Pen Testing und Schwachstellen-Scanning

Kurzreferenz

Version: 1.0

Überarbeitet: Juni 2023

Inhalt

Einführung

Wenn es darum geht, die Sicherheit der Systeme und Netze eines Unternehmens zu bewerten, werden häufig zwei Methoden eingesetzt: Penetrationstests ("Pen Testing") und Schwachstellen-Scans.

Sie haben zwar das gleiche Ziel, nämlich Schwachstellen in einem System aufzudecken, unterscheiden sich aber in ihren Ansätzen und Zielen. Dieser Leitfaden soll als Kurzreferenz dienen, um den Unterschied zwischen Pen-Tests und Schwachstellen-Scans zu verstehen.

Definition von Penetrationstests

Beim Penetrationstest, der oft auch als ethisches oder "White Hat"-Hacking bezeichnet wird, werden reale Angriffe auf einem System oder Netzwerk simuliert, um Schwachstellen zu ermitteln und die potenziellen Auswirkungen dieser zu bestimmen.

Hier sind die wichtigsten Punkte:

- **Ziel** - Das Hauptziel von Penetrationstests besteht darin, Schwachstellen auszunutzen und sich unbefugten Zugang zu Systemen oder sensiblen Daten zu verschaffen, um den Grad des Risikos und die Wirksamkeit von Sicherheitsmaßnahmen zu bewerten.
- **Vorgehensweise** - Pen-Tester verwenden verschiedene Techniken, Tools und Methoden, um reale Angriffe nachzuahmen und die Aktionen eines tatsächlichen Hackers zu simulieren.
- **Varianten** - Pen-Tests können sowohl aus interner als auch aus externer Sicht durchgeführt werden. Bei internen Pen-Tests werden die Sicherheitsmaßnahmen innerhalb eines Netzwerks, z. B. von Servern und Workstations, bewertet. Bei externen Pen-Tests wird die Sicherheit von Systemen bewertet, auf die über das Internet zugegriffen werden kann, z. B. Websites oder Cloud-Infrastrukturen.

Bei einem Pen-Test kann versucht werden, sich unbefugten Zugang zum Reservierungssystem des Hotels zu verschaffen, Gästebuchungen zu manipulieren oder Schwachstellen im Wi-Fi-Netzwerk auszunutzen, um Gästedaten abzufangen.

Schwachstellen-Scanning

Schwachstellen-Scanning ist ein Prozess, der potenzielle Schwachstellen in einem System oder Netzwerk identifiziert und meldet. Der Schwerpunkt liegt dabei auf der Erkennung von Sicherheitsschwachstellen, Fehlkonfigurationen oder veralteten Softwareversionen.

Berücksichtigen Sie die folgenden Aspekte:

- **Zielsetzung** - Das Scannen zielt darauf ab, bekannte Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Sie liefern eine Momentaufnahme der Sicherheitslage des Systems zu einem bestimmten Zeitpunkt.
- **Ansatz** - Schwachstellen-Scanner automatisieren den Prozess des Scannens von Systemen oder Netzwerken, um Schwachstellen zu entdecken, indem sie diese mit einer Datenbank bekannter Schwachstellen vergleichen.
- **Varianten** - Schwachstellen-Scans können sowohl intern als auch extern durchgeführt werden. Beim internen Schwachstellen-Scanning wird die Sicherheitslage der Systeme innerhalb des Netzwerks bewertet, während sich das externe auf Systeme konzentriert, die dem Internet ausgesetzt sind, wie z. B. öffentlich zugängliche Webserver.

Im Gastgewerbe könnte ein Schwachstellen-Scan beinhalten, dass das Netzwerk eines Hotels auf veraltete Software-Versionen, ungepatchte Systeme oder falsch konfigurierte Firewalls gescannt wird, die einem Hacker möglicherweise einen Einstiegspunkt bieten könnten.

Unterschiede

Pen-Tests und Schwachstellen-Scans unterscheiden sich in mehreren Bereichen. Sie sind in der folgenden Tabelle zusammengefasst.

Bereich	Pen Testing	Schwachstellen-Scanning

Hacker	Mensch (ethische Hacker).	Automatisierte Tools oder Scanner.
Tiefe	Eingehende Analyse zur Ermittlung der Auswirkungen von Schwachstellen und der potenziellen Gefahrenzone.	Oberflächliche Identifizierung von Schwachstellen keine detaillierte Analyse der Auswirkungen.
Schwerpunkt	Betonung von Sicherheitsmängeln und Schwachstellen, die den Menschen betreffen.	Der Schwerpunkt liegt auf technischen Schwachstellen und Fehlkonfigurationen.
Methode	Systematisches und gezieltes Vorgehen, um Schwachstellen auszunutzen, Privilegien zu erweitern und sich unbefugten Zugang zu verschaffen.	Verwendet vordefinierte Signaturen und Muster, um Schwachstellen zu identifizieren.
Echtzeit	Hat die Fähigkeit, neue Schwachstellen zu identifizieren, die von Scannern möglicherweise nicht erkannt werden.	Eingeschränkte Fähigkeit, neue oder Zero-Day-Schwachstellen zu identifizieren, die nicht in der Datenbank des Scanners enthalten sind.
Ziel	Systeme, Netzwerke und Geräte innerhalb der Infrastruktur des Unternehmens.	Systeme, Netzwerke, Webanwendungen und Geräte, die mit dem Netzwerk verbunden oder dem Internet ausgesetzt sind.

Gemeinsamkeiten

Obwohl Pen-Tests und Schwachstellen-Scans viele Unterschiede aufweisen, haben sie auch bedeutende Gemeinsamkeiten. Zu diesen gehören:

- **Unterstützung von Unternehmen bei der Verbesserung ihrer Sicherheitslage**. Beide helfen Unternehmen, ihre allgemeine Sicherheit zu verbessern, indem sie Schwachstellen aufdecken, die von Angreifern ausgenutzt werden könnten. Durch die Behebung dieser können Unternehmen potenzielle Bedrohungen abmildern und ihren Schutz verbessern.

- **Sie tragen zu einer umfassenden Sicherheitsbewertungsstrategie bei**. Während sich Pen-Tests auf die aktive Ausnutzung von Schwachstellen durch simulierte Angriffe konzentrieren, bietet das Schwachstellen-Scanning einen systematischen und automatisierten Ansatz zur Identifizierung bekannter Schwachstellen. Zusammen bieten sie ein umfassenderes Verständnis der Sicherheitslandschaft eines Unternehmens.

- **Einhaltung des PCI DSS**. Pen-Tests und Schwachstellen-Scans sind im PCI DSS für Unternehmen, die mit Zahlungskartendaten arbeiten, ausdrücklich vorgeschrieben. Anforderung 11.2 schreibt regelmäßige interne und externe Scans vor, um potenzielle Schwachstellen zu identifizieren, und Anforderung 11.2.1 besagt, dass Unternehmen vierteljährlich externe Scans durch einen zugelassenen Scanning-Anbieter (ASV) durchführen müssen. Darüber hinaus schreibt Anforderung 11.3 vor, dass Organisationen jährlich oder nach wesentlichen Änderungen am Netzwerk oder an den Anwendungen Pen-Tests durchführen müssen.

- **Regelmäßige Bewertungen erforderlich**. Sowohl Pen-Tests als auch Schwachstellen-Scans erfordern regelmäßige Bewertungen, um eine kontinuierliche Sicherheit zu gewährleisten. Die Bedrohungslandschaft entwickelt sich ständig weiter, es entstehen neue Schwachstellen und die Systeme werden aktualisiert. Regelmäßige Evaluierungen helfen Unternehmen, potenziellen Risiken einen Schritt voraus zu sein.

- **Unterstützung bei der Identifizierung von Schwachstellen**. Beide Methoden sind wirksam bei der Identifizierung von Schwachstellen, bevor sie von böswilligen Hackern ausgenutzt werden. Pen-Tests nutzen verschiedene Techniken, um Schwachstellen zu identifizieren und auszunutzen, während Schwachstellen-Scans automatisierte Tools und Datenbanken verwenden, um bekannte Probleme zu erkennen.

- **Bereitstellung von Berichten mit Vorschlägen für Abhilfemaßnahmen**. Beide erstellen Berichte, in denen die erkannten Schwachstellen beschrieben und Abhilfemaßnahmen vorgeschlagen werden. Jene geben Aufschluss über die entdeckten Schwachstellen und enthalten Hinweise, wie sie zu beseitigen oder zu entschärfen sind.

- **Erforderliche Folgemaßnahmen**. Sowohl Pen-Tests als auch Schwachstellen-Scans können Folgemaßnahmen zur Behebung der festgestellten Probleme erforderlich machen. Die bloße Identifizierung von Schwachstellen reicht nicht aus; Unternehmen müssen Maßnahmen ergreifen, um diese Risiken zu beseitigen und abzumildern. Zu den Folgemaßnahmen kann die Anwendung von Patches, die Aktualisierung von Konfigurationen, die Verbesserung von Sicherheitskontrollen oder die Implementierung zusätzlicher Schutzmaßnahmen zur Behebung der identifizierten Schwachstellen gehören.

Durch die Nutzung dieser Gemeinsamkeiten können Unternehmen sowohl Pen-Tests als auch Schwachstellen-Scans als ergänzende Ansätze zum Schutz vor Bedrohungen einsetzen.

Schlussfolgerung

Penetrationstests und Schwachstellenscans sind wesentliche Bestandteile einer umfassenden Sicherheitsbewertungsstrategie.

Während Penetrationstests darauf abzielen, reale Angriffe nachzuahmen und Schwachstellen auszunutzen, um das Risiko und die Wirksamkeit der Sicherheit zu bewerten, konzentriert sich das Scannen von Schwachstellen auf die Identifizierung bekannter Schwachstellen und Fehlkonfigurationen.

Beide Methoden spielen eine entscheidende Rolle bei der proaktiven Sicherung von Systemen und Netzwerken und ermöglichen es Organisationen im Gastgewerbe, wie z. B. Hotels, potenzielle Schwachstellen zu erkennen und zu beheben, bevor sie von böswilligen Akteuren ausgenutzt werden.

Über Venza

Venza ist ein führender Anbieter von Sicherheits- und Datenschutzlösungen, die das Gastgewerbe unterstützen, Schwachstellen zu beseitigen und die Einhaltung von Vorschriften zu gewährleisten. Venza hilft mehr als 2000 Hotels weltweit und schützt Gäste und ihre Daten mit 360-Grad-Transparenz und proaktivem Risikomanagement vor Sicherheitsverletzungen. So können sich Hotelmanager auf den Gästeservice konzentrieren und das Vertrauen in ihre Marke stärken.

Besuchen Sie www.venza.io für weitere Details.

Kontact

Vertrieb: sales@venza.io

Kundenerfolg: success@venza.io