به‌نام ایزد یکتا

راهنمای جامع آزمون

CEH v10

Ric Messier

ترجمه: مهران تاجبخش

انتشارات پندار پارس

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶
www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸همراه: ۰۹۱۲۲۴۵۲۳۴۸

نام کتاب : **راهنمای جامع آزمون CEH v10**

ناشر : **انتشارات پندار پارس**

تالیف : **ریک ماسیر**

ترجمه : **مهران تاجبخش**

چاپ نخست : **بهار ۹۹**

شمارگان : **۵۰۰ نسخه**

طرح جلد : **رامین شکرالهی**

چاپ، صحافی : **روز**

قیمت : **۱۲۰۰۰۰ تومان** **شابک : ۸-۸۷-۸۲۰۱-۶۰۰-۹۷۸**

فهرست

پیش‌گفتار

آیا در فکر کسب گواهینامه هکر اخلاقی (CEH)هستید؟ بدون توجه به اینکه چه تخصص‌هایی در تست امنیت دارید- هک اخلاقی، تست نفوذ، عضویت در تیم قرمز و یا برآورد نرم‌افزارها- به دنبال کسب مهارت و دانش لازم در گواهینامه هکر اخلاقی هستید. استفاده از تکنیک‌های موجود در تست امنیت و هک اخلاقی باعث شده است تا سازمان‌ها شناخت بهتری درباره حملات و تهدیدهای بالقوه موجود داشته شوند. با توجه به اینکه امروزه حملات سازماندهی شده است، برای تشخیص و مقابله با آنها نیاز داریم تا از تکنیک‌ها و روش‌های مختلفی استفاده کنیم.

بدون در نظر گرفتن مخاطب این کتاب، باید در نظر داشته باشیم که بین ۸۰ تا ۹۰ درصد حملات امروزی مبتنی بر حملات مهندسی اجتماعی است. امروزه با توجه به استفاده از فناوری‌های دفاع در عمق و ایمن‌سازی ارتباط‌های خارجی شبکه سازمان، استفاده از روش‌های قدیمی مبتنی بر آسیب‌پذیری‌های تکنیکی موجود در تجهیزات و نرم افزارهای شبکه‌های سازمان، کارآیی ندارند. در حال حاضر تمرکز حملات بر روی استفاد ه از آسیب‌پذیری‌های موجود در داخل سازمان است و به همین دلیل است که سیستم‌های رومیزی داخل سازمان، هدف حمله و دستکاری قرار می‌گیرند.

این کتاب برای کمک به منظور فراگیری دانش و مهارت مورد نظر برای کسب گواهینامه هکر اخلاقی نوشته شده است. البته باید در نظر داشته باشید که علی رغم ارائه مطالب کامل و جامع در مورد مفاهیم و فناوری‌های موجود در این حوزه، کسب تجربه‌های عملی و کاربردی در بکارگیری آنها نقش بسیار مهمی ایفا می‌کند.

ارائه مطالب در حوزه هک و تست نفوذ بدون در نظر گرفتن موارد اخلاقی و قانونی امکان‌پذیر نیست، به همین دلیل است که در بخش های مختلفی از کتاب به این موارد اشاره شده است. شناخت این موارد و بکارگیری آنها باعث حفاظت از خود و افرادی که برای آنها کار می‌کنیم، خواهد شد. نسخه خیلی کوتاه و مختصر از جنبه‌های اخلاقی و قانونی هک و تست نفوذ این است که هیچگاه باعث خرابی و اختلال در سیستم کارفرما نشویم.

در پایان هر فصل مجموعه‌ای از سوالات ارائه شده است. این سوالات برای مرور مطالب ارائه شده در هر فصل است. سوالات به صورت چند گزینه‌ای ارائه شده و در همان قالب سوالات آزمون CEH است. خواندن دقیق مطالب هر فصل و پاسخ به سوالات در پایان هر فصل و کسب مهارت و تجربه عملی در مورد آنها می‌تواند باعث کسب موفقیت شما در آزمون CEH شود.

CEH چیست؟

گواهینامه هکر اخلاقی (Certified Ethical Hacker) به منزله تائید دانش و مهارت کافی دارنده آن برای اجرای پروژه‌های مختلف در حوزه هک اخلاقی و تست نفوذ می‌باشد.

CEH گواهینامه‌ای است که دارنده آن توانایی تشخیص آسیب‌پذیری‌ها و موارد امنیتی موجود و ارائه راهکارهایی برای از بین بردن و یا کاهش آنها را دارد. استفاده از هکر اخلاقی (CEH) یکی از راه‌هایی است که سازمان‌ها می‌توانند خود را در مقابل حملات محافظت کنند، زیرا هکر اخلاقی قادر است تا راه‌های حمله بالقوه موجود را پیش از مهاجم تشخیص دهد. با این هدف، یک هکر اخلاقی دقیقا همان مسیری را که یک مهاجم دنبال می‌کند طی می‌کند. اسکن آسیب‌پذیری‌های شبکه با استفاده از ابزارهای تست خودکار آسیب‌پذیری، به تنهایی کافی نیست. زیرا این ابزارها در برخی موارد دارای تشخیص‌های نادرست می‌باشند و علاوه بر آن قادر به شناسایی بسیاری از آسیب‌پذیری‌های موجود نمی‌باشند.

از آنجایی که سازمان‌ها نیاز به شناسایی نقاط آسیب‌پذیر در شبکه دارند، باید افرادی را برای این کار به‌کار گیرند، البته باید در نظر داشته باشیم که شناسایی آسیب‌پذیری‌های سازمان، کار بسیار پیچیده و دشواری است. استفاده از اسکنرها برای شروع مناسب هستند، اما شناسایی نقاط نفوذ و آسیب‌پذیری در شبکه‌هایی با ساختارهای پیچیده، نیازمند جمع‌آوری اطلاعات جزئی‌تر و نیز استفاده از راه‌کارهای نوآورانه و خلاق است. به همین دلیل است که سازمان‌ها ناگزیر از اسنفاده از هکرهای اخلاقی می‌باشند.

آزمون CEH به دو دلیل طراحی شده است. در این آزمون نه تنها دانش فنی عمیق متقاضی آن مورد سنجش قرار می‌گیرد، بلکه رعایت نکات و موارد اخلاقی و قانونی در روند استفاده از آنها نیز همواره مد نظر می‌باشد. سازمان‌ها با بکارگیری افرادی که دارای گواهینامه CEH می‌باشند، مطمئن می‌شوند که آنها علاوه بر داشتن دانش و توانایی لازم برای تست نفوذ و شناسایی آسیب‌پذیری‌های موجود در شبکه و فناوری‌های مورد استفاده سازمان، هیچگاه کاری که منجر به بروز اختلال و خرابی در سیستم‌ها و روندهای سازمان شود را انجام نمی‌دهند.

هدف کتاب

برای اینکه خواننده کتاب بتواند خود را برای گذراندن آزمون CEHv10 آماده کند، در این کتاب موضوعات زیر مطابق با آخرین سرفصل‌های ارائه شده برای آزمون CEHv10 ارائه شده است:

- مقدمه‌ای بر هک اخلاقی
- جمع‌آوری و یادداشت‌برداری
- اسکن شبکه
- سرشماری و برآورد
- آنالیز آسیب‌پذیری
- هک سیستم
- تهدیدهای بدافزار
- اسنیفرها
- مهندسی اجتماعی

- اختلال در سرویس
- دستکاری نشست
- گول زدن IDS و فایروال و هانی‌پات
- هک وب‌سرورها
- هک نرم‌افزارهای تحت وب
- تزریق SQL
- هک شبکه‌های بی‌سیم
- هک سیستم‌های موبایل
- هک اینترنت اشیاء
- فضای پردازش ابری
- رمزنگری

همانگونه که مشاهده می‌کنید، موضوعات بسیار متنوع و گسترده‌ای در آزمون CEH مد نظر است که علاوه بر کسب دانش و آگاهی در هر یک از آنها، نیاز به شناخت ابزارهایی که در هر مورد استفاده می‌شود داریم.

سرفصل‌های آزمون CEH بسیار فنی است و تنها شناخت تئوریک آنها برای گذراندن آزمون کافی نمی‌باشد. برای گذراندن موفق آزمون باید علاوه بر کسب دانش کافی در هر مورد، ابزارهای مورد استفاده در هر بخش را بشناسید و در استفاده از آنها مهارت و تجربه کافی را کسب کنید.

در باره آزمون

آزمون CEH حاوی ۱۲۵ پرسش چند گزینه‌ای است که برای آن ۴ ساعت زمان در نظر گرفته می‌شود. به عبارت دیگر برای پاسخ به هر پرسش به طور میانگین دو دقیقه زمان در اختیار دارید. برای ثبت نام در آزمون می‌توانید از طریق مرکز آزمون ECC و یا مرکز ثبت نام آزمون Pearson VUE اقدام کنید.

در حال حاضر آزمون CEH به صورت عملی نیز ارائه می‌شود که برای گذراندن آن، مسائلی واقعی ارائه می‌شود که باید آن‌ها را بررسی و نفوذپذیری آنها را آزمایش کنید و سپس نتایج بدست آمده را به صورت یک گزارش ارائه دهید. کسانی می‌توانند برای آزمون ثبت نام کنند که دست‌کم دارای ۱۸ سال سن باشند.

توزیع موضوعات در فصل‌های کتاب

در جدول زیر موضوعات آزمون CEHv10 به تفکیک فصل‌های کتاب آورده شده است. موضوعات آزمون به تکفیک فعالیت‌ها و دانش مورد نیاز آزمون CEV تفکیک شده است.

فصل	موضوع
فعالیت‌ها	
7, 14	توسعه و مدیریت سیستم‌ها
4, 5, 6, 7	آنالیز و بررسی سیستم‌ها
7, 8	تست امنیت و آسیب‌پذیری
1, 7	گزارش‌گیری
7, 8	مقابله و کاهش آسیب‌پذیری
1	موارد اخلاقی و قانونی
دانش	
2, 3	پیش زمینه
2, 11	آنالیز / برآورد
3, 13, 14	امنیت
4, 5, 6, 7	ابزارها، سیستم‌ها و برنامه‌ها
1, 4, 5, 6, 7, 14	روال‌ها و متدلوژی‌ها
1, 14	قوانین و آیین‌نامه‌ها
1	موارد اخلاقی و قانونی

در باره مترجم

با بیش از ۲۸ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت داشته و دارای مدارک بین‌المللی متعددی در حوزه شبکه، امنیت شبکه و تست نفوذ است که عبارتند از:

Network+, Microsoft Certified Professional (Windows 2016), CEH, Digital Forensics Examiner, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW security Professional, ISO27001 Lead Auditor.

در صورت نیاز به برقراری ارتباط با مترجم می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

فصل نخست

هکر قانونمند

در این فصل موضوعات زیر در آزمون CEH پوشش داده شده‌اند:

- دستورالعمل رفتار حرفه‌ای (Professional code of conduct)
- شرایط مناسب برای هک

به دنیای جالب امنیت اطلاعات، به‌ویژه به دنیای مهمی که ما آن را هکر قانومند می‌نامیم، خوش آمدید. یکی از دلایل مطالعه این کتاب گذراندن آزمون CEH و دریافت گواهینامه رسمی آن است. برخی‌ها مسیر دریافت آزمون را از طریق گذراندن دوره‌های آموزشی مدون و تخصصی که از جانب موسسه ECCouncil ارائه شده است، طی می‌کنند و برخی دیگر برای گذراندن آزمون، مسیر مطالعه شخصی به همراه کسب تجربه لازم در موضوعات مرتبط با آزمون را انتخاب می‌کنند. این کتاب نیز منبع مناسبی برای همه افرادی که به هر روشی قصد شرکت در آزمون CEH را دارند، به شمار می‌آید.

در این کتاب موضوعات مختلف و متنوعی در ارتباط با آزمون CEH پوشش داده شده است، و به اغلب آنها به طور فنی و تخصصی پرداخته شده است، بنابراین لازم است که شناخت و درک روشن و درستی از آنها را بدست آورید. این نوع شناخت و درک مطالب برای افرادی که قصد شرکت در آزمون عملی CEH را دارند، از اهمیت بیشتری برخوردار می‌باشد. در این فصل، به عنوان نقطه شروع، مطالب و موضوعات فنی مطرح نشده‌اند و هدف از این فصل ارائه شناخت کلی از مبانی آزمون CEH می‌باشد. در ابتدا با مبانی هکر قانونمند آشنا خواهید شد. مهترین بخش در واژه هکر قانونمند، کلمه اخلاقی (Ethical) می‌باشد. زمانی که قصد گذراندن آزمون CEH را داشته باشید، باید دستورالعمل و آیین نامه مربوط به آن را قبول کنید، بنابراین شناخت محتویات آن از اهمیت زیادی برخوردار می‌باشد، زیرا در همه فعالیت‌های حرفه‌ای در حوزه هکر قانونمند باید از آنها پیروی کنید.

در انتها نیز، با موسسه EC-Council و همچنین ساختار و قالب و آزمون‌های آن آشنا خواهید شد.

مروری بر اخلاق[1]

پیش از اینکه در مورد هک اخلاقی (قانونمند) صحبت کنیم، به یکی از جنبه‌های مهم آن یعنی اخلاق می‌پردازیم. همانگونه که مشاهده می‌کنید واژه اخلاق در ابتدا مطرح می‌شود[2] و به آن hacking ethically گفته نمی‌شود. بخش مهم آن در واژه ابتدایی آن است. واژه اخلاق چالش برانگیز است، زیرا مفهوم بین المللی ندارد و هر کسی در مورد آن برداشت شخصی خود را دارد. چه بسا موردی که برای شما غیراخلاقی محسوب می‌شود، برای دیگری اخلاق‌مدار باشد و یا برعکس. بنابراین شناخت دقیق و درست از این واژه و اینکه کدام موارد اخلاقی و کدامیک غیراخلاقی در نظر گرفته می‌شوند، از دیدگاه مدرک CEH از اهمیت ویژه‌ای برخوردار می‌باشند. پس از آن، شما به عنوان معتمد امکان دسترسی به منابع و اطلاعات حساس و مهم سازمان را خواهید داشت. برای اینکه بتوانید اعتبار حرفه‌ای خود را حفظ کنید، باید مراقب باشید که همه فعالیت‌های خود را در چارچوب اخلاقی انجام دهید. نه تنها باید خود را ملزم به اجرای همه عملیات مبتنی بر اخلاق حرفه‌ای بدانید، بلکه از شما انتظار می‌رود تا از بیانیه اخلاق (Code of ethics) نیز پیروی کنید.

به عنوان بخشی از بیانیه اخلاق، شما ملزم شده‌اید تا اطلاعاتی که بدست می‌آورید را خصوصی تلقی کرده و در محافظت و عدم افشای آنها تلاش کنید. زمانی که قصد حمله به سیستمی را دارید، اطلاعات حساس و مهمی از آن را در اختیار خواهید داشت. همچنین در رفت و آمد در سازمان نیز به اطلاعات مهمی از آن سازمان دست خواهید یافت. هرگونه سهل‌انگاری در نگهداری و محافظت از این اطلاعات باید نقض بیانیه اخلاق و خدشه در حفظ محرمانگی داده‌های سازمان خواهد شد.

ما فقط مجاز به افشای اطلاعاتی هستیم که افشای آنها برای افرادی که مرتبط با کارمان هستند، مجاز اعلام شده است. این اطلاعات شامل مواردی است که در حین اجرای پروژه شناسایی می‌شوند. در ضمن مجاز به افشای همه موارد موجود و بالقوه از تداخل منافع می‌باشیم. بسیار مهم است که تا حد امکان نامرئی باشیم و در مواردی که منجر به محافظت از کارمندان و مشتریان و منافع سازمان می‌باشند، کار درست را انجام دهیم. در ضمن در مواردی که اقدامات ما منجر به تأثیر در عملکرد تعداد زیادی کاربر در اینترنت شود، باید این موارد را به شکلی مسئولانه اعلام کنیم. این بدان معنی نیست که آن را در فروم‌های عمومی اعلان کنیم. باید آن را به مشتری، ذینفع‌های سازمان و تیم‌های واکنش سریع سازمان و همچنین کمیته مقابله با بحران سازمان اعلام کنیم.

---

[1] Ethics
[2] ethical hacking

به عنوان مثالی از یک رفتار در افشای مسئولانه اطلاعات، به عملکرد دان کامینسکی[1] توجه می‌کنیم. او یک رخنه جدی در سرویس DNS را پیدا کرد، که باعث تأثیر بر روی کاربران اینترنت می‌شد. او به طور مسئولانه و با صرف زمان زیاد با برندها و عرضه‌کنندگان سرویس مورد نظر تلاش کرد تا پیش از افشای آن، رخنه مورد نظر را برطرف کند. در انتها نیز وجود رخنه مورد نظر را برای اطلاع عموم منتشر کرد. او با اینکار از تهدید و خطری که کاربران اینترنتی با آن مواجه بودند، جلوگیری کرد.

در حین کار، به اطلاعات و منابع سازمان و یا مشتری خود دسترسی خواهید داشت. با توجه به بیانیه اخلاق، قبول کرده‌اید که از آنها در موارد و کاربردهای نادرست استفاده نکنید. در ضمن باید به هیچ یک از منابع و تجهیزات سازمان آسیبی نرسانید. البته زمان‌هایی وجود خواهند داشت که در زمان تست، برخی از سرویس‌های سازمان با اختلال روبرو شوند، که این موارد باید با هماهنگی و قبول سازمان انجام شوند. بنابراین یکی از توصیه‌هایی که همواره می‌شود، این است که یک راه ارتباطی دائمی و باز با افراد مسئول در سازمان داشته باشید، تا در صورت بروز هرگونه مورد غیرمنتظره به آنها اعلام شود، تا از بروز اختلالات و آسیب‌های ناشی از آن تاحد ممکن کاسته شود.

نیاز به ذکر نیست که اجازه انجام عملیات و رفتارهای غیرقانونی را ندارید. همچنین اجازه عضویت و ارتباط با گروه‌های غیرقانونی و هکرهای کلاه سیاه و همه سازمان‌های خلاف کار و غیرقانونی را نیز ندارید.

واژگان رنگ‌ها

تاکنون حتما واژه‌های کلاه سفید، کلاه سیاه و کلاه خاکستری را شنیده‌اید. هکرهای کلاه سفید کسانی هستند که عملیات خود را با هدف قانونی و خوب انجام می‌دهند. هکرهای کلاه سیاه رفتارهای مجرمانه و خلافکارانه دارند و معمولا کارهای آنها مصداق کارهای غیرقانونی است. هکرهای کلاه خاکستری در میانه این دو گروه قرار دارند. آنها رفتارهایی با اهداف خوب انجام می‌دهند، اما از تکنیک‌ها و روش‌های هکرهای کلاه سیاه استفاده می‌کنند.

تا زمانی که ارتباط حرفه‌ای خود را به شکلی کاملا روشن و واضح با مشتری خود حفظ کنید و آنها را در جریان همه اقدامات خود در ارتباط با سیستم‌های مرتبط با سازمان قرار دهید، آنگاه رفتار و عملکردتان اخلاق‌مدار و قانونی خواهد بود.

---

[1] Dan Kaminsky

مروی بر هک اخلاقی

این روزها، وقتی که به منبع اخبار نگاه می‌کنیم، نمی‌توانیم چیزی در ارتباط با سرقت داده‌ها، جرائم اینترنتی و حملات سایبری به افراد و سازمان‌ها را مشاهده نکنیم. آنچه که در اخبار می‌بینیم، در واقع مواردی بزرگ از نفوذهای متعدد به سازمان‌ها و دست‌کاری رکوردها و داده‌های افراد می‌باشند. اما آنچه که در این اخبار به آنها اشاره نمی‌شود، تعداد سیستم‌ها و تجهیزاتی است که مورد دست‌کاری و هک قرار گرفته‌اند. به عنوان مثال بر اثر آلودگی به بات‌نت میرای[1] تخمین زده می‌شود که در حدود بیش از صدهزار دستگاه آلوده شده باشد.

در هر سال، میلیون‌ها بدافزار جدید تولید می‌شوند، که برخی از آنها از آسیب‌پذیری‌هایی که به تازگی شناسایی و کشف شده‌اند، استفاده می‌کنند. از سال ۲۰۰۵، در هر سال حداقل ده میلیون رکورد اطلاعاتی مورد تخریب و دست‌کاری قرار گرفته است. در سال ۲۰۱۷، در حدود دویست میلیون رکورد اطلاعاتی مورد دست‌کاری و تخریب قرار گرفته است. این آمار تنها مربوط به کشور آمریکا می‌باشند. با توجه به اینکه در حدود ۲۵۰ میلیون نفر در آمریکا زندگی می‌کنند، بنابراین شاید بتوان نتیجه گرفت که تقریبا اطلاعات هر فرد آمریکایی حداقل یک‌بار مورد دست‌کاری و تخریب قرار گرفته است. برای وضوح مطلب باید توجه داشته باشیم که رکوردهای اطلاعاتی مربوط به افراد می‌باشند، نه سازمان‌ها.

همه مطالب فوق، به اهمیت ارتقای امنیت اطلاعات اشاره دارند. واضح است که برای جلوگیری از حملات، بهترین راه شناخت درست و صحیح آنهاست. ایده‌آل است، اگر بتوانیم حملات را دقیقا شبیه‌سازی کنیم. در صورتی که سازمان با حملات به صورت کنترل شده و از قبل مواجه شود، آنگاه می‌تواند در مقابل حملات از خود محافظت کند.

این نوع تست در مقابل حملات دقیقا همان کاری است که هکر اخلاقی انجام می‌دهد. همه موارد با هدف تشخیص مشکلات و ضعف‌های امنیتی سازمان و ارتقای امنیت آن انجام می‌شوند. شناسایی ضعف‌های امنیتی سازمان در ارتباط با شبکه و حتی رایانه‌های رومیزی انجام می‌شوند. تست‌های امنیتی سازمان برای تشخیص ضعف‌ها و آسیب‌پذیری‌های نرم‌افزارهای سازمان به منظور تشخیص نفوذپذیری آنها و در نهایت سیستم‌هایی که بر روی آنها اجرا می‌شوند، به‌کار برده می‌شوند. برای اجرای این نوع تست‌ها هکرهای قانونمند توسط سازمان‌ها استخدام شده و یا با آنها قرارداد می‌بندند. در سازمان‌ها سیستم‌ها و برنامه‌های کاربردی تحت وب وجود دارد، که آنها قصد تست و آزمایش آنها را دارند.

هکر اخلاقی با اسامی مختلفی نام برده می‌شود. به طور مثال در برخی از وظایف شغلی آنها از عنوان تست نفوذ استفاده می‌شود. در واقع همه آنها یک کار را انجام می‌دهند. یک متخصص

---

[1] Mirai botnet

تست نفوذ، نفوذپذیری ابزارهای تدافعی سازمان را کنترل می‌کند، این همان هدف هکر اخلاقی می‌باشد. در برخی موارد با نام تیم سرخ[1] مواجه می‌شویم، که در واقع مسئول نوع خاصی از تست نفوذ می‌باشد که در آن فرد تست نفوذ کننده به عنوان مهاجم در سازمان و شبکه تحت تست، در نظر گرفته می‌شود. اعضای تیم سرخ همانند مهاجم رفتار می‌کنند، بنابراین سعی می‌کنند تا مخفی بمانند تا قادر به تشخیص آنها نباشیم.

یکی از جنبه‌های چالش برانگیز فعالیت‌های هک قانونمند این است که باید همانند یک مهاجم فکر کنیم. تست‌های نفوذپذیری دارای چالش‌های مخصوص به خود می‌باشد و نیاز دارد که به شیوه‌ای دیگر بیاندیشیم. زمانی که قصد انجام عملیات تست نفوذپذیری و هک اخلاقی را داریم، داشتن و استفاده از یک متدولوژی مشخص لازم و ضروری می‌باشد، زیرا وجود آن تکرارپذیری و اعتبارسنجی عملیات انجام شده را تضمین می‌کند. متدولوژی‌های مختلفی در این حوزه وجود دارند. البته هر متخصصی از شیوه و روش مربوط به خود استفاده می‌کند که البته مراحل کلی آن بین تمامی متخصصان تست نفوذ و هک اخلاقی مشترک می‌باشند. در ادامه فصل به این موارد کلی و مشترک اشاره خواهیم کرد.

EC-Council انجام عملیات به صورت اخلاقی را برای کسانی که موفق به کسب مدرک CEH شوند، با قبول بیانیه اخلاق تضمین می‌کند.

متدولوژی هک اخلاقی

متدولوژی اصلی بر مبنای آنچه که مهاجمان در واقعیت انجام می‌دهند، طراحی شده است. شرکت‌ها و سازمان‌ها قادرند تا سطح امنیت خود را بر حسب اطلاعاتی که در هر سطح و مرحله بدست می‌آید، ارتقاء دهند.

یادداشت برداری و بازآفرینی[2]

هدف از این مرحله، جمع‌آوری اطلاعات از هدف مورد نظر می‌باشد. با توجه به اطلاعات جمع‌آوری شده، سطح فعالیت‌ها و عملیات محدودتر شده و از انجام عملیات خلاف اخلاق جلوگیری خواهد شد. اطلاعات جمع‌آوری شده شناخت کلی در مورد هدف را در اختیارمان قرار می‌دهد که معمولا فاقد جزئیات مربوط به آن می‌باشد. جمع‌آوری اطلاعات جزئی‌تر از هدف با استفاده از عملیات بازآفرینی انجام می‌شود. با توجه به ویژگی اینترنت و عملیاتی که سازمان‌ها در

[1] Red team
[2] Reconnaissance and Footprinting

اینترنت انجام می‌دهند، معمولا اطلاعات زیادی در ارتباط با سازمان‌های مختلف در اینترنت بدست می‌آوریم.

هدف از مرحله جمع‌آوری اطلاعات و بازآفرینی، شناخت اندازه و محدوده گسترش هدف تست نفوذ می‌باشد. با استفاده از ردپا می‌توانیم اندازه و نمایش سازمان را مشخص کنیم. به عبارت دیگر با استفاده از اطلاعات این مرحله، بخش‌های مختلف شبکه و میزبان‌ها و موقعیت آنها و کاربران سازمان را شناسایی می‌کنیم. از اطلاعات جمع‌آوری شده در این مرحله، در مراحل بعد استفاده خواهد شد.

اسکن و شمارش[1]

پس از اینکه بخش‌های مختلف شبکه و بلوک‌های موجود در آن را مشخص کردیم، نوبت به سیستم‌های قابل دسترس در آنها می‌رسد، که این اطلاعات در مرحله اسکن و شمارش بدست می‌آیند. در این مرحله اطلاعات مهمی نظیر سرویس‌هایی که در هر یک از میزبان‌ها فعال می‌باشند، نیز بدست می‌آیند. هر یک از این سرویس‌ها می‌توانند راهی برای نفوذ به سیستم مورد نظر باشند. با توجه به اینکه هدف، دسترسی به سیستم‌ها است، امکان انجام این کار با استفاده از نفوذ از طریق سرویس‌های فعال در سیستم‌های فعال در شبکه وجود دارد. در این مرحله نه تنها فهرستی از پورت‌های باز بدست می‌آوریم، بلکه سرویس‌ها و نرم‌افزارهای فعال در هر یک از پورت‌ها را نیز شناسایی می‌کنیم.

در این مرحله، امکان جمع‌آوری اطلاعاتی که توسط سرویس‌های فعال تولید می‌شوند نیز وجود دارد. این موارد شامل نرم‌افزارهای ارائه دهنده سرویس نظیر nginx و Apache و IIS به عنوان سرویس دهنده وب می‌باشند. در این میان سرویس‌هایی وجود دارند که نه تنها جزئیاتی را در ارتباط با نرم‌افزارها، بلکه در مورد داخل سازمان نیز در اختیارمان قرار می‌دهند، به عنوان مثال نام کاربران سازمان. در صورتی که در سرورهای SMTP سازمان، جستجوی صحیح انجام دهیم، امکان دسترسی به نام‌های کاربری معتبر را خواهیم داشت. از سرورهای ویندوز سازمان با استفاده از پروتکل‌های SMB[2] و CIFS[3] می‌توان اطلاعات مفیدی را بدست آورد. با استفاده از این پروتکل‌ها، امکان دسترسی نام پوشه‌های اشتراکی و نام‌های کاربری و آیین نامه‌های تعریف شده وجود دارد. هدف از این مرحله جمع‌آوری اطلاعات حداکثری برای استفاده در مراحل بعدی می‌باشد. با توجه به ابعاد و اندازه‌های شبکه هدف، انجام عملیات این مرحله زمان‌بر می‌باشد، در صورتی که اطلاعات بیشتری در این مرحله جمع‌آوری کنیم، مراحل بعدی بهتر انجام خواهند شد.

---

[1] Scanning and Enumeration
[2] Server Message Block
[3] Common Internet File Systems

دسترسی یافتن[1]

به عقیده بسیاری، دسترسی یافتن به هدف، مهمترین بخش از عملیات تست نفوذ می‌باشد، و برخی دیگر آن را جالب‌ترین بخش آن می‌دانند. در این بخش امکان ارائه آسیب‌پذیر بودن سرویس‌های فعال در شبکه سازمان وجود دارد. آسیب‌پذیر بودن سرویس‌ها با بهره‌برداری[2] از آنها برای نفوذ اثبات می‌شوند. در این مرحله یکی از ویژگی‌های اصلی هک اخلاقی نمایان می‌شود، نتیجه این مرحله به جای نفوذ و دست‌کاری اطلاعات و منابع سازمان، با مستندسازی ارائه می‌شود.

حملات تخصصی، نظیر آنهایی که به دنبال آسیب‌پذیری‌ها با استنفاده از کنترل سرویس‌های شبکه می‌گردند، در اغلب موارد به عنوان روشی برای نفوذ و دست‌کاری سیستم هدف تصور می‌شوند، اما در واقعیت آنچه که باعث دسترسی به سیستم‌ها می‌شود، عمدتا از جمله حملات مهندسی اجتماعی محسوب می‌شوند. این یکی از دلایلی است که اهمیت شمارش در سیستم هدف را توجیح می‌کند. زیرا معمولا برای دسترسی به سیستم هدف از حملات مهندسی اجتماعی استفاده می‌شود. راه‌های مختلفی برای اجرای حمله مهندسی اجتماعی وجود دارد، نظیر ارسال یک فایل آلوده به بدافزار به سیستم هدف و در اختیار گرفتن کنترل سیستم مورد نظر با استفاده از آن و یا بدست آوردن اطلاعات هویتی کاربران (نام کاربری و رمز عبور) با استفاده از روش‌های مختلف مهندسی اجتماعی.

مکانیزم دیگری برای جمع‌آوری اطلاعات کاربران، ترغیب آنها به ورود و مشاهده یک وب‌سایت آلوده می‌باشد. این وب‌سایت می‌تواند با استفاده از یک بدافزار که مهاجم بر روی سیستم مورد نظر قرار داده است، بارگذاری شود. با توجه به موارد ذکر شده مشخص است که بدافزارها نقش بسیار مهم و مؤثری بر عملیات دسترسی به سیستم هدف ایفا می‌کنند.

معمولا از شما برای اجرای حملات مهندسی اجتماعی درخواست نمی‌شود. سازمان‌ها از شیوه‌های مختلفی برای ارتقای امنیت استفاده می‌کنند، که در این میان مقابله با حملات مهندسی اجتماعی نیز در نظر گرفته شده است. به همین ترتیب حملات فیشینگ و یا حملات مبتنی بر وب نیز خواسته نمی‌شود و همچنین انتظار اجرای آنها توسط کاربران سازمان نمی‌رود. بنابراین نباید با توجه به سادگی اجرای این نوع حملات برای ایجاد دسترسی به سیستم‌ها، به استفاده از آنها متکی بود.

---

[1] Gaining Access
[2] Exploiting

حفظ دسترسی

پس از اینکه وارد سیستم هدف شدید، با توجه به بازسازی حملات واقعی باید در این مرحله دسترسی خود را به سیستم هدف حفظ کنید. در صورتی که مدیریت کاربر سیستم هدف را در اختیار داشته باشید، اگر سیستم هدف خاموش شود، آنگاه کنترل آن نیز از دست شما خارج خواهد شد، و به عبارت دیگر باید مجدد به آن نفوذ کنید. با توجه به اینکه تضمینی برای استفاده از آسیب‌پذیری‌ها و نقاط ضعف برای دسترسی به سیستم‌ها وجود ندارد، بنابراین امکان دارد که در دفعه بعد امکان نفوذ و دسترسی به سیستم هدف وجود نداشته باشد. زیرا امکان دارد تا اجرای یک به‌روزرسانی و یا نصب وصله امنیتی در سیستم هدف، باعث رفع آسیب‌پذیری موجود در آن شود. بنابراین پس از نفوذ به سیستم باید از شیوه‌هایی استفاده کنیم تا با استفاده از آنها امکان مشاهده رخدادها در سیستم هدف و همچنین سایر بخش‌های شبکه را داشته باشیم.

در این مرحله نیز بدافزارها می‌توانند کمک مؤثری بکنند. به عنوان مثال، می‌توانیم یک روت کیت[1] بر روی سیستم هدف نصب کنیم تا با استفاده از آن یک درپشتی[2] در آن ایجاد کنیم تا با استفاده از آن عملیات و حضور شما در سیستم مخفی شوند. علاوه بر آن برای حفظ دسترسی بر روی سیستم هدف باید نرم‌افزارهای دیگری را بر روی آن قرار دهیم. برای این کار نرم‌افزار مورد نظر را پس از ورود به سیستم مورد نظر، بر روی آن کپی می‌کنیم.

این مرحله به سادگی آنچه که بیان شد، نمی‌باشد. پارامترهای متعددی برای تضمین حفظ دسترسی به سیستم هدف مطرح می‌باشند. راه‌های مختلفی برای حفظ دسترسی به سیستم هدف وجود دارند، که بر اساس ویرایش و به‌روزرسانی انجام شده در سیستم‌عامل هدف، این روش‌ها دشوارتر خواهند بود. بنابراین این مرحله از هک اخلاقی با چالش‌های متعددی همراه می‌باشد، زیرا راه و گزینه مشخصی برای دست‌یابی به آن وجود ندارد.

مخفی کردن شواهد

مخفی کردن ردپاها شامل پنهان کردن و یا حذف شواهد بر جای مانده از دسترسی به سیستم هدف می‌باشد. علاوه بر آن باید عملیاتی که در آینده بر روی سیستم هدف اجرا می‌کنیم را نیز مخفی کنیم. برای این کار از یک بدافزار استفاده می‌کنیم تا از ثبت هرگونه لاگ جلوگیری کرده و در ضمن اطلاعات نادرستی را از سیستم بر روی شبکه گزارش کند.

---

[1] Rootkit
[2] Backdoor

نکته‌ای که باید به آن توجه داشته باشید این است که عملیات حذف ردپا و شواهد، خود ممکن است به عنوان یک رخداد در نفوذ به شبکه مدنظر قرار گیرد. به عنوان مثال، اگر فایل لاگ سیستم را پاک کنیم، این رخداد غیرمعمول، خود به منزله نفوذ به سیستم و حذف شواهد مربوط به آن خواهد بود. البته حذف فایل لاگ به معنی نفوذ قطعی به سیستم نمی‌باشد ولی شواهد کافی برای بررسی سیستم هدف از نقط نظر نفوذ به آن را در اختیارمان قرار می‌دهد. بنابراین عملیات پاک کردن ردپا و شواهد، بسیار چالش برانگیز می‌باشد.

خلاصه

بیان مفهوم و منظور دقیق و مشخص از واژه اخلاق بسیار سخت و دشوار می‌باشد. برای ثبت نام و پس از قبولی در آزمون CEH باید یک بیانه اخلاق را قبول کنید. همواره باید در همه عملیات هک اخلاقی در ارتباط با پرسنل و کارکنان سازمان، به صورت حرفه‌ای رفتار کنید. در هرمرحله از عملیات باید مسئولیت همه عواقب ناشی از عدم اعتماد را بپذیرید.

فصل دوم

مبانی شبکه

در این فصل موضوعات زیر از آزمون CEH پوشش داده می‌شوند:

- **فناوری‌های شبکه**
- **پروتکل‌های ارتباطی**
- **فناوری‌های ارتباطی**
- **توپولوژی‌های شبکه**
- **زیر شبکه**

علی رغم اینکه حجم مطالب آزمون CEH که در این فصل پوشش داده می‌شوند، زیاد می‌باشند، اما فراگیری مطالب این فصل برای مباحثی که در فصل‌های آتی به آنها اشاره خواهند شد، لازم و ضروری می‌باشند. علاوه بر آن، ممکن است که بگویید، وقتی که من پشت یک رایانه نشسته‌ام و سیستمی را هک می‌کنم، نیازی به برقراری ارتباط با شبکه ندارم. در برخی موارد، در حملات مختلف و یا به طور مشخص اقدام‌های تدافعی، استفاده از فناوری‌های شبکه و پروتکل‌های ارتباطی لازم می‌باشند.

برای درک چگونگی عملکرد شبکه، شناخت مفهوم ارتباط پروتکل‌های شبکه لازم می‌باشد. مدل‌های مفهومی که برای بیان ارتباط پروتکل‌های شبکه مورد استفاده قرار می‌گیرند، مدل OSI و TCP/IP نام دارند.

باید با توپولوژی‌های شبکه آشنایی داشته باشید. توپولوژی در واقع مدلی مفهومی برای بیان ساختار و ارتباط اجزای تشکیل دهنده شبکه می‌باشد. اولین چیزی که با استفاده از توپولوژی شبکه مشخص می‌شود، اجزای فیزیکی و موقعیت آنها می‌باشد و البته مشخص است که در هر شبکه انتظار داریم تا اجزای موجود در آن امکان برقراری ارتباط با یکدیگر را داشته باشند. آنچنانکه در ادامه مشاهده خواهید کرد، هر بخش از شبکه دارای آدرس‌های مختلفی می‌باشند. زیرا هر بخش از شبکه باید با پروتکل‌های مختلف که در لایه‌های گوناگون قرار دارند، ارتباط برقرار کنند.

با حرکت از لایه‌های پایین شبکه به سمت بالا، با پروتکل‌هایی مواجه خواهیم شد که شناخت بهتری از آنها دارید: IP، TCP، UDP. با توجه به اینکه این پروتکل‌ها نقش اصلی در ارتباط‌های شبکه ایفا می‌کنند، باید شناخت دقیقی از آنها داشته باشید، زیرا نه تنها برای تست سیستم بلکه برای یافتن آسیب‌پذیری‌های موجود در سیستم‌ها مورد استفاده قرار خواهند گرفت.

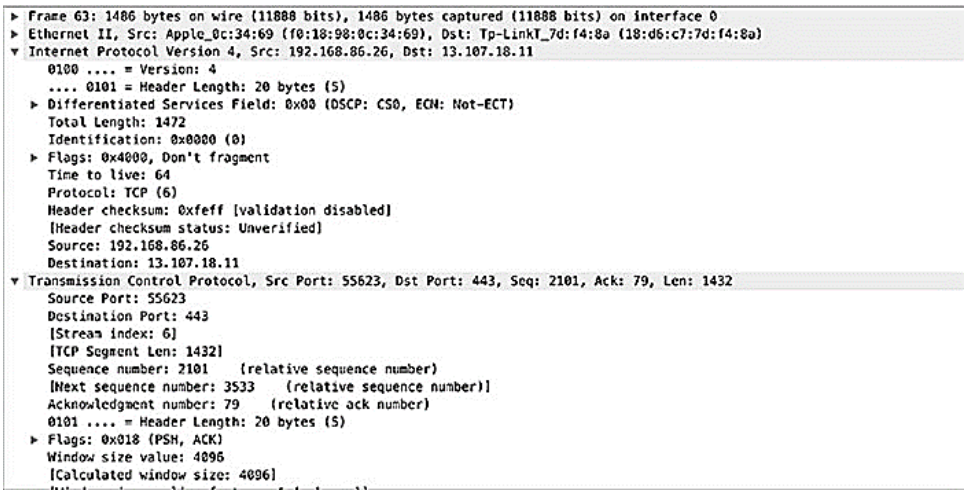
یکی از راه‌های معمول برای ارائه خدمات فناوری اطلاعات، به‌ویژه در مواردی که کاربران سیستم در خارج از سازمان قرار داشته باشند، استفاده از ارائه‌دهندگان خدمات (SP[1]) می‌باشد. فضای ابری، یکی از گزینه‌هایی است که می‌تواند در این موارد مورد استفاده قرار گیرد. وجود سرویس دهنده‌ها و همچنین سازمان‌هایی که از آنها استفاده می‌کنند، چالش‌های متعددی را برای برآورد و حفظ امنیت و همچنین تست نفوذپذیری در آنها ایجاد می‌کند. بنابراین شناخت سرویس دهنده‌های خارجی فناوری اطلاعات از اهمیت زیادی برخوردار می‌باشند.

مدل‌های ارتباطی

دسترسی به سیستم‌ها در شبکه از طریق آدرس‌های آن‌ها امکان‌پذیر می‌باشند. مشکل اصلی آنجاست که هر یک از سیستم‌ها از آدرس‌های متعددی استفاده می‌کنند. آدرس‌ها بهترین گزینه برای تفکیک عملیاتی است که توسط پروتکل‌های منتاظر با آنها انجام می‌شوند.

مدل‌های ارتباطی با استفاده از لایه‌های پروتکل بیان می‌شوند. نکته مهم در این مدل لایه‌ای این است که هر لایه دارای وظیفه و عملکرد مخصوص به خود می‌باشد. در واقع در زمان برقراری ارتباط بین دو سیستم در شبکه، لایه‌های متناظر در دو سیستم با یکدیگر مرتبط خواهند بود، زیرا پروتکل‌های موجود در این لایه‌ها بایکدیگر مشابه خواهند بود. این مطلب در مورد سایر لایه‌ها و پروتکل‌های موجود در آنها نیز صحیح می‌باشد. به عنوان مثال، مجموعه‌ای از عنوان‌های بسته‌های ترافیکی در شبکه در شکل زیر نشان داده شده است. لایه و پروتکلی که این عنوان بسته ترافیکی را در فرستنده ایجاد کرده است، تنها با استفاده از لایه و پروتکل همسان آن در طرف مقابل (گیرنده) خواندن می‌باشد.

[1] Service Providers



عنوان بسته ترافیکی

پروتکل ها

پیش از اینکه جلوتر رویم، لازم است تا با مفهوم پروتکل نیز آشنا شویم. پروتکل در واقع مجموعه‌ای از قوانین می‌باشد که شرایط برقراری ارتباط را مشخص می‌کند. زمانی که فرد آشنایی را در خیابان مشاهده می‌کنید، به او سلام می‌کنید. او هم در جواب پاسخ شما را می‌دهد. این یک پروتکل برای برقراری ارتباط می‌باشد. شما می‌دانید که در این مواقع چه چیزی را بگویید و طرف مقابل هم می‌داند که پاسخ آن را چگونه بدهد. در رایانه هم پروتکل‌ها اینگونه عمل می‌کنند.

با توجه به اینکه دو مدل ارتباطی وجود دارد، نه تنها عملکرد هر لایه، بلکه پروتکل‌های موجود در هر لایه را نیز شرح خواهیم داد. پس از پایان این بخش، با دو روش متفاوت، ولی نه غیرمشابه، چگونگی برقراری ارتباط با استفاده از پروتکل‌ها در شبکه و تبادل پیام بین سیستم‌ها آشنا خواهید شد.

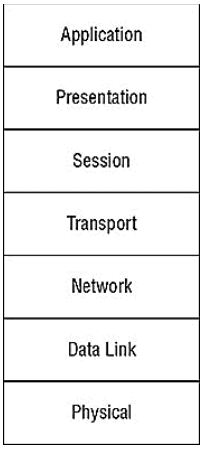
تفکیک فعالیت‌های ارتباطی شبکه در لایه‌های مختلف، به این معنی است که این فعالیت‌ها ماژولار کار می‌کنند. به عبارت دیگر به راحتی می‌توان یکی از پروتکل‌ها را از یک لایه برداشت و آن را با یک پروتکل جدید جایگزین کرد. پروتکل‌ها نیازی به شناخت جزئیات عملکرد هر یک ندارند، زیرا برای برقراری ارتباط، تنها کافی است که عملکرد آن را بشناسند.

مدل OSI[1]

پیش از اواخر دهه ۱۹۷۰، سیستم‌های ارتباطی از پروتکل‌های اختصاصی استفاده می‌کردند، بنابراین بیان مفهومی رخدادهای انجام شده در آن‌ها دشوارتر خواهند شد. هر پروتکل، ارتباط‌های مختلف را با استفاده از شیوه‌های مختلف تعریف می‌کند. در اواخر دهه ۱۹۷۰، سازمان جهانی استاندارد (ISO[2]) اقدام به تعریف مجموعه‌ای از استانداردهای ارتباطی نمود. هدف از انجام این کار، امکان برقراری ارتباط بین محصولات عرضه شده توسط برندهای مختلف بود. در صورتی که عملیات ارتباطی شبکه به صورت مفهومی تفکیک شود، نقاط ارتباطی بین آنها مشخص‌تر می‌شوند و امکان برقراری ارتباط بین آنها راحت‌تر می‌شود.

در سال ۱۹۷۸، مدل اولیه استاندارد ارتباطی اعلام شد. پس از بهینه‌سازی، با نام مدل OSI منتشر شد. این مدل شامل ۷ لایه می‌باشد. زمانی که در مورد یکی از فعالیت‌های مشخص در شبکه صحبت می‌کنیم، متخصصان شبکه آن را به یکی از لایه‌های این مدل نسبت می‌دهند. در زیر به چگونگی عملکرد این مدل به طور مختصر اشاره خواهیم کرد.

در شکل زیر ۷ لایه مدل OSI نشان داده شده است. شرح عملیاتی در این مدل را از بالاترین لایه آن (لایه مرتبط با کاربر) شروع می‌کنیم و تا پایین‌ترین لایه آن ادامه می‌دهیم.



مدل ۷ لایه OSI

پس از اینکه پیامی در لایه هفتم (لایه برنامه کاربردی) ایجاد شد، عملیاتی که در لایه‌های مختلف مدل OSI انجام می‌شوند را شرح خواهیم داد. البته برای اغلب افراد عملیات مختلف در لایه‌های موجود در این مدل از پایین به بالا شرح داده شده است.

---

[1] Open System Interconnection
[2] International Standard Organization

برنامه کاربردی (لایه هفتم): لایه برنامه کاربردی نزدیکترین لایه به کاربر می‌باشد. البته این به آن معنی نیست که این لایه تنها محدود به برنامه‌های کاربردی است. در لایه‌ها همواره از پروتکل‌ها صحبت می‌شود. در این لایه پروتکل‌هایی قرار دارند که برای برقراری ارتباط برنامه‌های کاربردی مختلف در شبکه مورد نیاز می‌باشند. با استفاده از این پروتکل‌ها، منابع مورد نیاز تعریف خواهند شد و سپس بین آنها ارتباط برقرار می‌شوند. به عنوان مثال، پروتکل HTTP[1] یکی از پروتکل‌های این لایه می‌باشد. با استفاده از آن ارتباط بین صفحات در سمت کاربر و سرور برقرار خواهد شد.

ارائه (لایه ششم): این لایه مسئولیت آماده‌سازی داده‌های مورد نیاز لایه ۷ را بر عهده دارد. این لایه دسترسی لایه داده به اطلاعات مناسب و با قالب صحیح را تضمین می‌کند. در زمان برقراری ارتباط بین سیستم‌ها، امکان دارد که قالب داده‌های موجود در طرفین ارتباط از قالب‌های یکسان استفاده نکنند، بنابراین لایه ششم ایجاد هماهنگی بین آنها را تضمین می‌کند.

نشست (لایه پنجم): وظیفه این لایه حفظ ارتباط برنامه‌های کاربردی بین نقاط پایانی در ارتباط شبکه‌ای می‌باشد. فناوری RPC[2] مثالی از عملیاتی است که در این لایه انجام می‌شود. در این لایه عملیاتی برای اشتراک فایل‌ها نیز انجام می‌شود. لایه برنامه کاربردی، مدیریت منابع را انجام می‌دهد، زیرا در لایه نشست، انتقال صحیح فایل‌ها را تضمین می‌کند.

انتقال (لایه چهارم): در این لایه عملیات تقسیم‌بندی پیام‌ها برای آماده‌سازی آنها پیش از انتقال انجام می‌شود. در این لایه عملیات تسهیم‌بندی ارتباط نیز انجام می‌شود. TCP و UDP پروتکل‌های این لایه می‌باشند. این پروتکل‌ها از پورت‌ها برای تعیین آدرس استفاده می‌کنند، بنابراین سیستم‌های دریافت کننده، امکان شناسایی برنامه کاربردی ارسال کننده ترافیک را دارند.

شبکه (لایه سوم): لایه شبکه پیام‌ها را بین نقاط انتهایی ارتباط ارسال می‌کند. این لایه عملیات انتقال پیام‌ها را با استفاده از آدرس‌ها و مسیریابی انجام می‌دهد. IP یکی از پروتکل‌های این لایه می‌باشد.

ارتباط داده (لایه دوم): یکی دیگر از آدرس‌هایی که برای برقراری ارتباط در شبکه مورد استفاده قرار می‌گیرد، مک آدرس (MAC[3]) نام دارد. این آدرس‌ها در لایه دوم مورد استفاده قرار می‌گیرند، با استفاده از این آدرس‌ها درگاه‌های ارتباطی شبکه شناسایی شده و ارتباط بین سیستم‌ها به

[1] Hyper Text Transport Protocol
[2] Remote Procedure Calls
[3] Media Access Control