Power Cyberspace Surveying and Penetration

[a]Jindong He, [b]Zhou Zheng , [c]Shanshan Lei

[a]13950407229@139.com, [b]380580552@qq.com, [c]utaulss@foxmail.com

Fujian Power Co., Ltd. Electric Power Research Institute, Digital Technology Research Center, Fujian, China

Abstract: In view of the power information security problems such as the blind area, noise and the delay of the latest general vulnerability risk perception in the existing network asset detection and network security penetration, this paper constructs a set of cyberspace surveying and penetration test system based on vulnerability risk matching identification. The surveying process of fingerprint identification of network assets is described in detail, and the timeliness and noise problems of the whole network segment scanning of power information assets are solved by using the parallel optimization of prime number domain original root processing. Vulnerability risk matching identification and automated penetration test queue are used to generate security situation guidance of network assets based on vulnerability risk matching identification to improve the accuracy of security perception.

Keywords: cyberspace surveying; penetration test; security situation awareness; network security; cyber assets attack system

1. Introduction

With the promotion of energy Internet strategy, the wide application of information and communication technology and "Internet plus" in the power grid, the power system has gradually broken its closeness and exclusiveness, and the construction and deployment of open, interactive and widely interconnected power information business system has become more and more extensive [1-2]. With the continuous construction and development of various power information systems, the interweaving and cross-border integration of artificial intelligence, 5G, and energy internet on the network also forms a part of the power information network space. The surveying and mapping technology of power information network space can detect network resources (such as power dispatch information, relay protection signals, substation monitoring information, power market marketing data, etc.) in the power information network space, obtain network elements such as IP assets, ports, and their fingerprint information in the information network, and provide strong technical support for the security management of soft and hard assets in the power system and information system anti infiltration and anti theft [3-4]. The traditional network detection method based on manual statistics of network assets relying on client probes is no longer able to support diversified business scenarios, and gradually reveals its shortcomings in the process of network security supervision.

At present, there are blind spots in network asset surveying and mapping. The existing network asset statistics rely on manual form filling and server probes to discover the risks of

MSIEID 2023, December 08-10, Guangzhou, People's Republic of China

DOI 10.4108/eai.8-12-2023.2344726

network asset underreporting and unauthorized port construction, resulting in incomplete coverage of subsequent network security inspections and posing significant security risks; At the same time, the efficiency of surveying and mapping is low and there is noise. The existing server probe based network asset detection methods require the installation of clients on each device, which is highly invasive, costly, with incomplete coverage and low efficiency. At the same time, it is necessary to enable the Simple Network Management Protocol (SNMP) to collect network communication information. The cumbersome process can lead to full risk hazards, and in severe cases, it can affect the normal business flow in operation. Finally, the potential latest vulnerability risk cannot be perceived in real time. The existing network asset security situation is based on the network asset mapping results combined with the result set of automated Penetration test script verification, while the Penetration test script cannot automatically match the latest generic vulnerability risk. There is a security risk that cannot be perceived in real time due to the latest generic vulnerability risk of the existing version of network assets. Therefore, based on the current situation of network asset information security, this paper studies and designs the network space mapping and Penetration test system for power information from three aspects: network asset fingerprint identification, automated penetration queue and common vulnerabilities&exposures (CVE) matching and identifying security situational awareness, effectively mapping the network space of power information in an all-round way, It can improve the stability and execution efficiency of automated Penetration test, and enhance the awareness of the latest CVE vulnerabilities.

2. Management framework and business system of cyberspace mapping and Penetration test

2.1 Management Structure

The cyberspace mapping and Penetration test system realizes the full life cycle management for the security of power information network assets from three stages: cyberspace mapping, penetration message queue testing, and security situational awareness analysis[5].

Cyberspace mapping and penetration message queue test establish fingerprint rule library according to the business scenario where the power information is located, including but not limited to operating system, support software, Internet of Things equipment, power secondary equipment, WEB middleware, Content management system (CMS), development framework, application components, etc. Scheduling and distributing network space mapping tasks in a load balancing manner, creating diverse business scenarios, configuring typical or custom ports, configuring scheduled or patrol tasks, detecting surviving hosts, identifying surviving host content, and determining open port parameters and number of surviving hosts. Finally, based on the fingerprint rule feature library, the network asset graph information of the network spatial mapping result set is established. This architecture uses the penetration message queue mechanism to decouple the task strategy preparation, Data and information visualization analysis, situation awareness report generation and vulnerability penetration detection core business, so as to maintain the independence of core business. This distributed deployment mode achieves normal operation without interfering with the power network and business system. The web crawler function module with authentication function captures the latest vulnerability data of well-known CVE institutions in real-time, uses Elasticsearch fulltext search engine technology to establish a CVE knowledge base, matches existing network assets through fingerprints, identifies potential CVE risk network assets based on version numbers, and provides disposal guidance plans to generate a network asset security situation guidance report based on CVE matching recognition.

2.2 Service Infrastructure

The service infrastructure of the cyberspace mapping and Penetration test system is divided into three layers: ① the data storage layer is used for distributed storage of network assets, facility fingerprints, vulnerability data, etc.; ② The business communication layer is composed of message queues and communication protocol declarative state transitions (Representational State Transfer, REST) and Remote procedure call (RPC) protocols to realize the interconnection of data transmission between businesses [6-7]; ③ The business processing layer uses Microservices to realize the independent decoupling of each business [8-9]. This paper will introduce the construction of network asset space map, automated message queue Penetration test, and CVE matching identification security situational awareness.

3. Penetration test System and Key Technologies

3.1 Cyberspace Surveying and Mapping Technology Based on Fingerprint Recognition of Network Assets

The cyberspace mapping technology based on network asset fingerprint recognition aims to detect all IP assets, ports, and their fingerprint information under the target network segment, including but not limited to asset operating systems, port protocols, port services and version numbers, software and hardware asset fingerprint information, etc. Perform hierarchical Cartesian set matching on a given network fingerprint (IP, port, operating system) to obtain a complete network device fingerprint, and then draw a spatial map of enterprise real-time network assets. Cascade Cartesian matching first uses an IP address and the corresponding port to perform a Cartesian set, mapping the IP and port, with a total of 65535 ports or 1000 conventional ports according to industry definitions; Then perform Cartesian set matching of the operating system based on IP. Considering that the port protocol has default and specific attributes, the port protocol is mapped, and based on this, the Cartesian set of port services and version numbers is matched to obtain a network asset spatial graph.

The traditional full connection scanning is the most basic transmission control protocol (TCP) scanning mode, which requires the establishment of a complete TCP session and consumes a lot of system resources to complete three handshake sessions. Considering the actual scenario of asset detection in the entire network segment of an enterprise, this system only sends the first Synchronize Sequence Numbers (SYN), and then REST cancels the connection and performs a hash stateless scan of the detection address. The value is saved in the cache, and the SYN response from the target device is implemented by a dedicated receiving module waiting for reception to achieve asset detection.

This article compares the speed and efficiency of three mainstream scanning technologies, Zmap, Masscan, and Nmap, as shown in the following figure.

Table 1. Comparative analysis of scanning experiments

Scan	Time/min	Efficiency	Time/min	Efficiency
Scan VLAN	10.*.*0/24		125.*.*0/24	
Masscan	6.45	212/886	2.57	180/454
Zmap	10.72	224/942	7.4	343/1242
Nmap	30.65	230/1084	15.92	368/1885

The experimental results are illustrated in Table 1. In an experimental environment of CentOS7/1000 kb×S-1/Intel i7/16 G, conventional TOP1000 port scanning was performed. The time consumption of Masscan and Zmap is directly proportional to the number of scanning targets, while Nmap takes a long time and has fluctuations in multiple experiments, which is related to the runtime environment of the target network segment; In terms of scanning efficiency, Nmap is the best, followed by Zmap, and Masscan exhibits significant packet loss. All three greatly reduce the cost of state recording. The strategy of scanning addresses in this system adopts a hybrid address generation strategy of Zmap and Masscan [10], which enhances the randomness of adjacent scanning addresses, reduces the pressure of scanning on the target network within the same IP address range, and optimizes the implementation of efficient resource utilization [11].

4 Model Description

W provide a formal description of the network space expression model, as shown in equations (1) to (5).

$$M =< O(t), E(t) > \tag{1}$$

in which

$$O(t) = \{o_1(t), o_2(t), \dots, o_n(t)\} \tag{2}$$

$$o_i(t) = \{p(t), sp(t, s, l), g(t, s, l), a(t), \dots\} \tag{3}$$

$$E(t) = \{e_1(t), e_2(t), \dots, e_n(t)\} \tag{4}$$

$$\begin{aligned} e_1(t) = [<o_u(t), o_v(t)>, sp(t,s,l) \\ g(t, s, l), p(t), s(t), ...] \end{aligned} \tag{5}$$

In equations (1) to (5), M represents the network space representation model, O (t) represents the multi granularity set of spatiotemporal objects representing nodes in the model, t represents time, and each spatiotemporal object $o_i(t)$ is composed of multiple time-related features such as p (t) attribute features, s_p (t, s, l) spatiotemporal features, g(t, s, l) geometric features, and a (t) behavioral features. The lifecycle of each object oi (t) is [tb, te], s_p(t, s, l) spatiotemporal features and g (t, s, l) geometric features, where s represents the viewpoint distance in the scale or visualization engine, l represents which layer belongs to the physical layer, logical layer, or cognitive layer when expressed, and behavioral feature a(t) is a series of behavioral events generated over time; E(t) represents the set of edges representing the network spatial relationships in the model. In equation (5), o_u (t) and o_v (t) represent the two nodes corresponding to edge e_i (t). sp (t, s, l) represents the position of the edge when drawing the representation, which is also related to time t, scale or viewpoint distance s in the visualization engine, as well as the level l of the representation, G(t, s, l) represents the shape of an edge when expressed, such as line width, line color, etc. p (t) represents the attribute information associated with the edge, s (t) represents the state information corresponding to the edge, such as connectivity, etc. Each edge e_i (t) also has a lifecycle [t_b, t_e]. From the formal description of the model, it can be seen that O(t) corresponds to the network space resources to be expressed, E(t) represents network space relationships, and a(t) represents network space events.

5. Experiment analysis of network space mapping and Penetration test system

This paper develops a network space mapping and Penetration test system covering information collection, scanning and detection, vulnerability utilization and other links, aiming at multiple scenarios and multiple types of vulnerabilities in the power information network, to accurately and proactively troubleshoot potential security vulnerabilities in enterprise business systems. The system calls the message notification queue after real-time scanning, and the queue notifies the asset responsible person of the scanning result. The asset responsible person receives the message through the client, queries the list of asset security hazards, and achieves the effect of accurate accountability and accurate repair. The penetration report generated by the system accurately counts the number of asset IPs and port data under the IP, and provides opening instructions and protocol descriptions for each port, providing open security suggestions. The report also covers the results of the Proof of concept (POC) special scan for ports, realizing targeted modifications. The inspection report generated by the system can be used by enterprises for self inspection and rectification, in order to further improve the level of safety protection. The following figure shows the main testing interface of the cyberspace surveying and penetration testing system, displaying information such as asset overview, asset overview, and asset details.

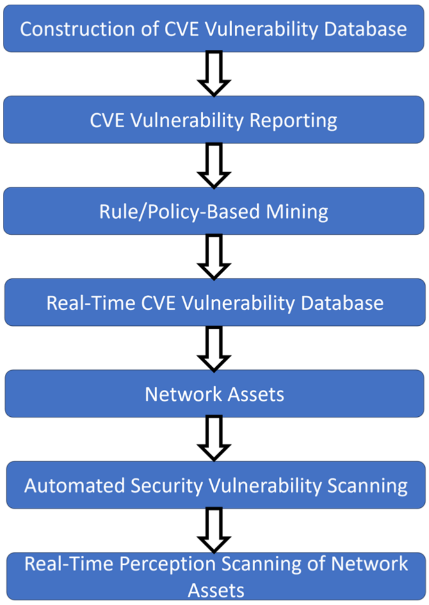
Construction of CVE Vulnerability Database
CVE Vulnerability Reporting
Rule/Policy-Based Mining
Real-Time CVE Vulnerability Database
Network Assets
Automated Security Vulnerability Scanning
Real-Time Perception Scanning of Network Assets

Figure 1. Security situation perception process

Figure 1 shows the business process of security situational awareness analysis report.The cyberspace mapping and Penetration test system has been deployed in a provincial power company of the State Grid, realizing the management and control of the information system equipment account, and the software resources such as IP address, service, port of the full caliber information equipment can be checked and managed. This system defines personalized scanning by configuring relevant scanning parameters. The intelligent scanning processing engine module reads the configuration parameters and quickly scans assets based on the mixed address strategy of Zmap and Masscan. POC is used to verify assets one by one and obtain asset related security information, including the survival status of registered IP addresses, port opening status, illegal IP addresses, and port lists. By logging the scanning process of each asset and implementing visual scanning, it is beneficial for process tracking and bug elimination [12-15]. Ultimately, the asset safety hazard list and related information are recorded in the database and cannot be modified, providing technical support for the company to establish a dedicated fingerprint and POC library for power information assets.

6. Conclusion

The construction and deployment of open, interactive, and widely interconnected power information business systems are becoming increasingly widespread. Electric energy is the foundation and pillar of the country, and its information security risks cannot be ignored. Aiming at the existing practical production problems, this paper constructs the power information oriented cyberspace mapping and Penetration test system from asset mapping, CVE security situation quasi real-time awareness, automated Penetration test and other aspects, explores the information security supervision technology for diversified business scenarios, and will continue to deepen the application research from the aspect of asset fingerprint feature recognition.

Acknowledgments: This research was supported by the project "Research on Key Technologies of Power Network Space Mapping and Defense Decision-making" (project code: 52130422003R) of State Grid Fujian Electric Power Co., Ltd.

References

[1] Li Zeke，CHEN Zewen，WANG Chunyan，et al. Network security threat tracing technology of power monitoring system[J]. Electric Power Engineering Technology，2020，39(2)：166-172(in Chinese).

[2] CAO Xiang，HU Shaoqian，ZHANG Yang，et al. Design and implementation of power universal security access zone based on dual isolation[J]. Electric Power Engineering Technology，2019，38(2)：152-158(in Chinese).

[3] ZHOU Yang，XU Qing，LUO Xiangyang，et al. Research on definition and technological system of cyberspace surveying and mapping[J]. Computer Science，2018，45(5)：1-7(in Chinese).

[4] XU Ruzhi，WANG Yufei. A study on electric power information network-oriented security situation awareness[J]. Power System Technology，2013，37(1)：53-57(in Chinese).

[5] GUO Jing，JIANG Haitao，WANG Ziying. Research on security testing technology of mobile application in power system[J]. Electric Power Engineering Technology，2018，37(4)：102-108(in Chinese).

[6] LIU Mingda，SHI Yijuan，CHEN Zuoning. Distributed trusted network connection architecture based on blockchain[J]. Journal of Software，2019，30(8)：2314-2336(in Chinese).

[7] ZHANG Ning，WANG Yi，KANG Chongqing，et al. Blockchain technique in the energy Internet：preliminary research framework and typical applications[J]. Proceedings of the CSEE，2016，36(15)：4011-4022(in Chinese).

[8] LI Gang，MENG Huan，ZHOU Guoliang，et al. Energy management analysis and scheme design of microgrid based on blockchain[J]. Electric Power Construction，2018，39(2)：43- 49(in Chinese).

[9] ZHANG Jun，GAO Wenzhong，ZHANG Yingchen，et al. Blockchain based intelligent distributed electrical energy systems：Needs，concepts，approaches and vision[J]. Acta Automatica Sinica，2017，43(9)：1544-1554(in Chinese).

[10] LI Jianjin，LUO Fan，LI Junye，et al. Construction of de-privacy encryption extraction model for big data in smart grid[J]. Electric Power Information and Communication Technology，2019，17(6)：
8-13(in Chinese).

[11] LIU Nian，YU Xinghuo，ZHANG Jianhua. Coordinated cyber attack：inference and thinking of incident on Ukrainian power grid[J]. Automation of Electric Power Systems，2016，40(6)：
144-147(in Chinese).

[12] ZHOU Lijing，WANG Licheng，SUN Yiru，et al. BeeKeeper：a blockchain-based IoT system with secure storage and homomorphic computation[J]. IEEE Access，2018(6)：43472-43488.

[13] NOOR S，YANG Wentao，GUO Miao，et al. Energy demand side management within micro-grid networks enhanced by blockchain[J]. Applied Energy，2018(228)：1385-1398.

[14] GONG Gangjun，ZHANG Tong，WEI Peifang，et al. Research on intelligent trading and cooperative scheduling system of energy Internet based on blockchain[J]. Proceedings of the CSEE，2019，39(5)：1278-1289(in Chinese).

[15] GONG Gangjun，WANG Huijuan，ZHANG Tong，et al. Research on electricity market about spot trading based on blockchain[J]. Proceedings of the CSEE，2018，38(23)：6955-6966(in Chinese).