

Penetrations Tests Im Unternehmen Angriffe Auf Dienste Programme Und Netzwerke By Thomas Werth

Penetrationstests für cloud dienste durchführen. cyber sicherheit und ethical hacking für ihr unternehmen. e government penetrationstest mittelstandswiki. penetrationstest holzhofer consulting gmbh münchen. mitarbeiter im visier der penetrationstester. social engineering penetration test bp networks. penetration test pwc. penetrationstest der it security check. redfox infosec gmbh penetration tests ablauf und. penetrationstest ist nicht gleich it daily net. testing fraunhofer aisec. 0aa8740 penetrationstests m unternehmen angriffe auf. so können unternehmen iam für die cloud richtig umsetzen. rainbow six siege ubisoft verklagt ddos for hire dienst. penetrationstest schutzwerk. penetrationstest thinking objects security.

Copyright : [Discover our free PDF eBook collection and start your journey to greatness](#)

Das Sicherheitsniveau eines Netzwerks und seiner Systeme kann nur durch gezielte Überprüfungen festgestellt und bewertet werden. Damit die Ergebnisse nicht zufällig sind, sondern jederzeit nachvollzogen werden können, muß bei den Penetrations-Tests unbedingt strukturiert gearbeitet werden. Thomas Werth, der Autor der gleichnamigen Java-Attacke und der Backdoor RATTE für das Umgehen von Firewalls, die beide Bestandteile von SET sind, stellt mit diesem Buch einen systematischen Leitfaden für Sicherheitsadministratoren zusammen. Er zeigt Angriffe auf verschiedene Netzwerktypen, einzelne Dienste und in Unternehmen weit verbreitete Programme. Dabei sind die Ziele jedes Angriffs einzeln aufgeschlüsselt und die verschiedenen Verfahren werden genau beschrieben, mit denen versucht wird, Zugriff auf das jeweilige System und seine Daten zu erlangen. Unter anderem werden Firewalls überwunden, SAP-Systeme kompromittiert, Webbrowser überlistet und Backdoors implementiert. Damit sich der Leser die Installation der zahlreichen Einzelwerkzeuge spart, werden die Testreihen im Buch mit der Spezialdistribution Backtrack durchgeführt. Alle Arbeitsmittel werden aber so ausführlich beschrieben, daß sich jeder auch seine eigene Testumgebung aufbauen kann. Marc Ruef: In 'Die Kunst des Penetration Testings' habe ich mich auf die konzeptionellen und strategischen Aspekte von Sicherheitsüberprüfungen konzentriert. Thomas Werth geht einen Schritt weiter und zeigt die konkreten Angriffsverfahren für Dienste, Programme und Netzwerke. Die

Themen:- Testmethodik nach dem Open Source Security Testing Methodology Manual (OSSTMM)- Die Exploit-Frameworks Metasploit, Social Engineering Toolkit und Web Application Attack and Audit Framework- Informationsgewinnung im Internet und über Social Engineering- 26 Serverdienste abtasten und angreifen- Unbekannte Dienste erkennen und untersuchen- Authentifizierungen umgehen - Implementieren von Backdoors- WLANs knacken- Firewalls umgehen- Terminalsysteme kontrollieren- Anwendungen penetrieren: Internet-Browser, SAP ERP, Office-Dokumente und TrueCrypt

