Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/46/20241511

The building and the test of campus intranet security

Gu Weihong

Ulink College of Shanghai, Shanghai, 201615, China

peterguweihong@gmail.com

Abstract. There will be many different students of different ages inside a campus and using their laptops or mobile phones. However, their personal information is very valuable for criminals. To prevent hackers from having access to students' information, the campus's intranet should be well-secured. This paper is mainly focusing on how to build and measure the security level of a campus's intranet system from different approaches, including basic topology and advanced device configuration. The research will use concepts of basic red-team knowledge and basic penetration testing tools like "NMAP", "SQLMAP", Burp suite and "KALI Linux". To make sure that all the security rules are operating as intended, a planned penetration test should be conducted. The plan will be discussed and some advice are given at the end of this paper. The main idea of this paper is to give some instructions for beginners to set up a large scale network and build the security system for it.

Keywords: Campus intranet, Internet security, penetration test, firewall, intranet construction.

1. Introduction

The rapid expansion of information technology brings both convenience and security issues. Information leakage, denial-of-access attacks, denial-of-service attacks and hacking are the most common kinds of issues. Students or teachers who are not familiar with computers may download trojans or malware. Personal information of school members can be sold at a high price, so many people are trying to get access to some school's intranet and download those things. At the same time, nobody wants their personal data and the confidential servers in the internal network to be controlled by malicious hackers. On 26 May 2021, the National Computer Network Emergency Response Technical Team of China (CNCERT) pointed out that during the COVID-19 pandemic, multiple attacks are increasing [1]. In order to defend and prevent this kind of event, a well-built and well-secured intranet is important. However, it is hard to monitor such a number of campuses in the whole city or town, especially the intranet. Needs for scheduled security measuring and threat discovery are important. In this paper, the solution of intranet monitoring, security testing and central monitoring will be discussed. The security issues can cause large-scale information leakage or ransomware virus infection. For schools, information on servers and staff computers is important, same as students' devices. A highly secured network environment can protect those from malicious hackers, in order to prevent personal information leaks.

DOI: 10.54254/2755-2721/46/20241511

2. Intranet Security Architecture: from Client to Boundary

2.1. User Awareness

First thing first, the users should be taught basic cyber security knowledge, especially the students inside the campus. “People are the greatest weakness.” Many cyber-attacks against campuses start with a collection of relevant personnel’s information. It is always discovered that some students put their grades, names, ages and birthdays on public websites. The information can be very useful because hackers can use it to create a dictionary for brute-force attacks. This is called “Social engineering”, which is a method of cyber-attack based on using others’ information. So, the campus should enhance students’ awareness of personal information protection.

2.2. Endpoint Protection: Client-side Protection

There are various kinds of endpoint antimalware software like Norton 360, Kasberkey, Semantic endpoint protection and so on. Their integrated malware scanning engine can prevent the user from visiting malicious websites and accidentally running viruses. This technology mainly relies on the malware sample library.

Internet security industry companies have collected millions of malware samples in their databases. Those samples are being analyzed by professional security engineers to find out how they spread and what damage they will cause. The result of the analysis is also stored in the malware library.

The malware library is used by the antimalware software to analyze the files. The software compares the files’ “MD5” verification value to known malware and judges whether malicious codes are hidden in the files.

Each computer inside the campus intranet should be installed with antimalware software and controlled by an antivirus management backend. Besides, the endpoint protection software should always be checked if the filtration rules are applied and if the malware library is up to date or not.

2.3. Network Isolation: Prevent Unauthorized Access

For large-scale campuses, there will be thousands of devices including client devices, network infrastructure devices and servers. To prevent untrusted and unauthorized access to servers, the intranet should be divided into different groups based on IP address. The most well-known technology is called VLAN (Virtual LAN). By applying different VLANs with different access levels, the normal users are restricted to only accessing the servers that are allowed to be accessed instead of all the servers. Furthermore, when a computer is controlled by malicious personnel, he or she will not be able to perform any other attack against core servers.

2.4. Boundary Security: Filtrate Malicious Code and Block Suspicious Connections

Since all the traffic will run through the boundary gateway and then to the public Internet, high-performance firewalls should be installed between the campus intranet and the Internet to detect potential threats and block malicious connections. More sophisticated firewalls will cover a greater number of layers, while basic firewalls will only work on a lower number. Firewalls that can inspect multiple layers have a higher level of functionality and are more efficient. Adding layer awareness enables the firewall to support sophisticated applications and protocols; furthermore, additional layer coverage boosts the firewall's setting granularity. By expanding the layers under examination, a firewall can also offer highly user-focused services like user authentication. A more advanced application-proxy gateway firewall can impose user authentication and log events to individual users, but it typically does not deal with specific users when operating on layers 2 and 3 [2].

3. Penetration Test: Simulate Real-Life Cyber-Attacks and Find Security Shortage

Penetration tests can be completed by the campus IT department or external red teams. Its purpose is to find out the vulnerability of the network and give out a report. The test is not intended to hack and get sensitive data like normal attacks. It is mainly focused on security issue discovery and reporting.

DOI: 10.54254/2755-2721/46/20241511

The penetration test team will perform attacks by firstly gathering information about the target. There are several frequently spotting information leakage points: website open to the public, misconfigured internal website,

If passwords and accounts of internal Virtual Private Network or web platforms are leaked, hackers can access the intranet easily by simply logging in with the account. The next step of hacking will be able to continue with intranet access.

3.1. Social Engineering

Many campuses have their contact email address listed on the official website. For example, the recruitment information and complaint mailbox. One way of gaining access to the intranet is to control the personal computer by sending emails with malicious files. When internal staff who lack security awareness check the emails, they may download and directly open the malicious file causing their computer to be controlled by hackers. This kind of attack is called phishing, a method of taking advantage of human weaknesses. Besides, during penetration tests, testers may perform web forgery to deceive the relevant personnel into entering sensitive information.

3.2. Vulnerabilities of Web Application

For those web applications open to the public, this kind of threat must be noticed. Penetration tests will first use tools like “Nmap” or POC (Proof of concept) scripts to scan the website. For example, a website that lacks important software updates and maintenance may have high-risk vulnerabilities. Common vulnerabilities like SQL injection, remote code execution, cross-site scripting, file upload and CSRF (Cross-Site Request Forgery). Insecure Direct Object References: Direct access to things like files, directories or database keys. Without an access control check or other protection, attackers can use these references to gain access to unauthorized data [3]. These kinds of vulnerabilities can provide chances for testers to upload remote control trojans or directly operate the database, even getting the highest privilege of the webserver.

3.3. Firewall/Antimalware Software Bypass

During attack simulation, testers will have to use different methods to bypass the firewall in order to upload trojans. The firewall detects the feature of a trojan connection by unpacking the data package. Testers may use different coding of shellcode or trash data to avoid being detected. The same method is also being used to bypass antimalware software installed on the target server. This test’s purpose is only to do further penetration tests inside the intranet. Methods like “Changing the Signatures”. Most of the malware detectors detect malware from their signature. However, signature modification is one of the ways of bypassing the anti-virus software. At first, the malicious signature should be identified. The simplest way to find the malicious signature is to delete some parts of the virus file and test the resulting file to some virus scanners until the malware is no longer recognized as malicious. But a valid file header should be kept. This method can be used to remove the malware signature. The signature needs to be altered after the step of extraction is complete. Hexediting the signature is the most effective method of altering the signature. Tini’s signature is recognized by all 41 anti-virus engines. Tini listening port is 777, which is le61 in hexadecimal. Consequently, it is possible to find the part and modify it to port 443, which is 01bb in hexadecimal [4].

3.4. Intranet Lateral Movement

When the penetration test team gains control of one or multiple machines inside the intranet, they will perform lateral movement. Lateral movement means using methods including Scanning technology: scanning can be separated into scanning for information and scanning for vulnerabilities. Password cracking technology: this technology is primarily employed in direct penetration. After the attacker obtains the information about the username through scanning or other methods. Password brute force is engaged to test the password of the compromised system by using the dictionary. The password may allow attackers to enter the system lawfully. Network sniffing Technology [5]: data transmitted through

DOI: 10.54254/2755-2721/46/20241511

a network can be captured by intercepting data packets to gain a username and password for authentication or other valuable information about the compromised system. When data is transferred over a network in plaintext, network capturing can instantly obtain crucial information without decrypting. Deception technology: a certain identity is used to determine whether a target is granted a particular right. If an attacker can get access to or camouflage the identity, it can get access to or deploy the operation of the target. Cheating over IP, WEB, Address Resolution Protocal and spoofing over Domain Name Server and e-mail are commonly seen [6]. Vulnerability utilization technology: the vulnerabilities that occur on system platforms, application service software, and program security faults can be the breaking point of attack [7]. To continue exploiting intranet computers. During this stage, intranet administrators should notice the logs and alerts from the firewall and antimalware software management panel and block those malicious actions. This is also an important security issue: manual monitoring. Some malicious logons should be noticed. For example, a student account is logged on the internal file server and establishes a connection to other servers. The connections are usually created by password spray tools for guessing weak passwords of other accounts. Tools like Medusa can use a dictionary to perform brute force attacks. A dictionary contains commonly used passwords both collected from the Internet and customized combinations. There is a potential threat for hackers to get accounts with higher privileges. However, logs may not be able to present all messages. Some password acquisition tools like lslsass, gsecdump and mimikatz can successfully execute the password hash without leaving any logs [8].

3.5. Sensitive File and High-Value Target Discovering

During intranet scanning, servers like Active Directory controllers, virtual machine servers and file servers are high-value targets. It means sensitive information can be gathered from those servers, including personal information of staff, teachers and students, passwords and account lists and databases. If any hacker gains access to those files, it will be very harmful to campus members' personal security. Usually, the penetration test will set these kinds of computers to be the final targets. A comparison of fingerprints is used to identify web servers and web applications [9]. The test will end by getting the high privilege of high-value targets or getting the list of sensitive documents.

Table 1. High-value targets

IP	Scan Method	Port Open	Name	Domain/Workgroup	OS
10.20.100.2	ICMP 3ms	445,3389	DC-01	Test.com	Windows10/Server 206
10.20.100.8	ICMP 6ms	80,443,3389	HYPERV-SERVER	Test.com	Unknown platform
10.20.100.14	ICMP 4ms	445,8080	File-Server	Test.com	Windows 8/Server 2012
10.20.100.15	ICMP 3ms	3306	Database-Server	Test.com	Windows 10/Server 2016
10.20.100.18	ICMP 3ms	80,443,445	NAS-A	WORKGROUP	Unknown Platform

3.6. End of the Penetration Test

After successfully accessing the high-value targets, the penetration test team will write all the actions they take and what vulnerabilities are detected during the test to a report. Besides, all the backdoors and trojans should be cleaned up in order to prevent other people from using them to gain the control of intranet. Finally, the report will be finished by both the red team (attacker), blue team (defence) and white team (server maintenance) in order to give out a detailed security issue summary. What's more, the logs including logon events on different servers, and antimalware software alerts should be cleaned to restore the original state. Backdoors used in this test must be analyzed and added to the malware

DOI: 10.54254/2755-2721/46/20241511

library to prevent others from using it again. IT administrators of the campus intranet must be informed to fix the issues discovered. The test must come out with one or two vulnerabilities since there is no systems without vulnerabilities.

4. Centralized Management of Multiple Campus Intranets

In order to monitor and alert the local administrator, a centralized management platform should be used. Usually, creating an SD-WAN (Software Defined Wide Area Network) is suitable for managing the server clusters. More Internet applications, including DNS, DHCP(Dynamic Host Configuration Protocol), and web servers, are being deployed in the cloud as a result of the development of cloud computing [10]. SD-WAN can monitor the whole intranet including server system state, system log, alert log and user behavior. In this way, any kind of attack against any one of the campus intranets can be alerted in a short time. IT administrators can quickly notice the attacks and block the source Ips. Besides, this technology is also compatible with Internet access control which means students' and staff' Internet access can be managed. For example, rules of block students from connecting to malicious websites and websites with unhealthy information.

5. Conclusion

The large-scale intranet of the campus needs high-security levels. The special user group of it requires features like auto threat discovery and deletion. A scheduled penetration test should be applied to check whether all the security rules are working in order. The campus should also teach students and staff how to identify malicious programs and how to protect their personal information.

There are still some shortages appearing nowadays. Many campus IT administrators set weak passwords for intranet devices for easy maintenance and access; the attack alert is usually not functioning because nobody is monitoring the management platform. This paper concludes fundamental campus intranet security construction, is not very detailed. It is recommended to search for specific information about intranet construction and penetration tests. In the future, research will mainly focus on automatic threat cleanout and auto-centralized management. Manual management will only be applied when high risks are occurred.

References

[1] Rui Zheng, Hao Ma, Qiuyun Wang, Jianming Fu, Zhengwei Jiang. Assessing the Security of Campus Networks: The Case of Seven Universities; Sensors 2021, 21(1), 306:1-3

[2] Yaxuan Qi; Fei He; Xiang Wang; Xinming Chen; Yibo Xue; Jun Li. OpenGate: Towards An Open Network Services Gateway; Comput. Commun. 2011, 21, 2

[3] Mahin Mirjalili, Alireza Nowroozi, Mitra Alidoosti. A survey on web penetration test.2014,111:3.1-4

[4] Farid Daryabar, Ali Dehghantanha, Hoorang Ghasem Broujerdi. Investigation of Malware Defence and Detection Techniques; The Society of Digital Information and Wireless Communications, 2011, 646:B

[5] B. Prabadevi; N. Jeyanthi; Ajith Abraham. An Analysis of Security Solutions for ARP Poisoning Attacks and Its Effects on Medical Computing; International Journal of System Assurance Engineering and Management 2020, 3 (1)

[6] Mayoon Yaibuates; Roungsan Chaisricharoen. A combination of ICMP and ARP for DHCP Malicious Attack Identification; 2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), 4(2).

[7] Minglei Li; Yuliang Lu; Hui Huang; Chao Zhang; Jiazhen Zhao. Research on Automatic Exploitation of House of Spirit Heap Overflow Vulnerability; 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 5.

[8] Detecting Lateral Movement through Tracking Event Log.2017.06.12; 68

DOI: 10.54254/2755-2721/46/20241511

[9] Dechun D. Firewall and The Security of Campus Intranet[J]. Journal of Qujing Normal College, 2001.

[10] Dewang Gedia, Levi Perigo. NETO-APP: A NETWORK ORCHESTRATION APPLICATION FOR CENTRALIZED NETWORK MANAGEMENT IN SMALL BUSINESS NETWORKS; Interdisciplinary Telecom Program, University of Colorado Boulder; 3