درس امنیت شبکه

فعالیت اول– مرحله شناسایی حملات سایبری

مرجع: Certified Ethical Hacking Study Guide, V.8 فصول ۴ و۵و ۶

CEH Lab Manual فصول ۲و ۳و ۴

هدف از این فعالیت آشنایی با مفاهیم و انجام برخی فعالیت های عملی مربوط به فاز اولیه حملات سایبری است. حملات سایبری با شناسایی سیستم های مورد حمله آغاز می گردد. فاز شناسایی خود به سه مرحله اصلی Footprinting، Scanning و Enumeration تقسیم می شود. اسکن و enumeration , با یکدیگر مورد بحث قرار می گیرند, برای اینکه بسیاری از ابزارهای هک , هر دوی این کار ها را انجام می دهند. در طول اسکن، هکر به دنبال جمع آوری اطلاعاتی است که می توانند به هکر کمک کنند تا بداند چه نوع اکسپلویت می تواند برای هک کردن سیستم استفاده شود. سه نوع اصلی اسکن port scanning، network scanning و vulnerability scanning است. مراجع تعیین شده را مطالعه و به سئوالات زیر پاسخ دهید.

الف- در مورد مفاهیم Footprinting، Scanning و Enumeration جداول زیر را تکمیل نمایید.

مرحله شناسایی	نوع اطلاعاتی که بدست می آید
Footprinting	
Scanning	
Enumeration	

نوع اسکن	هدف
اسکن پورت (port scanning)	
اسکن شبکه(network scanning)	
اسکن آسیب پذیری(vulnerability scanning)	

ب- فعالیت های زیر را اجرا و نتایج را به همراه screenshot های مربوطه در گزارش فعالیت ثبت و تحویل نمایید:

این آزمایش ها بصورت مرحله به مرحله و حتی با اسکرین شات در کتاب CEH Lab Manual آورده شده و کافیست شما با دنبال کردن این ساختار , همانند آن را اجرا و گزارش مربوطه را در LMS ارسال نمایید .

Footprinting

ب-۱- آزمایشات ۱ تا ۱۰ فصل ۲ کتاب CEH Lab Manual مربوط به footprinting را مرور و لیست آنها را در گزارش خود بیاورید. به انواع ابزارهای مورد استفاده و کارکرد هر یک دقت نمایید.

ب-۲- یکی از آزمایشات ۲ تا ۱۰ فوق را اجرا و نتایج را مطابق دستورالعمل گزارش کنید.

Scanning

ب-۳- از فصل ۳ کتاب CEH Lab Manual مربوط به Scanning یکی از آزمایشات سوم (Amap)، ششم (Nmap)، هفتم (Netscan Tools Pro) یا هجدهم (The Dude) را انجام و گزارش نمایید.

Enumaration

ب-۴- از فصل ۳ کتاب CEH Lab Manual مربوط به Enumeration مشخص نمایید چه نوع اطلاعاتی از طریق اسکنرهای NetBios (مانند SuperScan) و چه نوع اطلاعاتی از طریق اسکنرهای SNMP (مانند SolarWinds) قابل ابتیاع است.

ب-۵- یکی از آزمایشات ۲ یا ۵ را اجرا و گزارش نمایید.

توجه کنید که screenshot ها باید شامل Desktop شما و نشاندهنده اطلاعات شخصی شما باشد. در غیر اینصورت هیچ امیتازی تعلق نخواهد گرفت.هر گونه تقلب یا کپی برداری در بررسی تمرین ها در نظر گرفته نخواهد شد .