Penetration Tests und Vulnerability Scans

Know-how Der Penetration Test ist ein Mittel, um mögliche Fehler zu erkennen und damit die IT-Sicherheit zu erhöhen. Ein strukturiertes Vorgehen ist dabei sehr wichtig, um eine qualifizierte Aussage über den Stand der eingesetzten IT-Mittel zu erhalten und diese in Vergleich zu setzen.

Von Andreas Wisler

Der IT-Alltag ist oft von Hektik, Stress und finanziellem Druck begleitet. Sehr schnell kann es geschehen, meist unabsichtlich, dass eine Härtungsmassnahme eines Systems nicht greift oder eine Testregel in der Firewall vergessen geht. Ebenfalls gehören ständige Änderungen, Erweiterungen und Anforderungen an Netzwerke und an IT-Systeme zum Daily-Business der Administratoren. Wenn aber ein (IT-)Mitarbeiter das Unternehmen verlässt, geschieht die Übergabe oft nicht optimal. Dass dabei die Dokumentation gerne vernachlässigt wird, zeigen diverse Studien.

Standards

Im Gegensatz zu IT-Revisionen gibt es im Bereich der Penetration Tests weder gesetzliche Vorgaben noch Richtlinien. Entsprechend sind der Ablauf, die Methodik und die Art der Dokumentation von Unternehmen zu Unternehmen sehr unterschiedlich. Seit einigen Jahren gibt es aber Versuche, diesen Missstand zu beheben.

Zu den bekanntesten Verfahren gehört sicherlich das Open Source Security Testing Methodology Manuel (OSSTMM). Das OSSTMM ist bezüglich technischen Security Audits kompatibel zu gängigen Standards und Weisungen wie ISO/IEC 27001/27002, IT-Grundschutz-Katalogen oder SOX.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Studie zur Organisation und Durchführung von Penetration Tests mit dem Titel «Durchführungskonzept für Penetrationstests» erstellt. Zusätzlich werden die rechtlichen Rahmenbedingungen dargestellt, die im Umfeld von Penetration Tests zu beachten sind. Die Studie stellt keine Anleitung zum Hacken von Netzen und Systemen dar, daher wurde bewusst auf detaillierte technische Anleitungen und Beschreibung von Werkzeugen, die in Penetration Tests verwendet werden, verzichtet. Ein Praxis-Leitfaden für IT-Sicherheits-Penetration-Tests ergänzt das Dokument.

Weiter sehr empfehlenswert ist der inoffizielle Pentest-Standard. Auch wenn das Dokument schon ziemlich in die Jahre gekommen ist, zeigt es die verschiedenen Schritte und Hintergrundinformationen.

Schritte eines Penetration Tests

Der Ablauf eines Penetration Tests sieht generell wie folgt aus: Workshop – Testphase – Bericht – Präsentation.

In einem ersten Workshop werden die Ziele des Penetration Tests definiert. Hier muss auch klar die Motivation festgehalten werden, die einen potenzieller Hacker antreiben würde. Zudem wird festgehalten, wie weit die beauftragten Hacker gehen dürfen. Die Möglichkeiten eines gezielten Angriffs umfassen ein Blackbox-Hacking von aussen (überhaupt keine Informationen über die Zielsysteme), ein Hacking mit teilweisem oder komplettem Wissen über die interne Infrastruktur (White- oder Grey-Hacking) und können durch netzwerkinterne Tests inklusive Social Engineering ergänzt werden.

Die Testphase wird anschliessend ausführlich beschrieben. Dazu hier nur zwei Bemerkungen: Wichtig ist es, nie das Ziel der Tests aus den Augen zu verlieren. Schnell kann es in der Flut von Informationen geschehen, dass ein falscher Weg eingeschlagen wird. Im Gegensatz steht dazu, dass die Kreativität der Angriffe nicht ausser Acht gelassen werden darf. Ein stures Vorgehen nach Checklisten zeigt offenbart nicht immer das gesamte Bild.

Der Bericht und die Präsentation zeigen das Vorgehen, die eingesetzten Tools sowie die Erkenntnisse aus den Ergebnissen. Sollten Schwachstellen ersichtlich sein, sind diesen Massnahmen zu zuweisen und in einer Prioritätenliste festzuhalten. Zudem sind, soweit möglich, Zusammenhänge aufzuzeigen und in einem gesamtheitlichen Kontext darzustellen.

Der Penetration Test

Der erste Schritt des Penetration Tests umfasst die Informationssuche. Welche Informationen sind im Internet verfügbar, sei dies auf der Homepage des Unternehmens oder über Ergebnisse von Suchmaschinen. Auch Seiten zur Stellensuche sind eine gute Quelle. Sucht die Firma zum Beispiel nach Oracle-Spezialisten, wird vermutlich auch Oracle als Datenbanklösung eingesetzt.

SCHRITTE EINES PENETRATION TESTS

Quelle: Gosecurity

Der Ablauf eines Penetration Tests folgt generell dem Schema Workshop – Testphase – Bericht – Präsentation. Ein strukturieres Vorgehen hilft, mögliche Schwachstellen zu erkennen und geeignete Massnahmen zur Behebung zu treffen.

Weitere Informationen liefern auch so genannte Success Stories, in denen ein Lieferant ausführlich beschreibt, welche Lösung er bei der einer untersuchten Firma platziert hat. Das Internet vergisst dabei wenig. Wurde zum Beispiel in einem Forum eine (technische) Frage platziert, kann diese auch nach Jahren noch abgerufen werden. Ebenfalls sind Namen von Personen, eventuell sogar mit einer E-Mail-Adresse versehen, ideal für die weiteren Angriffe. Tools wie Maltego stellen diese Zusammenhänge grafisch dar und erleichtern damit die Auswertung.

Weitere Informationen liefern WHOIS und DNS. Welche Angaben sind zu den IP-Adressen festgehalten? Verfügt das Unternehmen über weitere IP-Adressen? Welche Informationen stehen in den DNS-Einträgen? In den TXT-Einträgen sind regelmässige Hinweise zu eingesetzten Produkten via Adobe, Microsoft 365, Zertifikate oder ähnliches zu finden.

Nachdem bereits viele Informationen zur Verfügung stehen, gilt es, das Angriffsziel einzuschränken. Ein IP- und Portscan liefert die dazu notwendigen Informationen. Es soll geklärt werden, welche IP-Adressen antworten und welche offenen Ports im Internet ersichtlich sind. Daraus leiten sich die interessanten Ziele ab. In der Regel antworten dabei die Standard-Ports (d.h. Ports, die bekannt sind, oft unter 1024, beispielsweise Port 443 für HTTPS). Die Erfahrung zeigt, dass sich viele spannende Ports auch oberhalb der 50'000-Grenze befinden. Es lohnt sich, trotz grossem Zeitbedarf, alle 65'535 möglichen Ports durchzusehen. Gleichzeitig mit dem offenen Port sollte die entsprechende Header-Information ausgelesen werden. Viele Systeme sind sehr auskunftsfreudig und teilen mit, wer sie sind und vor allem in welcher Version sie vorliegen. Eine Schwachstellen-Suche in öffentlichen Vulnerability-Datenbanken zeigt, ob sich das antwortende Programm auf dem aktuellen Softwarestand befindet oder nicht. Falls nicht, sind vermutlich bereits Tools, so genannte Exploits, im Internet verfügbar, die gegen diese Schwachstelle eingesetzt werden können.

Als weitere Möglichkeit stehen Vulnerability-Scanner auf der Liste. Diese verursachen jedoch einen grossen Lärm. Je nachdem, ob alle Personen der zu untersuchenden Firma Bescheid wissen, können diese bereits zu einem frühen Zeitpunkt eingesetzt werden. Sie dienen dazu, nebst den bereits erwähnten Ports, auch Informationen zum Betriebssystem, Banner (Antworten auf Anfragen), die Kontrolle von bekannten Sicherheitslücken, Verbesserungsvorschläge und automatisch generierte Berichte zu erstellen.

Nach diesen Tests stehen sehr viele Informationen zur Verfügung, die es gilt, weiter zu verwerten. So können Skripts missbraucht, SQL-Abfragen manipuliert und Schwachstellen in der gefundenen Software ausgenutzt werden. Login-Angaben für Webseiten, E-Mail, FTP, VNC, RDP und für viele weitere Programme können durch Dictionary (d.h. durch Wörterbücher) oder Brute-Force-Attacken (dem wilden Durchprobieren) geknackt werden. Hier benötigt man aber viel Zeit, ausser es werden schwache Passworte verwendet.

Schwachstellen in Windows-Systemen

Obwohl dem Betriebssystem von Microsoft Schlechtes nachgesagt wird, kann es doch sicher betrieben werden. Die Erfahrung zeigt, dass die meisten Schwachstellen durch installierte Dienste verursacht werden. Jeder Dienst, vor allem die nicht benötigten, aber laufenden, erhöhen die Angriffsfläche eines Systems. Erfahrungsgemäss wird das schnelle Patchen gerne vernachlässigt und dadurch einem potenziellen Angreifer die Arbeit unnötig erleichtert. Sind in einer Firewall zusätzlich (zu) viele Ports geöffnet, wird die Gefahr einer erfolgreichen Attacke erhöht.

Wie bereits erwähnt, gibt der Port-Scan die ersten Informationen auf mögliche Schwachstellen bekannt. Sind typische Windows-Ports offen, wie Kerberos (88), RPC und Netbios (135-139), LDAP (389), SMB/CIFS (445), SQL-Server (1433), AD Global Catalog (3268) und Terminal Services (3389) kann eine genauere Analyse weitere Informationen liefern. Hier lohnt sich der Einsatz eines umfassenden Scanners wie Nessus/OpenVAS oder der GFI Languard Network Security Scanner. Sind Lücken in den eingesetzten Versionen bekannt, geben dies die erwähnten Programme an. Nun muss nur noch im Internet das entsprechende Angriffs-Tool gefunden werden. Google hilft hier sicherlich am schnellsten weiter, jedoch auch spezialisierte Seiten wie Packetstorm liefern oft ein passendes Programm.

Kann ein Zugriff auf eine Anmeldeseite aufgebaut werden, sollten zuerst die möglichen Ziele identifiziert werden. In der Regel werden Accounts nach einer gewissen Anzahl Fehlversuchen gesperrt. Davon ausgenommen ist jedoch meistens der Administrator. Obwohl reizvoll, ist der Administrator oft kein ideales Angriffsziel, da er (hoffentlich) gut überwacht wird. Sind keine Einschränkungen vorhanden, das heisst kein Sperren bei einer gewissen Anzahl fehlerhaft eingegebener Passwörter, kann jeder beliebige Account verwendet werden. Verschiedene Programme helfen, Passwörter zu erraten. Sei dies mittels

Passwort-Datenbanken oder dem Durchprobieren aller Möglichkeiten. Passwort-Datenbanken umfassen eine Vielzahl bekannter Kennwörter. Viele dieser stammen aus erfolgreichen Hack-Angriffen im Internet. Solche Tabellen können mehrere Millionen Kombinationen enthalten.

Immer wieder geschieht es, dass für die Server-Administration der Port 3389 (Terminal Services / Remote Desktop Protocol) auch durch die Firewall hindurch geöffnet wird. So kann die IT oder der externe Support jederzeit auf den Server zugreifen. Dieses Vorgehen öffnet einem Hacker einen optimalen Zugang zum System. Im Internet sind Tools verfügbar, die Brute-Force-Attacken auf diesen Port durchführen können. TSGrinder ist ein solches Tool, welches RDP-Verbindungen öffnet und ein Passwort nach dem anderen aus einer Textdatei an die Gegenseite schickt. Die Empfehlung ist daher eindeutig: Terminal Services dürfen nur via VPN erreichbar sein.

Eine weitere Sünde ist der direkte Zugriff auf den SQL-Server. Sobald der Port 1433 offen ist, kann eine Attacke gefahren werden. Auch hier kann versucht werden, dass Kennwort zu erraten.

Schwachstellen in Unix-Systemen

Auch unter Unix sind Schwachstellen bekannt. Typische Ports, die als Angriffsziel interessant sein können, sind: ssh (22), telnet (23), finger (79), exec (512), login (513) und shell (514).

Ist finger geöffnet, kann als erstes abgefragt werden, welche Benutzer gerade am System angemeldet sind: finger @<IP> liefert diese Antwort. Das Tool hydra kann anschliessend einen Angriff auf das Passwort starten. Dafür wird zum Beispiel eine Verbindung auf den Telnet-Server gestartet: hydra –l <Benutzer> -P <Passwortliste> <IP> <Dienst>. Als Dienst können auch für über 60 weitere Dienste eingesetzt werden. Dazu gehören Cisco, Oracle, HTTP, mySQL, Oracle, SAP, SMTP, VNC oder Vmware.

Sind NFS-Freigaben auf dieses System vorhanden, können diese mit showmount –e <IP> angezeigt werden. Ein Anziehen dieser Freigaben kann dann anschliessend mit mount geschehen.

RPC-basierte Dienste sind ein beliebtes Angriffsziel. Daher liefert das Tool rpcinfo –p <IP> genauere Informationen (gibt es auch für Windows Server > 2012). Alternativ kann dies auch mit nmap geschehen (nmap –sUV <IP>). Mit diesem Aufruf stehen alle notwendigen Informationen für einen weiteren Angriff zur Verfügung. Um welches System handelt es sich? Welche Applikationen sind installiert? Sind Schwachstellen dafür bekannt?

Schwachstellen in Web-Anwendungen

Die Betriebssysteme werden immer sicherer. Daher verlagern sich die Angriffe auf leichtere Ziele. Zu den beliebtesten gehören Web-Anwendungen. Immer mehr Applikationen bieten einen zusätzlichen Zugriff via HTTPS. Bei den immer komplexer werdenden Web-Anwendungen kommen auch Schwachstellen vor.

Browser-Plugins wie Web Developer (verfügbar für Chrome und Firefox) können Web-Formulare ändern, beispielsweise Längenbeschränkungen aufheben und schreibgeschützte Felder beschreibbar machen, Hidden-Felder verändern, Cookies ansehen und verändern und vieles mehr.

Damit eine Webseite und die übertragenen Daten einfach untersucht werden können, lohnt sich der Einsatz eines Proxys. Die Burpsuite ist ein sehr populärer Web-Proxy, der die Daten vor dem Versenden anzeigt und die Möglichkeit bietet, Modifikationen vorzunehmen. Dies ist vor allem dann interessant, wenn in Formularen so genannte Hidden-Felder übertragen werden. Diese können so noch verändert werden, was oft die Möglichkeit bietet, auf fremde Daten zuzugreifen. Damit nicht manuell die gesamte Webseite untersucht werden muss, durchsucht Burp automatisch die Seite und folgt allen Links.

Trotz vielen Fachberichten und Warnungen gibt es immer noch Formularfelder, welche den eingegebenen Inhalt ungeprüft an Datenbanken weiterreichen. SQL Injection heisst dieses Angriffsszenario, welches versucht, die Anfragen zu manipulieren. Ein Aufruf mit ´or 1=1 -- liefert in einer SQL-Abfrage ein Ergebnis, das immer wahr ist. Wird dies ohne Prüfung direkt weitergereicht, können alle Antworten unabhängig des Suchbegriffs ausgelesen werden. Klappt dies, kommen weitere Abfragen zum Zug, mit dem Ziel, herauszufinden, welche SQL-Server-Version eingesetzt wird, welche Datenbanken existieren sowie wie die genauen Inhalte anzuzeigen sind.

Eine weitere Gefahr bei Web-Seiten ist Cross Site Scripting (XSS). Hier werden jedoch nicht Daten ausgelesen, sondern fremder Code in die echte Seite eingeschleust. Wiederum geschieht dies über schlecht ausgewertete Formularfelder. Ob die Seite dafür anfällig ist, lässt sich leicht mit <script>Alert(´XSS Test´)</script> testen. Öffnet sich bei der Eingabe in ein Eingabefeld ein zusätzliches Fenster, ist die Seite anfällig auf Cross Site Scripting. Das gefährliche daran ist, dass sich ein Benutzer auf der richtigen Seite befindet (ersichtlich an der Internet-Adresse in der Browserleiste), jedoch einen falschen Inhalt angezeigt bekommt. Werden so vertrauliche Informationen eingegeben, gelangen diese an den Angreifer und nicht an die Webseite.

Diese umfassenden Tests sind in der Regel nicht in einem Tag durchzuführen. Zu vielfältig sind die möglichen Angriffsflächen und Möglichkeiten. Neben der Definition der eigenen Sicherheitsbedürfnisse gehört zu einem funktionierenden Sicherheits-Regelkreis das kritische Hinterfragen, ob die definierten Ziele mit den getroffenen Massnahmen erreicht wurden. Der Penetration Test liefert dabei eine unparteiische Drittmeinung. Das strukturiere Vorgehen hilft, mögliche Schwachstellen zu erkennen und geeignete Massnahmen zur Behebung zu treffen. ■

DER AUTOR

Andreas Wisler ist Inhaber der Firma Gosecurity. Er ist CISA, CDPSE, ISO 22301, 27001 sowie der erste Schweizer ISO 27701 Lead Auditor. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen beim Aufbau eines ISMS und der Erlangung des ISO-27001-Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch.