تحليل ومناقشة مشروع أمن سيبراني

في هذا التحليل، نستعرض الأسئلة التي طرحتها الأستاذة على الطالب أثناء مناقشة مشروعه، والذي يركز على استخدام أدوات مثل `nmap` ، `netdiscover` ، و `Metasploit` لتنفيذ هجوم على جهاز في الشبكة المحلية.

الجزء الأول: أداة `netdiscover` (اكتشاف الشبكة)

❓ سؤال الأستاذة (0:13): ما هي الوظائف الأساسية لأداة `netdiscover` ؟

💬 إجابة الطالب:

تُعطينا الـ Mapping الخاص بالشبكة، وتُستخدم في الـ Device Detection (تكتشف نوع الجهاز)، وهي ضرورية في الـ Security (الأمن)، وتُستخدم في الـ Penetration Testing (اختبار الاختراق)، وتُعتبر سريعة.

✔ التقييم:

الإجابة صحيحة. لخص الطالب وظائف الأداة بشكل جيد. فهي أداة استطلاع نشط وسلبي للشبكات المحلية، تعمل عبر إرسال واستقبال حزم ARP لاكتشاف الأجهزة المتصلة بالشبكة.

❓ سؤال الأستاذة (0:38): في أي طبقة (Layer) تعمل أداة `netdiscover` ؟

💬 إجابة الطالب:

تُستخدم في `Layer 2` والتي هي طبقة الشبكة (Network Layer).

❌ التقييم والتصحيح:

الإجابة خاطئة جزئياً.

التصحيح: الأداة تعمل بالفعل في **Layer 2**، لكن `Layer 2` هي **طبقة ربط البيانات (Data Link Layer)** وليست طبقة الشبكة. طبقة الشبكة (Network Layer) هي `Layer 3` . تعتمد الأداة على بروتوكول ARP لاكتشاف الأجهزة، وهو بروتوكول يعمل في طبقة ربط البيانات (Layer 2).

❓ سؤال الأستاذة (0:43): ما الفرق بين الوضع النشط (Active Mode) والوضع السلبي (Passive Mode) في الأداة؟

💬 إجابة الطالب:

الوضع السلبي (Passive Mode) يعطينا حركة مرور بيانات (ARP Traffic) بدون الحاجة لإرسال أي حزم (packets).

✔ التقييم:

الإجابة صحيحة. الوضع السلبي يقوم فقط بالاستماع إلى حزم ARP الموجودة على الشبكة، بينما الوضع النشط يقوم بإرسال حزم ARP بشكل فعال لاكتشاف الأجهزة. إجابته

كانت دقيقة.

❓ سؤال الأستاذة (2:55): ماذا يفعل الخيار `-r` الذي استخدمته؟

💬 إجابة الطالب:

الخيار `-r` يحدد نطاق (range) عناوين IP التي سيتم فحصها في الشبكة. (شرح ذلك أثناء كتابة الأمر).

✔ التقييم:

الإجابة صحيحة. الخيار `-r` (range) يُستخدم لتحديد نطاق معين من عناوين IP لفحصها بدلاً من فحص الشبكة بالكامل، مما يجعل الفحص أكثر تركيزاً وسرعة.

الجزء الثاني: فحص الثغرات والاستغلال (`nmap` و `Metasploit`)

❓ سؤال الأستاذة (6:56): ما هي الثغرات التي وجدتها بعد الفحص؟

💬 إجابة الطالب:

وجدت ثغرة في بروتوكول SMB، وهي ثغرة تنفيذ التعليمات البرمجية عن بعد (Remote Code Execution). ذكر أيضاً أنها مرتبطة بأنظمة ويندوز القديمة مثل XP.

✔ التقييم:

الإجابة صحيحة. أظهر الطالب فهمه لنتائج فحص `nmap` ، حيث حدد بشكل صحيح الثغرة الخطيرة `MS17-010 (EternalBlue)` في بروتوكول SMB، وهي بالفعل ثغرة RCE شهيرة.

❓ سؤال الأستاذة (17:10 - ضمنياً): ما هي وظيفة كل من `RHOST` و `LHOST` في Metasploit؟

💬 إجابة الطالب:

(من خلال تطبيقه) قام بضبط `RHOST` على عنوان IP الخاص بالجهاز الهدف (ويندوز)، وضبط `LHOST` على عنوان IP الخاص بجهازه (كالي لينكس).

✔ التقييم:

الإجابة صحيحة (من خلال التطبيق).

- `RHOST (Remote Host)` : هو عنوان IP للجهاز الضحية الذي يتم استهدافه.
- `LHOST (Local Host)` : هو عنوان IP لجهاز المهاجم، والذي سيتلقى الاتصال العكسي (Reverse Shell) من جهاز الضحية بعد نجاح الهجوم.

تطبيقه كان صحيحاً 100%.

❓ سؤال الأستاذة (18:07): ما هي الصلاحيات التي حصلت عليها بعد الاختراق؟

💬 إجابة الطالب:

استخدم الأمر `getuid` وأظهر أن الصلاحيات هي `NT AUTHORITY\SYSTEM` .

✔ التقييم:

الإجابة صحيحة. صلاحيات `NT AUTHORITY\SYSTEM` هي أعلى مستوى من الصلاحيات على نظام ويندوز، مما يعني أنه حصل على تحكم كامل بالجهاز.

❓ سؤال الأستاذة (18:33 - ضمنياً): كيف تمسح آثارك من الجهاز؟

💬 إجابة الطالب:

أجاب بأنه سيستخدم الأمر `clearev` لتنظيف سجلات الأحداث (Logs).

✔ التقييم:

الإجابة صحيحة. الأمر `clearev` في Meterpreter يُستخدم لمسح سجلات الأحداث (Application, System, Security) في نظام ويندوز، وهي خطوة أساسية لإخفاء آثار الهجوم.

❓ سؤال الأستاذة (22:04): ماذا يفعل الأمر `hashdump` ؟

💬 إجابة الطالب:

يقوم باستخراج الهاشات (Hashes) الخاصة بكلمات المرور للمستخدمين من ملف SAM.

✓ التقييم:

الإجابة صحيحة. الأمر `hashdump` يستخرج تجزئات (hashes) كلمات المرور من قاعدة بيانات Security Account Manager (SAM) على نظام ويندوز، والتي يمكن بعد ذلك محاولة كسرها للحصول على كلمات المرور.

ملخص وتقييم عام لأداء الطالب

أظهر الطالب أداءً عملياً قوياً جداً وفهماً جيداً لخطوات اختبار الاختراق من مرحلة الاستطلاع إلى مرحلة ما بعد الاستغلال. كان واثقاً في استخدام الأدوات وقادراً على شرح وظيفة معظم الأوامر التي استخدمها.

- **نقاط القوة:** مهارة تطبيقية عالية، فهم جيد لآلية عمل Metasploit، معرفة بالخطوات العملية للهجوم.
- **نقاط تحتاج للتحسين:** بعض الخلط في المفاهيم النظرية الأساسية مثل طبقات OSI Model.

الخلاصة: بشكل عام، كانت المناقشة ناجحة وأظهرت أن الطالب قام بالمشروع بنفسه ولديه الكفاءة العملية المطلوبة.