HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE-ONLINE-KURS

M 63

Ein neuer zweitägiger Kurs in deutscher Sprache

Hardening Microsoft Environments

Lernen von den Profis – Ihre Trainer sind Friedwart Kuhn, Heinrich Wiederkehr, Lennart Brauns, René Mathes – Zwei der vier genannten Referenten leiten den Kurs.

Kursbeschreibung

Angriffstechniken der Kategorie „Credential Theft“ und „Credential Reuse“ sind in den letzten Jahren zu einer der größten Bedrohungen für Microsoft Windows-Umgebungen herangewachsen. Begünstigt wurde diese Entwicklung in den letzten Monaten durch die signifikante Verbesserung und weite Verbreitung von Angriffstools, wie etwa mimikatz, *Windows Credential Editor* oder *Bloodhound.* Dies führte dazu, dass bis dahin theoretisch mögliche Angriffe praktisch umsetzbar wurden. Nachdem ein Angreifer initial auf einem einzelnen System Fuß fassen konnte, dauert es, unter der Anwendung der vorher genannten Methoden, oft keine 48 Stunden, bis die gesamte Active Directory Infrastruktur, inklusive der Domain Administratoren Credentials, kompromittiert ist. Fehlerhafte Konfiguration von Active Directory-Trusts erlaubt es Angreifern, von einem Forest zum anderen zu springen. Doch wie ist mit einer solchen Bedrohung umzugehen? In diesem zweitägigen Intensivseminar werden verschiedene technische und organisatorische Maßnahmen vorgestellt, um sowohl einzelne kritische Microsoft Windows-Systeme, vom Mitgliedssystem bis zum Domain Controller, als auch hochpriveligierte Active Directory Accounts bestmöglich vor Credential Theft zu schützen und den unautorisierten Einsatz gestohlener Credentials möglichst frühzeitig zu erkennen und zu unterbinden.

Fortsetzung auf Seite 2

29.-30. September 2021, Online
08.-09. Dezember 2021, Online
08.-09. Februar 2022 – Online

Diese Veranstaltung wird als Weiterbildung bei Rezertifizierungsmaßnahmen von verschiedenen Instituten anerkannt.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

Hardening Microsoft Environments

M 63

Ein neuer zweitägiger Kurs in deutscher Sprache

Eine Teilnahme am Kurs ist von jedem PC/Laptop mit stabiler Internetverbindung aus möglich. Es wird keine zusätzliche Software benötigt. Wir empfehlen die Verwendung von Google Chrome - falls möglich, andernfalls sind Firefox und Edge auf Chrome Basis unterstützt. Wir empfehlen eine direkte Internetverbindung. Wenn der Zugriff über ein VPN erfolgt, kann es zu qualitativen Einschränkungen kommen, die nicht in unserem Einflußbereich liegen. Auch der Zugriff auf das Training erfolgt über den Browser. Übungen können also ebenfalls realisiert werden, ohne dass zusätzliche Software benötigt wird. Die Schulung wird selbstverständlich live aus dem ERNW-Studio übertragen. Das Kursmaterial, sowie mögliche Demos und natürlich die Trainer sind stets sichtbar und werden je nach Erfordernis gezeigt bzw. hervorgehoben. Das Schulungsmaterial stellen wir Ihnen zusätzlich im Vorfeld elektronisch zur Verfügung. Fragen werden direkt von den Trainern beantwortet. Mikrofon und/oder Kamera sind optional, Sie können die Fragen auch über einen Chat stellen.

Das Seminar beginnt mit einer kurzen Einführung, in der die Relevanz und Tragweite von Credential Theft und Credential Reuse verdeutlicht werden und wie sich die Denkweise aus Verteidigersicht ändern muss, um diese Bedrohungen effektiv adressieren zu können. Nach dieser Einleitung wird technisch tiefer eingestiegen und die Grundlagen von Authentifizierungsmechanismen in Microsoft Windows-Umgebungen werden auf profunde Art und Weise beleuchtet. Schwerpunkte sind hierbei vor allem die Rolle des Local Security Authority Subsystem (LSASS) und das Zusammenspiel mit dem NTLM- und Kerberos-Protokoll sowohl in Bezug auf die lokale Authentifizierung als auch auf die Kerberos-basierte Netzwerkauthentifizierung. Insbesondere die Funktionsweise von Kerberos und seine Implementierung in Active Directory, sowie wie dies von einem kompetenten und motivierten Angreifer ausgenutzt werden kann, werden im Detail erläutert.

Aufbauend auf diesem Wissen können dann die relevanten Schwachstellen und Bedrohungen, inklusive ihrer resultierenden Angriffsszenarien verstanden werden. Weitergehend werden verschiedene Angriffstechniken vorgestellt, die am zweiten Tag dann praktisch umgesetzt werden: Diese reichen vom vergleichsweise einfachen Pass-the-Hash zu komplexen Arten wie dem sog. „Golden Ticket“. Anhand praktischer Übungen werden die relevanten Angriffe von den Teilnehmern durchgeführt, um ein Grundverständnis für die Angreiferseite zu vermitteln:

- Pass-the-Hash
- Pass-the-Ticket
- Overpass-the-Hash/Pass-the-Key
- Golden, Silver & Inter Realm Tickets

Nachdem die Bedrohungen und Risiken näher eingegrenzt wurden, werden Maßnahmen vorgestellt und diskutiert, um die Effektivität von Credential Theft und Credential Reuse einzuschränken. Diese setzen sowohl auf der Designebene als auch auf prozessualer und technischer Ebene an. Zu den wichtigsten Maßnahmen zählen hierbei:

- Admin Tiering /Credential Partitioning
- Sichere Administration
- Sichere Konfiguration von Trusts
- Credential Guard
- Authentication Policy Silos
- Security Monitoring
- u.v.m.

Auch auf Windows Server 2016 und Windows 10 spezifische neue Kontrollen, wie Credential Guard und Device Guard wird eingegangen werden.

Bei der Diskussion der Maßnahmen wird sowohl auf ihre Wirksamkeit als auch die Umsetzbarkeit im realen Betrieb eingegangen. Besonderes Augenmerk wird hierbei auf das Security Monitoring im Active Directory gelegt, da dieses eine entscheidende Rolle in der Erkennung und Risikominimierung von Credential Reuse Angriffen spielt. Dabei wird nicht nur das Active Directory Auditing durch das Security Event Logging beleuchtet, sondern auch wie ganz spezifisch Pass-the-Hash oder Golden Ticket Angriffe erkannt werden können.

Begleitet wird der Vortrag des Seminars von praktischen Übungen und Demonstrationen, um das Theoretische zu veranschaulichen und das Gelernte anzuwenden.

Hardening Microsoft Environments

M 63

Ein neuer zweitägiger Kurs in deutscher Sprache

Seminarinhalte

Tag 1

Einführung

- Relevanz und Aktualität von Credential Theft und Credential Reuse
- Grundlagen der Windows Authentifizierung
- Security Subsystem Architecture in Windows
- Local Security Authority Subsystem Service
- Lokale Authentifizierung
- LM/NTLM Netzwerkauthentifizierung
- Kerberos Netzwerkauthentifizierung

Credential Theft & Reuse Angriffe

- Einführung in mimikatz
- Pass-the-Hash
- Pass-the-Ticket
- Overpass-the-Hash/Pass-the-Key
- Golden & Silver Ticket
- PtT in Ubuntu und Mac OS X

Praktische Übungen zu allen genannten Angriffstechniken

Erster Überblick über die relevanten Maßnahmen zur Risikominimierung

- Reorganisation der Active Directory Struktur und Administrationspraktiken
- Technische, Credential-Theft-spezifische Maßnahmen
- Security Monitoring & Logging

Tag 2

Detaillierte Betrachtung und Diskussion der relevanten Maßnahmen zur Risikominimierung

- Voraussetzungen
- Organisation- und Designmaßnahmen
  - o Admin Tiering
  - o ESAE Forest
- Technische Maßnahmen
  - o Sichere Administrationshosts
  - o Sichere Konfiguration von Domain Controller & Domain-Membern
  - o Credential-Theft-spezifische Maßnahmen
  - o Neue Kontrollen eingeführt mit Windows Server 2016 und Windows 10

Active Directory Monitoring

- Überblick über das Windows Event Logging
- Allgemeine Monitoring-Maßnahmen
- Zentralisiertes Logging
- Grundlagen der Advanced Audit Policy
- Spezifische Monitoring-Maßnahmen
  - o Konkrete, zu auditierende Events
    - Account-Nutzung
    - Software-Installation
    - Dienst-Installation
    - Registry-Auditing
  - o Erkennung von PtH, PtT und Golden Tickets

Praktische Übung zur Erstellung einer Advanced Audit Policy

HM TRAINING SOLUTIONS ON-SITE SERVICE

Alle HM Training Solutions Seminare stehen auch firmenintern zur Verfügung. Sie können auf den Bedarf Ihrer Organisation zuge schnitten werden. Weitere Details erhalten Sie unter der Telefonnummer +49 (0) 6022 508 200.

Hardening Microsoft Environments

M 63

Ein neuer zweitägiger Kurs in deutscher Sprache

Warum Sie teilnehmen sollten

Das Seminar versetzt Sie damit in die Lage, folgende Fragen qualifiziert zu beantworten:

- Welche Bedrohungen gehen von Credential Theft & Credential Reuse aus und welche Risiken ergeben sich daraus?
- Welche Maßnahmen mindern bestmöglich die Effektivität von Credential Theft- und Credential Reuse-basierten Bedrohungen in Active Directory-Umgebungen?
- Welche Maßnahmen führen zu einer möglichst frühzeitigen Erkennung von Credential Theft und Credential Reuse?
- Welche Aufwände und Kosten bringen Implementierung und Betrieb dieser Maßnahmen mit sich?
- Wie kann EMET effektiv in der Unternehmensinfrastruktur eingesetzt werden?

Zielgruppen

- IT-Sicherheitsbeauftragte
- Windows & Active Directory Administratoren
- Projektmanager mit Sicherheitsfokus
- Infrastruktur- und Systemarchitekten
- Systemintegratoren
- IT-Leiter & Datenschutzbeauftragte

Teilnahmevoraussetzungen

- Eigener Laptop
- Wir stellen die Möglichkeit bereit sich über RDP mit der virtuellen Testumgebung zu verbinden.
- Die Verbindung wird über Wifi oder Ethernetkabel hergestellt.

Teilnehmerstimmen zum Kurs

»Lernen von Dozenten, die wirklich Ahnung haben.«
Robert Bosch GmbH, Stuttgart

»Komplexe Themen verdaubar vermittelt.«
Hug Kern-Liebers, Sebastian Fehrenbacher, IT-Projektleiter, Schramberg

»Selbst als Windows-Laie war der Kurs verständlich. Tolle Trainer mit Praxis-Erfahrung.«
Angela Espinosa, Deutsche Lufthansa, Frankfurt/M.

»Inhaltlich auf sehr hohem Niveau, sehr gute persönliche Betreuung, sehr wertvolle Informationen.«
Andreas Lingelbach, Gruppenleiter Windows, Citrix, SAP,
stellv. Bereichsleitung, Kommunale Datenzentrale Mainz

»Herr Kuhn und Herr Wiederkehr sind zwei äußerst kompetente Redner. Spannendes Seminar in einem super Hotel.«
GESIS Gesellschaft für Informationssysteme mbH, Hendrik Will,
Engineer Server Team Infrastruktur und Betrieb, Salzgitter

»Sehr praxisnah, viele Beispiele genannt fernab der Folien. Super! Anwendungsszenarien aufgezeigt, die auch leicht implementiert werden können«
Doreen Michaelis, System Admin./AD-Admin.,
Robert Koch-Institut, Berlin

„Super Schulung, geht sehr in die Tiefen des Systems.“
Malte Hübner, Admin., Computer-Centrum Nord

„Sehr kompetente Trainer die auch bei Nachfragen jenseits der reinen Schulungsunterlagen nie ins Schlingern kamen und alles direkt und umfassend beantworten konnten.“
Jens Roesen, Security Manager, Universität Würzburg

Hardening Microsoft Environments

M 63

Ein neuer zweitägiger Kurs in deutscher Sprache

Profil der Seminarleiter

Der Kurs wird von zwei der vier genannten Referenten gehalten.

Ihr Trainer, Friedwart Kuhn ist ein führender Experte im Bereich von Windows Sicherheit im Allgemeinen und Active Directory-Sicherheit im Besonderen. Er kennt das Active Directory seit es auf dem Markt ist und hat in über 15 Jahren eine Vielzahl von Projekten um die Themen Windows- und Active Directory Sicherheit geleitet. Seine Aufgabentätigkeit um fasst alle Projektaspekte vom sicheren Design bis zum sicheren Betrieb von großen Microsoft-Umgebungen. Herr Kuhn arbeitet schwerpunktmäßig im Bereich des Security Assessments von Microsoft-basierten Umgebungen, und ist dort als Pentester sowohl auf der Angreiferseite als auch als Auditor und Consultant auf der Verteidigerseite tätig. Seine jahrelange Referententätigkeit, aber auch sein technischer Hintergrund ermöglichen es ihm, auf Schulungen allen Beteiligten technische aber auch organisatorische Sachverhalte einfach nahe zu bringen. Als Sprecher auf internationalen Sicherheitskonferenzen und -kongressen vermittelt er komplexe sicherheitsrelevante Themen auf eine anschauliche und verständliche Art und Weise. Friedwart Kuhn ist Mitinhaber der ERNW GmbH und leitet ein eigenes Team von ausgewiesenen Sicherheitsexperten.

Ihr Trainer, René Mathes ist langjähriger Auditor und Penetrationstester. Im Rahmen seiner Tätigkeit als IT-Security Consultant berät er seit über 10 Jahren ein umfassendes Portfolio unterschiedlichster Kunden: Mittelstand bis weltweit aufgestellte „Global Player“, Werbung bis Schwerindustrie. Als Tutor entwickelt er Kurse, die er deutschlandweit zum Beispiel für Teilnehmer aus der Welt der Finanzen hält.

Ihr Trainer, Lennart Brauns ist Security Consultant bei der ERNW GmbH und Teil des Microsoft Security Teams @ ERNW. In langjähriger Tätigkeit für Unternehmen der kritischen Infrastruktur hat Herr Brauns umfassende Kenntnisse über Microsoft Windows, Active Directory und Microsoft Azure erworben.
Seine Schwerpunkte liegen in der Forschung sowie der Konzeption und Bewertung verschiedener Bereiche von Windows-Umgebungen.
Neben Sicherheitstrainings konzentriert sich seine Arbeit auf Audits und Pentests von Unternehmensnetzwerken mit dem Schwerpunkt Active Directory.

Ihr Trainer, Heinrich Wiederkehr ist Security Consultant bei der ERNW GmbH und Teil des Microsoft Security Team@ERNW. Seine Schwerpunkte liegen in der Forschung sowie der Konzeption und Bewertung verschiedener Bereiche von Windows-Umgebungen. Neben Sicherheitstrainings konzentriert sich seine Arbeit auf Audits und Pentests von großen Unternehmensnetzwerken mit dem Schwerpunkt Active Directory.

DETAILS ZUM ANMELDEFORMULAR

Drei Wege zur Anmeldung

Per Post: Bitte dieses Anmeldeformular ausfüllen und an HM Training Solutions senden.
Per Fax: Bitte dieses Formular an folgende Faxnummer senden: +49 (0) 6022 508 9999.
Per E-Mail: **Info@hm-ts.de**
Per Webseite: https://www.hm-ts.de

Gebühren

1.990 €. + 19% MwSt. (für unsere Teilnehmer*innen aus Österreich, Schweiz usw. berechnen wir den Nettobetrag).

Bestätigungsbrief

Ihre Anmeldung bestätigen wir per Mail oder Brief. Er enthält Details über die Veranstaltung.

Änderungen

HM Training Solutions behält sich das Recht vor, bei Eintreten nicht vorhersehbarer Umstände das Seminar räumlich und/oder zeitlich zu verlegen, einen anderen Referenten ersatzweise einzusetzen oder die Veranstaltung zu stornieren. Weitergehende Ansprüche bestehen nicht.

Stornierung seitens des Teilnehmers

Bitte reichen Sie Stornierungen schriftlich per Post, Fax, (Fax-Nr. +49 (0) 6022 508 9999) oder Email (info@hm-ts.de), ein. Bestätigte Anmeldungen können bis zu sechs Wochen vor Seminarbeginn kostenfrei storniert werden, danach berechnen wir die gesamte Seminargebühr. Eine Übertragung an einen Ersatzteilnehmer istm jederzeit möglich.

Firmeninterne Seminare

Alle Trainings von HM Solutions können auch firmenintern und zugeschnitten auf den Bedarf der jeweiligen Organisation durchgeführt werden. Weitere Informationen erhalten Sie unter der Telefon-Nr. +49 (0) 6022 508 200.

Die Teilnehmerzahl ist begrenzt. Wir berücksichtigen Ihre Anmeldung in der Reihenfolge des Eingangs.

ANMELDEFORMULAR

Hardening Microsoft Environments

- ❒ **(M 63) 29.-30. September 2021, Online**
- ❒ **(M 63) 08.-09. Dezember 2021, Online**
- ❒ **(M 63) 08.-09. Februar 2022, Online**

❒ Bitte reservieren Sie _____ Platz/Plätze **zum Einzelpreis von 1.990 €** + 19% MwSt. (für unsere Teilnehmer*innen aus Österreich, Schweiz usw. berechnen wir den Nettobetrag).

Wir senden Ihnen die Kursdokumentation als pdfs vor Kursbeginn zu!

Herr/Frau Vorname Nachname

_____

Funktion _____

Firma _____

Adresse _____

_____

_____

Postleitzahl _____ Ort _____

Land _____

Telefonnummer _____

Mobilfunknummer _____

E-Mail _____

Unterschrift _____

BUCHUNGSREFERENZ HM63

Zahlung

❒ Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

_____

_____

_____

_____

PO-Nummer _____

Zusätzliche Teilnehmer

1. Herr/Frau Vorname Nachname

_____

Funktion _____

2. Herr/Frau Vorname Nachname

_____

Funktion _____

3. Herr/Frau Vorname Nachname

_____

Funktion

© 2021 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.