

Hacking I

Netzwerkangriffe verstehen

Im Rahmen der Cyber Security kann ein wirksamer Schutz vor Angriffen aus dem Internet oder dem eigenen Netzwerk nur gewährleistet werden, wenn die mit der Sicherheit betrauten Personen die Motivation und der Herangehensweise der unterschiedlichen Angreifer kennen und verstehen. In diesem Seminar wird das methodische Vorgehen eines Hackers von der Informationsbeschaffung über die Planung bis zur Durchführung eines Angriffs vorgestellt. Einen weiteren wichtigen Aspekt bildet die Analyse eines Sicherheitsvorfalls mit Hilfe der digitalen Forensik. Die Kursinhalte werden anhand praktischer Übungen vertieft. In einer Testumgebung lernen Sie die Methodik eines Hackers kennen, um dann in einem Testnetz aktive Angriffe zu simulieren. So ist es Ihnen möglich, Ihr eigenes Netzwerk auf Schwachstellen zu überprüfen und gegen Angriffe abzusichern.

Kursinhalt

- Motivation und Methodik der Angriffe
- Werkzeuge von Hackern
- Malware – Von Viren bis Rootkits
- Sniffing und Man-in-the-Middle-Angriffe
- LAN und WLAN-Angriffe
- Protokolle missbrauchen
- Informationsbeschaffung – Reconnaissance und Enumeration
- Netzwerke auskundschaften
- Portscan und Fingerprinting
- Vulnerability Checks
- Exploitation mit Metasploit
- Kennwortangriffe
- Methoden der Digitalen Forensik
- Angriffsspuren sichern
- Sicherheitsvorfälle analysieren

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Diese Schulung richtet sich an Personen, zu deren Aufgabe die Sicherung des Netzwerks und der angeschlossenen Server vor Hackerangriffen zählt.

Voraussetzungen

Gute IP-Kenntnisse sowie Grundkenntnisse zu Router-Netzen sind erforderlich. Praktische Erfahrung im Umgang mit Netzwerken ist sehr hilfreich. Der Kurs TCP/IP – Protokolle, Adressierung, Routing ist eine gute Vorbereitung.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/HACK

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	5 Tage CHF 3.075,-
Termine in Österreich	5 Tage CHF 3.075,-
Termine in der Schweiz	5 Tage CHF 3.690,-
Online Training	5 Tage CHF 3.075,-
Termin/Kursort	Kurssprache Deutsch
13.05.-17.05.24 Düsseldorf	05.08.-09.08.24 Zürich
13.05.-17.05.24 Online	09.09.-13.09.24 Frankfurt
01.07.-05.07.24 Berlin	09.09.-13.09.24 Online
01.07.-05.07.24 Hamburg	14.10.-18.10.24 Online
01.07.-05.07.24 Online	14.10.-18.10.24 Wien
05.08.-09.08.24 München	18.11.-22.11.24 Düsseldorf
05.08.-09.08.24 Online	18.11.-22.11.24 Online

Stand 14.04.2024

Inhaltsverzeichnis

Hacking I – Netzwerkangriffe verstehen

1	Netzwerkangriffe – Ein Motiv und Vorgehen	3.6.3	NDP Attacks	6.2.5	Application Scanning
1.1	Vielfältige Bedrohungen	3.6.4	ICMPv6 angreifen	6.3	Scans aus Sicherheits-Sicht
1.2	Klassifizierung von Angreifern	4	Sniffing in geschwichten Netzen	7	Schwachstellenanalyse
1.2.1	Freizeitthacker	4.1	Daten mitlesen	7.1	Schwachstellen aufdecken
1.2.2	Professionelle Angreifer	4.1.1	Sniffing – Ein lokaler Angriff	7.1.1	Mehrwert der Schwachstellenanalyse
1.2.3	Wirtschaftliche Interessen	4.1.2	Sniffing Tools	7.1.2	Hintergründe der Schwachstellenanalyse
1.2.4	Cyberterrorismus	4.2	LANs im Wandel der Zeit	7.1.3	Grenzen der Schwachstellenanalyse
1.3	Motivation zum Angriff	4.2.1	Switching – Das Prinzip	7.2	Arten von Schwachstellenanalysen
1.3.1	Sabotage	4.2.2	Broadcast und Multicast – Flooding	7.2.1	Umfang der Schwachstellenanalyse
1.3.2	Spionage	4.3	Man in the Middle Attacks	7.2.2	Continuous Vulnerability Management
1.3.3	Missbrauch	4.3.1	Flooding des Switches	7.2.3	Mit oder ohne Anmeldung
1.4	Angriffe – Das Vorgehen	4.3.2	Port Stealing	7.3	Schwachstellenanalyse in der Praxis
1.4.1	Ziele lokalisieren	4.3.3	IPv4 – ARP Cache Poisoning	7.3.1	Cloud-based Scans
1.4.2	Angriffsziel festlegen	4.3.4	IPv6 – Neighbor Cache Poisoning	7.3.2	Reporting
1.4.3	Angriffsplan erstellen	4.4	Tools für Sniffing Attacks	7.4	Tools zur Schwachstellenanalyse
1.4.4	Angriff ausführen	4.4.1	Ettercap	7.4.1	Nessus – Der Tenable Scanner
1.4.5	Nachbereitung des Angriffs	4.4.2	Ettercap-Plugins	7.4.2	OpenVAS und Greenbone
1.5	Quellen für Hackertools	4.5	Schutz durch Verschlüsselung	7.4.3	Rapid7 – Nexpose und insight VM
1.5.1	Pen Testers Framework – PTF	4.5.1	Der TLS-Verbindungsaufbau	7.4.4	Qualys Cloud Platform
1.5.2	Linux-Hacking-Distributionen	4.5.2	SSL/TLS Interception Attack	8	Penetrations-Tests
1.5.3	Kali Linux anpassen	5	WLAN-Angriffe	8.1	Penetrations-Test – Hintergründe
1.5.4	Mobile Endgeräte als Angriffswerkzeug	5.1	WLAN – Sicherheitsüberlegungen	8.2	Planung von Penetrations-Tests
2	Informationsbeschaffung	5.2	WLANs auskundschaften	8.2.1	Auftrag und Zieldefinition
2.1	Unternehmensinformationen sammeln	5.2.1	Der Monitor Mode	8.2.2	Rechtliche Rahmenbedingungen
2.1.1	Das WWW als Informationsquelle	5.2.2	Die SSID ermitteln	8.2.3	Klassifizierung von Penetrations-Tests
2.1.2	Suchmaschinen verwenden	5.2.3	WLAN-Sniffing	8.2.4	Berichterstattung
2.2	Zielnetze und Server lokalisieren	5.2.4	Verschlüsselung und Authentisierung in WLANs	8.3	Penetration Testing Standards
2.2.1	RIPE & Co. – Wem gehört das Netz?	5.3	WEP – Angriffe ganz einfach	8.4	Varianten von Penetration Tests
2.2.2	DNS – Wer hat die Domain registriert	5.4	WPA und WPA2: Wi-Fi Protected Access	8.4.1	Physical Assessment
2.2.3	Mailserver auskundschaften	5.4.1	WPA1/2 – PSK-Angriff	8.4.2	Netzwerk-Infrastruktur
2.3	Footprinting durch DNS	5.4.2	WPA1/2 – Deauthentication	8.4.3	Exploitation von Servern
2.3.1	Nslookup, dig und Co.	5.4.3	WPA1/2 – Cracking	8.4.4	Social Engineering
2.3.2	Zonentransfers	5.5	WPS-Angriffe	8.5	Pentesting Frameworks
2.3.3	Wörterbuchangriff auf die Zone	5.6	WLAN-Cracking-Tools	8.5.1	Metasploit
2.3.4	Reverse Lookups	5.6.1	Wifite	8.5.2	Armitage – Ein GUI für Metasploit
2.4	Netzwerke auskundschaften	5.6.2	Airgeddon – WLAN Attack Toolset (1/3)	8.5.3	Post Exploitation
2.4.1	Passiv – Einfach nur lauschen	5.6.3	Fern Wifi Cracker	8.6	Kenntwort-Sicherheit hinterfragen
2.4.2	Aktive Varianten	5.7	WPA1/2-Enterprise – Sicherheit durch IEEE 802.1X	8.6.1	Kenntwörter erraten
2.4.3	Traceroute zum Firewall-Scanning	5.8	WPA3 – Verbesserte Sicherheit	8.6.2	Password Sniffing
3	Netzwerke angreifen	5.8.1	Easy Connect und PMF statt WPS	8.6.3	Offline Password Cracking
3.1	Gefahren im internen Netz	5.8.2	Dragonblood – Authentication Attacks	8.6.4	Online Password Guessing
3.2	Infrastruktur-Angriffe	5.9	Rogue AP Attacks	9	Digitale Forensik
3.2.1	Physikalische Schutzmaßnahmen	5.9.1	Airbase-ng – Evil Twin Attack	9.1	Forensik und Digitale Forensik
3.2.2	IEEE 802.1X - LAN-Access kontrollieren	5.9.2	Berate-ap – Rogue WPA1/2 AP	9.2	Modelle und Vorgehen
3.2.3	Visibility – Das Netzwerk im Blick behalten	5.9.3	Angriff auf WPA1/2-Enterprise	9.2.1	Secure – Beweissicherung
3.3	LAN-Attacks	5.10	Captive Portal Attacks	9.2.2	Analyse – Daten auswerten
3.3.1	Angriffe auf ARP	5.10.1	WifiPumpkin3 – WLAN Attack Framework	9.2.3	Present – Bericht erstellen
3.3.2	Spanning-Tree-Angriffe	5.10.2	Schutzmaßnahmen gegen Captive Portal Attacks	9.3	Computerforensik
3.3.3	Autokonfiguration von Trunks	5.11	DoS auf Management Frames	9.3.1	Speicherforensik
3.4	IPv4 und ICMPv4 Attacks	6	Port Scanning	9.3.2	Mobile Device Forensik
3.4.1	Routing Protokolle angreifen	6.1	Port Scanning – Applikationen detektieren	9.3.3	Betriebssysteme untersuchen
3.4.2	VRPP und HSRP-Angriffe	6.1.1	IPv4 vs. IPv6-Scans	9.3.4	Anwendungen analysieren
3.4.3	DHCP-Angriffe	6.1.2	TCP Scanning	9.4	Netzwerk Forensik
3.5	Tools für Layer2/3-Angriffe	6.1.3	UDP Scanning	9.4.1	Netzwerkverkehr aufzeichnen
3.5.1	Hyenae	6.1.4	Scanning Tools	9.4.2	Log-Dateien auswerten
3.5.2	Yersinia	6.2	Advanced Scanning	9.5	Cloud Forensik
3.5.3	Scapy	6.2.1	OS Detection	9.6	Linux-Forensik-Distributionen
3.5.4	Scapy-Angriff am Beispiel HSRP	6.2.2	Applikationen detektieren		
3.6	IPv6 – Neue Funktionen, neue Möglichkeiten	6.2.3	Version Detection		
3.6.1	ATK6 – Die THC-Toolsammlung	6.2.4	Script Scanning		
3.6.2	Adressen – Randomized statt EUI64				

