لابراتوار ۱

هکرها و انگیزه آنها و روش‌های حمله *Hacker*ها

هدف از لابراتوار:

- آشنایی با هکرها
- انواع حملات و *Attacks*ها به شبکه
- انگیزه هکرها
- جمع‌آوری گزارش‌ها و *Attack*های شبکه
- بررسی سازمان و اهمیت اطلاعات مربوط به آنها

تجهیزات موردنیاز برای این لابراتوار:

- یک کامپیوتر با دسترسی به اینترنت برای تحقیقات
- یک کامپیوتر با نرم‌افزار *PowerPoint* یا نرم‌افزار مشابه برای ارائه مطالب
- *Video Projector* و صفحه نمایش برای ارائه مطالب

در این لابراتوار انواع حملات یا *Attack*هایی که توسط *Hacker*ها یا سایر افراد مهاجم برای دسترسی به اطلاعات و سایر منابع شبکه صورت می‌گیرد تشریح خواهد شد.

قبل از تشریح انواع حملات ما در مورد یک *Attacker* یا یک *Hacker* که به سیستم شبکه حمله می‌کنند، صحبت خواهیم کرد.

اگر بخواهیم گروه‌بندی روی *Hacker*های مختلف و انگیزه آنها داشته باشیم هکرها به گروه‌های زیر تقسیم خواهند شد.

black hat (**هکر کلاه سیاه**): این هکرها به هکرهای بدذات و بداندیش هم معرف هستند و انگیزه این هکرها برای حمله، انتقام جویی، و سوءاستفاده مالی و اقتصادی می‌باشد.

white hat (**هکر کلاه سفید**): این هکر جزء دسته هکرهایی است که معمولاً به قصد تست سیستم امنیتی به یک شبکه یا یک سیستم حمله می‌کند.

grey hat (**هکرهای کلاه خاکستری**): این هکرها ترکیبی از هکرهای کلاه سفید و کلاه سیاه هستند و با انگیزه‌های موجود در هر دو گروه ممکن است به یک سیستم شبکه‌ای حمله کنند.

Phreakers: این گروه از هکرها تماس‌های تلفنی ارزان قیمت را به وجود می‌آورند.

> **نکته اول درباره آموزش امنیت**: اگر شما کارشناس امنیت یا مدیر ارشد امنیت یک شرکت می‌باشید، مطالعه چند کتاب نمی‌تواند به تنهایی مفید باشد، بلکه شما باید مرتباً گوش بزنگ وقایع امنیتی در سایت‌ها و مجلات و انجمن‌های امنیتی باشید.

امروزه سرقت اطلاعات از شبکه‌های کامپیوتری به اندازه سرقت منازل مسکونی گسترش یافته است. یک سارق در صورتی‌که قصد سرقت منزل شما را داشته باشد، ابتدا باید یکسری اطلاعات درباره شما و منزل شما داشته باشد اطلاعاتی از قبیل اینکه در چه زمانی شما از منزل خارج و در چه زمانی مراجعه می‌کنید و همچنین اطلاعاتی از قبیل مجهز بودن منزل شما به سیستم‌های امنیتی و ضد سرقت از قبیل دوربین‌های مدار بسته و آژیر و اینکه آیا شما در منزل سگ نگهبان نگهداری می‌کنید یا خیر. پس یک سارق منزل اطلاعات زیادی درباره منزل شما قبل از سرقت تهیه می‌کند. همچنین یک سارق اطلاعات یا یک *Attacker* قبل از حمله و سرقت، اطلاعات بسیاری درباره شبکه شما جمع‌آوری خواهد کرد و این اطلاعات به *Attacker* کمک خواهد کرد که به راحتی بتواند حمله را آغاز و مدیریت نماید.

حال ممکن است شما برای افزایش امنیت منزل مسکونی خود از قفل‌های ضد سرقت و قفل‌های اضافی و مجهز کردن منزل به دوربین‌های مدار بسته و سیستم هشدار سرقت و حتی نگهبان استفاده نمایید. ولی در صورتی‌که در کل ساختمان شما یک راه ورودی (*Back door*) وجود داشته باشد که آن را بدون محافظت رها کرده باشید، مطمئن باشید که سارق از همان در پشتی و بدون حفاظت برای ورود به منزل شما استفاده خواهد کرد.

در شبکه‌های کامپیوتری نیز یک *Attacker* می‌تواند یک در پشتی (*Back door*) ایجاد و یا از یک در پشتی برای دسترسی و ورود به شبکه شما استفاده نماید و این نکته را به خاطر داشته باشید که در شبکه‌های کامپیوتری باید روزنه‌ها و درهای پشتی ورود به شبکه را شناسایی و آنها را محافظت کنید و کلیه نقاط آسیب‌پذیری را با استفاده از یک راه کار خوب امنیتی پوشش دهید. هیچ وقت فراموش نکنید که *Hacker*ها با استفاده از ابزارهای پویش، *Scan* پورت‌ها و پویشگر شبکه و همچنین استفاده از دستور *Ping* در حال شناسایی و پویش شبکه و به دست آوردن اطلاعات درباره شبکه شما می‌باشند.

یکی از مسائل دیگری که شبکه شما را در معرض تهدید قرار می‌دهد استفاده هکرها از روش مهندسی اجتماعی *Social Engineering* می‌باشد که هکر در این حالت خود را به جای یک مدیر یا یک کاربر مجاز جا می‌زند و با ایجاد اعتماد و صحبت کردن با کاربران و حتی مدیر شبکه قصد به دست آوردن اطلاعات حساس شبکه را خواهد داشت. در یک شرکت بزرگ که مثلاً ۶۰۰۰ هزار کاربر وجود داشته باشد، مدیر شبکه و حتی مدیر سیستم‌های بخش‌های مختلف شناخت کاملی از کاربران ندارند؛ حال فرض کنید یک هکر از داخل شرکت با مدیر شبکه تماس بگیرد و خود را کاربر مجازی که پسوردش را فراموش کرده است معرفی کند و از مدیر شبکه بخواهد که پسوردش را *Reset* کند.

نکته: متأسفانه برخی از مدیران شبکه و کاربران شبکه اهمیت و حساسیت امنیت شبکه را به درستی درک نمی‌کنند. وقتی با یکی از مدرسین امنیت کشور کانادا مورد امنیت صحبت می‌کردم به شوخی به من گفت؛ شما ایرانی‌ها به هر سؤالی که پرسیده شود پاسخ می‌دهید و این یعنی آسیب‌پذیری شما در برابر حملات مهندسی اجتماعی که یک هکر به راحتی از این روش قادر به دسترسی به اطلاعات موردنظر خواهد شد.

در این بخش انواع حملات *Attack*ها را تشریح خواهد شد.

Attack

زمانی که شخصی سعی می‌کند که کنترل امنیتی شبکه یا حتی کامپیوتر شما را درهم بشکند و اطلاعات شما را سرقت کند و به عبارتی شبکه شما مورد حمله یا یک *Attack* قرار خواهد گرفت.

باید از انواع حملات و تهدیدهای امنیتی که شبکه شما را تهدید می‌کند درک و آشنایی کافی داشته باشید.

Spoofing: در این روش *Source Address* در یک بسته اطلاعاتی تغییر می‌کند به طوری که *Destination* (مقصد بسته اطلاعاتی) متوجه این تغییر نشود و تصور کند که بسته اطلاعاتی از مبدأ معتبر رسیده است.

Man-in-the-middle: *Capturing* اطلاعات و استراق‌سمع و تغییر اطلاعات موردنیاز دربسته و فرستادن آن به سمت *Server* می‌باشد.

Denial of service (DoS): فرستادن تقاضاهای جعلی و ترافیک‌های بزرگ برای از کار افتادن سرویس‌های شبکه‌ای مثال افزایش محتویات *Routing Table* و *DNS Record*ها که *Client*های واقعی شبکه در اثر بار ترافیکی ایجاد شده قادر به دسترسی به سرویس‌های موردنیاز شبکه نباشند.

Replay: *Capturing* یا ضبط اطلاعات و فرستادن آن به طرف *Server* در زمان‌های بعد خواهد بود.
Packet sniffing: استفاده از برنامه‌هایی که بسته‌های اطلاعاتی را *Capture* کنند و اطلاعات داخل آن را آشکار کنند، مانند کلمه‌های رمز و سایر اطلاعات مورد استفاده هکرها
Social engineering: مهندسی اجتماعی این روش از روش‌هایی است که از کامپیوتر استفاده نمی‌شود و تکنیک‌هایی برای گول زدن کاربر برای به سرقت بردن کلمه رمز و اطلاعات حساس آنها می‌باشد.
Mail Spamming: استفاده از *E-mail Server* برای ارسال ایمیل‌های فراوان و غیرواقعی خواهد بود.
Website Deface: تغییر محتویات یک وب سایت توسط یک هکر می‌باشد که برای سازمان‌ها از بدترین نوع حملات محسوب می‌شود.
Physical attack: خراب‌کاری سخت‌افزاری و آسیب‌رساندن به *Router*ها و *Switch*ها و *Server* و سایر تجهیزات شبکه می‌باشد.
Trojan horse: یک برنامه به ظاهر خوب ولی در دل این برنامه یک نرم‌افزار جاسوسی شبیه‌سازی شده است که کاربر در صورت استفاده از آن آلوده خواهد شد.
Worm: برنامه‌های مخرب که برای هدف خاص نوشته می‌شوند و در اینترنت به سرعت پخش می‌شوند.
Virus: یک برنامه بداندیش که برای موارد خاص طراحی می‌شود و به صورت مخفی خودش را منتشر خواهد کرد و بیشتر فایل‌های اجرایی را تحت تأثیر قرار می‌دهد.
Password cracking: برنامه‌هایی هستند که با بکارگیری یک *Dicionary* کلمات مختلف را جهت پیدا نمودن رمز عبور به یک سیستم پیشنهاد خواهند کرد.
Password guessing: حدس زدن کلمه عبور پسورد به صورت دستی یا اتوماتیک مخصوصاً برای کلمات رمزی که از نظر قوانین *Password*ها *Secure* نباشند.

انگیزه هکرها

انگیزه‌های بی‌شماری ممکن است وجود داشته باشد که شخصی یا گروه خاصی اطلاعات سازمان شما را تهدید کنند. در زیر، لیستی از این موارد تشریح خواهد شد:
***Vengeance* یا انتقام‌جویی**: مثلاً یکی از کارمندان اخراجی شرکت یا سازمان یا یک رغیب کاری که قصد انتقام‌جویی از شرکت یا سازمان شما را داشته باشد.
جاسوی: خیلی از هکرها ممکن است در قبال دریافت پول قصد به دست آوردن اطلاعات سازمان‌های دولتی را برای جاسوسان و افراد دیگر داشته باشند.
Publicity: خیلی از هکرها ممکن است به علت ناکارآمد جلوه‌دادن یک *Application* و ثابت‌کردن ضعف‌های امنیتی یک سیستم به شبکه شما نفوذ کنند.
سرقت و استفاده مالی: خیلی از هکرها با سرقت اطلاعات حساس مالی و استفاده از آن قصد سوءاستفاده مالی را خواهند داشت.

مرحله ۱: تحقیق درباره انواع *Attack*ها

در این مرحله لیستی از انواع *Attack*ها را که روی شبکه شناسایی نموده‌اید در فرم زیر با دقت وارد کنید.

• **Name of attack:**	•
• **Type of attack:**	•
• **Dates of attacks:**	•
• **Computers/Organizations affected:**	•
• **How it works and what it did:**	
• **Mitigation options:**	
• •	
• **References and info links:**	
• • •	
• **Presentation support graphics (include PowerPoint filename or web links):**	
• •	

مرحله ۲: تحقیق درباره انواع ابزارهای *Audit*

در این مرحله درباره انواع نرم‌افزارها و ابزارهای *Audit* یا ابزارهای بررسی و تحت نظر گرفتن شبکه در اینترنت تحقیق کنید، این ابزارها به شما کمک خواهند نمود که با بررسی گزارش‌های آنها تا حدودی موارد آسیب‌پذیر شبکه را تشخیص دهید.

ابزارهای *Audit* را بعد از بررسی در فرم زیر وارد نمایید.

• **Name of tool:**	•
• **Developer:**	•
• **Type of tool (character-based or GUI):**	•
• **Used on (network device or computer host):**	•
• **Cost:**	•
• **Description of key features and capabilities of product or tool:**	
•	

• • • • • • • • •
• **References and info links:**
• •
• **Presentation support graphics:**
• •

مرحله ۳: بررسی سازمان و اهمیت اطلاعات

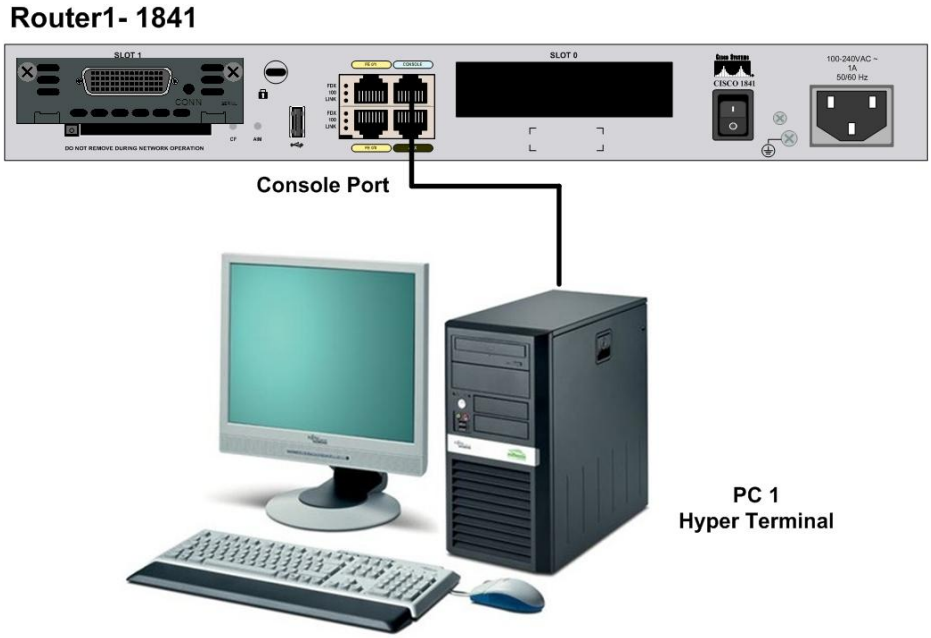
در این مرحله یک سازمان را بررسی کنید و به صورت مکتوب تعیین کنید چه اطلاعاتی در این سازمان مهم و حیاتی می‌باشد و این اطلاعات چگونه محافظت شده‌اند.

هر سازمانی یکسری اطلاعات خواهد داشت که مهم و حیاتی است برخی از اطلاعات مهم به شرح زیر می‌باشد:

- اطلاعات نظامی و حفاظتی برای سازمان‌های نظامی
- اطلاعات و فرمول‌های شیمی برای شرکت‌های پتروشیمی
- اطلاعات حساس مالی برای شرکت‌های تجاری
- اطلاعات و حساب‌های پولی مشتریان برای بانک‌ها و مؤسسات اعتباری
- نقشه‌ها و مدل‌های طراحی برای شرکت‌های هواپیمایی
- نقشه و مدل‌های طراحی برای شرکت‌های خودروسازی
- کدهای نرم‌افزاری و امنیتی برای شرکت‌های نرم‌افزاری
- اطلاعات ملی و ثبت مشخصات فردی برای ادارات دولتی
- سوابق آموزشی و تحصیلی برای مراکز آموزشی و دانشگاه‌ها
- اطلاعات، نامه‌ها و عکس‌های خصوصی در کامپیوترهای شخصی

لابراتوار ۲

اتصال *Router* به کامپیوتر برای پیکربندی (*Config*)



هدف از لابراتوار:

- اتصال یک *Router* از طریق *Console Cable* به یک *PC*
- شناسایی پورت *Console Port* روی *Router*
- شناسایی پورت *Serial* روی *PC*
- شناسایی کابل *Console* و نقشه اتصال آن
- اتصال *Router* به *PC* جهت پیکربندی
- تنظیم برنامه *HyperTerminal* و اتصال به *Router* به منظور پیکربندی آن

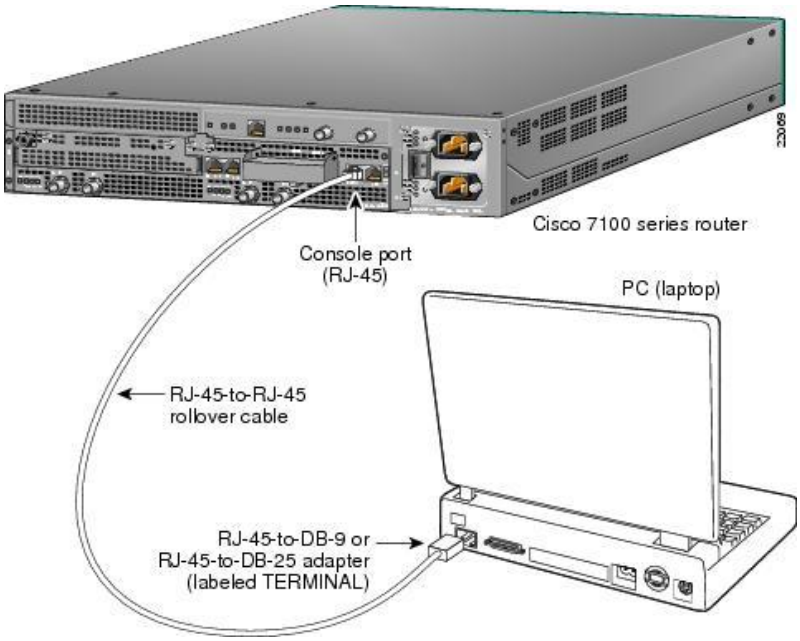
تجهیزات موردنیاز برای این لابراتوار:

- یک کامپیوتر دارای پورت سریال یا *serial interface* همراه با نرم‌افزار *HyperTerminal*
- روتر سیسکو *Cisco Router*
- کابل *Console cable* یا *rollover Cable*

در این لابراتوار قصد داریم که یک *Router* را به منظور پیکربندی به وسیله کابل *Console* یا *rollover cable* به یک *PC* متصل نماییم.

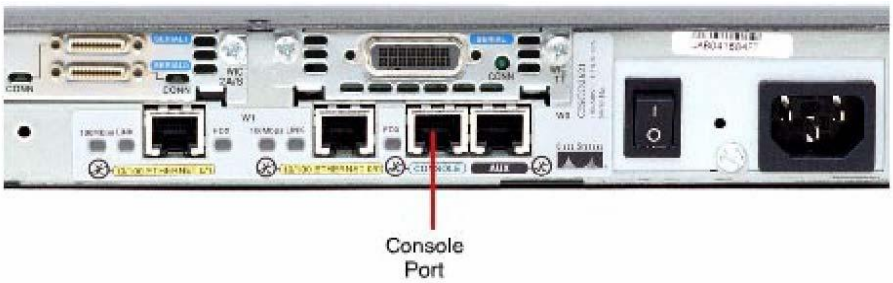
شما می‌توانید از طریق اتصال با *Console Port* تجهیزات شرکت سیسکو مانند *Router*ها و *Switch*ها و... را پیکربندی نمایید. تجهیزات شرکت سیسکو همیشه برای بار اول از طریق اتصال با پورت *Console* پیکربندی خواهند شد که بعد از دسترسی به روش *Console* می‌توانید دسترسی از طریق سایر روش‌های دیگر مانند *Telnet* و دسترسی با استفاده از خط تلفن از راه دور را پیکربندی و فعال نمایید.

در این روش *Router* یا سوئیچ یا دیگر تجهیزات شرکت سیسکو از طریق پورت *Console* و از طریق کابل *Console Cable* به کامپیوتر متصل می‌شوند همان‌طور که در تصویر زیر مشاهده می‌کنید.

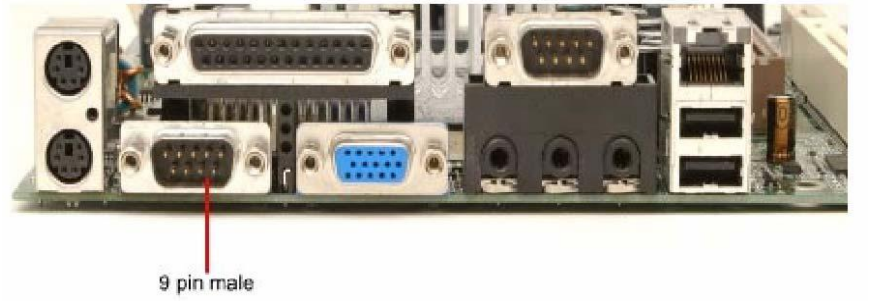
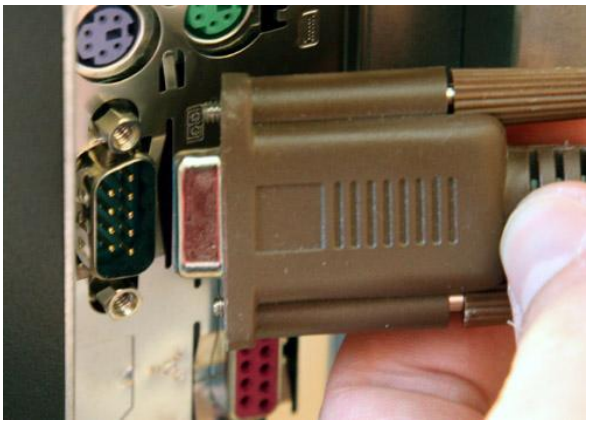


مرحله ۱: شناسایی اینترفیس *Console* برروی *Router*

در تصویر بعد *Cosole Port* را در پشت یک *Router* مشاهده می‌کنید، به محل قرارگیری این پورت توجه کنید. این پورت در پشت روتر با عبارت *Con 0* یا *Console 0* مشخص شده است.



مرحله ۲: شناسایی پورت سریال *serial interface (COM 1 or 2)* برروی *PC*

در تصویر زیر یک پورت *serial interface (COM 1 or 2)* را در پشت *PC* که یک کانکتور ۹ پایه هست را مشاهده می‌کنید به محل قرارگیری آن توجه کنید بعضی از *PC*ها دارای اتصالات سریال ۲۵ پایه می‌باشند.

در تصاویر زیر محل اتصال سریال ۹ پایه را مشاهده می‌کنید.