PRACTICAL APPROACH FOR SECURING WINDOWS ENVIRONMENT: ATTACK VECTORS AND COUNTERMEASURES

Abdurrahman Pektaş[1] and Ertuğrul Başaranoğlu[2]

[1]Department of Computer Engineering, Galatasaray University, Istanbul, Turkey [2]Ziraat Technology, Istanbul, Turkey

ABSTRACT

Today, with the advancement of information technology, companies need to use many technologies, platforms, systems and applications to effectively maintain their daily operations. This technology dependence has created a serious complexity in the business network which increases the attack surface and attracts cyber criminal's attention. As a result, the number of cyber-attacks targeting corporate environment is dramatically increased. To identify security holes in a network, penetration tests are performed by internal sources (employees) and external sources (outsource companies or third parties). Microsoft domain penetration testing,is one of the most important scopes of penetration testing, which aims to expose the weaknesses in Microsoft domain environment. If the domain environment is not structured securely, it can be abused by attackers and causes serious damage to the organization. In this study, we present a penetration methodology for Windows domain environment called MSDEPTM providing key metrics for Microsoft domain penetration testing. More specifically, the fundamental steps of the attack vectors from the hacker point of view, root causes of these attacks, and countermeasures against the attacks are discussed.

KEYWORDS

Penetration testing, Microsoft domain environment, securing Windows, information security, vulnerability assessment

1. INTRODUCTION

Nowadays, information security has become more and more important issue both for individuals and corporate entities or associations. Corporates tend to protect their computing infrastructure and critical assets from attackers by applying security countermeasures. As it is well-known fact that one of the most important environments in a corporate network is Microsoft domain environment. For this reason, the cyber criminals highly target Microsoft domain. To ensure security in a corporate network, system administrators and security teams defend domain environment either in offensive and defensive ways.

Penetration testing, one of the most effective way to secure a network, can be defined as a technique for exploring the existing security holes and vulnerabilities in a computing system or a network to protect information assets before real attackers exploit them. The primary aim of the penetration testing is to discover the ways to hack a system from hacker's perspective. Microsoft penetration testing is one of the most important measurement to secure the assets and systems that are joined to the domain and it is also important to secure related (or connected) systems with Microsoft active directory.

DOI: 10.5121/ijnsa.2017.9602

Generally, the penetration testing can be divided into two categories black-box and white box. In black box penetration testing, the pentesters aim to exploit the computer system remotely without any prior knowledge. On the other hand, the white box penetration testing, the internal attacker who already knows internal networks and possible weaknesses in these networks assess the security level [1-3].

Although many pentesting methodologies exist, there is not enough research on Windows penetration testing. In this paper, we present a penetration testing methodology focused on the analysis of the Microsoft domain environment. We discuss different techniques, as well as possible countermeasures available to mitigate attack vectors and vulnerabilities. Specifically, every step of the proposed methodology is described in detail and comprehensively, such as the tools, attack vectors, root causes, as well as countermeasures.

The reminder of the paper is organized as follows: the following section presents the related works. Section 3 describes the proposed penetration test methodology for Microsoft Windows domain environment. Section 4 introduces the countermeasures against the presented attack scenarios. Finally, conclusions are presented in Section 5.

2. RELATED WORK

2.1. PENETRATION TESTING

There are different methodologies to conduct penetration testing. In general, the penetration testing can be split into four phases: reconnaissance, scanning, exploitation and gaining persistent access. These four steps can be extended into sub-phases such as post exploitation, password cracking, vulnerability analysis, etc. Some of the current related works in penetration testing are given as follows:
In [4], Setiawan et al. present the general steps about conducting penetration testing focussing on finding and exploiting vulnerabilities in Windows OS. In the experiments, some steps of the pentesting including scanning vulnerabilities, brute-force password guessing, gaining persistent access to the computer via backdoors, privilege escalation, etc. are analyzed.

In [5], the authors analyzed the vulnerabilities and attacks targeting of the wireless communication by performing the penetration test in a laboratory environment. The authors developed a wireless auditing tool which is capable of detecting denial of service attacks, rouge access points and WEP/WPA/WPA2 pre-shared cracking.

In [6], penetration testing and auditing of the Linux OS is presented. Various types of attack vectors are analyzed in detail. Moreover, the author discussed the network auditing process and forensic investigation in order to be used their research as a reference for security practitioners to prevent cyber-attacks. [7] proposed an heuristic-based attack graph generation approach integrating different stages of security assessment process. The authors also recommend cost-driven mitigations for vulnerabilities.

Mehtre et al. [8] present the current trends of pen testing and vulnerability assessment. Then, they the introduce step by step guide for vulnerability assessment and penetration testing. The use case of some open source tools which are frequently used for performing penetrations testing is given with hints related to these tools. The interested readers can refer to [9-12] for additional works.

2.2. PENETRATION TESTING METHODOLOGIES

There are variety of standards, guidelines and methodologies that are prepared by organizations to carry out penetration testing in an orderly fashion. These can be listed as follows:

PTES (Penetration Testing Execution Standard): PTES [13] is prepared by a group of people that work in different sectors. It presents a penetration testing methodology that consists of 7 sections: pre-engagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation post-exploitation and reporting. Although PTS is well prepared, it has not yet been finalized. This standard forms a framework for all scopes of pen testing and draws a general framework for all categories of penetration testing (for example, web, wireless, Microsoft domain, network equipment, etc.). However, MSDEPTM provides penetration testing steps specifically to the Microsoft domain environment and does not include the first and last steps of the PTES. These steps present additional techniques (such as using built-in command sets or getting the dump file of the LSASS process) against situations where an attack method is unsuccessful (such as could not obtaining a Meterpreter shell) or an attack is not feasible (such as running Mimikatz tool [14] on critical servers). In addition, PTS does not presents the countermeasures against each attack step and technique.

CEH (Certified Ethical Hacker): CEH [15] is prepared by Ec-Council. It presents a penetration testing methodology that consists of 5 phases: reconnaissance, scanning-enumeration, gaining access, maintaining access and clearing tracks. The penetration test phases provided by CEH cover all attack steps like MSDEPTM and CEH. It also contains best practices for planning and reporting steps. In addition, CEH lists the different tools used in the penetration tests and countermeasures against each attack like MSDEPTM, but CEH does not examine each step with different techniques and does not provide in-depth penetration testing of Windows domain.

OSSTMM (The Open Source Security Testing Methodology Manual): OSSTMM [16] is prepared by ISECOM (The Institute for Security and Open Methodologies). It presents a penetration testing methodology that consists of 6 sections: information security, process security, Internet technology security, communications security, wireless security and physical security. OSSTMM explores penetration testing in general and theoretical perspective and introduces a control-based methodology.

OWASP TG (Open Web Application Security Project Testing Guide): OWASP TG [17] is prepared by OWASP (Open Web Application Security Project). It presents a penetration testing methodology that consists of 10 sections: configuration and deployment management, identity management, authentication, authorization, session management, data validation, testing for error handling, testing for weak cryptography, business logic testing and client side testing. The OWASP guide merely describes web application penetration testing in a very detailed fashion including attack steps and techniques with various tools, examples and possible countermeasures.

ISSAF (Information Systems Security Assessment Framework): ISSAF [18] is prepared by Open Information Systems Security Group (OISSG). ISSAF – is a three-phase framework that aims to provide security assessment for real-world scenarios. The Second phase of ISSAF presents a penetration testing methodology consisting of 9 steps: information gathering, network mapping, vulnerability identification, penetration, gaining access and privilege escalation, enumerating further, compromise remote users/sites, maintaining access and cover tracks. Like other methodologies, ISSAF does not cover all attack vectors targeting Windows OS.

3. MICROSOFT DOMAIN ENVIRONMENT PENETRATION TEST METHODOLOGY

In this section, we present a penetration methodology for Windows domain environment. The proposed methodology includes a set of attack vectors that consists of a specific set of tools and techniques. MSDEPTM leads us to exploit the entire Windows domain.

The ultimate goal of Windows penetration testing is to gain Windows domain admin privileges and thereby get control on the entire domain components [19-21]. For example, a domain admin can login to any computer and access all files, processes, registry hives, etc. By default, the most important privileges on a local Windows machine are administrators group and SYSTEM user; in a Microsoft domain environment (i.e. active directory server) are domain admins or enterprise admins groups. Generally, during penetration tests, a pentester requests a standard user account and a computer which is provided to a new starting employee by company.

MSDEPTM consists of 10 steps as shown in Figure 1. As show in Figure 1, the proposed methodology has 2 starting points. First one is gaining local administrator (or SYSTEM) user privileges on the given computer by breaking physical security. The second start point is the network scanning step. During penetration test, critical information is collected from compromised systems (or network) and pentester tries to compromise new systems to achieve more critical information and privileged accounts. If necessary, privilege escalation attacks, pivoting, bypassing endpoint security applications can be performed to achieve this goal.

After having domain admin (or enterprise admin) privileges, some outputs of the Microsoft domain environment penetration tests are shared with other pentest concepts such as the database, web application etc., or vice versa. The details of each step along with different techniques of MSDEPTM is elaborated in the following subsections.

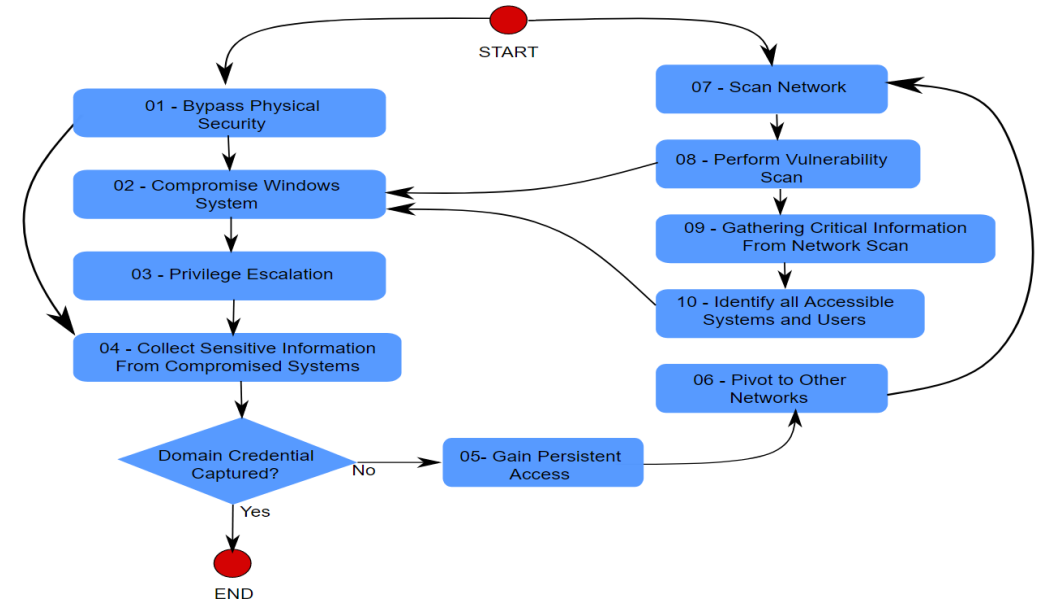

Figure 1. The overview of the proposed Microsoft domain penetration testing methodology

3.1. BYPASSING PHYSICAL SECURITY

Accessing disk system and getting SYSTEM privileges on a standard domain computer is one of the first steps in Microsoft domain environment penetration testing. To bypass physical security a Linux live image that has NTFS module can be used [22, 23]. This step can be analyzed under in two different headings: accessing disk system and accessing session.

Accessing Disk System: By accessing disk system of a PC, user and system critical files can be collected. For example, C:\Users directories or subdirectories such as desktop or downloads, backup directories, separated disk drives are important files and all of these files can be exported by accessing file disk. Besides these objects, SAM and SYSTEM files are the most important two files which hold local user names and password hashes. By exploiting these two files, pentesters can acquire local users and password hashes which are used in the following attack strategies, like pass the hash attack, and password cracking. Two main techniques can be used for this step:

- Technique - 1: samdump [24] and bkhive [25] command line tools can be used.
- Technique - 2: Ophcrack tool [26] can be used.

Accessing Session: By accessing disk system, pentesters aim to get SYSTEM privileges on the computer. After getting SYSTEM privileges, it is possible to log on this computer by a new administrator user. Three main techniques can be used for this step:

- Technique - 1: Applications that can be accessed on Windows logon screen such as sethc.exe, utilman.exe, magnify.exe, osk.exe, narrator.exe can be replaced with Windows command line tool (cmd.exe).

- Technique - 2: By using Launch Start-up Repair trick, it is possible to access disk system without using a live image. After accessing disk system, the previous technique (Technique - 1) can be performed.

- Technique - 3: It is possible to reset an administrator user password or create a new administrator user by using chntpw [27] tool.

3.2. COMPROMISING SYSTEM

By exploiting operating system, server-side application or configuration vulnerabilities, it is possible to access user or system privilege on a remote computer. It is also possible to compromise a computer by using client-side attacks, for example, web-based attacks. In this research, we only analyzed server-side vulnerabilities in three headings.

Exploiting Operating System Vulnerabilities: Remotely accessible services on Windows OS such as RemoteRPC, SAMBA shares, etc. can include some critical vulnerabilities. These vulnerabilities can be used by pentester to compromise a machine. MS03-026, MS04-007, and MS08-067 are the most common vulnerabilities in Windows services.

Exploiting Application Vulnerabilities: Third party server applications installed on Windows OS might have critical vulnerabilities. An attacker can compromise systems by exploiting these vulnerabilities. A chat and freesshed applications are examples of such kind of applications.

Exploiting Configuration Vulnerabilities: The most common vulnerability in corporate domain environment is that the IT administrators generally use the same user account with the same credentials (i.e. same username and password). The main reason behind this vulnerability is that the IT stuff employs the same disk image for all computers. By having plain text password (or

even password hash) obtained from a compromised computer, it is possible to compromise other computers by using the same credentials. Two main techniques can be used for this step:

- Technique - 1: Sysinternals' Psexec tool [28], provided by Windows, can be used to compromise remote computer by using local administrator's plain text password. However, the main limitation of psexec is that it does not support authentication with user hashes.
- Technique - 2: Metasploit Framework's (MSF) [29] psexec or psexec_psh modules can be used to compromise remote computer by using local administrator password or hash.

3.3. PRIVILEGE ESCALATION

After getting access to a computer, privilege escalation step is generally needed to access more sensitive information. Privilege escalation can be performed in various forms such as from standard local user to local administrator, from local administrator to local SYSTEM, from the SYSTEM user to a domain user, from domain user to Domain Administrator user etc. Four main techniques can be used for this step:

- Technique - 1: Sysinternals Psexec tool can be used to escalate privileges from local administrator account to SYSTEM account.
- Technique - 2: MSF bypassuac_injection module or custom scripts can be used to escalate privileges from restricted environment to less restricted one.
- Technique - 3: Operating system vulnerabilities such as MS10-015, MS13-053, MS15-051, and MS16-032 can be used to escalate privileges from standard user to SYSTEM account.
- Technique - 4: Operating system vulnerabilities such as MS14-068 can be used to escalate privileges from standard domain user to domain admin account.

It is also possible to escalate privileges by capturing tokens or passwords of logged on users. These techniques will be introduced in the subsection 3.4.

3.4. COLLECTING CRITICAL INFORMATION FROM THE COMPROMISED SYSTEM

Collecting information from a compromised system is one of the most important steps in penetration testing [30, 31]. User names, groups, domain information, password hashes of local users, currently logged on user accounts and their tokens, plain text passwords that are stored on the memory or disk can dramatically affect the success of penetration testing. This step can be analyzed with five different subtitles.

Information about Local System and Domain: One of the first steps on a compromised system is gathering information about the system. Local users (and passwords or hashes) and groups, domain objects such as domain users and groups, group policies, network shares, network information, installed applications, etc. are very useful and firstly collected by pentesters after exploiting a Windows OS.

Password Hashes and Related Files: Local or domain user's password hashes and related files - such as SAM, SYSTEM and NTDS.dit - are very important for Microsoft domain environment. The password hashes are used for pass-the-hash attacks. Windows OS allows users to authenticate to remote Windows machine by using the hash of a user's password. Besides that, these hashes can also be cracked by brute force or dictionary attacks. John the Ripper [32], Ophcrack and Cain

& Abel [33] tools can be used for cracking password hashes. Four main techniques can be used for this step:

- Technique - 1: Local administrator user can get a copy of SAM and SYSTEM file from registry hive by using a registry editing tool.
- Technique - 2: Local administrator users can get password hashes by using hacking tools such as Cain & Abel and fgdump [34].
- Technique - 3: Password hashes can be exported from SAM and SYSTEM files by using Linux Ophcrack tool, Linux samdump2 or bkhive tools, Windows Cain & Abel tool, etc.
- Technique - 4: Local or domain password hashes can be extracted by using Meterpreter hashdump command, MSF hashdump or smart_hashdump modules.
- Technique - 5: NTDS.dit and SYSTEM files can be exported by using volume shadow copy feature and domain password hashes can be extracted by esedbtools [35] and ntdsxtract [36] tools.

Tokens on Memory: Tokens impersonate users. This feature makes tokens important. Two main techniques can be used for this step:

- Technique - 1: Meterpreter commands such as steal_token and migrate or incognito extension can be used for token impersonation.
- Technique - 2: Custom Powershell scripts such as InvokeTokenManipulation [37] can be used for token impersonation.

Clear Text Passwords on Memory: Clear text passwords of logged on users can be captured from memory. Two main techniques can be used for this step:

- Technique - 1: WCE [38] and Mimikatz executable files can be used.
- Technique - 2: LSASS process dump file can be used.

Information on the Disk System: Passwords, backup files and recently used files can also be useful during the test. Three main techniques can be used for this step:

- Technique - 1: Powershell commands or scripts can be used to collect critical information from the file system.
- Technique - 2: Saved logon user credentials can be captured from applications.
- Technique - 3: Saved user credentials on group policies can be decrypted.

3.5. MAINTAINING THE PERSISTENCE

After compromising a computer system, the gaining persistent access is really beneficial while conducting pentest. Three fundamental techniques can be used for this step:

- Technique - 1: Auto start mechanisms such as Autorun, registries, services, DLLs can be used. Meterpreter persistence command is automatized for this step.
- Technique - 2: "Image File Execution Options" registry hive can be employed.

- Technique - 3: The Golden ticket that can be created by using krbtgt user password hash can be used to maintain the access to Microsoft domain environment.

3.6. PIVOTING TO UNREACHABLE NETWORKS

It is essential to further enumerate and reach to other networks and systems, which is called pivoting. Through pivoting, pentester can gain access to unreachable network via the compromised machine. Two main techniques can be used for this step:

- Technique - 1: Meterpreter route or portfwd commands, MSF autoroute post or socks4a auxiliary modules, Linux proxy chains tool [39] can be used.
- Technique - 2: Remote desktop connection or standard command line over the compromised system can be used.

3.7. NETWORK SCANNING

Identifying all computers and services offered in a network helps to compromise PCs. By default, 445/TCP and 139/TCP ports are opened on Windows systems. If remote desktop is enabled on the computer, then 3389/TCP port is opened. To discover Windows machine these ports can be scanned with the help of network scanning tools such as Nmap [40], Zenmap [41], Ncat [42], Hoping [43], etc.

3.8. VULNERABILITY SCANNING

After discovering open services on Windows systems, identifying vulnerabilities is an important step towards the hacking computer. Two main techniques can be used for this step:

- Technique - 1: Vulnerability scanners such as Nessus [44], Nexpose [45], Qualys [46] or OpenVAS [47] can be used to identify vulnerabilities on the remote computers.
- Technique - 2: Scripts such as WindowsExploit-Suggester [48] or Windows Privesc Check [49] can be used to identify vulnerabilities on the compromised system.

3.9 COLLECTING CRITICAL INFORMATION FROM NETWORK

Sometimes, domain users share sensitive information with their colleague via network shares such as SMB, NFS, FTP without using any access restriction. Moreover, some of the network services use clear text passwords in network transmission, which helps pentesters to collect them by sniffing network traffic. Two main techniques can be used for this step:

- Technique - 1: Sniffer tools like tcpdump [50], Wireshark [51], Cain & Abel, Ettercap [52] can be used to collect information on the network.
- Technique - 2: Metasploit modules, Nmap scripts, custom batches or scripts can be used to discover network shares.

3.10. IDENTIFYING ACCESSIBLE SYSTEMS AND USERS

After collecting user credentials from all compromised systems or other fields of penetration testing, pentester tries to spread on the domain environment as much as possible. Three main techniques can be used for this step:

- Technique - 1: Hydra [53], Medusa [54], Ncrack tools [55] or Crowbar (formerly known as Levye) script [56] can be used with plain text credentials to identify possibly accessible Windows computers.
- Technique - 2: MSF smb_login can be used with password hashes or plain text password to identify possibly accessible Windows systems.
- Technique - 3: MSF smb_enumusers_domain or psexec_loggedin_users modules can be used to identify logged on users on possibly accessible Windows systems

4. MITIGATIONS AGAINST MICROSOFT DOMAIN ENVIRONMENT ATTACKS

There has been a significant increase in the cyber-attacks over the past decades. Consequently, the states, companies and even individuals are obliged to secure and to defend their information carefully. The following recommendations are vital for securing Windows domain and mitigating against attacks targeting Microsoft domain environment that are discussed in Section 3.

4.1. BIOS CONFIGURATION

To protect information systems against physical security attacks, system administrators should use up-to-data BIOS firmware and enable password protection to restrict unauthorized access to BIOS configuration.

4.2. DISK ENCRYPTION

Attackers can bypass BIOS password protection by using a Dock Station. As a defender, to prevent accessing file system without authorization, the entire hard drive should be encrypted by applications such as BitLocker [57] by using hardware (such as TPM) protection.

4.3. NETWORK SEGMENTATION

Intrusion Detection Systems should be taken in place to detect and block network attacks and anomalies on the corporate network. Computers should be separated into different networks according to their security levels. For example, the following separation might be considered:

- Production, test and development servers
- Database and web application servers
- Clients and system admins
- Clients, internal servers and DMZ servers

should be separated into different networks.

4.4. SERVICE CONFIGURATION

Services that can be accessible from the public Internet increase attack surface. Therefore, system administrators should ensure that all services are configured by taking all possible safety precautions. First and foremost, unnecessary services should be disabled and all service accounts should be removed from the computer.

4.5. PASSWORD SECURITY

Passwords are the last line of defence hackers. For this reason, brute-force password guessing attacks and dictionary attacks can be effective on systems configured with easily predictable password. Thus, system administrators should ensure that a secure password policy (minimum length, complexity, change period, history, lockout, etc.) is applied via domain group policy [58].

4.6. COUNTERMEASURES AGAINST PASS THE HASH ATTACK

To avoid pass the hash attack, all local admin accounts should have different passwords. Unnecessary administrative shares, i.e. C:, $ADMIN, file and printer sharing should be disabled.

4.7. COUNTERMEASURES AGAINST CREDENTIAL THEFT ON MEMORY

Credential theft is one of the recent and important attacks. If possible, restrict privileged domain user accounts to log on to workstations, otherwise logout these accounts after finishing the task. All computers should be up-to-date systems and secured with endpoint protections.

4.8. COUNTERMEASURES AGAINST PASS THE TICKET (GOLDEN TICKET) ATTACKS

Monitoring domain controllers, especially unusual credential logons, should be considered.

4.9. BASIC CONTROLS AND HARDENINGS

System administrators should harden computers. For this reason, CIS [59], NIST [60] or TUBITAK [61] guiding documents can be used for hardening and also companies can create custom baselines to secure Windows OS.

4.10. UTILIZATION OF CRITICAL ACCOUNTS

System administrators should ensure the security of the domain critical groups such as enterprise admins or domain admins. Monitoring group membership activities, different accounts on daily tasks, delegated permissions should be considered.

4.11. PATCH MANAGEMENT

An effective patch management process can dramatically decrease attacks [62]. System administrators, security assurance team and other related teams should define period, prioritization and method of the patches by using a central patch management tool.

4.12. BACKUP MANAGEMENT

Nowadays, ransomwares increase the importance of the backups. System administrators should define period, prioritization and method of the backups by using a central backup management tool. Besides, it should not be forgotten the security of the backup files.

4.13. LOG MANAGEMENT AND MONITORING

Although there is security preventions, there is no 100% security. So it is very important to have an effective log management. Collecting log is not enough; effective correlation rules and proper alarms should be configured on the corporate network. Security operators should identify systems, prioritization, storage and collecting method of the logs and alarms by using a central log management tool. It should not be forgotten the security of the log files.

4.14. IDENTITY AND ACCESS MANAGEMENT

As workers periodically join and depart corporates and sometimes change their team security team should define access control process to grant and revoke access to computing resources. To this end, a central identity and access management tool can be used.

4.15. ACTIVE DIRECTORY AUDITS

Active Directory audits should be considered on Microsoft domain environment. At least, the following audits can be performed:

- Commonly used user accounts or service accounts
- User accounts that have not logged on for a while,
- User accounts having non-expire passwords,
- Disabled or departured users,
- User accounts that belong to 3rd parties,
- Membership of the critical users - such as Enterprise Admins, Domain Admins, Oracle Admins, Network Admins-
- Empty groups or OUs.

4.16. INFORMATION SECURITY AWARENESS

Everyone - including system administrators, third-party vendors, visitors, janitors, senior managers - on the corporate is responsible for the information security. Companies should establish and maintain information security awareness programs and senior managers should give adequate importance to information security.

4.17. Summary and Comparison In this study, we introduce a 10 step Microsoft Domain penetration testing methodology called MSDEPTM. Each steps of MSDEPTM is presented as rows in Table-1. In contrast, the countermeasures against these attacks discussed in Section 4 is presented as columns in Table 1. Table 1 summarizes the mapping of the attacks and countermeasures for Microsoft domain environment. As it is well-known fact backup management provides preventative maintenance, 12th countermeasure (e.g. backup management) is not matched with any attack step.

Table 1. Mapping of the Attacks and Mitigations For Microsoft Domain Environment

Counter Measures / Attack Vector	BIOS Configuration	Disk Encryption	Network Segmentation	Service Configuration	Password Security	Pass The Hash	Credential Theft On Memory	Pass The Ticket	Basic Controls and Hardenings	Utilization of Critical Accounts	Patch Management	Backup Management	Log Management	Access Management	Active Directory Audits	Information Security Awareness
Bypassing Physical Security	✓	✓							✓				✓			
Compromising System					✓	✓			✓		✓		✓	✓	✓	✓
Privilege Escalation				✓			✓		✓	✓	✓		✓			✓
Collecting Critical Information From The Compromised System				✓	✓		✓		✓				✓			✓
Maintaining The Persistence								✓	✓		✓		✓			
Pivoting To Unreachable Networks			✓										✓	✓		✓
Network Scanning			✓						✓				✓			
Vulnerability Scanning				✓					✓		✓		✓			
Collecting Critical Information From Network			✓		✓				✓				✓			✓
Identifying Accessible Systems and Users						✓	✓		✓	✓			✓			✓

The Microsoft Domain Environment Penetration Testing Methodology (MSDEPTM) presented in this research is compared with the state-of-the art studies (including standards, guidelines, or

methodologies) in Table 2. After all, the proposed method is the only one focused on Windows platform and discussed the attacks and their countermeasures in detail as well as the related attacking tools. As shown in Table 2, the comparison of the methodologies is done according to the following criteria.

- Owner: the owner of the specified methodology
- Last update time: the last update time of the methodology. Number of step / section: the number of the step or section in the methodology
- Different techniques: Whether the specified methodology proposes different techniques.
- Scope: The scope of the methodology
- Countermeasures: Whether the methodology includes mitigations against attacks
- Tools: Whether the specified methodology recommends the tools for attacks.

Table 2. Comparison between MSDEPTM and the state of the art pentesting methodologies

	PTES	CEH	OSSTMM	OWASP-TG	ISSAF	MSDEPTM
Owner	Group	Ec-Council	ISECOM	OWASP	OISSG	Pektas et al.
Last Update Time	2014	2016	2010	2013	2006	2017
Number of Step / Section	7	5	6	10	9	10
Different Techniques?	+	+	-	+	+	+
Scope	General	General	General	Web	General	Microsoft
Countermeasures	-	+	+	+	+	+
Tools	+	+	-	+	+	+

5. CONCLUSION

In many corporations, the majority of their systems - servers and especially client computers - are Microsoft. These systems are generally joined to Windows domain infrastructure to manage them easily. System administrators should ensure that Windows domain environment is secured with enough security precautions. Because, in case of a successful attack on the domain environment, all of these systems can be compromised by cyber criminals.

In this paper, we proposed a Microsoft domain environment penetration testing methodology called MSDEPTM. MSDEPTM presents the key metrics for penetration testing and describes the fundamental steps of Microsoft domain environment attacks from the hacker point of view, root causes of these attacks, and countermeasures against the attacks. We also compare our proposed method with the other state of the art penetration testing methodologies for emphasizing our contributions. We believe that the proposed methodology can help system admins and security operators to build secure Windows environment.

REFERENCES

[1] Mohd Ehmer, Khan, and Farmeena, Khan, (2012), "A comparative study of white box, black box and grey box testing techniques." International Journal of Advanced Computer Sciences and Applications, Vol. 3, No. 5, pp 1-12.

[2] Andrew Kerney, Zuehlke, (2017), "An Analysis of Tools, Techniques, and Mathematics Involved in a Penetration Test", B.S. Thesis, Appalachian State University.

[3] Jai Narayan, Goel and Asghar, Mohsen Hallaj and Kumar, Vivek and Pandey, Sudhir Kumar, (2016), "Ensemble based approach to increase vulnerability assessment and penetration testing accuracy", International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), pp. 330-335.

[4] Deris, Stiawan and Mohammad, Yazid Bin Idris and Abdul, Hanan Abdullah and Mohammed, AlQurashi and Rahmat, Budiarto. (2016), "Penetration Testing and Mitigation of Vulnerabilities Windows Server", IJ Network Security, Vol. 18, No. 3, pp. 501-513.

[5] Shao-Long, Wang and Jian, Wang and Chao, Feng and Zhi-Peng, Pan, (2016), "Wireless Network Penetration Testing and Security Auditing", ITM Web of Conferences, Hangzhou, Zhejiang, China, Vol. 7.

[6] Deris, Stiawan and Mohd, Idris and Abdul, Hanan Abdullah, (2015), "Penetration Testing and Network Auditing: Linux", Journal of information processing systems, Vol. 11, No. 1, pp. 104-115.

[7] Nirnay, Ghosh and Ishan, Chokshi and Mithun, Sarkar and Soumya, K Ghosh and Anil, Kumar Kaushik and Sajal, K Das, (2015), "Netsecuritas: An integrated attack graph-based security assessment tool for enterprise networks", Proceedings of the 2015 International Conference on Distributed Computing and Networking, Goa, India.

[8] Sugandh, Shah & Babu, M Mehtre, (2014), "An overview of vulnerability assessment and penetration testing techniques", Springer Journal of Computer, pp. 27-49.

[9] Emre, Caliskan, (2015), "Virtual Penetration Testing With Phase Based Vulnerability Analysis", M.S. Thesis, Middle East Technical University, The Gaduate School Of Informatics Institute.

[10] Kemal, Altundağ, (2016), "Windows kimlik doğrulama güvenlik fonksiyonu: tehditler ve önlemlerin kontrol listelerine uyarlanması", M.S. Thesis, Istanbul Sehir University, The Grad. School of Natural and Applied Science [In Turkish].

[11] Saba, Mansouri, (2016), "Network security parameters and their optimization", M.S. Thesis, Dokuz Eylül University, Computer Science.

[12] Aleatha, Shanley & Michael, N Johnstone, (2017), "Selection of penetration testing methodologies: A comparison and evaluation", 13th Australian Information Security Management Conference, Perth, Western Australia, pp. 65-72.

[13] Internet: http://www.pentest-standard.org, 28.07.2017.

[14] Internet: https://github.com/gentilkiwi/mimikatz, 22.10.2017

[15] Internet: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh , 22.10.2017

[16] Internet: http://www.isecom.org/research/osstmm.html , 22.10.2017

[17] Internet: https://www.owasp.org/images/1/19/OTGv4.pdf, 22.10.2017

[18] Internet: https://sourceforge.net/projects/isstf, 22.10.2017

[19] Mike, O'Leary, (2015), "Attacking the Domain", Cyber Operations, pp. 237-281.

[20] Halton, Wolf, & Weaver, Bo, (2016), "Kali Linux 2: Windows Penetration Testing", Packt Publishing.

[21] Daniel Dalalana, Bertoglio and Zorzo, Avelino Francisco, (2017), "Overview and open issues on penetration test", Vol. 23, No. 1, pp 2-16.

[22] Mikko, Vatanen, (2014), "Intrusion Detection During IT Security Audits", M.S Thesis, Jamk University of Applied Sciences

[23] Jesse, Varsalone & McFadden, Matthew, (2011), "Defense Against the Black Arts: How Hackers Do what They Do and how to Protect Against it", CRC Press Publishing.

[24] Internet: http://http.us.debian.org/debian/pool/main/s/samdump2/ , 22.10.2017

[25] Internet: http://http.us.debian.org/debian/pool/main/b/bkhive/ , 22.10.2017

[26] Internet: http://ophcrack.sourceforge.net/ , 22.10.2017

[27] Internet: http://www.chntpw.com/download/ , 22.10.2017

[28] Internet: https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx , 22.10.2017

[29] Internet: https://www.metasploit.com , 22.10.2017

[30] Oriyano, Sean-Philip, (2016), "CEH v9: Certified Ethical Hacker Version 9 Study Guide", John Wiley & Sons. Publishing.

[31] Filip, Holik and Horalek, Josef and Marik, Ondrej and Neradova, Sona and Zitta, Stanislav, "Effective penetration testing with Metasploit framework and methodologies", IEEE 15th International Symposium onComputational Intelligence and Informatics (CINTI), pp. 237-242.

[32] Internet: www.openwall.com/john , 22.10.2017

[33] Internet: http://www.oxid.it/cain.html , 22.10.2017

[34] Internet: http://sectools.org/tool/fgdump/ , 22.10.2017

[35] Internet: https://github.com/libyal/libesedb/tree/master/esedbtools , 22.10.2017

[36] Internet: http://www.ntdsxtract.com/ , 22.10.2017

[37] Internet: https://github.com/clymb3r/PowerShell/blob/master/Invoke-TokenManipulation/Invoke-TokenManipulation.ps1 , 22.10.2017

[38] Internet: www.ampliasecurity.com/research/windows-credentials-editor/ , 22.10.2017

[39] Internet: http://proxychains.sourceforge.net/ , 22.10.2017

[40] Internet: https://nmap.org/ , 22.10.2017

[41] Internet: https://nmap.org/zenmap/ , 22.10.2017

[42] Internet: https://nmap.org/ncat/ , 22.10.2017

[43] Internet: http://www.hping.org/hping3.html , 22.10.2017

[44] Internet: http://www.tenable.com/products/nessus-vulnerability-scanner , 22.10.2017

[45] Internet: https://www.rapid7.com/products/nexpose , 22.10.2017

[46] Internet: https://www.qualys.com/ , 22.10.2017

[47] Internet: www.openvas.org/ , 22.10.2017

[48] Internet: https://github.com/GDSSecurity/Windows-Exploit-Suggester , 22.10.2017

[49] Internet: https://github.com/pentestmonkey/windows-privesc-check , 22.10.2017

[50] Internet: www.tcpdump.org/ , 22.10.2017

[51] Internet: https://www.wireshark.org/ , 22.10.2017

[52] Internet: https://ettercap.github.io/ettercap/ , 22.10.2017

[53] Internet: https://www.thc.org/thc-hydra/ , 22.10.2017

[54] Internet: http://foofus.net/goons/jmk/medusa/medusa.html , 22.10.2017

[55] Internet: https://nmap.org/ncrack , 22.10.2017

[56] Internet: https://github.com/galkan/crowbar , 22.10.2017

[57] Sven, Türpe, Andreas, Poller, Jan, Steffan, Jan-Peter, Stotz, Jan, Trukenmüller, (2009), "Attacking the bitlocker boot process", International Conference on Trusted Computing. Oxford, UK, pp. 183–196.

[58] Karen Scarfone & Murugiah Souppaya, (2017), "Guide to enterprise password management", NIST Special Publication.

[59] Internet: https://benchmarks.cisecurity.org/downloads/benchmarks , 22.10.2017

[60] Internet: https://web.nvd.nist.gov/view/ncp/repository , 22.10.2017

[61] Internet: https://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar-3.html , 22.10.2017

[62] Karen, Kent & Murugiah, Souppaya, (2006) "Guide to computer security log management", NIST Special Publication.

Authors

Abdurrahman Pektaş received his B.Sc. and M Sc. at Galatasaray University and his PhD at the University of Joseph Fourier, all in computer engineering, in 200 9, 2012 and 2015, respectively. He is a senior researcher at Galatasaray University. His research interests are analysis, detection and classification of malicious software, machine learning and security analysis tool development.

Ertuğrul Başaranoğlu received his B.Sc. at Galatasaray University and his in computer engineering at Istanbul Sehir University in 2010 and 2016, respectively. He is senior penetration testing and security expert at Ziraat Technology. His research interests are application security, reverse engineering and penetration testing.

.