Endpoints and Systems Lab2

الأجهزة/النقاط الطرفية والأنظمة - تطبيق عملي 2

إعداد: إسماعيل محمد قطان

Prepared by: Ismail Muhammed Kattan

التاريخ: أكتوبر/ تشرين الأول 2025

Date: October, 2025



# **🧪 LAB: Windows PowerShell for Security Analysts**

## **🎯 Objectives**

في نهاية هذا الـ Lab، ستكون قادرًا على:

1. فتح PowerShell كمسؤول واستخدام أوامر أساسية.
2. تعديل إعدادات الأمان الخاصة بتشغيل السكربتات.
3. استكشاف الخدمات والعمليات باستخدام أوامر PowerShell.
4. استخدام أنابيب الأوامر (Piping) لتحليل البيانات.
5. استيراد دوال PowerShell واستخدامها في التحقيق الأمني.

## **⚙️ Part 1: Opening PowerShell**

### **الخطوات:**

1. افتح قائمة **Start** واكتب **PowerShell**.
2. انقر **Right Click → Run as Administrator**.

تحقق من أنك في مسار النظام:

| PS C:\Windows\System32> |
| --- |

## 

## **🔐 Part 2: Checking and Changing Execution Policy**

### **الهدف:**

معرفة سياسة تشغيل السكربتات الحالية وتغييرها لتسمح بتشغيل السكربتات الموثوقة.

### **الأوامر:**

| get-executionpolicy |
| --- |

🔸 النتيجة الافتراضية تكون غالبًا:

| Restricted |
| --- |

لتغييرها إلى الوضع الموصى به:

| set-executionpolicy RemoteSigned |
| --- |

اضغط **Y** ثم **Enter** للموافقة.

## 

## **📖 Part 3: Exploring PowerShell Help**

### **الهدف:**

استكشاف نظام المساعدة للتعرف على الأوامر ووظائفها.

### **الأوامر:**

| get-help  get-help Get-Service -examples  get-help Get-Service -detailed  get-help Get-Service -full |
| --- |

💡 استخدم | more بعد أي أمر لتصفح النتائج صفحة بصفحة:

| get-help | more |
| --- |

## 

## **🧩 Part 4: Listing and Filtering Services**

### **الهدف:**

عرض الخدمات وتشغيل عوامل تصفية لإظهار فقط الخدمات النشطة.

### **الأوامر:**

عرض جميع الخدمات:

| get-service |
| --- |

عرض الخدمات التي تعمل فقط:

| get-service | where-object {$\_.status -eq "Running"} | more |
| --- |

## 

## **🪟 Part 5: Using Out-GridView**

### **الهدف:**

عرض النتائج في واجهة رسومية تفاعلية يمكن فرزها وتصفيتها.

### **الأوامر:**

| get-process | out-gridview |
| --- |

🔹 جرب الفرز حسب **CPU(s)** أو **ProcessName** أو **Memory Usage**.

## 

## **📦 Part 6: Importing and Running PowerShell Modules**

### **الهدف:**

تعلم كيفية استيراد دوال أو سكربتات خارجية وتحليل الشبكة.

### **المثال:**

استيراد ملف دالة خارجية:

| import-module -name C:\Users\Administrator\Downloads\Get-NetworkStatistics.psm1 -verbose |
| --- |

تشغيل الدالة بعد الاستيراد:

| Get-NetworkStatistics | format-table |
| --- |

🔹 هذا يعرض قائمة العمليات التي تستمع على منافذ معينة، مفيد جدًا في التحقيقات الأمنية.

## 

## **🧠 Part 7: Security Considerations**

* استخدم دائمًا PowerShell بصلاحيات المسؤول فقط عند الحاجة.
* لا تشغل سكربتات من الإنترنت إلا بعد التحقق من توقيعها الرقمي.

راقب العمليات والخدمات المشبوهة باستخدام:

| get-process  get-service |
| --- |