SECURITY PENETRATION TEST ON FCSE'S IT SERVICES

Radoslav Bozhinovski, Vesna Dimitrova, Boro Jakimovski, Sasko Ristov

Faculty of Computer Sciences and Engineering

Skopje, Macedonia

ABSTRACT

Network security penetration tests are an excellent method for evaluating the network security level of a company's IT services. The method of penetration testing is complex and without the appropriate care, disastrous effects on the systems that are being tested can happen. This paper gives an overview on how a penetration test can be successfully done. The penetration tests were made on the network of Faculty of Computer Science and Engineering (FCSE) in Skopje.

The methodology used in this paper is showing the process that penetration testers should go through. The idea behind the methodology is that the penetration testers should follow a pre-defined format during tests.

The purpose of this paper is to document and describe how a pen test should be performed and what the potential impacts and effects could be. The results of the realized series of penetration tests show many security flaws on several IT systems and this paper proposes measures how to mitigate the risks to acceptable levels.

I. INTRODUCTION

Penetration test (pen test) is a method for evaluating the computer security or network by simulating an attack from a/or (a group of) malicious hacker/s. This process involves an active analysis of the system from potential vulnerabilities that could result from a poor configuration, misconfiguration or a new vulnerability. This method involves active exploitation of security vulnerabilities [1].

There are two types of pen tests [2], depending on whether there are performed: from inside or outside the organizations network. The former is defined as a security assessment test from inside the organization where the attacker has some level of authorized access. The latter is defined as a security assessment test from the outside where the pen tester does not have authorized means of accessing the organization's systems.

Depending on whether this test is done with knowledge of the systems and networks or not, there are two different ways of conducting a pen test [3]. The first way is known as a "black box", which means that no information is known about the assessed IT systems. The second way is known as a "white box", which means that all or the most of the information about assessed IT systems are known to the pen tester.

The main goal of the penetration testing is to identify and report on security vulnerabilities allowing the organizations to close these issues in a planned manner and significantly raise their level of security.

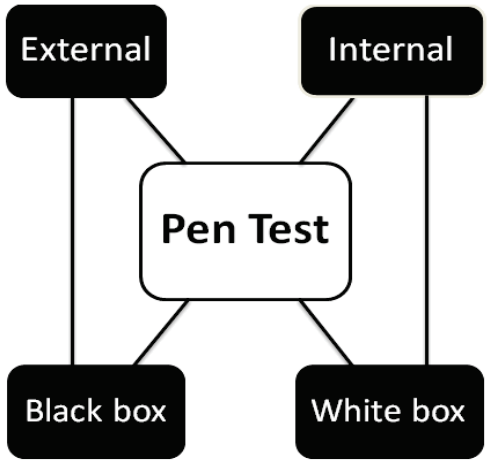

Figure 1: Types of Pen Tests.

In this paper we assessed several FSCE network services using our adapted methodology and we proposed measures how to mitigate the network vulnerabilities to an acceptable level. The rest of the paper is organized as follows. Section II defines the proposed methodology used in the security assessment. In Section III we elaborate the results of the assessments and in Section IV we propose measures how to mitigate the risks of threats in order to improve the security of FCSE's ICT systems. Finally we conclude our work in Section V.

II. METHODOLOGY

This paper uses a methodology of work as proposed by the National Institute of Standards and Technology (NIST) SP 800-115 [4], a program for the certification of ethical hackers (CEH) [5] and the methodology recommended by the Open Information Systems Security Group (OISSG) [6]. The different stages based on these methodologies are summarized in the following section.

A. Stages

Stage 1: Planning and Preparation – comprises steps to exchange initial information, plan and prepare for the test. Prior to the testing, an agreement is signed from both parties.

Stage 2: Reconnaissance – comprises information gathering using the Internet to gather available information about the target. This is the initial stage of any information security audit, which many people tend to overlook. There are two types of reconnaissance based on whether the information is gathered passively using the Internet and without direct interaction with the target or actively when the information is obtained by direct interaction with the target.

Stage 3: Scanning – comprises scanning the network for specific information collected and received from the previous stage to produce a probable network topology for the target. In this stage network mapping was used to fine tune the information previously received and to confirm or dismiss some hypotheses regarding the target systems. Furthermore, vulnerability identification was performed enumerating all discovered vulnerabilities, estimating the probable impact on the system and identifying the vulnerable services in order to detect the exploitable weak points.

Stage 4: Penetration – comprises gaining unauthorized access by circumventing the security measures in place and trying to reach a level of access as wide as possible. Furthermore, there are various techniques such as privilege escalation to gain administrative privileges. Furthermore, the internal network and internal resources can be enumerated.

Stage 5: Maintaining access – comprises several tools such as covert channels, backdoors, and root-kits, to ensure the access and remain undetected as long as possible. This stage is outside of the scope of this paper.

Stage 6: Covering the tracks – comprises activities to hide files, clear the logs, circumvent anti-virus, and circumvent integrity checking, etc. with the purpose to remain undetected. This stage is outside of the scope of this paper.

Stage 7: Reporting – comprises producing a written report that describes in detail the results from the tests and the recommendations for improvement. This stage is outside of the scope of this paper. The reporting and documentation about what's done is in [7].

B. *Common Vulnerability Scoring System*

According to the methodology for ranking vulnerabilities proposed by the Common Vulnerability Scoring System (CVSS) [8], the detected vulnerabilities were classified into four groups according to the impact and damage that are caused to the system or the application. They are classified as:

- *Critical* risk vulnerability, if the score for vulnerability is 10 of 10;
- *High* risk vulnerability, if the score for vulnerability is in the range of 7 to 9;
- *Medium* risk vulnerability if the score is in the range of 4 to 6; and
- Low risk vulnerability, if the score for vulnerability is in the range of 1 to 3.

According to this open standard, the level of risk is determined through several stages where each vulnerability is ranked independently and the direct impact to the target host is only determined.

C. *Testing Tools*

In this section we describe the tools that we have used during the security assessment and pen tests.

Nmap [9] is a program that gives us information about ports, services and hosts. It allows us to create a network map. With his scripting language, also we can get the OS version and name, trace route, test hosts for certain vulnerability and more.

Hping3 [10] is a de facto tool for security auditing and testing firewalls and networks. It is packet generator and analyzer for TCP/IP protocol. With his scripting language it is possible to write low level TCP/IP packet manipulation and analysis in short time.

Metasploit [11] is a tool for developing and executing exploit code against a remote machine. It also provides testing to the vulnerabilities of computer systems in order to protect them.

Nessus [12] is a comprehensive vulnerability scanner. This scanner scans for known vulnerabilities against live hosts.

III. RESULTS

In this section, only the results from stages 1, 2, 3 and 4 described in Section II will be discussed. The results from stages 5, 6 and 7 are presented in [7].

Reconnaissance was performed on the addressing space that was assigned by FCSE. Using publicly available information about FCSE, searching for background information, searching through DNS and WHOIS services about the addressing space that was given, we were able to detect the operating system (OS) version, fully qualified domain names, web servers as well as DNS servers, how long the systems and servers were active and the last modifications that have been made on the content on the web servers, email address, etc.

After the starting information about the systems, the scanning was done when open ports were found. We used Nmap because this program sends specially crafted packets to the target host and then analyzes the responses. It also provides a variety of features for probing computer networks. We found a list of all up hosts and their open ports and services as well as the OS version. Through scanning we found two firewalls and IDS, but they were not the only one. For verifying the results we used hping3 and Metaspoit which confirmed the results found. After scanning the network, there was a clear picture of the network topology of FCSE. Next, we identify the vulnerabilities of the founded services that were running. Nessus gave some results about the vulnerability. Aditionaly we used techniques like banner grabbing, searching for known vulnerabilities based on the version of the service, perform a false positive verification, etc. so we found more useful vulnerabilities. At this stage, we ranked the found vulnerabilities. So, a plan was made on how to penetrate the network.

The tests were performed for a second time. Figure 2 describes the results from the second attempt.

Severity	Name	Type	Total
High	SNMP Agent Default Community Name (public)	SNMP	12
High	rlogin Service Detection	Service detection	1
High	FTP Anonymous Read/Write Permissions	FTP	1
Medium	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
Medium	DNS Server Recursive Query Cache Poisoning Weakness	DNS	1
Medium	DNS Server Spoofed Request Amplification DDoS	DNS	1
Medium	mDNS Detection	Service detection	4
Medium	SSL/TLS Renegotiation DoS	General	1
Medium	SSL Medium Strength Cipher Suites Supported	General	1
Low	Unencrypted Telnet Server	Misc.	13

Figure 2: Founded vulnerabilities on FCSE systems.

We detected 3 high risk vulnerabilities on a total of 14 devices, 6 medium risk vulnerabilities on a total of 9 devices and 1 low risk vulnerability on 13 devices.

The first vulnerability was SNMP Agent Default Community Name (public) [13]. This vulnerability allows an attacker to read SNMP data from the remote device. The data includes system time, IP addresses, processes running, routing information, information about virtual LANs (vlan) and more. We also found the private community strings that allowed us to change the information on the remote machine. We identified 3 community strings that were used: public, private and internal.

The next vulnerability that was identified was the rlogin Service Detection [14]. This service is dangerous in the sense that it was not ciphered, so anyone could "sniff" the data that passed between the rlogin client and rlogin server.

We identified a FTP server with read/write permissions for an anonymous user that allowed us to penetrate further into the network.

Throughout the pen test, we detected a DNS server that had multiple vulnerabilities. This DNS server was vulnerable to DNS Server cache snooping remote information disclosure [15]. This vulnerability allows a remote attacker to determine which domains have recently been resolved via the DNS Server and therefore which hosts have been recently visited.

The DNS Server recursive query cache poisoning weakness [16] is a vulnerability to this DNS Server where it was possible to query the remote name server for third party names. Because this DNS Server is for internal use, the vector of attack is limited only to employees or guest access. Because this server allowed these queries over UDP, then the host can be used further to bounce a Denial of Service (DoS) attack against another network or system.

DNS Server spoofed request amplification Distributed DOS (DDoS) [17] is an attack about sending small packets of information to the server that will respond with a much larger packet to a specific target. To direct the amplified traffic to the intended target, the attacker must spoof the source address in the request, resulting in all of the responses to be sent back to the victim.

Another vulnerability that was found was mDNS detection [18]. This service is using the Bonjour protocol, which allows gaining information of the remote host such as OS name, version, hostname and etc.

One host is vulnerable to SSL/TLS renegotiation DoS [19]. The remote service encrypts the traffic using TSL/SSL and permits users to renegotiate the connection. The requirements for renegotiating for connection are asymmetric between the client and the server, where the server is performing several times more work. Since the remote host does not appear to limit the number of renegotiations for a single TSL/SSL connection, this allows the client to open several simultaneous connections and repeatedly renegotiate them, possible leading to a DoS attack.

Another host was found to be vulnerable to SSL medium strength cipher suites supported [20]. This vulnerability is all about the length of the encryption key where the key is between 56 and 112 bits long where is much easier to crack then if todays conventional lengths would have been applied.

The last vulnerability found was an unencrypted telnet server [21]. This vulnerability refers to an unencrypted communication between the server and the client. After sniffing the communication, we could obtain sensitive data such as usernames and/or passwords.

As information disclosure, we found a checkpoint firewalls on two hosts and Osiris IDS on one host.

The new penetration plan was made and we started penetrating the network, first with the FTP server that allowed for anonymous users to have read/write privileges. We successfully placed a document there. Due to the pre-determined limitations as discussed in the methodology, we did not penetrate further into the internal network nor did we do an internal reconnaissance and internal network mapping, but with this proof of concept, we were able to show that is possible to penetrate into the network. Then we used the network printers and successfully printed a few pages on them. We had full control over the network printers.

IV. Proposed Measures

To prevent founded vulnerabilities in Section III, we propose several measures.

The vulnerability of SNMP protocol can be solved [13] if the SNMP service is turned off when not in use. Another option would be to filter the incoming UDP traffic on port 161. As a third option, changing the default community string to something different as public, private or internal is recommended.

The best way to fix the vulnerability of rlogin service [14] is to disable this service and use SSH instead. Another option is to comment out the 'login' line in 'etc/inetd.conf".

The found vulnerability (misconfiguration) to the FTP server can be solved if the access to this server is limited. That means that only authorized users can use this server and the anonymous access should be disabled. Eventually allowing monitoring is also desirable where only the root user will have access to the results.

The found vulnerabilities to the DNS Server show that there is a need for reconfiguration of the server. If the recommendations [22] from Microsoft are followed, then this vulnerability should not happen again.

Because there is no code fix as this is a configuration problem, the vulnerability DNS Server cache snooping remote information disclosure can be solved [15] if public access is not allowed to the DNS server performing the recursion. Another option is to disable recursion.

The vulnerability DNS Server recursive query cache poisoning weakness can be solved according to the proposed decision by Nessus by restricting recursive queries to the hosts that should use this name server.

The suggested actions that should be taken to mitigate [17] the vulnerability DNS Server spoofed request amplification DDoS are to disable recursion on authoritative name servers with the global BIND configuration option 'recursion no', and prevent BIND from answering this queries for a zone outside of the server's authority.

Recommended actions [18] to mitigate mDNS vulnerability is either to block incoming traffic on the UDP port 5353 or filter incoming traffic on this port.

About the vulnerability SSL/TSL renegotiation DoS, the best way is to contact the vendor and apply the newest patches. This is because we could not find the exact vendor. The best way to mitigate [20] the SSL medium strength cipher suites supported vulnerability is to reconfigure the affected application and if possible to avoid using medium strength cipher again.

The last vulnerability is Unencrypted Telnet server. To mitigate [21] this vulnerability it is recommended to disable the telnet service and replace it with technologies like SSH, TSL or VPN. These technologies will ensure that communication will be encrypted and will not allow eavesdropping.

V. CONCLUSION

Penetration test represents the state of the systems at a certain time. The process of application, system and network security is a continuous one because as soon as the test is complete, another system or application can be added that might produce different results if the test is performed again.

This is the reason why there is no security system that is not vulnerable. This also refers to the security system that FCSE has.

Different methodologies exist to fulfill specific claims. These help to choose the best strategy and try to modify and find the best variation of the standard methodology to conduct a successful pen test. In this paper we defined our methodology using three existing methodologies.

During the pen test, the initial data that we have produced differed from the data obtained two months later. So, we can confirm that between the two scans fixes, patches and securing the vulnerabilities and the security flaws have occured.

Numerous and very inventive possibilities to penetrate into ICT systems exist, however also numerous and very inventive opportunities exist to defend against these attacks. Experience shows that there is no absolute security protection, but the risks of access by unauthorized, unauthenticated user to the computer systems and networks must be mitigated to acceptable levels.

REFERENCES

[1] D. Kennedy, J. O'Gorman, D. Kearns and M. Aharoni, "Metasploit: The Penetration Tester's Guide", San Francisco, June 22, 2011, ISBN-10: 1-59327-288-X

[2] Sans Institute (2002), "Penetration Testing - Is it right for you". Available at: http://www.sans.org/reading_room/whitepapers/testing/penetration-testing-you_265

[3] RedSphere, "Penetration Testing". Available at: http://www.redsphereglobal.com/content/penetration-testing

[4] NIST (2008), "Technical Guide to Information Security Testing and Assessment". Available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[5] EC-Council (2013), "ceh core concepts - offered free to every official ceh v7 students". Available at:

http://eccouncil.org/courses/certified_ethical_hacker.aspx

[6] OISSG (2008), "Penetration Testing Methodology". Available at:

http://www.oissg.org/wiki/index.php?title=PENETRATION_TESTING_METHODOLOGY

[7] R. Bozhinovski, "Анализа на безбедноста на системите на ФИНКИ користејќи пенетрациски 'black box' тест", BSc, Thesis, Skopje, 2013

[8] CVSS (2007), "A Complete Guide to the Common Vulnerability Scoring System Version 2.0" Available at: http://www.first.org/cvss/cvss-guide.pdf

[9] G. Lyon, "Nmap: Network Scanning", January, 01, 2009, ISBN-10: 0-9799587-1-7. Available at: http://nmap.org

[10] Salvatore Sanfillipo (2006), "HPING 3". Available at: http://www.hping.org/hping3.html

[11] Rapid7 (2013), "Metasploit". Available at: http://www.metasploit.com

[12] Tenable Network Security (2013), "Nessus: the Industry Standard Vulnerability Scanner". Available at: http://www.tenable.com/

[13] SecuriTeam (2000), "Default Community Names of the SNMP Agent". Available at: http://www.securityspace.com/smysecure/catid.html?id=10264

[14] Easy Solutions (2009), "110205: Rlogin Service Detection". Available at: https://dvs.easysol.net/threats/details.cgi?id=110205

[15] Tenable Network Security (2013), "DNS Server Cache Snooping Remote Information Disclosure". Available at: http://www.tenablesecurity.info/plugins/index.php?view=single&id=12217

[16] Internet Corporation for Assigned Names & Numbers (2008), "DNS Cache Poisoning Vulnerability Explanations and Remedies". Available at: http://www.iana.org/about/presentations/davies-viareggio-entropyvuln-081002.pdf

[17] Security Tools News & Tips (2009), "DNS Amplification Attack", Available at: http://securitytnt.com/dns-amplification-attack/

[18] Fortinet (2013), "mDNS Detection". Available at: http://www.fortiguard.com/search.php?action=detail_by_vuln_id&data=31352

[19] OSVDB (2013), "73894: Multiple Vendor SSL/TLS Implementation Renegotiation DoS". Available at: http://osvdb.org/show/osvdb/73894

[20] Tenable Network Security (2013), "SSL Medium Strength Cipher Suites Supported". Available at: http://www.tenable.com/plugins/index.php?view=single&id=42873

[21] Rapid 7 (2013), "Nexpose Vulnerability Database". Available at: http://www.rapid7.com/vulndb/lookup/telnet-open-port

[22] Microsoft (2013), "Deploying Secure DNS". Available at: http://technet.microsoft.com/en-us/library/cc772661%28WS.10%29.aspx