(Anti-)Hacking für Administratoren

Kursnummer: 6710

Ziele

In diesem Workshop simulieren Sie, nach einer umfangreichen Einführung in die Grundlagen der IT-Sicherheit, die Rolle des Angreifers bzw. Hackers. Sie attackieren dafür extra installierte Computersysteme bis hin zu Windows 10 und auch Windows Server 2016.

Sie erhalten einen zumeist praktischen Einblick in die Vielfalt der Methoden und Werkzeuge der Angreifer auf Netzwerke, Computersysteme und Dienste. Durch diesen Perspektivwechsel soll das Bewusstsein für Sicherheitsrisiken und Schutzmaßnahmen - und somit die Sicherheit in Unternehmen erhöht werden.

Inhalt

Modul 00 - Einführung
• In diesem Modul erhalten Sie neben der Einführung unter anderem auch einen detaillierten Überblick über den zeitlichen und inhaltlichen Ablauf des Workshops.

Modul 01 - Grundlagen der IT-Sicherheit
• Dieses Modul enthält Informationen über die Gründe für Cyberangriffe, sowie die verschiedenen Arten von Angreifern (Hackern), mit denen man sich als Administrator oder auch Systemverantwortlicher konfrontiert sieht. Weiterführend werden die häufigsten Arten von Sicherheitslücken, sowie auch die zumeist genutzten Methoden bei Hackerangriffen erläutert. Darüber hinaus erfahren Sie wichtige, grundlegende Informationen zu den rechtlichen Grundlagen rund um die IT-Sicherheit.

Modul 02 - Planung und Vorbereitung von Angriffen
• In diesem Modul erfahren Sie, mit welchen Möglichkeiten Angreifer an die notwendigen Informationen gelangen, um Unternehmen oder auch Unternehmensmitarbeiter im Internet ausfindig zu machen. Die Informationsgewinnung wird Ihnen anhand einer Auswahl an Tools und Methoden praktisch vorgestellt. Nachdem ein Angreifer sein potentielles „Opfer“ ausfindig gemacht hat, recherchiert er oft auf verschiedene Weisen nach weiteren Informationen über das betroffene Unternehmen. Hierbei bedient er sich neben den gängigen Suchmaschinen u. a. auch den Informationen in Newsgroups, Boards usw. und verwendet weitere, speziell zur Recherche entwickelte Tools und Methoden. Diese werden Ihnen in diesem Modul ausgiebig und detailliert erklärt.

Modul 03 - Moderne Angriffstechniken
• Nachdem Sie erfahren haben, wie Angreifer ihre Opfer ausfindig machen und nach möglichen Schwachstellen forschen können, befasst sich dieses Modul nun mit den eigentlichen, oft der Recherche gleichauf folgenden Angriffsszenarien. In diesem Modul erhalten Sie einen umfangreichen Überblick über moderne Tools und Methoden, die von Hackern zum Einbruch in Computernetzwerke der weltweit angesiedelten Firmen, Behörden und Institutionen, sowie auch in Computersysteme genutzt werden. Hierbei sollen Sie die verschiedenen Merkmale der Tools und Vorgehensweisen erkennen, um die Sicherheitsrichtlinien in Ihrem Netzwerk darauf ausrichten zu können.

Modul 04 - Gefahren durch Viren, Würmer, Trojaner & Rootkits
• Die Gefahr durch Viren, Würmer, Trojaner, Malware, Ransomware und Rootkits bedroht nicht nur die vielen privat genutzten PCs und Mobiltelefone, sondern insbesondere auch die in Unternehmen betriebenen Computersysteme und Server - und natürlich insbesondere die darin verarbeiteten und gespeicherten Unternehmensdaten. In diesem Modul werden die aktuellen Gefahren, sowie die möglichen Abwehrmaßnahmen anhand praktischer Beispiele detailliert erläutert.

Modul 05 - Angriffe auf Drahtlosnetzwerke (WLANs)
• Die Mobilität der Mitarbeiter steht in Unternehmen und Behörden immer mehr im Vordergrund. Hierbei werden häufig mobile Geräte, wie zum Beispiel Tablet-PCs, Smartphones und Notebooks eingesetzt, mit denen man sich über Drahtlosnetzwerke (Wireless LANs) oder Bluetooth auf die Unternehmensnetzwerke und -server verbindet, um Daten abzurufen oder zu speichern. In diesem Modul werden Ihnen Tools und Methoden aufgezeigt, mit denen Angreifer die drahtlosen Netzwerke ausspähen oder gar hacken können. Die Veranschaulichung soll Ihnen für die mögliche Absicherung der drahtlosen Netzwerkkomponenten und -geräte, u. a. mithilfe der Spezifikation IEEE 802.1x dienlich sein, die Ihnen im Verlauf des Workshops detailliert erklärt wird.

Modul 06 - Firewalls, IDS & Honeypots
• In diesem Modul erhalten Sie einen grundlegenden Überblick über Firewall-Lösungen verschiedener Hersteller. Zudem werden Ihnen mögliche Lösungen zum Einrichten von Netzwerk- oder Hostbasierten IDS-Systemen und sogenannter Honeypots praktisch erklärt, um Angriffe von Hackern frühzeitig erkennen, sowie nach Möglichkeit abwehren und im Bedarfsfall auch rückverfolgen zu können.

Modul 07 - Einführung in Penetrationstests
• Um mögliche Sicherheitslücken aufdecken und beseitigen zu können, müssen das eigene Netzwerk, sowie die darin enthaltenen Server und Clients regelmäßig auf mögliche Schwachstellen untersucht werden. In diesem Modul erfahren Sie mehr über die Planung,

ce - corporate education GmbH
Bonner Str. 178
50968 Köln
Fon: +49 221 | 29 211 6 - 0
Fax: +49 221 | 211 6 -19

Niederlassung Essen
Zeche Zollverein 4/5/11
Katernberger Str. 107
45327 Essen
Fon: +49 201 | 89 06 00 30
Fax: +49 201 | 89 06 00 39

E-Mail: info@ce.de
Web: www.ce.de

(Anti-)Hacking für Administratoren

Kursnummer: 6710

Vorbereitung, Durchführung und Auswertung von sogenannten Penetrationstests.

OPTIONALE MODULE:
Modul 08 - Grundlagen der Kryptografie
Modul 09 - Einführung in das BSI-Grundschutzkompendium

Zielgruppe

System- und Netzwerkadministratoren, IT- und Systemverantwortliche, IT-Sicherheitsbeauftragte, IT-Architekten

Voraussetzungen

• Kenntnisse und Fähigkeiten in der Konfiguration und Verwaltung von Windows-Betriebssystemen • Grundlegende Erfahrung in der Verwaltung von Netzwerkdiensten • Kenntnisse zu LANs (Local Area Networks) - lokalen Netzwerken • Kenntnisse und Fähigkeiten im Umgang mit TCP/IP

Ihr Ansprechpartner

Dagmar Kedwesch

Manager Customer Relation | Köln

Fon: 0221 | 29 21 16 - 11
Mobil: 0178 | 72 13 76 5

E-Mail: vertrieb@ce.de

Ihr Ansprechpartner

Hartmut Nithack

Manager Customer Relation | Essen

Fon: 0201 | 89 06 00 - 30
Mobil: 0178 | 33 66 17 3

E-Mail: vertrieb@ce.de