarities**. In the initial phase, the entire network was at a "low" risk level, but, with the deepening of the attack phase, the attacker gradually realized the purpose of the invasion and the corresponding security risk and deficiencies were also increasing. Then the risk level was transformed to "medium", which is verified as true by the applied examinations and tests.

- **Differences.** Two cases are taken into account as follows; for the case t = 2, the attack ends in almost 1.8 h. During this period, the risk continues to increase. The results confirm that the change in the network situation may reflect the actual attacks of the method used.

For the case t = 1.5, along with the vulnerability applied by the defender, the attacker cannot continue to invade the host M5, so the invasion ends in almost 1.4 h, which indicates that the total network risk can be effectively reduced by strengthening the defense strategies.

Also, the results show that the predictions can be updated according to the defense strategies adaptively.

Acknowledgements

To the Tecnológico Nacional de México/Instituto Tecnológico Superior de Huauchinango.

Financing

Funding: This work was funded by Tecnológico Nacional de México/Instituto Tecnológico Superior de Huauchinango.

Conclusions

To optimize the prediction of the current network situation with this predictive method, two fundamental contributions are achieved in this paper.

1. The general factors of the network situation, such as attacker, defender and environment are taken into account to reflect dynamically and in real time the attack-defense confrontation feature.

2. The security situation is displayed from two levels (host and network) based on comprehensive attack prediction information.

Specifically, a prediction method of network security situation using the Bayesian attack graph presented in this paper through assessing the adversary's attack capability and combining the already detected alert events, it is possible to analyze the subsequent attack behaviors.

Based on that, the underlying security risk of the host and network are quantitatively calculated with the CVSS and asset information. The results show that this method is feasible, flexible and of low computational complexity in contrast to other similar studies.

This solution can achieve the purposes of an accurate attack, achieving intent recognition, route detection and probability of success through predictive action. In addition, the time cost of each step in the iterations makes it possible to calculate attack scenarios.

By quantifying the attack threat, the IT system administrator can assess the severity of the critical threat to assets and further infer and control the security situation in a timely manner. As we all know, the attack threat is always hidden within a network. Once an exploit occurs, the latent risk will be brought to the table, causing a series of security issues.

In the future of further research, an effective security strengthening strategy could be implemented based on the predictions of the security situation of each network, moreover, considering that all routes can be used to penetrate the system and to violate critical assets, the cost and benefit are different for each case and thus what is associated with the selected route. Therefore, to achieve security improvement on a cost-benefit basis in a budget constrained scenario is the key point in this research.

References

[I]. Security Information and Event Management tool. (s/f). Microfocus.com. Recuperado el 30 de enero, 2023, de https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm.

ISSN: 2531-2197

[II]. Allsopp, W. (2017). Advanced penetration testing: Hacking the world's most secure networks. John Wiley & Sons. Recuperado el …(agregar fecha de consulta) de https://ns2.elhacker.net/descargas/manuales/Hacking%20y%20Seguridad%20informatica/advancedpenetrationtesting.pdf

[III]. Schiffman, "Sistema de puntuación de vulnerabilidad común (CVSS) ". Recuperado el … de https://www.first.org/cvss/

[IV]. Box, G. E. P and Jenkins, G.M., (1976). "Time series analysis: "Forecasting and control," Holden-Day, San Francisco. Recuperado el …

[V]. Snort - network intrusion detection & prevention system. (n.d.). Snort.org. Recuperado el 11 de febrero, 2023, de https://www.snort.org/

[VI]. Métodos y fórmulas para la Suavización exponencial simple. (n.d.). Recuperado el 12 de febrero, 2023, de https://support.minitab.com/es-mx/minitab/20/help-and-how-to/statistical-modeling/time-series/how-to/single-exponential-smoothing/methods-and-formulas/methods-and-formulas/

[VII]. Box, G. E. P and Jenkins, G.M., (1976). "Time series analysis: „Forecasting and control," Holden-Day, San Francisco. Es la misma que la IV

[VIII]. Métodos basados en grafos. Recuperado el 14 de marzo, 2023, de http://pdg.cnb.uam.es/pazos/cursos/bionet_UAM/Grafos_CAguirre.pdf

[IX]. Taha, H. A. (2010). Investigación de Operaciones: Una Introducción (9a ed.). Pearson. Recuperado … de https://frh.cvg.utn.edu.ar/pluginfile.php/54151/mod_resource/content/1/Introducci%C3%B3n%20a%20la%20Investigaci%C3%B3n%20de%20Operaciones%20%289na%20ed%29%20-%20Hillier%20%20Lieberman.pdf

[X]. Fernandez, et al., (2020). CADENAS DE MARKOV - Métodos cuantitativos para la toma de decisiones III (1ª ed.). Universidad Politécnica de Cataluña. Recuperado el … de https://upcommons.upc.edu/bitstream/handle/2117/96718/9788498806113.pdf?sequence=1

[XI]. Diogenes, Y., & Ozkaya, E. (2023). Cybersecurity - attack and defense strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing. Recuperado de …

[XII]. Allsopp, W. (2017). Advanced penetration testing: Hacking the world's most secure networks. John Wiley & Sons. Es la misma que la II

[XIII]. Villamizar, C. (2020, October 22). ¿Qué es NIST Cibersecurity Framework? GlobalSuite Solutions. Recuperado el … de https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/

[XIV]. NVD - home. (s/f). Nist.gov. Recuperado el 05 de enero, 2023, de https://nvd.nist.gov/

[XV]. Allsopp, W. (2017). Advanced penetration testing: Hacking the world's most secure networks. John Wiley & Sons. Es la misma que la II Y XII

ISSN: 2531-2197