Engineer

Penetrationstest

Ein erlaubter Angriff zeigt, welche Fehler ausnutzbar sind

Was es ist

Ein Penetrationstest, oft Pentest genannt, ist ein Sicherheitstest, bei dem die Prüfer reale Angriffe nachahmen, um die Sicherheitsfunktionen einer Anwendung, eines Systems oder eines Netzwerks zu umgehen. NISTs Technical Guide to Information Security Testing and Assessment, SP 800-115, weist darauf hin, dass dies oft echte Angriffe auf reale Systeme und Daten mit den Werkzeugen und Techniken von Angreifern bedeutet. Die kürzere Definition in SP 800-53 Rev. 5, NISTs Katalog der Sicherheits- und Datenschutzkontrollen, ergänzt, dass die Prüfer typischerweise unter bestimmten Einschränkungen arbeiten. Genau das trennt den Test vom Angriff: Er ist autorisiert, begrenzt und vor Beginn schriftlich vereinbart.

Von anderen Sicherheitstests unterscheidet ihn das Ziel. Ein Schwachstellenscanner vergleicht seine Beobachtungen mit Beschreibungen bekannter Fehler und meldet mögliche Schwachstellen. Ein Penetrationstester versucht, den Fehler auszunutzen. SP 800-115 beschreibt den Unterschied klar: Scanner prüfen nur, ob eine Schwachstelle möglicherweise existiert. Die Angriffsphase eines Penetrationstests nutzt sie dagegen aus, um ihre Existenz zu bestätigen. Die meisten Tests suchen auch nach Kombinationen: Schwächen auf einem oder mehreren Systemen, die gemeinsam mehr Zugriff ermöglichen als jede allein.

Der OWASP Web Security Testing Guide (WSTG) merkt an, dass diese Technik auch Black-Box-Testing und Ethical Hacking genannt wird. Das Team prüft von außen, ohne vorherige Kenntnis des internen Aufbaus des Ziels, und verhält sich wie ein Angreifer. Häufig erhält es dennoch ein oder mehrere gültige Benutzerkonten.

Zwei Entscheidungen prägen jeden Test. Die erste ist der Ausgangspunkt. Ein externer Test beginnt außerhalb des Netzwerks mit kaum mehr als den vereinbarten Zieladressen. Ein interner Test beginnt darin, gewöhnlich mit den Zugriffsrechten eines normalen Mitarbeiters, und versucht von dort durch Rechteausweitung weiterzukommen. Die zweite Entscheidung ist, wer davon weiß. SP 800-115 bezeichnet offene Tests als White-Hat-Tests: Sie laufen mit Wissen und Zustimmung des IT-Personals. Verdeckte Tests oder Black-Hat-Tests laufen ohne dessen Wissen, aber mit vollständiger Kenntnis und Erlaubnis der höheren Führungsebene.

SP 800-115 teilt die Arbeit in vier Phasen. Eine Fußnote ergänzt, dass dies nur eine von vielen vertretbaren Gliederungen ist. In der Planung werden Regeln vereinbart, die Genehmigung der Leitung dokumentiert und Ziele gesetzt. Der eigentliche Test beginnt mit der Erkundung. Diese sammelt Informationen über das Ziel, scannt es und vergleicht die Ergebnisse mit Schwachstellendatenbanken wie der US National Vulnerability Database sowie dem eigenen Wissen der Prüfer. Die Angriffsphase, laut Leitfaden „das Herzstück jedes Penetrationstests“, versucht jede mögliche Schwachstelle auszunutzen. Eröffnet ein Exploit neuen Zugang, kehren die Prüfer aus der neuen Position zur Erkundung zurück. Die Berichterstattung begleitet alle drei Phasen und endet mit einem Bericht, der die gefundenen Schwachstellen auflistet, ihr Risiko bewertet und erklärt, wie sie behoben werden können. Andere Verfahren gliedern dieselbe Arbeit anders: Der Penetration Testing Execution Standard (PTES), den der WSTG als Referenzmethodik aufführt, verwendet sieben Phasen, von den Vorabsprachen bis zur Berichterstattung.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ein Penetrationstest?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

Warum es wichtig ist

Der Bericht eines Scanners ist eine Liste von Möglichkeiten. Manche lassen sich in Ihrer Umgebung nicht ausnutzen. Ein Scanner erkennt auch keinen Fehler, den noch niemand beschrieben hat, oder einen, der erst aus zwei harmlos wirkenden

Schwächen entsteht. Ein Penetrationstest beantwortet eine andere Frage: Was könnte ein Angreifer hier tatsächlich tun und wie weit käme er? SP 800-115 nennt weitere Erkenntnisse: wie gut ein System echten Angriffsmustern widersteht, welches Können ein Angreifer bräuchte, welche zusätzlichen Gegenmaßnahmen helfen würden und ob die Verteidiger den Angriff bemerken und reagieren.

Deshalb haben seine Ergebnisse auch für Menschen Gewicht, die nie Scanner-Ausgaben lesen. Der Befund, dass ein Außenstehender ohne Konto die Kundentabelle gelesen hat, ist ein Nachweis, keine Wahrscheinlichkeit. SP 800-115 beschreibt Penetrationstests als iterativen Prozess, der minimale Zugriffsrechte für weitergehenden Zugang nutzt. Ein guter Bericht zeigt diese Kette Schritt für Schritt, damit eine Korrektur sie an ihrem günstigsten Glied unterbrechen kann.

Derselbe Realismus macht den Test teuer und riskant. NIST nennt ihn arbeitsintensiv, sagt, dass er große Fachkenntnis erfordert, und warnt davor, dass Systeme während des Tests beschädigt oder funktionsunfähig werden können. Erfahrene Prüfer reduzieren dieses Risiko, können es aber nie vollständig ausschließen. Viele ihrer Aktivitäten, etwa Angriffe zum Kompromittieren von Systemen, sind nach den eigenen Richtlinien einer Organisation gewöhnlich verboten. Dafür gibt es die Einsatzregeln, die Rules of Engagement (ROE): ein vor Testbeginn vereinbartes Dokument, das dem Testteam die Befugnis zu festgelegten Aktivitäten erteilt und zu nichts darüber hinaus.

Es ist außerdem eine Technik unter mehreren, kein eigenständiges Gesamturteil. Der WSTG beobachtet, dass viele Teams Penetrationstests zur wichtigsten Sicherheitsprüfung einer Webanwendung machen. Er argumentiert dagegen, sie sollten weder die Hauptprüfung noch die einzige sein. Webanwendungen sind fast immer individuell entwickelt. Eine Prüfung von außen ähnelt daher eher Forschung als der Suche nach bekannten Fehlern in Standardprodukten. Zudem kommt der Test spät im Entwicklungszyklus, nach Festlegung von Entwurf und Code. Haben die Prüfer nur die fertige Anwendung, aber keinen Zugang zum Quellcode, ist ein Penetrationstest laut Leitfaden trotzdem eindeutig besser als gar keine Prüfung.

Die Häufigkeit ergibt sich aus den Kosten. SP 800-115 schlägt vor, dass angesichts hoher Kosten und möglicher Auswirkungen ein jährlicher Test der Netzwerke und Systeme einer Organisation genügen kann, mit regelmäßigen, leichteren Scans dazwischen. Manche Standards verlangen ihn auch ausdrücklich.

Der WSTG weist darauf hin, dass PCI DSS, der Datensicherheitsstandard der Zahlungskartenbranche, eine eigene Anforderung an Penetrationstests mit externen und internen Tests definiert.

Wie es in der Praxis aussieht

Der Großteil eines Penetrationstests wird vor der ersten Anfrage entschieden. Anhang B von SP 800-115 ist eine Vorlage für Einsatzregeln. Sie umfasst Zweck und Umfang, Beteiligte und Zeitplan, Kommunikation und Abbruchbedingungen, einbezogene und ausgeschlossene Systeme, erlaubte und verbotene Aktivitäten, den Umgang mit Testdaten, die Berichterstattung und eine Unterschriftenseite. Eine gekürzte Fassung für einen externen Test eines Webshops könnte so aussehen. Sie wurde für diesen Artikel verfasst; Namen und Adressen stammen aus den für Dokumentation reservierten Bereichen.

```
EINSATZREGELN: externer Test von shop.example.com

Zweck           Ermitteln, welche Schwachstellen ein Außenstehender ausnutzen
                kann und wie weit jede davon führt.
Ziele           203.0.113.10 bis 203.0.113.20, Inhaberschaft in WHOIS geprüft
Ausschlüsse     203.0.113.15 (Zahlungsanbieter, keine Testberechtigung); jeder
                vom Shop aufgerufene Drittanbieterdienst
Konten          Zwei Kundenkonten und ein Supportkonto
Zeitraum        3. bis 14. November, 19:00 bis 06:00 CET, außerhalb der
                Geschäftsspitzen
Tester-IPs      Nur 198.51.100.7 und 198.51.100.8
Erlaubt         Bestätigte Schwachstellen ausnutzen, um ihre Wirkung zu zeigen;
                Daten der Testkonten lesen; eine gekennzeichnete Testdatei
                hochladen und am Ende entfernen
Verboten        Dienstverweigerungsangriffe; Kundendaten ändern oder löschen;
                Social Engineering; physischer Zutritt
Abbruch         Ausfall des produktiven Shops, sichtbare echte Kundendaten oder
                Anzeichen eines echten Eindringlings: abbrechen,
                Sicherheitsverantwortlichen anrufen
Fortsetzung     Nur nach schriftlicher Freigabe des Sicherheitsverantwortlichen
Testdaten       Sensibel; auf den Laptops des Testteams gespeichert; 30 Tage
                nach dem Abschlussbericht gelöscht
Berichte        Tägliche Statusnotiz; Abschlussbericht innerhalb von zehn
                Arbeitstagen
Unterschriften  Testteamleitung; Leitung der Informationssicherheit
```

Jede Zeile beantwortet eine Frage aus SP 800-115. Vor Testbeginn soll laut Leitfaden geprüft werden, dass jede öffentliche Zieladresse der Organisation gehört. Dafür verweist er auf WHOIS-Registrierungsdaten. Er empfiehlt, eine produktive Website abends statt zu geschäftlichen Spitzenzeiten zu testen. Er

fragt nach den Ausgangsadressen der Prüfer, damit Administratoren Testverkehr von einem echten Angriff unterscheiden können. Die Liste der Systeme, die nicht getestet werden dürfen, heißt Ausschlussliste. Die Regeln sollen Kriterien für einen Abbruch und einen Ablauf für die Fortsetzung nennen. Gefragt wird auch nach einem tatsächlich entdeckten Eindringling: Soll der Test dann stoppen, wann darf er weitergehen und auf wessen Anweisung? Mindestens die Leitung des Testteams und die höhere Führungsebene unterschreiben und bestätigen damit, dass sie den Umfang und seine Grenzen verstehen.

Unter solchen Regeln folgt die Angriffsphase dem WSTG-Muster für SQL-Injection. Ein Scan der Suchseite des Shops liefert Hinweise auf eine mögliche Schwachstelle. Der erste Beleg ist ein Datenbankfehler nach Eingabe eines einfachen Anführungszeichens. Danach sendet der Prüfer gezielt aufgebaute Eingaben, die die Grammatik der Abfrage verändern. Bestätigt ist die Schwachstelle erst, wenn die Abfrage Daten liefert, die sie nicht liefern sollte. Enthielten diese Daten die Sitzung des Supportkontos, würde der Prüfer sich als Support anmelden und von dort erneut suchen. Der Bericht würde den gesamten Weg zeigen: ein ungefiltertes Feld, eine offengelegte Sitzung und eine Supportansicht mit Zugriff auf jede Bestellung.

Ein solcher Test steht neben anderen Prüfungen und ersetzt sie nicht. Der Bericht über ein Programm für kontinuierliche Sicherheitsscans aus der Arbeit der Gründerin unter NextMariner beschreibt automatisch laufende statische Analysen, dynamische Tests gegen eine laufende Instanz und Abhängigkeitsprüfungen. Daneben stehen schriftliche Sicherheitsaudits mit Bedrohungsmodell und Bewertung anhand des OWASP-Testleitfadens. Die Seite begründet diese Kombination: Scanner finden bereits beschriebene Problemklassen. Im Bedrohungsmodell werden die Probleme benannt, die einer bestimmten Plattform eigen sind.

Wo es schiefgeht

Ohne schriftliche Genehmigung testen. Ein mündliches „Los geht’s“ der Teamleitung deckt keine durch Unternehmensrichtlinien verbotenen Angriffe ab und schützt weder die Prüfer noch die Auftraggeber. Schreiben Sie zuerst die Einsatzregeln. Lassen Sie sie vor jeglichem Datenverkehr von der Leitung des Testteams und der höheren Führungsebene unterschreiben.

Fremde Adressen testen. Eine aus einem alten Diagramm kopierte Zielliste kann inzwischen fremde Adressen enthalten. Gemeinsam genutzte Plattformen platzieren andere Kunden neben Ihnen. Prüfen Sie wie von SP 800-115 verlangt die Zugehörigkeit jeder öffentlichen Zieladresse zur Organisation und nehmen Sie jeden Drittanbieterdienst namentlich in die Ausschlussliste auf.

Einen Scan als Penetrationstest verkaufen. Ein Scanner-Bericht mit neuem Deckblatt nennt Möglichkeiten, keine Nachweise. Verlangen Sie für jeden Befund einen Beleg der Ausnutzung: was der Prüfer getan hat, welchen Zugang es eröffnete und was der nächste Schritt gewesen wäre.

Den Test zur einzigen Sicherheitsprüfung machen. Ein einzelner Test sieht eine Stichprobe der Risiken zu einem Zeitpunkt von außen. Der WSTG ordnet Bedrohungsmodellierung dem Entwurf zu, Code-Review und Quellcodeanalyse der Entwicklung und Penetrationstests der anschließenden Testphase. Führen Sie alle durch. Nutzen Sie den Penetrationstest, um zu bestätigen, was frühere Prüfungen nicht klären konnten.

Ohne Abbruchregel beginnen. Legen die Prüfer einen produktiven Dienst lahm oder entdecken Hinweise auf einen echten Eindringling, wird unter Druck improvisiert, wenn niemand die Befugnis zum Stoppen und Wiederaufnehmen vereinbart hat. Schreiben Sie Abbruchkriterien, eine Telefonkette und einen Ablauf zur Fortsetzung in die Einsatzregeln.

Die Ergebnisse wie gewöhnliche Daten behandeln. Ein Penetrationstestbericht ist eine Karte der Schwachstellen, die ein Gegner ausnutzen könnte. SP 800-115 empfiehlt, Testergebnisse als sensibel zu behandeln. Vereinbaren Sie vor Beginn, wie Befunde gesammelt, übertragen, aufbewahrt und vernichtet werden, und beschränken Sie den Kreis der Empfänger des vollständigen Berichts.

Befunde ohne erneuten Test schließen. Eine Korrektur kann unvollständig sein oder an einer anderen Stelle als der Fehler ansetzen. Der WSTG nennt Versuche zur erneuten Ausnutzung früher gefundener Schwachstellen fokussierte Penetrationstests. Sie zeigen, ob bestimmte Fehler im bereitgestellten Code tatsächlich behoben sind. Führen Sie vor dem Schließen eines Befunds den ursprünglichen Exploit gegen jede Korrektur erneut aus.

Von einem verdeckten Test Vollständigkeit erwarten. Laut SP 800-115 untersucht ein verdeckter Test den möglichen Schaden eines Gegners. Er prüft nicht jede Kontrolle und findet nicht jede Schwachstelle; meist dringt er über die einfachsten Schwächen ein. Wählen Sie einen offenen Test für eine breite Abdeckung und einen verdeckten, wenn Sie erfahren wollen, ob die Verteidiger etwas bemerken.

Weiterführende Lektüre

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment — NISTs Leitfaden zur Planung und Durchführung von Sicherheitstests, mit den vier Phasen eines Penetrationstests und einer Vorlage für Einsatzregeln.
- OWASP Web Security Testing Guide v4.2: Einführung — wie Penetrationstests neben Review und Quellcodeanalyse einzuordnen sind und weshalb sie nicht die einzige Technik sein sollten.
- OWASP WSTG v4.2: Methoden für Penetrationstests — ein kurzer Überblick über PTES, die PCI-DSS-Empfehlungen, PTF, NIST SP 800-115 und OSSTMM.
- NIST SP 800-53 Rev. 5: Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen — NISTs Katalog der Sicherheits- und Datenschutzkontrollen, dessen Kontrolle CA-8 Penetrationstests und ihre Einsatzregeln behandelt.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist ein Penetrationstest?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/penetration-test/