به نام خدا

۱- هک قانونمند را تعریف نمائید؟ ص۴

هک قانونمند نوعی هک است که با مجوز سازمانی و برای افزایش امنیت انجام می‌گیرد.

۲- اکسپلویت را تعریف کرده و انواع آنرا نام ببرید. ص۴

اکسپلویت (exploit) قطعه‌ای از نرم افزار، ابزار یا تکنیک است که مزایای آسیب پذیریها را دارد و می‌تواند منجر به ایجاد دسترسی، از دست دادن یکپارچگی، یا حمله DoS بر روی یک سیستم کامپیوتری شود.

اکسپلویت به دو دسته : Remote Exploit و Local Exploit تقسیم می گردد.

۳- انواع حملات را نام برده و تعریف نمائید؟ ص ۶

حملات می‌توانند به دو دسته پسیو و اکتیو تقسیم شوند. حملات اکتیو، سیستم یا شبکه را تغییر می‌دهند ولی حملات پسیو، به دنبال جمع ها آوری اطلاعات از سیستم هستند. حملات اکتیو، بر روی دسترسی پذیری، یکپارچگی، و صحت داده‌ها موثر هستند در حالیکه حملات پسیو، محرمانگی را مختل می‌کنند.

۴- انواع هکرها را نام برده و مختصرا توضیح دهید؟ ص ۹

هکرها در سه دسته قرار می‌گیرند: کلاه سفید، کلاه سیاه و کلاه خاکستری.

کلاه سفیدها: اینها افرادی خوبی هستند که از مهارت هک‌شان برای اهداف دفاعی استفاده می‌کنند . هکرهای قانونمند معمولا در دسته کلاه سفیدها قرار می‌گیرند.

کلاه سیاه ها: اینها افراد بدی هستند. هکرهای شرور یا crackerها از مهارتشان برای اهداف غیر قانونی استفاده می‌کنند.

کلاه خاکستری ها: اینها هکرهایی هستند که بسته به شرایط، ممکن است بصورت دفاعی یا مخرب عمل کنند. (حزب باد)

۵- انواع تست نفوذ را نام برده و تعریف نمائید؟ ص ۱۵

الف) تست بدون دانش (جعبه سیاه)

تستی که بدون هیچ دانشی صورت می‌گیرد با نام تست جعبه سیاه (Black box) شناخته می‌شود. تست جعبه سیاه، یک هکر خارجی را شبیه سازی می‌کند که هیچ دانشی ها در مورد شبکه یا سیستم هدف ندارد.

ب) تست با دانش کامل (جعبه سفید)

تست جعبه سفید، رویکرد متضاد در برابر تست جعبه سیاه دارد. در این شکل از تست امنیتی، فرض می‌شود که تست کننده امنیتی، دانش کامل از شبکه، سیستم و زیرساخت دارد.

ج) تست با دانش جزئی (جعبه خاکستری)

در این تست، هدف این است که بدانیم کارمندان چه چیزی را می‌توانند به دست آورند. این نوع تست، ممکن است برای سازمان ها بسیار مفید باشد برای اینکه بسیاری از حملات توسط کارمندان داخل سازمان شروع می‌شوند .

۶- مهندسی اجتماعی را تعریف نمائید. ص ۳۱

مهندسی اجتماعی، روشی غیر فنی برای شکستن امنیت سیستم یا شبکه است. فرآیند گول زدن کاربران یک سیستم و تحریک آنها برای دادن اطلاعاتی که برای دور زدن مکانیزم های امنیتی استفاده می‌شود را مهندسی اجتماعی می‌گویند .

۷- متدلوژی اسکن چیست؟ مراحل آن را نام ببرید. ص ۳۹

فرآیندی است که هکر، شبکه را اسکن می‌کند. این متدلوژی، هکر را مطمئن می‌سازد که همه اطلاعات‌لازم برای انجام حمله، جمع‌آوری شده است:

۱.بررسی سیستم های فعال/۲.بررسی پورت های باز/۳.شناسایی سرویس ها/۴.شناسایی سیستم عامل/۵.ترسیم نقشه شبکه بر اساس سیستمهای آسیب پذیر/۶.اسکن آسیب پذیری/۷.آماده سازی پروکسی ها/۸.حمله!

۸- Rootkit را تعریف نمائید. ص ۷۹

rootkit، نوعی برنامه است که اغلب برای مخفی کردن برنامه‌ها روی سیستم قربانی به کار می‌رود. Rootkitها شامل backdoor هستند تا به هکر کمک کند بطور متوالی و راحت به سیستم دسترسی پیدا کند.

۹- انواع روش های استراق سمع اکتیو را نام برده و توضیح دهید. ص ۱۱۵

دو روش برای انجام استراق سمع اکتیو وجود دارد: ARP spoofing و flooding .

ARP spoofing، گرفتن MAC address مربوط به gateway شبکه و در نتیجه دریافت همه ترافیکی که به مقصد gateway می‌روند به سیستمی است که sniffer دارد .

هکر می‌تواند سوئیچ را با سرازیری ترافیک زیاد ،flood کند تا عملکرد آن به عنو ان سوئیچ مختل شود و مثل هاب، ترافیک را به تمام پورت‌های خود ارسال کند. این نوع حملات به سیستمی که sniffer دارد اجازه می‌دهد که تمام ترافیک روی شبکه را بدست‌آورد.

۱۰- تکنیک DNS Poisoning را تعریف نمائید. ص ۱۱۶

هکر، آدرس‌های IP ورودی‌های DNS را برای یک وب سایت مسموم می‌کند و آن را با آدرس IP سروری‌که هکر کنترل می کند جایگزین می‌کند. سپس ورودی‌های جعلی برای فایل‌هایی که روی این سرور وجود دارند می‌سازد که با آنهایی که در سرور هدف وجود دارند، مشابه باشد.

۱۱- حمله DoS و انواع آن را تعریف نمائید. ص ۱۲۴

در حملات DoS هدف این است که اجازه سرویس دهی به کاربران قانونی گرفته شود. دو نوع حمله DoS وجود دارد : حملات DoS می‌تواند توسط یک سیستم به یک سیستم دیگر (DoS ساده) یا توسط چندین سیستم به یک سیستم انجام شود (DDoS).

۱۲- انواع آسیب پذیری‌های وب سرور را نام ببرید. ص ۱۴۳

وب‌سرورها نیز مثل سیستم‌های دیگر می‌توانند مورد حمله هکر قرار گیرند. برخی از مهم‌ترین آسیب پذیری‌های وب سرورها عبارتند از :

- پیکربندی نادرست نرم افزار وب سرور (IIS،Apache و ...)
- مشکلات سیستم عامل یا نرم افزارها یا خطا در کد برنامه
- آسیب پذیر بودن نصب های پیش فرض سیستم عامل یا نرم افزار وب سرور، و عدم به روز رسانی آنها
- نداشتن فرآیندها و سیاست‌های امنیتی صحیح

۱۳- عبارات Hotfix و Service Pack را تعریف نمائید. ص ۱۴۷

hotfix، کدی است که ایرادی را در یک محصول برطرف می‌کند. ممکن است کاربران از طریق ایمیل یا وب سایت فروشنده از آن مطلع شوند. بعضی اوقات این hotfix ها ترکیب شده و بصورت پک توزیع می‌شوند که service pack نامیده می‌شود.

۱۴- SQL Injection چیست؟ ص ۱۶۵

نوعی سوء استفاده امنیتی است که هکر از طریق کادرهای فرم (Input Box) کدهای SQL را وارد می کند تا به منابع دسترسی پیدا نموده و یا داده ها را تغییر دهد.

۱۵- ضرورت امنیت فیزیکی چیست؟ ص ۱۹۲

به همان دلیل که نیاز به انواع دیگر امنیت دارید (فنی یا عملیاتی) به همان دلیل هم نیاز به معیارهای امنیت فیزیکی دارید و آن جلوگیری از هکرها برای دسترسی به شبکه و اطلاعات شماست . در صورت وجود ضعف‌های معیارهای امنیت فیزیکی، هکر می‌تواند به آسانی دسترسی پیدا کند. علاوه بر این، داده ها می‌توانند به دلایل طبیعی از بین روند یا خراب شوند، بنابراین، مدیران ریسک زمانیکه برنامه ای برای امنیت طراحی می‌کنند، مشکلات طبیعی را نیز در نظر بگیرند.

۱۶- چه کسی مسئول امنیت فیزیکی است؟ ص ۱۹۳

در یک سازمان، تمام افراد، مسئول اجرای سیاست‌های امنیت فیزیکی هستند. مامور امنیت فیزیکی سازمان، مسئول ایجاد استاندارد امنیت فیزیکی و پیاده سازی معیارهای امنیت فیزیکی است .

۱۷- موارد لازم جهت امنیت فیزیکی سرورها را نام ببرید. ص ۱۹۵

مهم‌ترین عامل در هر شبکه، سرور است و باید دارای امنیت بالا باشد. اقدامات زیر برای این منظور می‌تواند صورت گیرد:

- o برای ورود به اتاق سرور افراد باید احراز هویت شوند و تنها افراد مجاز حق ورود را داشته باشند
- o درب رک قفل باشد
- o راه اندازی (boot) سرور از طریق floppy و CD-ROM مجاز نباشد و درایوهای مربوط به آنها قفل باشد
- o سیستم عامل DOS باید از آنها پاک شود تا مهاجم نتواند سرور را بصورت راه دور و از طریق DOS راه اندازی کند.

۱۸- انواع رمزنگاری را نام برده و توضیح دهید؟ ص ۲۲۴

دو نوع اصلی رمزگذاری، رمزگذاری کلید متقارن و نامتقارن است.

رمزگذاری کلید متقارن، به این معنی است که برای رمزگذاری و رمزگشایی داده‌ها، از یک کلید استفاده می‌شود. ایراد این روش این است که روشی مطمئن برای به اشتراک گذاشتن کلید بین چندین سیستم وجود ندارد.

رمز گذاری کلید نامتقارن، برای پوشش ضعف مدیریت و توزیع کلید متقارن بوجود آمد . در این روش، از دو کلید یکی برای رمزگذاری و دیگری برای رمزگشایی استفاده می‌شود.

۱۹- SSH چیست؟ ص ۲۲۶

SSH برای ورود ، اجرای دستورات، و انتقال فایل به سیستم دیگر در شبکه، تونل رمز شده ایجاد می‌کند که جایگزین مطمئنی برای telnet محسوب می‌شود. SSH2 نیز نسخه امن‌تر SSH است که شامل SFTP است.

۲۰- **مراحل تست نفوذ را نام ببرید؟** ص ۲۳۱

تست نفوذ شامل سه مرحله است :

- مرحله پیش از حمله (pre-attack)
- مرحله حمله (attack)
- مرحله پس از حمله (post-attack)

۲۱- چارچوب قانونی تست نفوذ چیست؟ موارد آنرا نام ببرید. ص ۲۳۴

شخصی که تست نفوذ را انجام می‌دهد، باید از مسائل قانونی هک یک شبکه آگاه باشد حتی هک قانونمند.

مستنداتی که یک هکر قانونمند با مشتری برای انجام تست نفوذ امضا می‌کند، به شرح زیر هستند :

- محدوده کاری، برای تعیین اینکه چه چیزی باید تست شود
- توافق نامه عدم افشای اطلاعات (NDA)، در شرایطی که تست کننده، اطلاعات محرمانه را ببیند
- تعهد، به اینکه هکر قانونمند، از انجام عملیات خرابکارانه خودداری خواهد کرد

۲۲- پنج مورد از ابزارهای خودکار تست نفوذ را نام ببرید. ص ۲۳۴

SARA / X-Scan / IIS Internet Scanner / Core Impact / Retina / GFI Languard / Nessus

۲۳- تکنیک های شکستن Password را نام ببرید. ص ۶۲

پسوردها می‌توانند بصورت دستی شکسته شوند و یا اینکه با استفاده از ابزارهایی از قبیل روش دیکشنری یا brute-force، بصورت اتوماتیک شکسته شوند . یک روش موثر برای شکستن پسورد، دسترسی به فایل حاوی پسوردها در سیستم است که بصورت Hash شده نگهداری می شود.

۲۴-عناصر پایه ای امنیت را نام ببرید؟ ص ۱۱

امنیت شامل سه عنصر پایه‌ای است :

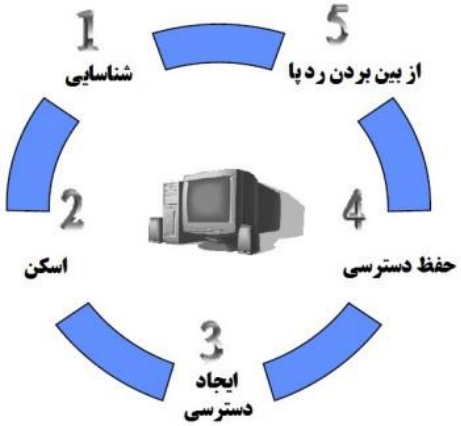
- محرمانگی (Confidentiality)
- یکپارچگی (Integrity)
- در دسترس بودن (Availability)

۲۵- Hacktivism چیست؟ ص ۹

Hacktivism، دلیل و انگیزه هک است . هکرها، معمولا انگیزه‌های اجتماعی و سیاسی دارند. بسیاری از هکرها، در فعالیت‌هایی چون deface کردن وب سایت، نوشتن ویروس، DoS، یا حملات مخرب دیگر شرکت می‌کنند. معمولا انگیزه هکرها (hacktivism) ، آژانس های دولتی و گروه‌های سیاسی هستند .

۲۶-پنج مرحله مختلف هک قانونمند را نام ببرید؟ ص ۷

هکر قانونمند، مراحلی را که هکر شرور انجام می‌دهد را انجام می‌دهد. شکل زیر، پنج مرحله‌ای که هکرها برای هک کردن سیستم ها انجام می دهند را توضیح می‌دهد:



ستاد جمع آوری سوالات