Hacking

Es gibt verschiedene Möglichkeiten zu hacken, und dieses Thema ist sehr interessant. Als Hobby-White-Hat-Hacker finde ich, dass es in diesem Bereich viel Wissen zu erlernen gibt. Hier werde ich einige Methoden festhalten, die ich erkundet habe.

Standardpasswörter

Einige Websites, einschließlich solcher von Regierungsbehörden, verwenden immer noch Standardpasswörter. Während viele Unternehmen oder Benutzer ihre Standardzugangsdaten ändern, versäumen es andere, dies zu tun. Benutzer sind oft faul, und Passwörter wie `12345678` sind immer noch weit verbreitet. Dies gilt insbesondere für ältere oder Nischensysteme.

nmap oder Netcat

Diese Tools werden verwendet, um die Ports eines Servers zu scannen. Achten Sie besonders auf häufig verwendete Ports wie 80, 22 und 443. Bei AWS-Instanzen ist der Standard-Benutzername `ec2-user`. Bei Azure-Instanzen ist es `azure-user`. Bei Google Cloud-Instanzen ist der Standard-Benutzername in der Regel `ubuntu` oder `google-cloud`. Bei anderen Cloud-Instanzen ist es normalerweise `root`.

Verwendung der Browser-Konsole

Die Browser-Konsole ist nützlich, um versteckte Informationen zu untersuchen. Manchmal sind kritische Daten im HTML- oder JavaScript-Code eingebettet, aber auf der Seite selbst nicht sichtbar.

Backdoors

Im Leben bieten Hintertüren unbefugten Zugang zu Gebäuden, oft unbemerkt oder ungeschützt, wie Parkplätze oder Seitentüren. In ähnlicher Weise können Systeme versteckte Hintertüren haben, die die normalen Sicherheitsprotokolle umgehen.

Social Engineering

Die Spitznamen, Geburtstage und Social-Media-Beiträge von Menschen können viele persönliche Informationen preisgeben. Oft werden diese Details verwendet, um schwache Passwörter zu erstellen. Bei Wi-Fi-Netzwerken kann die Kenntnis der Hausnummer oder anderer identifizierender Details helfen, das SSID oder das Passwort zu erraten.

SQL Injection

Für jedes Eingabefeld ist das Testen mit `? 1=1` eine gängige Technik, um Schwachstellen und potenzielle SQL-Injection-Punkte zu identifizieren.

Actuator- oder Health-APIs

Für API-Server bieten Anwendungen wie Spring Boot einen `/actuator`-Endpunkt, der Maschinen- und Anwendungsgesundheitsdaten bereitstellt. Andere Web-Frameworks verfügen ebenfalls über ähnliche Funktionen, die sensible Serverdetails preisgeben können.

Verkehrsüberwachung

Um zu verstehen, wie das Frontend mit dem Backend interagiert, können Sie Proxy-Anwendungen wie Charles Proxy auf macOS verwenden, um Anfrageprotokolle aufzuzeichnen und zu analysieren. Dies kann Ihnen Einblicke in die Pfade und den Datenaustausch zwischen den Komponenten geben.

Grenzen und Randfälle von APIs

Es ist wichtig, die Grenzen und Randfälle einer API oder eines Servers zu testen. Ein Distributed Denial of Service (DDoS)-Angriff versucht, die Anfragelimits zu überlasten. Darüber hinaus gibt es Randfälle, in denen APIs möglicherweise Zugriff auf eingeschränkte Daten ermöglichen. Das Testen dieser Szenarien kann dazu beitragen, sicherzustellen, dass die richtigen Zugriffskontrollen vorhanden sind.

Admin-Panels

Manchmal sind Admin- oder interne Panels nicht ausreichend geschützt. Es lohnt sich, den Zugriff auf Pfade wie `/admin` zu versuchen oder Subdomains wie `admin.xx.com` zu besuchen, um zu überprüfen, ob diese Bereiche ordnungsgemäß gesichert sind.