تمرین عملی دوم:

بخش اول:

هدف: آشنایی با ابزار nmap

عنوان آزمایش: استفاده از nmap برای اسکن شبکه

محیط آزمایشگاه:

اقدام به نصب چند ماشین مجازی بر روی سیستم خود کنید، با توجه به نیازهای آتی، اقدام به نصب یک نسخه ویندوز XP، ویندوز 7 و یک نسخه از Kali linux کنید.

مرحله‌ی اول: تنظیمات شبکه را طوری قرار دهید که سیستم ها یکدیگر را مشاهده (ping) کنند.

مرحله دوم: با استفاده از ابزارهای معرفی شده، سیستم‌های روشن در شبکه را شناسایی کنید.

مرحله سوم: توضیح دهید هر یک از موارد زیر چگونه عملیات اسکن شبکه را انجام میدهد، سپس به وسیله‌ی سوئیچ های nmap اقدام به اجرای آن ها توسط سیستم Kali، بر روی سیستم های روشن شبکه کنید.

- Nmap برای شناسایی سیستم عامل از چه سوئیچ استفاده میکند؟ اینکار چگونه انجام میشود؟
- Full connect scan چیست و چگونه انجام میشود.
- Stealth scan چیست و چگونه انجام میشود.
- UDP scan چیست و چگونه انجام میشود.
- Idle scan چیست و چگونه انجام میشود؟ انجام این نوع اسکن چه مزیتی نسبت به سایر اسکن ها دارد؟ این اسکن را انجام دهید، و به وسیله‌ی ابزار wireshark اقدام به مشاهده پیام ها کنید. نحوه‌ی انجام این اسکن را توسط پکت های شنود شده توسط wireshark توضیح دهید.

بخش دوم:

قسمت اول

هدف: نفوذ

عنوان آزمایش : بکارگیری اکسپلوییت ms08_067

محیط آزمایشگاه:

سیستم قربانی : سیستم عامل ویندوز XP سرویس پک ۱
سیستم نفوذگر : یکی از نسخه های سیستم عامل لینوکس به همراه فریم وورک متا اسپلویت(توصیه میشود از Linux Kali استفاده کنید)

پس از روشن کردن دو ماشین، از ping کردن متقابل آنها اطمینان حاصل کنید.(فایروال XP حتما خاموش باشد)

مرحله اول: تمام سیستم عامل های موجود در شبکه لوکال را به وسیله Nmap شناسایی کنید.
مرحله دوم: پس از یافتن سیستم عامل قربانی با دستور Nmap تمام پورت های آن را بررسی کنید. با مشاهده باز بودن پورت 445مراحل زیر را دنبال بفرمایید .

(لازم است پیش از اجرای اکسپلویت، از نصب نبودن وصله(patch) مربوط به این اکسپلویت اطمینان حاصل کنند. مشخصات وصله ی مربوطه در لینک زیر قابل دسترس است، کافی ست با بررسی ویندوز XP خود را بررسی کنید.
yon.ir/UYan1
مرحله سوم: با دستور msfconsole در ترمینالKali linux ، فریم وورک متا اسپلویت را فراخوانی کنید .
مرحله چهارم: با دستور مقابل اکسپلویت ms08_067 را انتخاب کنید use exploit/windows/smb/ms08_067_netapi

مرحله پنجم: با دستور زیر payload مربوطه راSet کنید: set payload windows/meterpreter/bind_tcp
مرحله ششم: با وارد کردن دستور show options مشخصات را مشاهده کنید، در ادامه برای مشخص کردن IP هدف، دستور زیر را وارد.
مرحله هفتم: نیازمندی های مربوط به اکسپلویت و پیلود مربوطه، شامل LOHST و RHOST را تکمیل کنید.
مرحله هشتم: با اجرای دستور exploit، اقدام به اجرای اکسپلویت مربوطه نمایید.
مرحله نهم: پس از اخذ دسترسی meterpreter، با کمک دستور help، اقدام به راه اندازی keylogger بر روی سیستم هدف کنید.
مرحله دهم: اقدام به تایپ شماره‌ی دانشجویی خود در ویندوز XP کنید.
مرحله یازدهم: با دستور keyscan_dump، اقدام به نمایش متن تایپ شده در Kali linux کنید.

از تمامی مراحل کار خود اسکرین شات گرفته، و به صورت یک فایل PDF همراه با توضیحات ارسال کنید.

قسمت دوم:

هدف: نفوذ

عنوان: ساخت بدافزار

محیط آزمایشگاه: سیستم عامل Kali liux، یک نسخه‌ی دلخواه از سیستم عامل ویندوز

مرحله اول: با استفاده از msfvenom و payload ذکر شده در قسمت اول بخش دوم، اقدام به ایجاد یک بدافزار با فرمت exe. کنید.

مرحله دوم: با استفاده از اکسپلویت multi/handler و پیلود ذکر شده در قسمت قبل، سیستم kali را آماده‌ی شنود بسته‌های دریافتی کنید.

مرحله سوم: با راه اندازی آپاچی سرور، بدافزار مربوطه را بر روی این وب سرور قرار دهید.
مرحله چهارم: توسط سیستم هدف، به وب سرور متصل شده و بدافزار مربوطه را اجرا کنید.
مرحله پنجم: دسترسی meterpreter را در kali نشان دهید.
مرحله ششم(نمره اضافی): بدافزار ساخته شده در به صورت یک backdoor، در پشت یک فایل jpg گذاشته و ادامه‌ی مراحل را انجام دهید تا دسترسی meterpreter را اخذ کنید.