کارگاه آموزشی

بررسی حملات PowerShell و شیوه مقابله با آن

مهندس مسلم حقیقیان

مرکز تخصصی آپا دانشگاه کردستان

چکیده: Windows PowerShell یک موتور خودکار قابل ارتقا از طرف مایکروسافت است که شامل یک پوسته خط فرمان همراه یک‌زبان اسکریپت نویسی است. اولین نسخه پاورشل در ماه نوامبر سال ۲۰۰۶ برای ویندوز XP، Server 2003 و Vistaمنتشر شد. آخرین نسخه PowerShell 5.0 با ویندوز ۱۰ ارائه شده است.

PowerShell، ضمن بهره‌گیری از دات نت، چارچوبی برای خودکارسازی اموراتی است که می‌تواند کاربردهای فراوانی برای مدیران شبکه، هکرهای کلاه‌سفید و مسئولین امنیت داشته باشد. یکی از مزایای آن، این است که دستورات آن در دو نسخه مختصر و کامل وجود دارند و قابلیت استفاده همزمان آن‌ها باهم نیز وجود دارد.

با توجه به قدرت بالای PowerShell در مدیریت سیستم‌عامل‌های مایکروسافت، کاربرد آن در این حوزه روزبه‌روز در حال گسترش است. در این کارگاه آموزشی، ضمن معرفی و آموزش استفاده از این ابزار، به بررسی بدافزارها و حملاتی که توسط PowerShell انجام می‌شود، پرداخته خواهد شد و شیوه مقابله با آنها نشان داده می‌شود. همچنین آسیب‌پذیری‌ها و حملات ابتکاری که پیش‌بینی می‌شود که در آینده با استفاده از این ابزار صورت بگیرد نیز ارائه می‌شوند.

سرفصل کارگاه:

- معرفی پاورشل
  - بررسی فرمان‌های پاورشل
  - کار با توابع مایکروسافت
  - استفاده از دات نت در پاورشل
  - فیلتر کردن خروجی‌ها
  - دسترسی‌های راه دور
- سیاست‌های امنیتی پاورشل و شیوه دور زدن آن‌ها
- بررسی نوشتن کیلاگر در پاورشل
- BruteForce رمز عبور سرویس‌ها، سیستم‌های محلی و راه دور
- بررسی پروفایل پاورشل و استفاده‌های غیر مجاز از آن
- بررسی روش سرقت رمز عبور با استفاده از پاورشل

- بررسی بدافزارهای Fileless در پاورشل
- ارزیابی امنیتی ویندوز توسط پاورشل
- مبهم‌سازی ورودی‌ها در پاورشل
- امن‌سازی و مقابله با حملات پاورشل

مدت زمان کارگاه: ۴ ساعت

زمان برگزاری: پنج‌شنبه ۱۷ اسفند ۱۳۹۶ – ساعت ۱۸-۱۴