Ausarbeitung ITSI - Pentesting

Latschbacher Lukas

April 30, 2024

Contents

1 Einleitung

In einer zunehmend digitalisierten Welt, in der Daten die Währung sind und Sicherheitsverletzungen täglich Schlagzeilen machen, ist der Schutz von Informationssystemen von entscheidender Bedeutung. Unternehmen, Regierungen und Organisationen sind sich der Notwendigkeit bewusst, ihre IT-Infrastruktur auf potenzielle Schwachstellen zu prüfen, um sich gegen Cyberangriffe zu verteidigen. In diesem Zusammenhang nimmt das Penetration Testing eine zentrale Rolle ein. Diese Ausarbeitung widmet sich daher der eingehenden Betrachtung des Penetration Testings im Kontext der IT-Sicherheit, insbesondere unter Berücksichtigung der Windows-Plattform.

Penetration Testing, auch bekannt als Ethical Hacking, ist eine proaktive Methode zur Identifizierung von Sicherheitslücken in einem Informationssystem. Dabei wird versucht, wie ein potenzieller Angreifer vorzugehen, um Schwachstellen aufzudecken, bevor sie von bösartigen Akteuren ausgenutzt werden können. Die Durchführung eines Penetration Tests erfordert ein tiefgreifendes Verständnis der zugrunde liegenden Technologien und Angriffstechniken sowie eine sorgfältige Planung und Durchführung, um die Integrität und Vertraulichkeit der getesteten Systeme zu wahren.

Insbesondere die Sicherheit von Windows-Systemen steht im Fokus vieler Organisationen, da Windows das am weitesten verbreitete Betriebssystem in Unternehmensumgebungen ist. Die Komplexität und Vielfalt von Windows-Systemen bieten sowohl Chancen als auch Herausforderungen für Sicherheitsfachleute. Daher ist es unerlässlich, ein fundiertes Verständnis der Windows-Sicherheitsmechanismen sowie der gängigen Angriffsmethoden zu entwickeln, um effektive Schutzmaßnahmen zu implementieren und Sicherheitsvorfälle zu verhindern.

Im Rahmen dieser Ausarbeitung werden wir zunächst die Grundlagen des Penetration Testings erläutern, einschließlich seiner Ziele, Methoden und Phasen. Anschließend werden wir uns eingehend mit der Sicherheit von Windows-Systemen befassen, indem wir potenzielle Angriffsvektoren identifizieren, Sicherheitsmechanismen analysieren und bewährte Praktiken zur Stärkung der Windows-Sicherheit diskutieren. Durch die Kombination von theoretischem Wissen und praktischen Einblicken wollen wir einen umfassenden Überblick über die Rolle des Penetration Testings im Kontext der Windows-Sicherheit bieten und damit einen wertvollen Beitrag zur IT-Sicherheit leisten.

2 Grundlagen von Pentesting

Penetrationtesting oder auch Pentesting ist dafür um Sicherheitslücken in IT-Systemen aufzufinden. Nicht nur Sicherheitslücken sondern auch die Schwierigkeit in ein System einzudringen wird durch einen Pentest bestimmt. Dadurch soll die Sicherheit erhöht werden und vor zukünftigen Angriffen geschützt werden. Sie werden von sogenannten "ethisch Hackern" durchgeführt, welche mit einer Genehmigung der Eigentümer Systeme angreifen um Securityissues aufzuspüren, damit diese danach behoben werden können. Die Angriffe finden mit den selben Methoden wie bei Angriffen von nicht ethischen Hackern statt. Weiters gibt es verschiedene Arten von Pentests, welche in einem der folgenden Kapitel erklärt werden.

2.1 Tools für Pentests

2.1.1 Vulnerability Scans

In der folgenden Auflistung befinden sich die besten Tools für Vulnerability Scans

- Acunetix ist ein Web-Vulnerability-Scanner, der über fortschrittliche Crawling-Technologie verfügt, um Schwachstellen zu finden und jeden Typ von Webseite zu durchsuchen – selbst solche, die passwortgeschützt sind.
- Wireshark ist ein kostenloses und Open-Source-Paketanalysetool. Es wird für Netzwerkfehlerbehebung, Analyse, Software- und Kommunikationsprotokollentwicklung sowie für Bildungszwecke verwendet. Ursprünglich hieß das Projekt Ethereal, wurde jedoch im Mai 2006 aufgrund von Markenproblemen in Wireshark umbenannt.
- Das Metasploit-Projekt ist ein Computersicherheitsprojekt, das Informationen über Sicherheitslücken bereitstellt und bei Penetrationstests und der Entwicklung von IDS-Signaturen hilft. Es gehört der Sicherheitsfirma Rapid7 mit Sitz in Boston, Massachusetts.
- OpenVAS ist ein Open-Source-Schwachstellen-Scanner, der von Greenbone Networks gepflegt wird. Der Scanner verfügt auch über einen regelmäßig aktualisierten Community-Feed, der über 50.000 Schwachstellentests enthält.
- John the Ripper ist ein kostenloses Passwortcracking-Software-Tool. Ursprünglich für das Unix-Betriebssystem entwickelt, kann es auf fünfzehn verschiedenen Plattformen ausgeführt werden.
- sqlmap ist ein Software-Dienstprogramm zur automatischen Entdeckung von SQL-Injektions-Sicherheitslücken in Webanwendungen.
- Burp Suite ist ein Web-Schwachstellen-Scanner, der häufig aktualisiert wird und sich mit Bug-Tracking-Systemen wie Jira integriert, um einfache Ticketgenerierung zu ermöglichen.

- Aircrack-ng ist eine Netzwerk-Software-Suite, die aus einem Detektor, einem Packetsniffer, einem WEP- und WPA/WPA2-PSK-Knacker sowie einem Analysetool für 802.11 Wireless LANs besteht. Es funktioniert mit jedem drahtlosen Netzwerk-Interface-Controller, dessen Treiber den Raw-Monitoring-Modus unterstützt und kann 802.11a, 802.11b und 802.11g Traffic abhören.

- Nessus ist einer der beliebtesten Schwachstellen-Scanner mit über zwei Millionen Downloads weltweit. Darüber hinaus bietet Nessus umfassende Abdeckung und scannt über 59.000 CVEs.

2.1.2 Port Scanning

- Nmap ist ein gratis open source security scanner, der auch von Organisationen für Netzwerkentdeckung, Bestandsaufnahme, Verwaltung von Service-Upgrade-Zeitplänen und Überwachung der Verfügbarkeit von Hosts oder Diensten verwendet wird. Die Features von Nmap sind active port scanning, host discovery, OS detection und application version detection. Active Port scanning erlaubt es in einem Netzwerk beziehungsweise bei bestimmten Hosts nach offenen Ports zu suchen. Host discovery kann Hosts die auf network requests reagieren identifizieren. OS detection kann das Betriebsystem und die Version eines Hosts herausfinden. Dabei können auch Details über das Netzwerk herausgefunden werden. Die Application Version detection kann herausfinden welche Apps laufen und welche Version diese haben.

- Unicornscan ist für die Features des asynchronen TCP und UDP scanning mit den ungewöhnlichen Scanpatterns bekannt. Diese bieten alternative Wege um Details über remote Betriebssysteme herauszufinden. Unicornscans Features sind asynchrones, stateless TCP scanning, asynchrones UDP scanning und ein IP port Scanner. Weiters hat die Software wie zuvor erwähnt das Feature aus der ferne das Betriebssystem und die Version dieses zu bestimmen.

- Angry IP Scanner ist ein kostenloses, plattformübergreifendes Netzwerk-Scan-tool, das für seine schnelle Scangeschwindigkeit dank seines Ansatzes mit mehreren Threads bekannt ist, der jeden Scan separat durchführt. Es benötigt keinen Installationsvorgang und kann einfach heruntergeladen und ausgeführt werden. Mit Angry IP Scanner können offene Ports in jedem entfernten Netzwerk gescannt werden, und es kann auch Webserver- und NetBIOS-Informationen erkennen. Die Ergebnisse des Scans können in TXT-, XML- oder CSV-Dateien exportiert werden, und es ermöglicht eine einfache Plugin-Integration mit der Java-Sprache.

- Netcat ist eines der ältesten Nezwerk-Scan-Tools, die letzte offizielle Version ist aus dem Jahr 2004. Jedoch gibt es mehrere Varianten die auf modernen Systemen funktionieren. Netcat kann TCP und UDP Ports

scannen, hat einen eingebauten Port-Scanner und kann über die Commandline benutzt werdne. Weiters sind verschiedene Varianten für Windows, Linux und macOS verfügbar.

- Zenmap ist das offizielle GUI für Nmap für Personen, die nicht die Commandline verwenden möchten. Die Scanergebnisse werden in einer Datenbankgespeichert, die danach durchsucht werden kann. Neue Scanergebnisse können mit früheren verglichen werden. Weiters können Port-Scan-Profile für häufig verwendete Porterkennungsoptionen gespeichert werden. Die restlichen Features sind gleich wie bei Nmap, da Zenmap nur ein GUI für Nmap ist.

2.2 Arten von Pentests

Die verschiedenen Arten von Pentests unterscheiden sich bei den Kosten, der Gründlichkeit und der Menge der vorgegebenen Informationen.

2.2.1 Black Box

Bei einem Black Box Penetrationstest bekommt der Pentester im Vorfeld keine Informationen über das zu testende Objekt. Bei dieser Art von Pentest müssen alle Informationen von der Testerin oder dem Tester herausgefunden werden. Diese Art kommt einem wirklichen Angriff am nächsten, ist aber dafür auch am aufwendigsten und teuersten.

2.2.2 Gray Box

Der Grey Box Pentest ist eine Kombination aus White Box und Black Box Test. Es werden der testenden Person grundlegende Informationen wie IP-Adressen, Domains und Benutzeraccounts gegeben. Das beschleunigt und vergünstigt den Test, da die Pentesterin oder der Pentester nicht nach diesen Informationen suchen muss. In der Praxis ist das die gängigste Form des Penetrationtests, da diese Art die Balance zwischen Effizienz, Gründlichkeit und Kosten hält.

2.2.3 White Box

Bei einem White Box Test werden der Testerin oder dem Tester Informationen über das Prüfobjekt wie Code, Domains, IP-Adressen, Benutzeraccounts oder auch Angaben über die Architektur des zu testenden Objekts bereitgestellt. Weiters ist diese Art des Tests auch sehr gründlich, daher auch sehr teuer.

2.2.4 Red Team Assessment

Bei einem Red Team Assessment Test werden alle verfügbaren Methoden und Techniken verwendet um ein System anzugreifen, daher ist diese Methode ein sehr ressourcenintensives Vorgehen, deshalb kommt es selten zum Einsatz.

2.2.5 Social-Engineering-Pentest

Bei dieser Art von Pentest werden nicht nur die herkömmlichen Methoden eines Penetrationstests verwendet, sondern es werden auch durch Social Engineering über die Mitarbeiter Informationen erlangt. Diese Tests sind darauf ausgelegt Schwachstellen in Unternehmen zu finden, welche im Nachhinein durch Schulungen von Mitarbeitenden behoben werden um ernsthafte Angriffe zu erschweren.

2.3 Phasen eines Pentests

Die meisten Pentests haben die folgenden Schritte. Diese sind für einen gründlichen und effizienten Penetrationstest notwendig.

2.3.1 Vorbereitung

Im ersten Schritt wird der Umfang des Tests ermittelt. Der Kunde und der Tester besprechen welche Objekte zu testen sind, welchen Umfang die Tests haben und wo die Grenzen liegen. Das wird mit einem Dokument vereinbart und eine Einverständniserklärung des Auftraggebers über die Tests wird dem Auftragnehmen gegeben. Es ist wichtig, dass der Umfang der Tests festgelegt ist, damit nicht möglicherweise schon bekannte Schwachstellen gefunden werden, die ohnehin schon bekannt sind, anstatt neue Schachstellen zu finden.

2.3.2 Informationsbeschaffung

Bei der Informationsbeschaffung sucht die Testerin oder der Tester nach Informationen über de Netzwerke, Domain Namen, Server und weitere Elemente um das System zu verstehen. Es werden so viele Daten wie möglich gesammelt um eine effektive Strategie zu erstellen.

2.3.3 Bewertung der Ergebnisse

In diesem Schritt werden die zuvor gesammelten Informationen bewertet um eine effektive Strategie zu erstellen. Danach wird eine Strategie erstellt und Tools ausgewählt, welche für den Test verwendet werden.

2.3.4 Angriffsversuch

Im 4. Schritt wird versucht Zugriff auf das System zu erhalten, indem alle Schwachstellen ausgenutzt werden, die zuvor gefunden wurden. Die Arten der Angriffe werden, wie in der zuvor erstellten Strategie festgelegt durchgeführt. Dies richtet sich danach, welche Art von Systemen und Schwachstellen ermittelt werden konnten. Nachdem ein erfolgreicher Zugriff erlangt wurde, wird der Zugriff genutzt um Daten zu stehlen, Netzwerk Traffic abzufangen oder Nutzerrechte zu verändern. Diese Daten werden dazu bentuzt um zu evaluieren, wie groß der Schaden ist, der angerichtet werden könnte, wenn diese Schwachstellen ausgenutzt werden.

2.3.5 Verfassung eines Berichts

Der letzte Schritt ist einen Bericht über die durchgeführten Tests zu verfassen. Dieser Bericht beinhaltet normalerweise Schwachstellen, welche Hacker nutzen könnten um Zugriff auf das System zu erlangen. Weiters auch Sensible Daten, die gestohlen werden könntne und Zeitangeben, wie lange es bräuchte um unerkannt im System schaden anrichten zu können.

2.3.6 Abschluss

Nachdem der Bericht verfasst wurde, wird dieser dem Auftraggeber übergeben. Dieser wird genutzt um die gefunden Schwachstellen zu beheben und Sicherheitsupgrades zu implementieren. Das sind zum Beispiel Durchsatzbegrenzungen, DDoS-Abwehr oder auch strengere Formularvalidierungen und -bereinigungen.

3 Windows Sicherheit

3.1 Windows Sicherheitsarchitektur

3.1.1 Benutzerkontensteuerung

Die Benutzerkontensteuerung (User Account Control (UAC)) ist ein seit Windows Vista eingebauter Sicherheitsmechanismus. Diese Funktion wurde eingeführt, weil viele User mit Admin Privilegien arbeiten und das auf gestartete Anwendungen übertragen wurden. Das stellt ein großes Sicherheitsrisiko dar, weil auch Malware so mit Adminrechten agieren kann. Mit der UAC erhalten alle Programme nur Rechte eines normalen Nutzers, egal welche Rechte der aktive User hat. Bei Bedarf können dem Programm mehr Rechte zugeschrieben werden, das ist durch ein Fenster mit einem Button gelöst. Dieser Mechanismus ist mit dem sudo in UNIX Systemen zu vergleichen.

3.1.2 Integrierte Sicherheitsfunktionen

Seit der neuesten Version von Windows wird mit dem Prinzip "Vertraue niemandem" vorgegangen. Das heißt, dass keine Apps und Programme vertrauenswürdig sind, solange das nicht nachgewiesen ist. Das Konzept beginnt beim Start von Windows 11. Dabei sorgt das TPM (Trusted Plattform Module) zusammen mit Secure Boot und UEFI dafür, dass das OS nur startet, wenn es nicht manipuliert wurde. TPM ist ein zusätzlicher Chip, der mittels Kryptografieschlüssel überprüft, ob das OS und die Firmware auch die Richtigen sind nicht etwas anderes, was es nur vorgibt OS oder Firmware zu sein.

3.1.3 Verschlüsselung

In Windows gibt es zur Verschlüsselung der Daten den sogenannten "BitLocker". Dieser ist auf dem Windows Laufwerk installiert und kann den ganzen PC oder einzelne Laufwerke verschlüsseln. Ein Passwort kann gesetzt werden um die Verschlüsselung aufzuheben und unbefugten Zugriff zu vermeiden. Der BitLocker beruht auf der Verwendung eines Hardwareelements namens TPM. Der Bitlocker erstellt einen Wiederherstellungschlüssel für die Festplatte, sodass beim Einschalten des Computers ein PIN erforderlich ist, um Zugriff zu erhalten. Außerdem gibt einen Wiederherstellungsschlüssel, der verwendet werden kann, wenn das Passwort vergessen wird.

3.1.4 Authentifizierung und Zugriffskontrolle

In Windows gibt es mehrere Authentifizierungsmöglichkeiten die als Zugriffskontrolle auf Elemente und Dateien dienen.

Für die Zugriffskontrolle mit einem Passwort gibt es Passwortrichtlinien. Für Passwörter für normale User gibt es keine festgelegten Richtlinien in Windows, jedoch können Systemadministratoren Passwortrichtlinien festlegen. Dabei gibt seitens Microsoft Empfehlungen, welche besagen, dass Passwörter mindestens

acht Zeichen lang sein sollen, gängige Passwörter wie 1234 verboten werden sollten und eine Registrierung für eine Multifaktorauthentifizierung erzwungen wird.

Weiters gibt es die Multifaktorauthentifizierung (MFA), welche mehrere Identitätsnachweise wie Tokens, biometrische Daten oder Passwörter erfordert.

Die Zugriffskontrolle kann vom Systemadministrator konfiguriert werden. Es können Usergruppen erstellt werden, um sicherzugehen, dass nur autorisierte User auf bestimmte Ressourcen zugreifen können und dass der Zugriff auf sensible Daten eingeschränkt ist.

3.1.5 Patch-Management

Patch-Management in Windows ist der Prozess der Verwaltung und Bereitstellung von Software-Updates, um Sicherheitslücken zu schließen, Fehler zu beheben und die Systemstabilität zu verbessern. Es umfasst die Identifizierung von Schwachstellen, die Planung von Patch-Zyklen, das Testen von Patches, die Bereitstellung auf produktiven Systemen, die Überwachung der Patch-Compliance und gegebenenfalls das Rückgängigmachen von Patches bei Problemen. Ein effektives Patch-Management ist entscheidend, um die Sicherheit und Leistung von Windows-Systemen zu gewährleisten.

3.1.6 Sicherheitsüberwachung und Protokollierung

Durch Ereignisprotokolle werden zum Beispiel Anmeldeversuche, Zugriffsfehler oder Änderungen an kritischen Systemeinstellung aufgezeichnet und gespeichert. Um zu garantieren, dass diese Protokolle nicht gelöscht werden oder durch Fehler verschwinden sollten diese auf einem anderen System gespeichert werden, damit im Ernstfall ein Backup davon besteht. Es kann auch festgelegt werden was protokolliert wird. Es können folgende Ereignisse in der Protokollierung aktiviert werden. Das sind Account Logon, Account Management, Detailed Tracking, DS Access, Logon/Logoff, Object Access, Policy Change, Privilege Use, Syste und Global Object Access Auditing.

3.1.7 Virtualisierung und Isolation

Virtualisierungsbasierte Sicherheit (VBS) nutzt Hardwarevirtualisierung und den Windows Hypervisor, um eine isolierte virtuelle Umgebung für das Hosten von Sicherheitslösungen zu schaffen und so Schutz vor Schwachstellen im Betriebssystem zu bieten. Es gibt 2 verschiedene Isolationsmodi, Prozessisolation und Hyper-V-Isolierung. Bei der Prozessisolation werden pro Container verschiedene Namespaces isoliert, das sind das Dateisystem, die Registrierung, die Netzwerkports, Prozess und Thread-ID-Bereich und der Objekt-Manager-Namespace. Die Hyper-V-Isolierung bietet eine erhöhte Sicherheit und umfassende Kompatibilität zwischen Host- und Containerversion. Dabei werden mehrere Containerinstanzen gleichzeitig auf dem Host ausgeführt, wobei jeder Container innerhalb eines hochgradig optimierten virtuellen Computer ausgeführt und erhält seinen eigenen Kernel. Durch den virtualisierten Computer

kann die Isolation auf Hardwareebene zwischen den einzelnen Containern und dem Host stattfinden.

3.1.8 Sicherheitsrichtlinien und Compliance

3.2 Methoden des Pentestings in Windows

3.2.1 Netzwerk-Pentesting

3.2.2 Web-Pentesting

3.2.3 Angriff auf die Benutzerkontensteuerung (UAC) und privilegierte Eskalation

3.2.4 Social Engineering-Angriffe gegen Windows-Benutzer

3.3 Praxisbeispiele

4 Stichwörter

4.1 Cloud Computing und Internet of Things

4.2 Automatisierung, Regelung und Steuerung

4.3 Security, Safety, Availability

4.4 Authentication, Authorization, Accounting

4.5 Algorithmen und Protokolle

4.6 Konsistenz, Datenstruktur und Visualisierung