AD Security Bootcamp

1 Lernziele

In einer vorbereiteten Umgebung mit kontinuierlicher Betreuung lernen die Teilnehmer im Laufe einer Woche, eine auf Windows und Active Directory (aber auch anderen Microsoft-Technologien wie Exchange, SQL und indirekt auch Entra ID) basierende IT-Umgebung

- auf ihre Sicherheit hin zu untersuchen
- zu härten
- in gehärtetem Zustand zu betreiben
- zu überwachen
- und aktiv gegen Angriffe zu verteidigen

Das Lernen erfolgt, getreu dem Prinzip eines „Bootcamp“, durch das selbstständige Erledigen der gestellten Aufgabe und nicht durch Erklärungen des Trainers. Selbstverständlich ist der Trainer dennoch stets präsent und hilft, falls man einmal nicht weiter weiß…

Der Akzent ist ganz klar auf Active Directory-Sicherheit gesetzt, daher werden viele Dinge wie Antimalware Evasion, Process Injection usw. als „machbar“ (aus Sicht des Angreifers) vorausgesetzt. Doch Obacht! Wird in anderen Bereichen geschlampt, wird der Angreifer dies evtl. auch für sich ausnutzen können!

2 Zielgruppe

System- und Sicherheits-Administratoren, die ihre Windows Security-Skills auf den Prüfstand stellen und verbessern wollen.

IT-Consultants, die aus dem Infrastruktur- in den Security-Bereich wechseln.

3 Voraussetzungen

Gute Kenntnisse der Windows-Administration.

Grundlegendes Verständnis von TCP/IP und klassischer Paket-Filter-Firewall (im Bootcamp wird pfSense benutzt).

Gute Kenntnisse der Active Directory-Administration.

Grundlegendes Verständnis der Active Directory-Security (*das Intensivseminar von Evgenij Smirnov wird empfohlen, falls Nachhol- oder Auffrischungsbedarf besteht*).

4 Ablauf und Dauer

Herzlichen Glückwunsch, Du hast eine historisch gewachsene IT-Umgebung geerbt.

An Deinem ersten Arbeitstag als System- und Sicherheitsadministrator erfährst Du, dass das Team, welches die IT-Infrastruktur aufgebaut und jahrelang betrieben hat, nicht mehr zur Verfügung steht. Die Vorstandsassistentin, die zufällig Enterprise Admin-Rechte hat, legt Deinen Account an und versieht ihn mit allen nur denkbaren Berechtigungen. Von nun an bist Du auf dich allein gestellt… nun, nicht ganz allein – der Bootcamp findet in Paaren statt, daher hast Du eine zweite Person, mit der Du dich austauschen, Aufgaben teilen und Maßnahmen abstimmen kannst; diese Person ist allerdings in genau der gleichen Situation wie Du.

Es ist Jahresendgeschäft, damit sind Wartungsfenster rar und nicht gerne gesehen, ungeplante Störungen der geschäftskritischen Anwendungen sind um jeden Preis zu vermeiden. Die Umgebung im Labor ist nicht groß, steht aber für eine deutliche größere Organisation, daher sind „Notfall-Migrationen“

von Anwendungen und Nutzern nicht plausibel. Auch ist die Anschaffung kostenpflichtiger Tools ein längerer Prozess, der während des Bootcamps auf keinen Fall abgeschlossen werden wird.

Was die frei verfügbaren Werkzeuge angeht, gibt es eine gute und eine schlechte Nachricht. Du darfst keine neue Software ohne Sicherheitsprüfung und Freigabe einsetzen, und deine Vorgänger haben auch nichts außer Bordmittel genutzt. Allerdings ist Dein Arbeitgeber Mitglied eines Branchenverbandes, und dort gibt es eine Freigabeliste von Tools, aus der Du dich ohne weitere Rücksprache bedienen kannst.

Doch die Angreifer schlafen nicht. Dein neuer Arbeitgeber stellt neuartige Produkte her, und die Konkurrenz hat Cyberkriminelle beauftragt, an die Forschungs- und Entwicklungs-Interna zu kommen und den Betrieb „deiner“ Umgebung möglichst lahm zu legen.

Natürlich hängt Dein Job – Du bist ja noch in der Probezeit – vom Erfolg der Verteidigung ab, nicht zuletzt deshalb, weil es den Job, solltest Du scheitern, gar nicht mehr gibt. Viel Glück!

4.1 Montag: Kennenlernen

Wir erledigen das Onboarding und drehen eine kleine Runde durch die „neue“ Umgebung. Dein Ansprechpartner ist nicht technisch, aber schon seit Urzeiten im Unternehmen und weiß genau, welche Anwendungen kritisch sind.

Wir werden auch über die Einschränkungen reden, welchen die Bootcamp-Umgebung unterworfen ist, denn diese sind entscheidend für den Erfolg der Gesamtoperation!

Am Nachmittag kannst Du anfangen, das Ausmaß der Misere zu begutachten, behutsam das Gröbste zu reparieren und die Tools für das Weitere zusammenzusuchen.

4.2 Dienstag: Härtung

Ihr habt den ganzen Tag Zeit, eure neue Umgebung auf die Angriffe der von der Konkurrenz beauftragten Hacker im Rahmen des möglichen vorzubereiten. Das Betreuer-Team hilft bei konkreten Fragen, sofern sie nicht die speziellen Anwendungen betreffen, sondern nur die Basis-Technologie.

4.3 Mittwoch: Was ist da los?

Irgendwann im Laufe des Mittwochs werden die ersten Anzeichen sichtbar (oder auch nicht, je nachdem, wie gut ihr seid), dass in der Umgebung Dinge passieren, die nicht „im Sinne der Company“ sind. Zum Teil erlauben euch diese Hinweise, übersehene Löcher in eurem Panzer noch schnell zu stopfen; nutzt diese Gelegenheit rechtzeitig aus!

4.4 Donnerstag: Unter Beschuss

Ihr solltet in der Lage sein, Bösartiges in euerer Infrastruktur zu erkennen und zu bekämpfen. Denkt daran, dass euch das endgültige Ziel der Angreifer bekannt ist!

4.5 Freitag: Wenn sich der Staub setzt

Nacheinander stellen die Teilnehmer-Teams die Findings, die ergriffenen Maßnahmen und das Ergebnis der Woche vor. Das Betreuer-Team ergänzt die Story mit Uptime-Statistiken, Tipps und Tricks und den Findings, die nicht aufgefallen sind.

Am Ende wird das Siegerteam gekürt (die Wertung beinhaltet die Uptime und den Erfolg der Verteidigung). Dieses bekommt einen kleinen, aber auffälligen Preis.