syracom
business efficiency engineering

Whitepaper | Pentest

Automatisierte Pentests als proaktive Cyber-Resilience-Taktik

brandeins /thema
2020 Heft 15
Beste Unternehmens-berater

Part of Consileon Group

Inhalt

Einführung / Problemstellung

Was ist Cyber Resilience?

Cyber Resilience beschreibt die Widerstands- und Anpassungsfähigkeit eines Unternehmens bezüglich Cyberangriffen, dem Ausfall von Systemkomponenten und Gefahren aus dem Netz. Damit spielen sowohl die Sicherheit vor Angriffen als auch der Umgang direkt während und nach einem Cyberangriff eine entscheidende Rolle. Der Auf- und Ausbau von Cyber Resilience ist eine vielfältige Aufgabe. Er erfordert sowohl das Etablieren einer positiven Fehlerkultur, die Entwicklung und Umsetzung vorausschauender Prozesse sowie die Nutzung passender Technologien.

Die Cyber Resilience der Infrastruktur

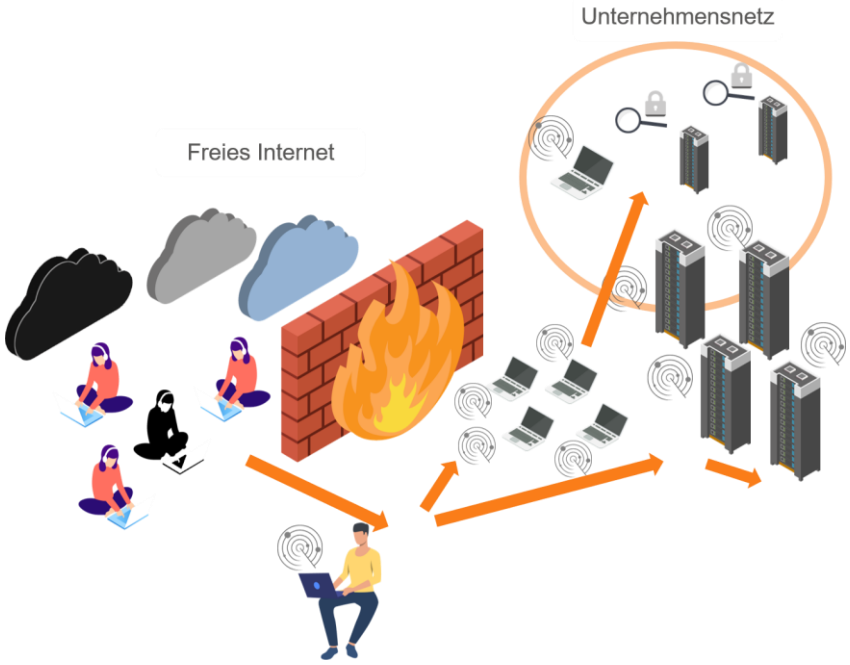
Für eine umfassende Cyber-Resilience-Strategie spielt insbesondere seit Beginn der Krise die Resilienz der IT-Infrastruktur eine entscheidende Rolle: Für diese bedeutet die enorm gestiegene Zahl der Remote-Zugriffe auf Anwendungen und Ressourcen einen massiven Belastungstest. Die Resilienz der Infrastruktur wird also zum entscheidenden Faktor – nicht nur, um den Status quo zu erhalten, sondern auch, um etablierte Infrastrukturen zu durchbrechen und gestärkt aus den aktuellen Herausforderungen hervorzugehen.

Um Vorfälle auf Infrastrukturebene zu verhindern, spielt eine enge Verzahnung aus Security Information and Event Management (SIEM), End Point Detection and Response (EDR) und dem Security Operation Center (SOC) eine entscheidende Rolle: SIEM ermöglicht einen ganzheitlichen Blick auf IT-sicherheitsrelevante Vorgänge, indem Meldungen und Logfiles unterschiedlicher Systeme gesammelt und analysiert werden. So können gefährliche Trends oder auffällige Ereignisse in Echtzeit erkannt werden. Über EDR können Endpunkte wie Clients und Server vor böswilligen Aktivitäten geschützt und kontinuierlich überwacht werden, während sicherheitsrelevante Systeme über das SOC als Sicherheitsleitstelle überwacht, integriert und analysiert werden können.

Im Falle eines Angriffs sollten die im SIEM definierten Regeln am Endpunkt über EDR greifen und das SOC mit geeigneten Maßnahmen reagieren und, je nach Bedarf, Mitarbeiter, Prozesse und Tools in Bewegung setzen, um die Bedrohung zu verhindern und daraus für künftige Vorgänge zu lernen. Für die Effektivität dieses Prozesses spielen ihr Automatisierungsgrad und die kontinuierliche Integration eine entscheidende Rolle: Je automatisierter die Abläufe, desto schneller kann auf einen Vorfall reagiert und die Wahrscheinlichkeit für menschliche Fehler minimiert werden. Zudem reduzieren sich auch die anfallenden Kosten.

Unser Lösungsansatz

Um die Cyber Resilience der Infrastruktur sicherzustellen, spielen Penetrationstests eine entscheidende Rolle: Durch die Einnahme der Angriffsperspektive können Schwachstellen aufgedeckt und geeignete Maßnahmen zur Behebung identifiziert werden. Jedoch zeigen sich bei der Qualität der eingesetzten Tests große Unterschiede. Viele Unternehmen setzen Vulnerability Scans auf allen bekannten Geräten oder statische, auf Agenten basierende Breach-and-Attack-Simulationen in abgeschotteten Bereichen ein.



Doch der Angriffsablauf einer Breach- and-Attack-Simulation ist statisch. Durch die Abschottung und die statischen Simulationen laufen reelle Angriffe von außen an gängigen IT-Sicherheitsmaßnahmen vorbei. Die regelmäßige Durchführung geeigneter automatisierter Penetrationstests von innen, kombiniert mit dem Know-how eines Security-Spezialisten, können diese Lücken schließen: Die Durchführung von innen ermöglicht eine realistische Simulation von Hackerangriffen, während kontinuierlich Erkenntnisse integriert und Schwachstellen identifiziert werden. Um diese zu beheben, erhalten Sie Berichte und Vorschläge zu geeigneten Maßnahmen.

PenTera als proaktive Cyber-Resilience-Maßnahme

Mit einem Fokus auf die Bedrohung von innen imitiert PenTera Hacker-Angriffe und automatisiert die Erkennung von Schwachstellen. Bei der Durchführung solcher ethischer Exploits, also der Ausnutzung von Schwachstellen ohne Gefährdung, bleibt ein unterbrechungsfreier Netzwerkbetrieb gewährleistet.

Detaillierte Berichte und vorgeschlagene Abhilfemaßnahmen unterstützen bei der Behebung von Schwachstellen.

- **Ohne Agenten**
  Keine Agenten auf den Zielsystemen, keine Netzwerkkonfigurationen. Penetrationstests mit physischem LAN-Zugriff ohne jegliche Zugangsdaten. So, wie ein Hacker arbeiten würde.
- **Harmlose Exploits**
  Wie ein Hacker führt PenTera Exploits durch, allerdings ethische Exploits, ohne den Service zu unterbrechen oder Schaden anzurichten: z. B. laterale Bewegung, externe Ausführung, Relaisangriffe, Knacken von Kennwörtern, Infiltrieren ethischer Malware und Rechteausweitung.
- **Sichtbare Angiffsvektoren**
  Jeder Schritt im Angriffsvektor wird detailliert dargestellt und protokolliert, um die „Kill Chain“des Hackers zu dokumentieren und zu erläutern.
- **Automatisiert**
  Durch Drücken von „Play“ oder über geplante Aufgaben wird ein Penetrationstest durchgeführt. Das Ergebnis wird durch einen ausführlichen Report dargestellt. Und es wird ausführlich erklärt, wie die gefundene Schwachstelle behoben werden kann.
- **Angriffs-Checkpoints**
  Bei missionskritischen Systemen kann der Sicherheitsbeauftragte eines Unternehmens die Steuerung für übergeordnete Exploit-Phasen übernehmen. Damit kann die Tiefe des Angriffs genau kontrolliert werden.
- **Priorisierte Behebung**
  Im Report werden die Schwachstellen nach Schweregrad priorisiert, sodass die kritischsten Schwachstellen zuerst behoben werden können. Es wird eine klar aufgestellte Übersicht der kritischen Schwachstellen samt Lösungsschritten angeboten.
- **Aktuellste Hackertechniken**
  Durch die permanente Weiterentwicklung und kurze Update-Zyklen sind die Penetrationstestverfahren immer auf dem neusten Stand.

- **Angepasste Prozessalarme**
  Sie können einen beliebigen Startpunkt sowie das Penetrationstestziel festlegen und einen zielgerichteten Angriffstest für eine bestimmte Schwachstelle oder für die Cyber-Widerstandsfähigkeit bestimmter Anwendungen durchführen.

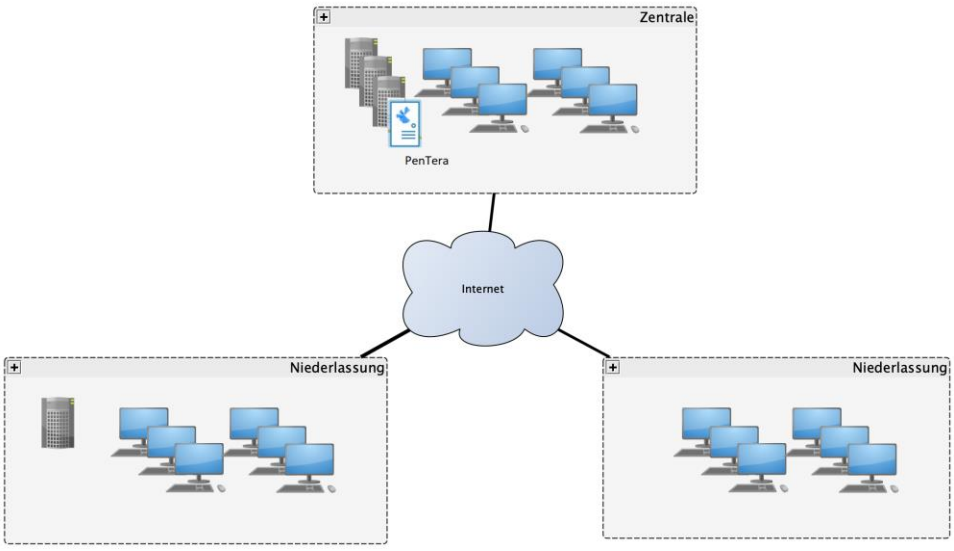
Installationsszenarien

Beispielhaft werden drei Installationsszenarien genannt.

Notebook

Trotz der Komplexität der Software ist PenTera schlank genug, um auf einem Notebook installiert werden zu können. Durch die mobile Installation kann PenTera einfach in andere Netzwerksegmente verbracht werden. Damit können Teilnetzwerke ohne Änderungen an der Firewall geprüft werden, es sind keine Routen nötig. Auch völlig isolierte Netzwerksegmente können somit problemlos geprüft werden.

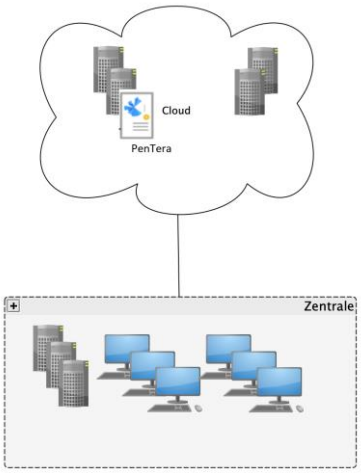
On-Premise



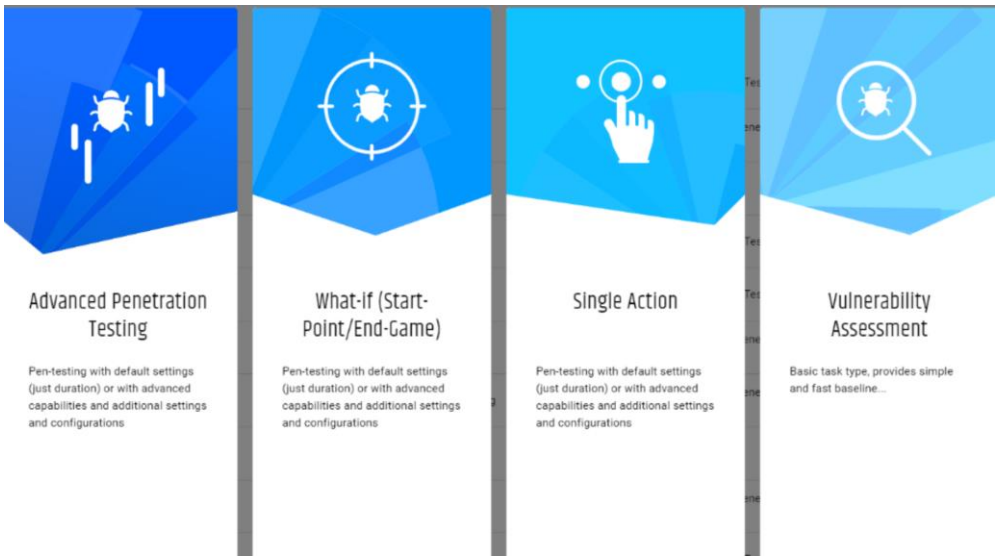
Installation auf einem Server in Ihrem Netzwerk mit Netzwerkzugang zu allen zu prüfenden Netzwerksegmenten. VLAN-Trunks werden unterstützt. Der Vorteil liegt hierbei in der ständigen Verfügbarkeit, es können z. B. jede Nacht bestimmte Testszenarien gefahren werden. Dies ermöglicht eine ständige Validierung und kontinuierliche Verbesserung.

Cloud

PenTera kann in einer Cloud-Umgebung installiert werden, z. B. AZURE. Der Zugriff ins Netzwerk kann über ein VPN oder eine VPN-Bridge abgesichert werden. Somit ist keine eigene Hardware nötig.



Testszenarien



Advanced Penetration Testing

Dies ist die vollständigste und gründlichste Art von Penetrationstest. Für diese Art von Test, der häufig als Black-Box-Penetrationstest bezeichnet wird, sind keine Anmeldeinformationen für den ersten Zugriff erforderlich.

What-If (Start-Point/End-Game)

Bei What-If- oder Gray-Box-Penetrationstests muss eine Anmeldeinformation für den ersten Zugriff angegeben werden, um den Penetrationstest zu starten. Bei dieser Art von Test können auch Dateinamen / Schlüsselwörter in Dateien angeben werden, z. B. Dateien auf einem Host, die ein Passwort enthalten. Bei technischen Usern wird dies durchaus verwendet.

Single Action

Dies ist ein kurzer, fokussierter Penetrationstest, der eine Reihe spezifischer Schwachstellentests in Ihrem Netzwerk ausführt.

Vulnerabilty Assessment

Mit dieser Option können Sie eine Schwachstellenanalyse des Netzwerks durchführen. Eine regelmäßige Durchführung wird häufig von Zertifizierungsorganisationen gefordert. Hier können die Tests vollautomatisch erstellt werden.

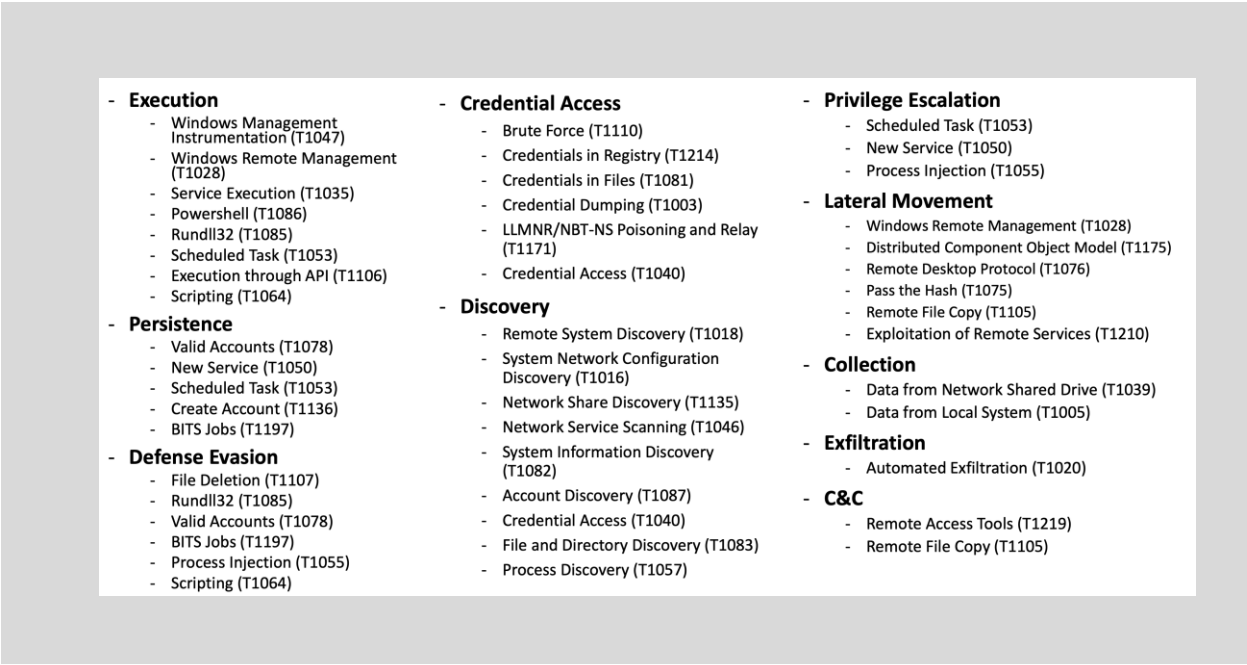
MITRE ATT&CK Framework Integration

ATTACK oder ATT&CK ist ein Akronym: Es steht für Adversarial Tactics, Techniques (ATT), & Common Knowledge (CK).

Das MITRE ATTACK Framework ist eine sich ständig weiterentwickelnde, global zugängliche Wissensbasis für cyberkriminelle Taktiken und Techniken, die auf realen Beobachtungen der letzten Jahre basiert. (http://attack.mitre.org)

PenTera integriert das MITRE ATTACK-Framework, um gängige Taktiken, Techniken und Verfahren (TTPs) abzubilden und zu dokumentieren, mit denen fortgeschrittene Bedrohungen, die Akteure gegen Unternehmensnetzwerke einsetzen, weiterentwickelt werden. Das ATTACK-Framework verwendet eine gemeinsame Terminologie und Taxonomie, um TTPs über verschiedene Arten von Gegnergruppen hinweg zu vergleichen.

PenTera MITRE Beispiel-Aktivitäten



PenTera-Anwendungsfälle

Bewertung der Passwortstärke

- PenTera sucht nicht nur nach Anmeldeinformationen im Netzwerk und versucht, diese zu verwenden, sondern versucht auch, die Kennwörter selbst so zu knacken. Das Knacken der Kennwörter läuft dabei so schonend ab, dass Konten nicht gesperrt werden.
- Das System kann versuchen, Anmeldeinformationen von Domänen, lokalen Accounts und Diensten zu entschlüsseln.
- Auf diese Weise können Sie die Kennwortrichtlinie für Anmeldeinformationen testen, die in Ihrem Netzwerk verwendet werden. Oft muss nicht die Richtlinie selbst verbessert werden, denn es gibt leider immer wieder Konten, die nicht der Richtlinie folgen.
- Die Bewertung der Passwortstärke ist eine gute Möglichkeit, das Bewusstsein der Anwender für Netzwerksicherheit zu erhöhen, indem gezeigt wird, wie einfach und schnell schlechte Passwörter im Vergleich zu guten Passwörtern geknackt werden können.

Ein neues Büro / Netzwerk aufbauen

- In der heutigen Welt bauen große, mittlere und sogar kleine Unternehmen ständig neue Netzwerke auf. Unabhängig davon, ob es sich um eine Migration in die Cloud, die Erweiterung in ein neues Gebäude oder die Umstrukturierung des Netzwerks handelt, kann PenTera jedes Mal ausgeführt werden, wenn Sie Netzwerkänderungen vornehmen, um zu überprüfen, ob diese Änderungen die Sicherheit Ihres Unternehmens nicht beeinträchtigt haben.
- PenTera wird auch häufig bei Fusionen und Übernahmen eingesetzt. Mit PenTera können Sie sofort die Sicherheit des erworbenen Unternehmens und die Geschäftsrisiken beurteilen, die Sie bei der Integration des Netzwerks in Ihr Unternehmen eingehen könnten.

Testen der Segmentierung und der internen Firewalls

- Nicht nur das interne Netzwerk und die Infrastruktur können mit PenTera analysiert werden – man kann auch überprüfen, ob isolierte Netzwerksegmente nicht doch erreichbar sind.
- Wenn sich PenTera in Segment A befindet und Segment B nicht erreichen kann, können Sie dennoch beide Segmente in einen Pentest einfügen und prüfen, ob PenTera diese Computer nicht nur scannen und auflisten, sondern auch tatsächliche

Exploits auf ihnen ausführen kann. Dies kann äußerst hilfreich sein, um zu zeigen, wie ein Angreifer in einem Netzwerksegment starten und in andere Segmente wechseln kann.

- Darüber hinaus lassen sich „Pivot-Maschinen“ identifizieren, Maschinen mit mehreren Netzwerkschnittstellen, sowie auch Schlüsselmaschinen, mit denen Angreifer seitlich in andere Segmente wechseln können.

Active-Directory-Lücken

- Manuelle Penetrationstester haben weder die Zeit noch die Möglichkeit, eine vollständige Analyse Ihres Active Directory (AD) durchzuführen und darin nach Berechtigungslücken zu suchen. Ein Tool wie PenTera hingegen sucht und identifiziert mehrere Schwachstellen in Ihrem AD wie zirkuläre verschachtelte Gruppen und Schattenadministratoren.

Erkennung von Malware

- Alle von PenTera verwendeten Nutzlasten sind sicher und werden vom dazugehörigen Entwicklungsteam von Grund auf neu erstellt. Diese Nutzdaten emulieren einen echten Zero-Day-Angriff und testen die Abwehr Ihrer Endpoint Protection (Virenscanner).
- Das Scannen nach Blacklist-Einträgen oder Signaturen ist heutzutage einfach zu umgehen. Daher ist es unerlässlich, eine verhaltensbasierte Abwehr (Behavioral Prevention) und auch die Möglichkeit zu haben, diese auf ihre Wirksamkeit zu testen. Dies bietet einen großen Mehrwert, da Sie sehen können, wie sich Ihre Endpoint Protection bei einem echten Angriff verhält.

SIEM-, EDR- und andere Sicherheitswarnungen

- PenTera testet alle Schichten Ihres Netzwerksicherheitskonzepts. Sie können die Warnmechanismen Ihrer anderen Sicherheitstools kontinuierlich analysieren und verbessern, indem Sie die Aktivitäten von PenTera mit denen Ihrer anderen Sicherheitstools wie SIEM- und EDR-Tools abgleichen.

Validierung der Wirksamkeit von Sicherheitsmaßnahmen

- Da PenTera einen Angriff nicht nur simuliert, sondern tatsächlich ausführt (mit harmlosen Exploits), kann überprüft werden, wie Ihre definierten Sicherheitsmaßnahm wirken – nicht nur die technischen Maßnahmen, sondern auch die definierten Prozesse.

- Sie können PenTera Anmeldeinformationen mitgeben, um einen Angriff auszuweiten. Das Tool kann auf diese Weise für Tischübungen verwendet werden, um festzustellen, ob Ihre Maßnahmen und Regularien ausreichen, um auch einem schweren Angriff zu widerstehen.

Optimierung des IPS / IDS-Alarmschwellenwerts

- PenTera verfügt über mehrere verschiedene „Stealthiness“ -Einstellungen, mit denen Netzwerkscans ausgeführt werden. Sie können mit verschiedenen Einstellungen testen und feststellen, ab welchem Level Sie IPS / IDS-Warnungen erhalten. Und diese Einstellungen weiter verfeinern, bis Sie die Angriffe erfassen, die Sie eskalieren möchten.

Validierung kritischer Assets

- Mit PenTera können Sie Ihre eigenen benutzerdefinierten kritischen Assets festlegen. Dies können Benutzerkonten, bestimmte Computer, IP-Bereiche, Webdienst-Anmeldeinformationen usw. sein. Auf diese Weise können Sie dem Tool mitteilen, was für Ihr Unternehmen am wichtigsten ist. Wenn es zu irgendeinem Zeitpunkt während eines Pentests möglich ist, auf diese Assets zuzugreifen, werden Sie sofort benachrichtigt und wissen, dass etwas gelungen ist, zu dem es nicht hätte kommen dürfen.
- Ein Beispiel für einen möglichen Anwendungsfall ist die Suche nach wichtigen Anmeldeinformationen / Kennwörtern für den Intranet-Service des Unternehmens, die in einem Browser wie Google Chrome gespeichert werden.

Rogue Asset Detection

- Es können ganze Subnetze oder Netzwerke gleichzeitig gescannt werden. Aus diesem Grund lassen sich häufig Geräte finden, von denen Ihr IT-Team nicht wusste, dass sie sich im Netzwerk befinden (Schatten-IT). IoT-Geräte, die nicht angeschlossen sein sollten, und anfällige Computer, die nicht unter der Kontrolle Ihres Unternehmens stehen, können mithilfe von PenTera leicht gefunden werden.
- Auch Geräte in Ihrem Netzwerk werden häufig gefunden, die von einem anderen Anbieter verwaltet werden, z. B. Druck-Dienstleister. Nicht selten haben diese Systeme tatsächlich ein vollständiges Windows-Betriebssystem, das nicht immer ordnungsgemäß aktualisiert werden kann, sodass ein Angreifer einen Einstiegspunkt in Ihr Netzwerk hat.

Standardkennwörter, die in OEM-Netzwerkgeräten verwendet werden

- PenTera kann auf Netzwerkgeräten wie Routern und Switches unter anderem prüfen, ob auf diesen Geräten die Anmeldeinformationen des Standards / Herstellers verfügbar sind. Dies ist besonders wichtig für größere Unternehmen, die möglicherweise ständig neue Netzwerke aufbauen.

IoT-Gerätesicherheit

- Während PenTera nicht unbedingt nach „Firmware“-Schwachstellen in speziellen Betriebssystemen sucht, verwenden fast alle IoT-Geräte immer noch gängige Protokolle wie FTP, SSH, RDP usw. Da sich das Tool in Ihrem Netzwerk befindet, kann es nach allen Arten von Netzwerkfehlkonfigurationen suchen, die es einem Angreifer ermöglichen, Anmeldeinformationen zu sammeln, um sie an anderer Stelle zu verwenden.

Überprüfung des vorhandenen Sicherheitskonzepts

- Dadurch, dass PenTera die Aktivitäten ausführt, die ein böswilliger Dritter ausführen würde, unterstützt das Tool Unternehmen bei der Validierung des Sicherheitskonzepts und konzentriert sich dabei auf Technologien, die möglicherweise nicht den Spezifikationen entsprechen. Auf diese Weise können Unternehmen Ressourcen für bestimmte Sicherheits-Fixes priorisieren oder Tools an ihrer Lebensdauer erkennen, da sie nicht mehr die Dienste ausführen, für die sie gekauft wurden.

Verbesserung der Testeffizienz

- Mit PenTera können Unternehmen von einer kontinuierlichen Sicherheitsüberprüfung profitieren, die das Beheben ihrer ausnutzbaren Schwachstellen weitaus schneller verbessert als bei herkömmlichen Penetrationstests. Durch die Automatisierung können sich manuelle Penetrationstest-Teams und RED-Teams auf spezifischere Aufgaben konzentrieren, während PenTera die Standardaufgaben im Netzwerk- und Infrastruktur-Penetrationstest übernimmt.
- Mit Gray-Box- und Single-Action-Tests können Testteams schneller arbeiten und sich auf bestimmte Aufgaben konzentrieren (z. B. Standard-Passwort-Scans). Durch die Anwendung von maschinellen Tests profitieren die Unternehmen in einem Bruchteil der traditionell beobachteten Zeit von den Ergebnissen. Durch die Möglichkeit, die Korrektur sofort zu prüfen, können Unternehmen außerdem erkennen, dass die Korrektur wirksam war.

Kontinuierliche Sicherheitsverbesserung

- PenTera ist in der Lage, die Cyber-Ausfallsicherheit des internen und Cloud-IaaS-Netzwerks eines Unternehmens konsistent zu bewerten. Durch die Anwendung der PenTera-Plattform auf diese Programme profitieren Unternehmen von einer einheitlichen Messung. Durch die Zuordnung von PenTera-Exploits zum MITRE Att&ck Framework erhalten Organisationen eine konsistente Sichtbarkeit ihrer Widerstandsfähigkeit gegenüber ATPs. Durch die Erhöhung der Frequenz und die Fähigkeit, gezielt nach Belieben zu testen, kann die Organisation ihre Änderungen der Cyber-Resilienz im Laufe der Zeit kontinuierlich verbessern.

Erfolgsgeschichten

Der kontinuierliche Einsatz von automatisiertem Pentesting kombiniert mit Security-Know-how zahlt sich aus. Nachfolgend wird anhand verschiedener Fälle aus der Praxis aufgezeigt, wie Schwachstellen identifiziert und nachhaltig behoben werden können, um Unternehmen langfristig Cyber-resilient zu machen.

- Im Rahmen eines automatisierten Pentests konnten Passwort-Hashes entschlüsselt und somit die Zugriffe auf das System erschlichen werden. Um dies künftig zu verhindern, wurden verschiedene Maßnahmen wie zusätzliche Prüfungen bei der Festlegung neuer Passwörter definiert.
- Beim Einloggen per Remote Desktop eines Domain-Administrators konnte die Anmeldeseite gefaked und vor die eigentliche Log-in-Seite geschoben werden, sodass das Administratorkennwort auf der Fake-Seite eingegeben wurde. Da solche Fakes mit bloßem Auge schwer zu erkennen sind, werden Remote-Desktop-Sitzungen künftig per Zertifikat abgesichert. Somit werden bei nicht vertrauenswürdigen Verbindungen künftig Zertifikatswarnungen angezeigt.
- Bei der Evaluation verschiedener Antivirensoftware-Produkte wurden automatisierte Pentests eingesetzt, um die Erkennungs- und Abwehrraten der einzelnen Lösungen zu prüfen – mit sehr unterschiedlichen Ergebnissen: Nicht jedes der getesteten Produkte war in der Lage, die Pentests im erwarteten Maß zu erkennen und abzuwehren.

Zusammenfassend können automatisierte Pentests eine Vielzahl an Anwendungsfällen von Cyberangriffen abdecken. Bei einer regelmäßigen Durchführung solcher Tests und der kontinuierlichen Integration der Ergebnisse in Form von geeigneten Maßnahmen kann die Cyber-Resilienz der IT-Infrastruktur nachhaltig verbessert und gestärkt werden.

business efficiency engineering

für exzellente Geschäftsprozesse

syracom ist ein unabhängiges Business- und IT-Beratungshaus, spezialisiert auf die Gestaltung effizienter und nachhaltiger Geschäftsprozesse.

Mit Fachexpertise und IT-Kompetenz verbinden syracom-Berater Business und IT. Das Unternehmen entwickelt maßgeschneiderte Lösungen für große und mittelständische Kunden unterschiedlicher Branchen. Experten begleiten den Kunden bei der digitalen Transformation seiner Geschäftsprozesse entlang der Wertschöpfungskette: von der Planung über die Steuerung und Optimierung bis zur Umsetzung. ***business efficiency engineering.***

syracom wurde 1998 vom heutigen Geschäftsführer Joachim Raczek gegründet. Seit 2012 gehören wir zur Consileon-Unternehmensgruppe, für die rund 430 Mitarbeiter bei einem Gesamtumsatz von ca. 65 Mio. Euro tätig sind.

Frank Hoffmann
Head of IT Security

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)

Fon: +49 6122 9176 0
frank.hoffmann@syracom.de
www.syracom.de