Penetrationstest-Konzept für Rogue Access Point Angriffe

Technische Grundlagen und Zielsetzung

Die Bewertung der Benutzer-Awareness bezüglich gefälschter WLAN-Netzwerke stellt einen kritischen Aspekt der IT-Sicherheit dar. Rogue Access Points – unerlaubt installierte WLAN-Zugangspunkte – tarnen sich als legitime Netzwerk-Infrastruktur und schaffen damit ein erhebliches Potenzial für Man-in-the-Middle-Angriffe. Das primäre Ziel dieses Penetrationstests liegt in der Prüfung der Erkennungsfähigkeiten von Netzwerk-Monitoring-Systemen sowie der systematischen Dokumentation von Sicherheitslücken im WLAN-Bereich.

WPA2-Angriffsvektoren umfassen verschiedene Methoden wie Handshake-Capture mit anschließender Offline-Bruteforce-Attacke, Evil Twin Angriffe zur Imitation bestehender Access Points, PMKID-basierte Angriffe sowie gezielte Deauthentication-Attacken zur Verbindungstrennung. Die technische Umsetzung erfolgt mittels Raspberry Pi 4 oder vergleichbarer Hardware, ergänzt durch USB-WLAN-Adapter mit Monitor-Mode-Unterstützung, externe Antennen für erweiterte Reichweite und portable Stromversorgung. Die Software-Architektur basiert auf Hostapd für die Access Point Konfiguration, Dnsmasq für DHCP- und DNS-Services, Apache oder Nginx als Webserver für das Captive Portal, sowie Wireshark/Tcpdump für Traffic-Monitoring und der Aircrack-ng Suite für spezialisierte WLAN-Penetration.

Testdurchführung und Angriffsszenario

Das Angriffsszenario gliedert sich in vier aufeinanderfolgende Phasen. Die Reconnaissance Phase beginnt mit dem systematischen Scanning bestehender WLAN-Netzwerke, der Identifikation häufig genutzter SSID-Namen und einer

detaillierten Signal-Stärke-Analyse der Ziel-Access Points. Im Evil Twin Setup erfolgt die Konfiguration einer identischen oder bewusst ähnlichen SSID mit höherer Sendeleistung als der legitime Access Point, wobei ein offenes oder schwach gesichertes Netzwerk implementiert wird. Die Captive Portal Implementation umfasst die Weiterleitung auf eine gefälschte Login-Seite mit originalgetreuer Nachbildung des Corporate Designs des Zielunternehmens sowie einen integrierten Credential-Harvesting Mechanismus. Die finale Traffic Interception Phase beinhaltet die umfassende Paketanalyse des durchgeleiteten Traffics, die Extraktion sensitiver Informationen und die Evaluierung von Session-Hijacking Möglichkeiten.

Die praktische Testdurchführung erfordert zunächst die Einholung einer schriftlichen Genehmigung, die präzise Definition von Testzeiten und -bereichen sowie die enge Koordination mit dem IT-Security Team. Die Execution umfasst die strategische Platzierung des Rogue AP in definierten Zielbereichen, kontinuierliches Monitoring der Verbindungsversuche, lückenlose Dokumentation aller Aktivitäten und Echtzeitanalyse des abgefangenen Traffics. Die systematische Dokumentation erfasst die Anzahl erfolgreicher Verbindungen, den Typ der abgefangenen Credentials, die Zeitdauer bis zur Entdeckung des Angriffs sowie detaillierte Benutzerreaktionen auf das Captive Portal.

Schutzmaßnahmen und Risikobewertung

Die Evaluation von Schutzmaßnahmen unterscheidet zwischen technischen Kontrollen und organisatorischen Maßnahmen. Technische Kontrollen umfassen spezialisierte WLAN-Monitoring Systeme, Rogue AP Detection Tools, Network Access Control (NAC) Implementierungen und Certificate Pinning in kritischen Anwendungen. Organisatorische Maßnahmen beinhalten umfassende Security Awareness Trainings, klar definierte WLAN-Nutzungsrichtlinien, etablierte Incident Response Procedures und regelmäßige Security Audits zur kontinuierlichen Verbesserung der Sicherheitslage.

Die Risikobewertung identifiziert schwerwiegende potenzielle Auswirkungen wie die Kompromittierung von Benutzer-Credentials, mögliches Lateral Movement im Netzwerk, unkontrollierte Datenexfiltration und resultierende Compliance-Verletzungen. Entsprechende Empfehlungen umfassen die zeitnahe Implementierung von WPA3-Enterprise Standards, das Deployment professioneller WLAN-Monitoring-Lösungen, verstärkte und regelmäßige Mitarbeiterschulungen sowie die Etablierung regelmäßiger

Penetrationstests als präventive Maßnahme. Bei der Durchführung sind rechtliche Aspekte zwingend zu beachten: ausschließliche Durchführung mit schriftlicher Genehmigung, strikte Einhaltung lokaler Gesetze und Vorschriften, lückenlose Dokumentation aller Testaktivitäten sowie die sichere und vollständige Löschung aller gesammelten Daten nach Testabschluss.