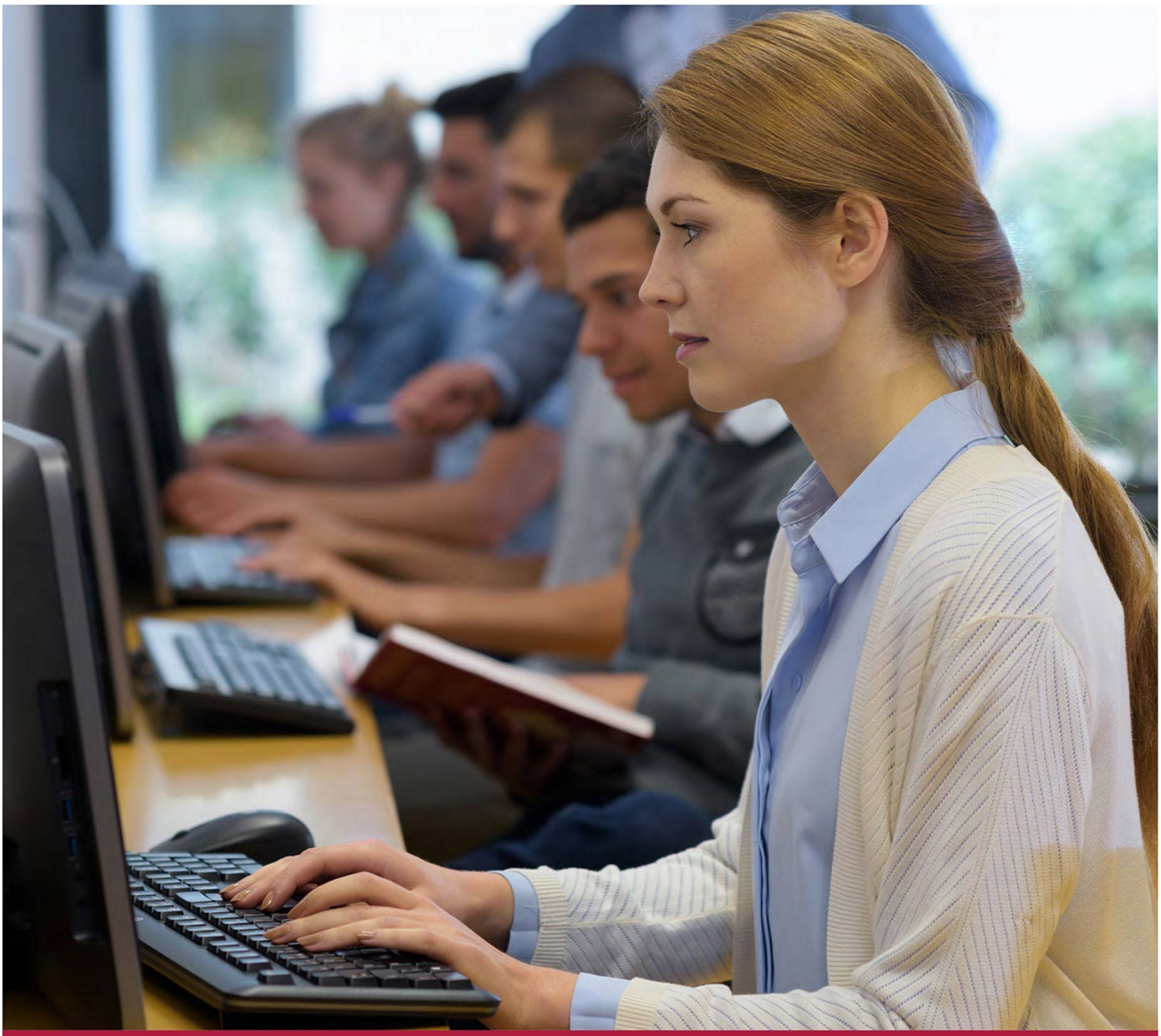
softline учебный центр



Microsoft Security Workshop: Implementing PowerShell Security Best Practices

Код курса: 40555

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Microsoft Security Workshop: Implementing PowerShell Security Best Practices

Код курса: 40555

Длительность	8 ак. часов
Формат	Очно; Дистанционно
Разработчик курса	Microsoft
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Представленный в 2006 году Windows PowerShell является языком сценариев, оболочкой командной строки и платформой сценариев на Microsoft .NET Framework. Несмотря на предназначенность для сценариев, Windows PowerShell обладает рядом характеристик, общих для языков программирования, включая объектно-ориентированную природу, расширяемость, подобный C# синтаксис и возможность взаимодействовать непосредственно с классами .NET, их свойствами и методами. Основной целью Windows PowerShell было помочь IT-специалистам и опытным пользователям контролировать и автоматизировать администрирование операционной системы Windows и приложений, работающих на Windows. Чтобы пользоваться преимуществами, обеспечиваемыми Windows PowerShell, и одновременно минимизировать связанные с безопасностью риски, важно понимать основные аспекты операционной безопасности Windows PowerShell. Еще один аспект, который важно рассмотреть в контексте курса, — это роль Windows PowerShell в вирусных атаках. Этот 1-дневный семинар по безопасности под руководством инструктора предоставляет теоретические знания и практическое обучение в отношении PowerShell. Вы познакомитесь с основами PowerShell, включая его архитектуру, выпуски и версии, а также основы взаимодействия с PowerShell. Затем вы изучите наиболее распространенные техники на основе Windows PowerShell, применяемые хакерами для использования существующего доступа к операционной системе Windows в целях упрощения установки вредоносного программного обеспечения, выполнения задач рекогносцировки, установки устойчивости на целевом компьютере и обеспечения горизонтального перемещения. Вы также познакомитесь с некоторыми средствами безопасности на основе Windows PowerShell, упрощающими тесты на проникновение, проведение экспертизы и реконструирование эксплойтов Windows PowerShell. В завершение курса вы предоставите краткий обзор рекомендуемых Blue Team технологий, предназначенных для реализации комплексной, углубленной защиты от атак на основе Windows PowerShell. Этот семинар является частью серии семинаров корпорации Microsoft в отношении обеспечения безопасности. И хотя прохождение вами каких-либо других курсов в рамках серии Security Workshop не является обязательным для прохождения этого семинара, мы настоятельно рекомендуем начать с первого курса серии — Microsoft Security Workshop: Enterprise Security Fundamentals.

Подробная информация

Профиль аудитории:

- Разработчики.

Предварительные требования:

- Хорошая база в получении доступа к простым командам Windows PowerShell и их использовании
- Текущая экосистема кибербезопасности
- Опыт администрирования и обслуживания Windows Client и Server и устранения соответствующих неполадок.
- Понимание и базовый опыт работы с технологиями сетей Windows, включая настройку сети Windows Firewall, DNS, DHCP, WiFi и понимание концепций служб cloud.
- Базовое понимание и опыт работы с Active Directory, включая функции контроллера домена, службы входа и понимание групповой политики.
- Знание и соответствующий опыт администрирования систем, использования Windows 10.

По окончании курса слушатели смогут:

- Предоставлять обзор Windows PowerShell
- Описывать выпуски и версии PowerShell
- Устанавливать и использовать Windows PowerShell и PowerShell Core
- Управлять выполнением локальных скриптов PowerShell
- Управлять удаленным выполнением Windows PowerShell
- Управлять удаленным выполнением PowerShell Core
- Описывать последствия использования Constrained Language Mode для безопасности
- Описывать архитектуру и компоненты Windows PowerShell DSC
- Рекомендовать конфигурацию аудита и ведения журнала Windows PowerShell
- Приводить примеры атак на основе Windows PowerShell
- Использовать средства безопасности на основе Windows PowerShell
- Предоставлять обзор связанных с безопасностью технологий на основе Windows PowerShell
- Реализовывать ведение журнала Windows PowerShell с использованием Desired State Configuration (DSC)
- Идентифицировать и устранять эксплойты на основе Windows PowerShell

Реализовывать Just Enough Administration (JEA)

Программа курса

Модуль 1: основы PowerShell

Представленный в 2006 году Windows PowerShell является языком сценариев, оболочкой командной строки и платформой сценариев на Microsoft .NET Framework. Несмотря на предназначенность для сценариев, Windows PowerShell обладает рядом характеристик, общих для языков программирования, включая объектно-ориентированную природу, расширяемость, подобный C# синтаксис и возможность взаимодействовать непосредственно с классами .NET, их свойствами и методами. Основной целью Windows PowerShell было помочь IT-специалистам и опытным пользователям контролировать и автоматизировать администрирование операционной системы Windows и приложений, работающих на Windows. С представлением .NET Core в 2016 году корпорация Microsoft расширила область PowerShell на другие платформы операционных систем, что

привело к появлению размещенного на GitHub проекта с открытым кодом под названием PowerShell Core. Вы можете использовать PowerShell Core на macOS 10.12, различных дистрибутивах 64-bit Linux, а также операционной системе 32-bit и 64-bit Windows, включая Windows 10, используемой на устройствах Advanced Reduced Instruction Set Computing Machine (ARM).

В этом модуле вы познакомитесь с основами PowerShell, включая его архитектуру, выпуски и версии, а также основы взаимодействия с PowerShell.

Уроки

- Обзор Windows PowerShell
- Выпуски и версии PowerShell
- Выполнение PowerShell

После прохождения этого модуля вы сможете:

- Предоставлять обзор Windows PowerShell
- Описывать выпуски и версии PowerShell
- Устанавливать и использовать Windows PowerShell и PowerShell Core

Модуль 2: PowerShell Operational Security

Чтобы пользоваться преимуществами, обеспечиваемыми Windows PowerShell, и одновременно минимизировать связанные с безопасностью риски, важно понимать основные аспекты операционной безопасности Windows PowerShell. В этом модуле вы узнаете о повышении безопасности операционной системы благодаря использованию встроенных функций и технологий Windows PowerShell, являющихся частью операционной среды Windows PowerShell. Еще один аспект, который важно рассмотреть в контексте этого модуля, — это роль Windows PowerShell в вирусных атаках. Согласно эмпирическим данным, в большинстве случаев Windows PowerShell используется как постэксплуатационный инструмент. Это значит, что в точке, когда запускается сеанс Windows PowerShell, у злоумышленника уже есть доступ к контексту безопасности, в котором работает целевая система или целевой пользователь. Именно этот тип сценария рассматривается в этом модуле. В этом случае Windows PowerShell служит мощным и чрезвычайно гибким механизмом для выполнения произвольных задач на локальных и удаленных компьютерах, что, кстати, и сделало Windows PowerShell очень популярным среди системных администраторов.

Очевидно, есть и другие типы атак, в которых Windows PowerShell используется для получения несанкционированного доступа к целевой системе. При таком типе сценария Windows PowerShell служит инструментом эксплуатации. Мы рассмотрим такие типы атак в последнем модуле этого курса.

Уроки

- Управление Local Script Execution
- Управление возможностями удаленного выполнения Windows PowerShell
- Управление возможностями удаленного выполнения PowerShell Core
- Language Mode

После прохождения этого модуля вы сможете:

- Управлять выполнением локальных скриптов PowerShell
- Управлять удаленным выполнением Windows PowerShell
- Управлять удаленным выполнением PowerShell Core
- Описывать последствия использования Constrained Language Mode для безопасности

Модуль 3: реализация безопасности на основе PowerShell

В предыдущем модуле вы узнали о ряде связанных с безопасностью функций, встроенных в Windows PowerShell, и технологиях, являющихся частью операционной среды Windows PowerShell и помогающих с принудительным применением таких функций. Цель этого модуля — представить наиболее распространенные и эффективные методы использования Windows PowerShell для повышения безопасности операционной системы. Такие методы включают следующее: > Защита от нежелательных изменений конфигурации с помощью PowerShell Desired State Configuration (DSC) > Реализация принципа предоставления минимальных прав в сценариях удаленного администрирования с использованием Just Enough Administration (JEA) > Отслеживание и аудит событий, которые могут указывать на попытки атак, благодаря использованию ведения журнала Windows PowerShell

Уроки

- Windows PowerShell DSC
- Just Enough Administration (JEA)
- Аудит и ведение журнала Windows PowerShell

После прохождения этого модуля вы сможете:

- Описывать архитектуру и компоненты Windows PowerShell DSC
- Реализовывать JEA
- Рекомендовать конфигурацию аудита и ведения журнала Windows PowerShell

Модуль 4: атаки на основе Windows PowerShell и их устранение

Организации не могут обеспечить комплексное определение слабых сторон в определении угроз безопасности и реагирование на них, фокусируясь только на стратегиях предотвращения нарушений. Понимание того, как не только обеспечивать защиту, но и как определять нарушения и реагировать на них, важно в такой же (если не в большей) степени, как и принятие мер для предотвращения возникновения нарушений. Планирование наихудших сценариев с помощью Red Teaming (реальной атаки и проникновения) позволяет организациям создавать необходимые возможности определения попыток атак и значительно улучшать реагирование на бреши в системе безопасности.

Red Teaming стал одним из главных частей разработки и обеспечения безопасности платформ и служб Microsoft. Red Team выполняет роль искушенных злоумышленников и позволяет корпорации Microsoft оценивать и повышать безопасность, усиливать защитные меры и обеспечивать большую эффективность всей программы безопасности. Red Teams позволяют корпорации Microsoft тестировать определение брешей и реагирование на них, а также точно измерять готовность к реальным атакам и их влияние.

Цель Blue Team — поиск креативных и надежных средств защиты для определения и срыва атак, оркестрированных Red Team. Blue Team состоит из выделенного набора служб реагирования на

угрозы безопасности или участников из различных организаций по реагированию на инциденты безопасности,

инженерных и оперативных групп. Независимо от состава, они являются независимыми и работают отдельно от Red Team. Blue Team следует установленным процессам безопасности и использует новейшие средства и технологии для определения атак и проникновения и реагирования на них.

В этом модуле мы сначала рассмотрим безопасность на основе Windows PowerShell со стороны Red Team. Мы изучим наиболее распространенные техники на основе Windows PowerShell, применяемые хакерами для использования существующего доступа к операционной системе Windows в целях упрощения установки вредоносного программного обеспечения, выполнения задач рекогносцировки, установки устойчивости на целевом компьютере и обеспечения горизонтального перемещения. Мы также познакомимся с некоторыми средствами безопасности на основе Windows PowerShell, упрощающими тесты на проникновение, проведение экспертизы и реконструирование эксплойтов Windows PowerShell. В завершение модуля и курса мы предоставим краткий обзор рекомендуемых Blue Team технологий, предназначенных для реализации комплексной, углубленной защиты от атак на основе Windows PowerShell.

Существует множество задокументированных эксплойтов, которые используют возможности Windows PowerShell для осуществления атак, целью которых являются недостатки безопасности, присутствующие в неисправленных или устаревших системах, или для развертывания в боковом направлении области таких атак при компрометации хотя бы одной системы. Обратите внимание, что обзор эксплойтов, представленных в этом модуле, не является исчерпывающим. Наше намерение — показать общие шаблоны, которым следуют такие эксплойты, и подчеркнуть важность подробной стратегии комплексной защиты.

Уроки

- Атаки на основе Windows PowerShell
- Средства безопасности на основе Windows PowerShell
- Краткий обзор связанных с безопасностью технологий Windows PowerShell

Лабораторная работа : реализация Windows PowerShell Security

- Реализация Windows PowerShell Logging с использованием DSC
- Выполнение атаки на основе Windows PowerShell
- Реализация Just Enough Administration

После прохождения этого модуля вы сможете:

- Приводить примеры атак на основе Windows PowerShell
- Использовать средства безопасности на основе Windows PowerShell
- Предоставлять обзор связанных с безопасностью технологий на основе Windows PowerShell
- Реализовывать ведение журнала Windows PowerShell с использованием Desired State Configuration (DSC)
- Идентифицировать и устранять атаки на основе Windows PowerShell

Реализовывать Just Enough Administration (JEA)

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.