هکر قانونمند

(CEH v9)

تست به همراه پاسخ تشریحی

مطابق با آخرین سرفصل آزمون بین‌المللی

ec-council – CEH v9

تألیف: ریموند بلاکمن

برگردان: مهندس مهران تاجبخش

انتشارات پندار پارس

۲۳۰ صفحه

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

info@pendarepars.com **www.pendarepars.com**

نام کتاب : **هکر قانونمند (CEH v9)، تست به همراه پاسخ تشریحی مطابق با آخرین سرفصل آزمون بین‌المللی ec-council CEHv9**

ناشر : **انتشارات پندار پارس**

تالیف : **ریموند بلاکمن**

برگردان : **مهران تاجبخش**

چاپ نخست : **دی ماه ۹۵**

شمارگان : **۵۰۰ نسخه**

طرح جلد : **رامین شکرالهی**

چاپ، صحافی : **روز**

قیمت : **۱۹۰۰۰ تومان** **شابک : ۱-۲۸-۸۲۰۱-۶۰۰-۹۷۸**

فهرست

پاسخ‌نامه‌ها

تقدیم به مادرم

به خاطر زحمات بی دریغش

و پسرم

که مایه امید و انرژی من است

پیش گفتار

ظهور و توسعه فناوری‌های نوین در حوزه فناوری اطلاعات و شبکه‌های کامپیوتری و قابلیت‌های موجود در آنها باعث شده است که استفاده از این فناوری‌ها در سازمان‌ها و موسسات مختلف اعم از دولتی و خصوصی و مالی و تجاری و بانک‌ها و ... روز به روز بیشتر شود؛ تا جایی که امروزه واحدهای فناوری اطلاعات به عنوان یکی از بخش‌های غیر قابل تفکیک در سازمان و موسسات مختلف تبدیل شده است. استفاده و به کارگیری هر فناوری جدید، افزون بر نکات مثبت، با نقاط ضعف و آسیب‌پذیری‌هایی نیز همراه است.

مهم‌ترین نقاط ضعف و آسیب‌پذیری‌هایی که در حوزه فناوری اطلاعات، راهبران و کاربران آنها را تهدید می‌کند را می‌توان به دو بخش انسانی و غیر انسانی تقسیم کرد. در بخش انسانی، عدم آموزش کافی و سهل انگاری و همچنین خطاهای کاربردی را می‌توان برشمرد و در بخش تهدیدهای غیر انسانی، نقاط ضعف و آسیب پذیری‌های ناشی از تنظیم و پیکربندی نامناسب و همچنین شناسایی آسیب‌پذیری‌های جدید در آن را می‌توان نام برد.

با توجه به اینکه شناسایی و مستندسازی آسیب‌پذیری‌ها و نقاط ضعف موجود به همراه بررسی و کشف نقاط ضعف و آسیب‌پذیری‌های جدید در سیستم‌های سخت‌افزاری و نرم‌افزاری مورد استفاده، و ارائه راه‌کارهای رفع و کاهش آنها نقش بسیار زیاد و موثری در ایمن‌سازی حوزه فناوری اطلاعات در سازمان و موسسات ایفا می‌کند، بنابراین نیاز به متخصصان تست نفوذ و یا هکر قانونمند که در این حوزه آموزش‌های تخصصی و مدونی را گذرانده‌اند، لازم و ضروری می‌باشد.

بدون تردید شناخته‌شده‌ترین، به‌روزترین و معتبرترین دوره آموزشی در حوزه تست نفوذ و هکر قانونمند، دوره CEH(Certified Ethical Hacking) می‌باشد که پس از رخداد ۱۱ سپتامبر ۲۰۱۱ در مرکز تجارت جهانی نیویورک، به طور جدی‌تر و سازمان یافته‌تر و در سطح وسیع‌تری توسط موسسه EC-Council مورد توجه قرار گرفت.

هم اینک بیش از ۱۵۰٫۰۰۰ نفر در سراسر دنیا این دوره تخصصی در حوزه تست نفوذ و هکر قانونمند را گذرانده و موفق به دریافت مدرک بین‌المللی آن شده‌اند.

با توجه به ظهور و پیدایش تهدیدها و آسیب‌پذیری‌های مختلف به همراه ارائه فناوری‌های نوین در حوزه‌های سخت‌افزاری و نرم‌افزاری و کاربردهای آنها، لازم است که متخصصان حوزه تست نفوذ و هکر قانونمند، پی‌درپی خود را به‌روز نگه دارند تا بتوانند با این چالش‌ها در حوزه فناوری اطلاعات به بهترین شکل ممکن برخورد نمایند. در همین راستا موسسه EC-Council به طور منظم و دست‌کم یک بار در سال اقدام به، به‌روزرسانی محتوا و برنامه آموزشی دوره CEH خود می‌نماید. هم اکنون این دوره آموزشی با آخرین برنامه و سرفصل و محتوای ارائه شده با عنوان CEHv9 مورد استفاده قرار می‌گیرد.

در برنامه آموزشی این دوره بیش از ۲۷۰ نوع روش حمله و نفوذ مورد بررسی قرار می‌گیرد و افزون بر آن در مجموعه آموزشی ارائه شده برای این دوره، بیش از ۱۴۰ کار عملی در قالب فعالیت‌های آزمایشگاهی بر گرفته

شده از سناریوهای واقعی با معرفی ۲۲۰۰ ابزار مختلف و به‌کارگیری بخشی از آنها به صورت عملی پیش‌بینی شده است.

با آزمون بین المللی CEHv9 بیشتر آشنا شویم

سرفصل و محتوای آموزشی و همچنین شرایط و قالب برگزاری آزمون بین‌المللی آن توسط موسسه EC-Council آمریکا به طور سالانه اعلام می‌گردد. البته در معرفی این دوره آموزشی به صراحت اعلام شده است که محتوا و سرفصل آموزشی و شرایط برگزاری آزمون می‌تواند بدون اطلاع قبلی در هر زمانی توسط موسسه EC-Council به‌روزرسانی شود و تغییر کند. این آزمون بین‌المللی دارای کد 50-312 است. این آزمون از ۱۲۵ پرسش چند گزینه‌ای تشکیل شده است و زمان برگزاری آزمون ۴ ساعت بوده و برای کسب موفقیت در آزمون، داوطلب باید دست‌کم ۷۰ درصد امتیاز در نظر گرفته شده برای آزمون را کسب کند. این آزمون توسط موسسات ECCEXAM / VUE برگزار می‌گردد.

موضوع های تشکیل دهنده این دوره آموزشی، ۲۰ عنوان به شرح زیر می‌باشند:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Netwrok
- Enumeration
- System Hacking
- Malware Threats
- Evading IDS, Firewalls and Honeypots
- Sniffing
- Social Engineering
- Denial of Services
- Session Hijacking
- Hacking Web servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- Cloud Computing
- Cryptography

محتوای موضوعی آزمون بین‌المللی CEHv9

- حوزه بررسی و برآورد تهدید و آسیب‌پذیری‌ها: ۱۶ درصد
- حوزه امنیت: ۲۶ درصد
- حوزه ابزارها / سیستم‌ها / نرم‌افزارها: ۳۲ درصد
- حوزه روش‌ها و متدها: ۲۲ درصد
- حوزه قوانین و آیین‌نامه‌ها: ۴ درصد

چه مطالبی را در این کتاب خواهید آموخت

در این کتاب مطالب در ۵ فصل ارائه شده است، بیش از ۶۰۰ پرسش چند گزینه‌ای برگرفته شده از آخرین تغییرات و به‌روزرسانی انجام شده در آزمون بین المللی CEHv9 می‌باشد.

تلاش شده است تا پرسش‌ها به گونه‌ای طراحی و ارائه شوند که تا حد زیادی به آزمون واقعی دوره بین المللی EC-Council CEH شباهت داشته باشد.

در پایان کتاب به تفکیک هر فصل از کتاب، پاسخ‌نامه به انضمام پاسخ تشریحی آنها نیز ارائه شده است.

گفتنی است که استفاده از این کتاب به عنوان تنها منبع آموزشی برای آماده‌سازی آزمون بین‌المللی CEH کافی نیست و بهترین کاربرد این کتاب در تست و ارزیابی میزان فراگیری دانش و همچنین آشنایی با نمونه سوالات آزمون بین‌المللی می‌باشد.

این کتاب برای چه کسانی است

با توجه به اینکه آشنایی با روش‌های گردآوری اطلاعات و شناسایی نقاط ضعف و آسیب‌پذیری‌ها و همچنین ابزارها و فناوری‌هایی که برای نفوذ استفاده می‌شوند، برای همه متخصصان امنیت و تست نفوذ و ادله الکترونیک لازم و ضروری می‌باشد، بنابراین مطالعه این کتاب به همه این گروه‌ها توصیه می‌گردد. هرچند، این کتاب می‌تواند برای همه کسانی که در حوزه امنیت فضای مجازی و تست نفوذ فعالیت می‌کنند و یا خود را برای آزمون بین‌المللی CEH آماده می‌کنند نیز مفید باشد.

درباره مترجم

با بیش از ۲۶ 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 چندین مدرک بین‌المللی در حوزه شبکه، امنیت شبکه و تست نفوذ است که عبارتند از:

Network+, 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

مهران تاجبخش

زمستان ۹۵

فصل نخست

تست‌های آمادگی آزمون ۱

۱- کدامیک از فعالیت‌های زیر عملیات شناسایی غیرفعال [۱] است؟

الف – جست‌وجو در کاغذها

ب – تماس با بخش منابع انسانی

ج – استفاده از فرمان nmap –sT

د – اجرای حمله مرد میانی[۲]

ه – نصب و راه‌اندازی یک نقطه دسترسی قلابی[۳]

۲- کدام روش رمزنگاری توسط انستیتو ملی استاندارد و فناوری[۴] به عنوان روش اصلی برای حفظ محرمانگی پس از الگوریتم DES انتخاب شد؟

الف – 3DES

ب – Twofish

ج – RC4

د –AES

۳- با استفاده از کدامیک از ابزارهای زیر می‌توان در شبکه‌ای که از پروتکل 802.3 استفاده می‌کند، اقدام به حمله مرد میانی نمود؟

الف – Ethercap

ب – Cain & Abel

---

[۱] Passive Reconnaissance

[۲] Man-in-The-Middle Attack (MiTM)

[۳] Rogue HotSpot

[۴] NIST – National Institute of Standard and Technology

ج – Wireshark

د – Nmap

۴- تفاوت میان یک فایروال سنتی و یک سیستم جلوگیری از نفوذ غیرمجاز[۱] کدام است؟

الف – فایروال ثبت رخداد (log) نمی‌کند.

ب – سیستم جلوگیری از نفوذ غیرمجاز بسته‌های را از بین نمی‌برد.

ج ـ سیستم جلوگیری از نفوذ غیرمجاز از قواعد مشخصی پیروی نمی‌کند.

د – سیستم جلوگیری از نفوذ غیرمجاز می‌تواندمحتویات بسته‌ها را موشکافی کند.

۵- چرا عملیات بررسی و اسکن شبکه هدف می‌بایست به آهستگی صورت گیرد؟

الف – برای اینکه سیستم تشخیص نفوذ غیرمجاز[۲] هشدار ندهد.

ب – انجام آهسته شبکه هدف جزو الزامات می‌باشد.

ج – به منظور فرار از فایروال

د – سرویس‌ها ممکن است که فعال نشده باشند، بنابراین بررسی و اسکن آهسته باعث می‌شود که بتوان آن را نیز مورد بررسی قرار داد.

۶- شما مدیر ارشد در واحد فناوری اطلاعات سازمان خود می‌باشید. مقرون به صرفه‌ترین روش مورد استفاده برای جلوگیری از حملات مهندسی اجتماعی کدام است؟

الف – نصب HIDS[۳]

ب – اطمینان از به‌روز بودن همه نرم‌افزارها

ج – رصد و کنترل همه فعالیت‌های رایانامه

د – اجرای آموزش‌های پیشگیری برای پرسنل

۷- در چارچوب عملیات هکر قانونمند در کدام مرحله اقدام به تغییر و یا حذف اطلاعات ثبت رخدادها می‌کنید؟

الف – اسکن و بررسی

---

[۱] IPS – Intrusion Prevention System

[۲] IDS – Intrusion Detection System

[۳] Host-Based Intrusion Detection System

ب – ایجاد دسترسی

ج – شناسایی

د – از بین بردن آثار و ردپاها

۸- مهاجم بر روی ایستگاه کاری هدف فرمان nmap –sT 192.133.10.5 را اجرا نموده است. او در کدام مرحله قرار دارد؟

الف – از بین بردن آثار و ردپاها

ب – تشخیص و شمارش

ج – بررسی و برآورد

د – ایجاد دسترسی

۹- کدامیک از الگوریتم‌های زیر از گروه الگوریتم‌های رمزنگار متقارن جریان داده[۱] می‌باشند؟

الف – AES

ب- ECC

ج – RC4

د – PGP

۱۰- مهم‌ترین جنبه اجرای پروژه تست نفوذ کدامیک است؟

الف – رسیدن به قالب معمول موافقت‌نامه طرفین

ب – مستندسازی همه عملیات و اقدامات

ج – پیدا کردن روش سریع گریز از تهدیدهای جدی

د – ایجاد مستندات لازم مورد استفاده گروه بیمه اطلاعات

۱۱ – شما مدیر بخش امنیت اطلاعات[۲] یک سازمان بزرگ فناوری می‌باشید. از شما خواسته شده است تا برای رمز نگاری سیستم‌های همراه جدیدی که سازمان در سال آینده میلادی ارائه می‌کند، روشی را ارائه نمایید. از کدامیک از استانداردهای رمزنگاری بیشتر ترجیح می‌دهید استفاده کنید؟

الف- RC4

---

[۱] Symmetric Stream Cipher

[۲] CISO – Chief Information Security Officer

ب – MD5

ج – ECC

د – Skipjack

۱۲ – عملیات اسکن بسته‌های SYN چه کار می‌کند؟

الف – قادر است تا یک ارتباط سه مرحله‌ای TCP را برقرار نماید.

ب– قادر است تا تنها یک ارتباط "نیمه باز" برقرار نماید.

ج – ارتباط نوع بسته ACK با سیستم هدف برقرار می‌کند.

د – همه گذرگاه‌های بسته در سیستم هدف را شناسایی خواهد نمود.

۱۳ – نقطه ضعف اصلی در ارسال درخواست از طریق پروتکل ARP کدام است؟

الف – در این بسته آدرس درخواست شده به همه ایستگاه‌های شبکه محلی ارسال می‌شود.

ب – بسته برگشتی حاوی آدرس درخواست شده به همراه نام کاربری و گذرواژه به‌صورت متن معمولی می‌باشد.

ج – آدرس درخواستی می‌تواند باعث حمله نوع اختلال در سرویس[۱] شود.

د – آدرس درخواست شده می‌تواند با استفاده از مک آدرس ایستگاه مهاجم جایگزین شود.

۱۴ – شما مدیریت امنیت اطلاعات در یک تارنمای شبکه اجتماعی معروف می‌باشید. اخیرا متوجه شدید که سرویس دهنده تارنمای شما با استفاده از نفوذپذیری روز صفر "SSL Heart Bleed" مورد دستکاری واقع شده است. نخستین اقدامی که به منظور مقابله با آن انجام خواهید داد، کدام است؟

الف – به‌روز آوری همه نرم‌افزارها در سرویس دهنده

ب – استفاده از کلیدهای رمزنگاری جدید

ج – توقف ارائه سرویس‌ها از طریق اینترنت

د – ایجاد محدودیت دسترسی به اطلاعات حساس و مهم

۱۵ – کدامیک از مراحل زیر نشان دهنده انجام موفقیت آمیز حمله مردمیانی به شبکه توسط مهاجم می‌باشد؟

الف – ایجاد دسترسی

ب – حفظ دسترسی

---

[۱] DoS – Denial of Service

ج – شناسایی

د – از بین بردن علائم و ردپاها

۱۶ – با استفاده از کدامیک از فناوری‌های استفاده از آسیب‌پذیری‌های[۱] زیر می‌توان درخواست SQL را در داخل آدرس تارنما[۲] بکار برد؟

الف – تزریق SQL[۳]

ب – انتقال کد بین تارنما[۴]

ج – حمله گول زدن (ماهیگیری با نیزه[۵])

د – تزریق کد SQL به کتابخانه Ruby on Rails

۱۷ – مقدار پیش فرض برای طول عمر بسته[۶] در سیستم‌عامل ویندوز ۷ کدام است؟

الف – ۶۴

ب – ۱۲۸

ج – ۲۵۵

د – ۲۵۶

۱۸ – با استفاده از کدامیک از مقادیر زیر به عنوان ورودی در فیلد مورد نظر می‌توانید آسیب پذیری آن را در مقابل حمله تزریق SQL آزمایش کنید؟

الف – SQL test

ب – admin and password

ج - !| or ||

د – 1’or’1’=’1

---

[۱] Exploit

[۲] URL – Uniform Resource Locator

[۳] SQL Injection

[۴] XSS – Cross Site Scripting

[۵] Spear Phishing

[۶] TTL – Time To Live

۱۹ – جنبه منفی استفاده از پروتکل SSH به همراه Telnet برای ایجاد امنیت کدام است؟

الف – پروتکل SSH ترافیک و اطلاعات هویتی را رمزنگاری می‌کند.

ب – امکان مشاهده فعالیت‌های مهاجم وجود ندارد.

ج – داده‌ها به‌صورت متن معمولی ارسال می‌شوند.

د- اطلاعی از کلید مورد استفاده ندارید.

۲۰ – حمله Ping of Death برای نخستین بار در چه زمانی مشاهده شد؟

الف – ۱۹۹۲

ب – ۱۹۸۹

ج – ۱۹۹۰

د- ۱۹۹۶

۲۱ – کدامیک از انواع ویروس‌های زیر آلودگی بیشتری ایجاد می‌کنند؟

الف- ویروس Melisa

ب – ویروس I Love You

ج – ویروس Blue Cross Punter

د – Stuxnet

۲۲ – شما بخشی از یک تیم پشتیبانی در سازمان می‌باشید. درخواستی از یکی از پرسنل سازمان دریافت می‌کنید مبنی بر اینکه سرعت رایانه وی به‌طور دوره‌ای کم می‌شود. افزون بر آن، کاربر اشاره می‌کند که مستندات از محل اصلی خودشان جابه‌جا می‌شوند و یا ناپدید می‌شوند. به همین منظور از راه دور به ایستگاه کاری موردنظر متصل می‌شوید. کدام بخش از سیستم موردنظر را مورد بررسی قرار خواهید داد؟

الف – بخش مربوط به پردازش‌ها در پنجره مدیریت برنامه‌ها

ب – C:\Temp

ج – بخش مربوط به ثبت رخدادها (Logs) در پنجره مدیریت برنامه‌ها

د- c:\Windows\System32\User

۲۳ – به عنوان یک مهندس شبکه، سفارشی را برای برقراری ارتباط بی سیم بین تجهیزات شبکه دو سازمان دریافت کرده‌اید. این تجهیزات بیش از ۲۰ مایل (بیش از ۳۵ کیلومتر) با یکدیگر فاصله دارند و در هر یک از سازمان‌ها بیش از ۴۰۰ پرسنل مشغول به کار می‌باشند و برای این کار بودجه‌ای در حدود ۲۰/۰۰۰ دلار تخصیص

داده‌اند. در هر یک از سازمان‌ها نیز یک کابل فیبرنوری (single-mode) وجود دارد. از کدام نوع آنتن برای برقراری ارتباط بی سیم استفاده خواهید نمود؟

الف – Multimode fiber

ب - VSAT[۱]

ج – Omni Direction

د- Directional

۲۴ – واژه کنترل مجموع[۲] در چه موردی کاربرد دارد؟

الف – داده‌ها در مقصد تغییر خواهند یافت

ب – عملیات سه مرحله‌ای ارتباط TCP به پایان رسیده است

ج – داده‌ها در زمان نگهداری و یا ارسال دچار تغییر شده‌اند

د- اندازه داده‌ها پس از ذخیره‌سازی

۲۵ – کدامیک از گزینه‌های زیر در مورد امن‌ترین طول کلید در پروتکل رمزنگاری RSA صحیح می‌باشد؟

الف – ۱۰۲۴ بیت

ب – ۲۵۶ بیت

ج – ۱۲۸ بیت

د – ۵۱۲ بیت

۲۶ – برای ایجاد عدم انکارپذیری[۳] در رایانامه، کدام الگوریتم را مورد استفاده قرار می‌دهید؟

الف – AES

ب – DSA

ج – 3DES

د – Skipjack

---

[۱] Very Small Aperture Terminal

[۲] Cechksum

[۳] nonRepudiation

۲۷ – کدامیک از گزینه‌های زیر شرایط مسابقه[۱] را توصیف می‌کنند؟

الف – وقتی‌که دو وضعیت در یک لحظه رخ دهند و این شانس به‌وجود آید که یک فرمان دلخواه مورد استفاده توسط کاربر با سطح دسترسی بالاتر، بتواند توسط کاربر غیرمجاز (دشمن) مورد استفاده قرار گیرد.

ب – جایی که یکی از دو وضعیت به‌وجود آمده، دیگری را کنسل کند و فرمان‌های دلخواه بتوانند بر اساس سطح دسترسی کاربر مورد استفاده قرار گیرند.

ج – وقتی‌که دو وضعیت موردنظر بتوانند در داخل یک حساب کاربری فعال شوند.

د- وقتیکه دو وضعیت موردنظر بتوانند در سطح دسترسی کاربر ارشد تر مورد استفاده قرار گیرند.

۲۸ – کاربران شبکه اعلام می‌دارند که امکان دسترسی به شبکه‌های خارج از شبکه سازمان را ندارند. شما به عنوان راهبر شبکه، قصد بررسی و جمع‌آوری اطلاعات از شبکه می‌نمایید. در تحقیقات خود متوجه می‌شوید که امکان دسترسی به شبکه‌های خارج از سازمان با استفاده از IP آدرس وجود دارد. دستور Ping با استفاده از نام تارنما کار نمی‌کند. دلیل این اشکال به‌وجود آمده کدامیک از موارد زیر می‌باشد؟

الف – فایروال ترافیک مربوط به سرویس دهنده DNS را مسدود کرده است

ب – سرویس دهنده DNS درست کار نمی‌کند.

ج – تارنماهای خارجی پاسخ نمی‌دهند.

د – بسته حاوی درخواست HTTP GET در خروجی توسط فایروال مسدود می‌شود.

۲۹ – شما راهبر شبکه مورد استفاده در شهر کوچک خود می‌باشید. اخیرا یک سیستم جلوگیری از نفوذ غیرمجاز (IPS) در شبکه نصب کرده‌اید. پس از نصب، از همان تنظیم‌های اولیه موجود در آن استفاده می‌کنید و تنظیم جدیدی بر روی آن انجام نداده‌اید. وقتی‌که صبح روز بعد فایل ثبت رخدادهای آنرا مشاهده می‌کنید، می‌بینید که شمار بسیار زیادی از فعالیت‌های انجام شده در شبکه در آن ثبت شده است که بررسی و مرور همه آنها کاری بسیار دشوار و طاقت فرسا خواهد بود. چه عاملی در سیستم موردنظر باعث ثبت رخدادها با این حجم بسیار زیاد شده است؟

الف – روشی که برای نصب و راه اندازی آن مورد استفاده قرار دادیم.

ب – حمله اختلال در سرویس (DoS) در شبکه رخ داده است.

ج – در شبکه محلی از طریق سوئیچ ترافیک به‌صورت حلقه ایجاد شده است.

---

[۱] Race Conditions

د – برای سیستم پیشگیری از نفوذ حد مرجع[۱] در نظر نگرفته‌ایم.

۳۰ – کدامیک از گزینه‌های زیر از جمله حمله سمت کاربر می‌باشند؟

الف – تبادل کد بین برنامه‌ها (XSS)

ب – حمله مرد میانی (MiTM)

ج – حمله چاه آب (Watering hole)

د – حمله اختلال در سرویس (DoS)

۳۱ – به عنوان متخصص تست نفوذ به همراه تعداد معدودی از افراد خاص در سازمان از انجام پروژه تست نفوذ در شبکه سازمان اطلاع دارید. به غیر از نام سازمان و محل آن هیچ اطلاع دیگری از شبکه سازمان در اختیار ندارید. نوع بررسی تست نفوذی که می‌بایست انجام دهید، کدامیک از گزینه‌های زیر می‌باشد؟

الف – تست جعبه خاکستری

ب – تست جعبه سفید

ج – تست جعبه سیاه

د – تست جعبه آبی

۳۲ – به عنوان مهاجم، شبکه هدف را پیدا کرده‌اید و در دو هفته آینده وقت خود را صرف مشاهده رفت و آمد پرسنل در سازمان می‌نمایید. همچنین مشاهده می‌کنید که چگونه افراد فاقد کارت شناسایی می‌توانند به بهانه حمل بسته‌های مختلف در سازمان رفت و آمد کنند. در انتهای زمان مذکور به یک جدول مشخص از گشت نگهبانی سازمان می‌رسید. این عملیاتی که انجام داده‌اید چه نام دارد؟

الف – پوشش هدف

ب – بدست آوردن دسترسی

ج – حفظ دسترسی

د – شناسایی

۳۳ – کدامیک از ابزارهای زیر با توجه به نتایج دقیق‌تری که ارائه می‌دهد مورد توجه بیشتر مهاجمان می‌باشد؟

الف – Ncat

ب – Nmap

---

[۱] Baseline

ج – Ping

د – Nslookup

۳۴ – با چه هدفی مهاجم با استفاده از ابزار Ncat اقدام به اجرای حمله اتصال باز TCP[۱] می‌نماید؟

الف – مهاجم قصد حمله به سیستم موردنظر را ندارد.

ب – مهاجم در استفاده از فرمان nmap دچار اشتباه عملیاتی شده است.

ج – مهاجم قصد برقراری ارتباط با سرویس‌های شبکه را دارد.

د – مهاجم قصد یافتن گذرگاه‌های باز برای برقراری ارتباط با شبکه را دارد.

۳۵ – چرا مهاجم از اتصال کابل مستقیم به کابل فیبر نوری شبکه پرهیز می‌کند؟

الف – هزینه انجام این کار خیلی زیاد است.

ب – اگر به‌درستی انجام نشود، باعث قطعی در کابل خواهد شد و موجب می‌شود که شبکه هدف متوجه شرایط غیر عادی شود.

ج – سرعت ترافیک شبکه به میزان زیادی کاهش می‌یابد.

د- اتصال مستقیم به کابل شبکه باعث اعلان در سیستم‌های IDS/IPS خواهد شد.

۳۶ – شما هکری هستید که توانسته‌اید به‌طور موفقیت آمیز به سرویس دهنده وب هدف نفوذ کنید. سپس در تارنمای سازمان هدف یک تغییر چهره ایجاد کرده‌اید و قابلیت تغییر سطح دسترسی به کاربر ارشد را نیز در آن سرویس دهنده پیدا کرده‌اید. پیش از اینکه در داده‌های موجود در سرویس دهنده نفوذ کنید، گام بعدی شما کدام است؟

الف – با استفاده از حساب کاربری جدید که ایجاد کرده‌اید، به سیستم وارد می‌شوید.

ب – به عقب برگشته و رخدادهای ثبت شده را ویرایش یا حذف می‌کنید.

ج – مطمئن می‌شوید که ارتباط کنونی قطع شده است.

د – از برقراری ارتباط دیگری اطمینان یافته و سپس از سیستم خارج می‌شوید.

۳۷ – مهم‌ترین نقطه ضعف استفاده از پروتکل Kerberos کدام است؟

الف – کلیدهای متقارن می‌توانند دستکاری شوند پس ایمن نیستند.

ب – Kerberos از رمزنگاری و کلیدهای ضعیف استفاده می‌کند و می‌تواند به‌راحتی شکسته شود.

---

[۱] Open TCP connection

ج – Kerberos از رمزنگاری متقارن استفاده می‌کند و می‌تواند به‌راحتی مورد سوء استفاده قرار گیرد.

د – با استفاده از حمله تکرار درخواست مجوز دسترسی[۱]، مهاجم می‌تواند به منابع و سرویس‌ها دسترسی پیدا کند.

۳۸ – در سیستم‌عامل ویندوز فایل حاوی رمزهای عبور در کجا قرار دارند؟

الف – C:\Windows\temp

ب – C:\Windows\config

ج – C:\Windows\accounts\config

د – C:\Windows\System32\config

۳۹ – اگر مهاجم از حمله XMAS Scan استفاده کند برای گذرگاه‌های بسته چه پاسخی را دریافت خواهد نمود؟

الف – RST

ب – RST/ACK

ج – No Response

د – FIN/ACK

۴۰ – چرا مهاجم پیش از اینکه برنامه آلوده خود را به سیستم هدف ارسال کند، آن را کدگذاری می‌نماید؟

الف – کدگذاری فایل هیچ منفعت اضافی ندارد.

ب – با کدگذاری فایل موردنظر، مهاجم در واقع آن را رمزنگاری می‌کند.

ج – با کدگذاری فایل با توجه به اینکه گذرگاه‌های مورد استفاده در آن مشخص نمی‌شوند، بنابراین می‌تواند از فایروال عبور کند.

د – با کدگذاری فایل موردنظر چون علائم مشخصه در آن (Signature) از بین می‌رود، بنابراین می‌تواند از سیستم‌های IDS/IPS عبور کند.

۴۱ – کدام رمز عبور ایمن‌تر می‌باشد؟

الف - 9Apple!

ب – pass123!!

ج – P@SSworD

---

[۱] Replay Ticket Granting Ticket

د – Keepyourpasswordsecuretoyourself

۴۲ – کدامیک از گزینه‌های زیر دستکاری سرویس دهنده DNS[۱] را شرح می‌دهد؟

الف – مهاجم مک آدرس‌ها را شنود می‌کند و سپس مک آدرس موردنظر خود را جایگزین مک آدرس سیستم هدف می‌کند.

ب – مهاجم IP آدرس خود را جایگزین IP آدرس سیستم هدف در نام دامنه می‌کند.

ج – مهاجم نام دامنه صحیح را با نام دامنه غیر واقعی جایگزین می‌کند.

د – مهاجم IP آدرس معتبر مترادف با نام دامنه موردنظر را با IP آدرس دلخواه خود جایگزین می‌کند.

۴۳ – کدامیک از گزینه‌های زیر امکان تقلب در گواهینامه‌های مورد استفاده در تائید هویت را به مهاجم می‌دهد؟

الف – Wireshark

ب – Ethercap

ج – Cain & Abel

د – Ncat

۴۴ – کدامیک از الگوریتم‌های رمزنگاری در پروتکل WEP مورد استفاده قرار می‌گیرد؟

الف – AES

ب – RC5

ج – MD5

د – RC4

۴۵ – در محل کار خود نشسته‌اید و توجه شما به فردی در پارکینگ که به همراه یک لپ تاپ که به آن یک آنتن بزرگ متصل شده است، جلب می‌شود، احتمالا این فرد در حال انجام چه کاری است؟

الف – پیدا کردن گذرواژه سیستم خود با استفاده از حدس و گمان[۲]

ب – حمله Wardriving

ج – حمله Warflying

د – برقراری ارتباط از طریق بلوتوث

---

[۱] DNS Poisoning

[۲] Brute Force Attack

۴۶ – به عنوان راهبر شبکه، IP آدرس شناخته شده‌ای را مشاهده می‌کنید که در حال برقراری تست ارتباط با شبکه خارجی می‌باشد(Ping). چه اتفاقی در حال رخ دادن است؟

الف – حمله Smurf

ب – دستکاری DNS

ج – حمله مرد میانی

د- آلوده‌سازی مسیر ارتباط شبکه با تروجان

۴۷ –کدامیک از گزینه‌های زیر بهترین توصیح برای حمله اختلال در سرویس است؟

الف – کامپیوتر هدف به ویروس آلوده شده است

ب – تنظیم نامناسب در سوئیچ باعث به‌وجود آمدن مسیر حلقه در شبکه شده است

ج – مهاجم گواهینامه تقلبی ارائه کرده است

د – مهاجم با برقراری ارتباط‌های نمی‌کاره در سرویس دهنده تا حد ممکن سعی کرده است تا همه حافظه در دسترس آن را اشغال کند.

۴۸ – در فایل رمزهای عبور ویندوز (SAM)، کدام مشخصه برای مهاجم می‌تواند نشان دهنده حساب کاربری راهبر باشد؟

الف – 500

ب – 1001

ج – ADM

د – ADMIN_500

۴۹ – کدامیک از مناطق اینترنتی زیر مربوط به شمال و جنوب آمریکا است؟

الف – RIPE

ب – AMERNIC

ج – LACNIC

د- ARIN

۵۰ – کدامیک از گزینه‌های زیر مربوط به آخرین اقدام در زمان اسکن کردن سیستم هدف است؟

الف – بررسی نقاط آسیب پذیری[۱]

ب – تشخیص سیستم‌های فعال

ج - پیدا کردن گذرگاه‌های باز

د – تشخیص سیستم‌عامل و سرویس دهندها

۵۱ – کدامیک از گزینه‌های زیر بهترین توضیح در مورد کد ۸ در بسته مربوط به پروتکل ICMP است؟

الف – دستگاه موردنظر فیلتر شده است

ب – مسیر شبکه صحیح نیست و یا یافت نشد

ج – درخواست برگشت پیام (Echo)

د- مقصد در دسترس نیست (Unreachable)

۵۲ – کدامیک از گزینه‌های زیر مربوط به محدوده گذرگاه‌های شناخته شده است؟

الف – 0 – 1023

ب – 0 – 255

ج – 1024-49151

د- 1 – 128

۵۳ – عبارت War Dialing به چه معنی است؟

الف – مهاجم حمله اختلال در سرویس را بر روی مودم انجام داده است

ب – مهاجم اقدام به شماره‌گیری کرده تا مودم‌های باز را شناسایی کند

ج – مهاجم از مودم به عنوان نقطه دسترسی قلابی (Twin Evil) استفاده کرده است

د- مهاجم در حال بررسی مودم‌های بسته است

۵۴ – با استفاده از کدامیک از پارامترهای زیر در فرمان Nmap می‌توان نوع سیستم‌عامل سیستم هدف را شناسایی کرد؟

الف - sO-

ب – sFRU-

---

[۱] Vunerabilities

ج - -sA

د – 0sX

۵۵ – با استفاده از کدام دستور در سطر فرمان سیستم‌عامل ویندوز، مهاجم می‌تواند همه سیستم‌های موجود در دامنه موردنظر را مشاهده کند؟

الف – netstat –R /domain

ب – net view /<domain_name>:domain

ج – net view /domain:<domain_name>

د- netsat /domain:<domain_name>

۵۶ – شما مسافری در ترمینال هواپیمایی می‌باشید. نگاهتان به مردی می‌افتد که در حال نگاه دزدکی به خانمی است که در حال کار کردن با تبلت خود است. این فرد احتمالا در حال انجام چه کاری است؟

الف – Wardriving

ب – نگاه از پشت سر (ShoulderSurfing)

ج – War Shouldering

د – Shoulder jacking

۵۷ – شما مهاجمی هستید که موفق شده‌اید یک آسیب‌پذیری از نوع تزریق SQL را در تارنمای هدف پیدا کنید. از کدامیک از کلید واژه‌های زیر برای دسترسی به بانک اطلاعات هدف در حمله تزریق SQL استفاده می‌کنید؟

الف – UNION

ب – ADD

ج –SELECT

د – JOIN

۵۸- کدامیک از گزینه‌ها به مفهوم تزریق کد در بخشی از داده‌ها در حافظه به منظور اجرای دستورات دلخواه اشاره می‌کند؟

الف – سرریزی بافر (Buffer Overflow)

ب – Crash

ج – سرریزی حافظه

د- سرریزی داده‌ها

۵۹ – کدامیک از فناوری‌های زیر می‌تواند باعث شود تا بین مسیر ارتباطی شبکه داخلی و خارجی قرار گیریم و ترافیک آن را رصد کنیم؟

الف – Proxy Server

ب – Firewall

ج – Router

د- Switch

۶۰ – به عنوان یک هکر، توانسته‌اید تا در یکی از سرویس‌های سیستم هدف آسیب‌پذیری پیدا کنید و به همین دلیل سرویس موردنظر را غیر فعال کرده‌اید. در این سرویس آسیب‌پذیری وجود دارد که می‌تواند به‌راحتی مورد نفوذ و سوء استفاده قرار گیرد. کدامیک از گزینه‌های زیر می‌تواند شرایط موجود را شرح دهد؟

الف – راهبر از به‌روزرسانی‌های نرم‌افزاری مناسب استفاده نکرده است

ب – سرویس دهنده به‌درستی تنظیم نشده است

ج – در شبکه با یک Honeypot سروکار دارید

د – فایروال به‌درستی تنظیم نشده است

۶۱ – فایل ثبت رخدادهایی که در آن آخرین فعالیت‌های انجام شده توسط آخرین کاربر در سیستم‌عامل لینوکس نگهداری می‌شود، کجا قرار دارد؟

الف - /var/log/user_log

ب- /var/log/messages

ج - /var/log/lastlog

د - /var/log/last_user

۶۲ – کدامیک از گذرگاه‌های زیر به‌طور پیش فرض برای پروتکل SSH مور د استفاده قرار می‌گیرد؟

الف – گذرگاه ۲۲

ب- گذرگاه ۲۱

ج – گذرگاه ۴۴۳

د- گذرگاه ۲۵

۶۳ – به عنوان متخصص تست نفوذ برای بررسی گروهی از سیستم‌های مشتری در نظر گرفته شده‌اید. به شما فهرستی از دارایی‌های مهم مشتری داده شده است. فهرستی از کنترل کننده‌های دامنه و فهرستی از دیسک‌های

مجازی اشتراکی داده شده است. به غیر از این موارد اطلاعات دیگری داده نشده است. تست نفوذ موردنظر از چه نوعی است؟

الف – تست کلاه سفید

ب - تست کلاه خاکستری

ج – تست جعبه خاکستری

د – تست کلاه قرمز

۶۴ – کدامیک از گزینه‌های زیر توضیحی مناسب برای عبارت Waewalking است؟

الف – تعیین مقدار TTL پس از عبور از یک فایروال می‌تواند گذرگاه باز را مشخص نماید.

ب – با استفاده از حمله اشباع Ping باعث بروز اختلال در سرویس در فایروال شده‌ایم

ج – اقدام به استفاده از روش ping sweet در فایروال نموده‌ایم.

د- تشخیص TTL پس از عبور از مسیریاب‌ها می‌تواند مشخص کننده سرویس دهنده‌ها و ایستگاه‌های فعال باشد.

۶۵ – کدامیک از ابزارهای زیر برای بررسی و برآورد آسیب‌پذیری در لایه ۳ مورد استفاده قرار می‌گیرد؟

الف – Cain & Abel

ب- John the ripper

ج –Ping-eater

د- Nmap

۶۶ – کدامیک از گذرگاه‌های زیر برای پروتکل IP مورد استفاده قرار می‌گیرند؟

الف – ۰ تا ۶۵۵۳۵

ب- هیچ گذرگاه

ج – ۵۳

د – ۸۰

۶۷ – کدامیک از دو پروتکل زیر مبتنی بر ارتباط نیستند (Cennectionless)؟

الف – IP/TCP

ب – IP/FTP

ج – IP/UDP

د- TCP/UDP

۶۸ – به فردی که سیستمی را با مجوز مورد بررسی قرار می‌دهد، چه می‌گویند؟

الف – کلاه سفید

ب- کلاه خاکستری

ج – کلاه سیاه

د- کلاه قرمز

۶۹ – مدیریت به‌روزرسانی نرم‌افزاری (Patch Management) کدام است؟

الف- فراهم کردن به‌روزرسانی‌ها به محض در دسترس بودن

ب- کنترل به‌روزرسانی‌های نرم‌افزاری پیش استفاده از آن در محیط واقعی

ج – فراهم کردن به‌روزرسانی‌های نرم‌افزاری در پایان هر ماه

د- تشخیص نقاط ضعف در شبکه کنونی و یافتن به‌روزرسانی‌های نرم‌افزاری مناسب برای حذف آنها

۷۰ – در کدامیک از لایه‌های OSI پروتکل FTP مورد استفاده قرار می‌گیرد؟

الف – دیدگاه (Session)

ب- کاربرد (Application)

ج – شبکه (Network)

د – انتقال (Transport)

۷۱ – در حمله heart bleed از کدام آسیب‌پذیری استفاده می‌شود؟

الف – Buffer overflow

ب- Man In the Middle

ج –Fraggle attack

د – Smurf attack

۷۲ – با استفاده از کدامیک از پارامترها در فرمان Nmap می‌توان فناوری اسکن XMAS را انجام داد؟

الف - sX-

ب - sS-

ج –xS

د - -sT

۷۳ – کدامیک از گزینه‌های زیر توضیح مناسبی برای واژه‌های fingerprint scan است؟

الف – جست‌وجوی آسیب‌پذیری‌ها

ب – استفاده از پارامتر sX– در فرمان Nmap

ج – تطابق خصوصیات از مرحله اسکن تا بانک اطلاعاتی با استفاده از Nmap

د- کنترل باز بودن گذرگاه‌های باز با استفاده از فناوری Firewalking

۷۴ – کدامیک از گزینه‌ها مربوط به حمله سمت کاربر بوده و هدف آن نرم‌افزارهای تحت وب است؟

الف – تزریق SQL

ب- تزریق بدافزار بین تارنما (Cross-site Malware injection)

ج – تزریق کد بین تارنما (XSS)

د- کدنویسی SQL

۷۵ – کدام گذرگاه زیر توسط پروتکل DNS مورد استفاده قرار می‌گیرد؟

الف – ۸۰

ب – ۸۰۸۰

ج – ۵۳

د – ۲۵

۷۶ – در لینوکس، در کدام فایل، اطلاعاتی همچون نام کامل کاربر و شماره تلفن و اطلاعات محل کار را می‌توان یافت؟

الف – shadow file

ب- passwd file

ج – userinfo file

د- useraccount file

۷۷ –با استفاده از نرم‌افزار تحلیل‌گر بسته‌ها در کدام قسمت بسته می‌بایست به دنبال فیلد FIN جست‌وجو کرد؟

الف – TCP – HREADER

ب – TCP – Packet

ج – UDP - Flags

د - TCP – Flags

۷۸ – در حمله fraggle از کدام نوع بسته برای اختلال در خدمات استفاده می‌شود؟

الف – TCP

ب – IP

ج – ICMP

د – UDP

۷۹ – کدام مقدار دستور العمل برای فراخوانی فرمان NOP (No Operation Procedure) استفاده می‌شود؟

الف – 0x99

ب – 0x91

ج -0xGH

د – 0x90

۸۰ – از کدام پروتکل برای به‌دست آوردن اطلاعات از سرویس دهنده استفاده می‌شود (Banner Grabbing)؟

الف – FTP

ب – IRC

ج – DNS

د- Telnet

۸۱ – کدام‌یک از عملکردهای زیر در پروتکل IPv6 مورد استفاده قرار نمی‌گیرد؟

الف – Multicast

ب – Anycast

ج – Unicast

د – Broadcast

۸۲ – وقتی‌که سرویس دهنده‌ای را با تنظیمات مشخص و به‌صورت مرحله به مرحله نصب می‌کنید، در واقع از چه چیزی استفاده می‌کنید؟