۱- مثلث امنیت یا CIA چیست؟

مثلث امنیت از سه قسمت محرمانگی یا **Confidentiality** ، یکپارچه سازی یا **Integrity** و در دسترس بودن یا **Availability** تشکیل شده است و جهت تامین امنیت داده ها در شبکه مورد استفاده قرار می گیرد که شرح این سه اصل به صورت زیر می باشد:

Confidentiality یا محرمانگی

به اقداماتی میگویند که برای اطمینان از محرمانه بودن اطلاعات انجام می شود تا از دسترسی افراد متفرقه به اطلاعات حساس جلوگیری شود. حتی گاهی نیاز است که دسترسی ها برای افراد مجاز نیز محدود شوند. همچنین باید داده ها بر اساس میزان و نوع آسیب هایی که ممکن است در صورت دسترسی افراد غیر مجاز به آن ها وارد شود دسته بندی شوند. استفاده از روش های رمزنگاری مختلف ، سخت افزارهای کنترل کننده مانند فایروال ها از روش های محرمانه سازی داده می باشند.

Integrity یا یکپارچه سازی

Integrityدقت و اطمینان در ارسال بسته ها است. داده ها نباید در انتقال تغییر کنند و باید اطمینان پیدا کنیم که داده ها توسط افراد غیر مجاز قابل تغییر نیست. این تغییرات صرفا از سمت انسان ها نیست ما باید اطمینان پیدا کنیم که حتی نویز های مغناطیسی باعث تغییر اطلاعات نمیشود. یک راه برای تآمین **Integrity**استفاده از مفهموی به نام **Checksum**است.

Availability یا در دسترس بودن

Availabilityاطمینان از در دسترس بودن است. ارائه پهنای باند ارتباطی مناسب و جلوگیری از وقوع اتفاقاتی که باعث شود سرور از دسترس خارج شود کار هایی است که حوزه این راس از مثلث خواهد بود. استفاده از **Redundancy**یا همان افزونگی، **Failover**و یا استفاده از **RAID**ها باعث میشود در هنگام بروز مشکلات، خسارت کاهش پیدا کنند.

۲- حمله روز صفر چیست؟ و روش های موثر جهت جلوگیر از آسیب توسط حمله روز صفر؟

حمله روز صفر یا **Zero Day Attack** یک حمله اینترنتی است که آسیب پذیری های نرم افزاری و سخت افزاری را هدف قرار می دهد. این حملات به گونه ای هستند که برای فروشندگان نرم افزارها و سخت افزارها یا آنتی ویروس ها ناشناخته می باشند. علت نامگذاری حمله روز صفر این است که قبل از اینکه هدف حمله از وجود آسیب پذیری آگاه باشد، حمله رخ می‌دهد. مهاجم، بدافزار را پیش از آنکه توسعه دهنده یا شرکت تولیدکننده نرم‌افزار فرصتی برای ایجاد یک پچ به منظور رفع آسیب پذیری داشته باشد، منتشر می‌کند. حملات روز صفر معمولاً بین زمانی که آسیب‌پذیری برای اولین بار پیدا می‌شود تا هنگامی که توسعه‌دهندگان برنامه ، راه‌حل لازم را برای مقابله با سوءاستفاده منتشر می‌کنند، رخ می‌دهند. این بازه زمانی معمولاً به عنوان پنجره آسیب پذیری (vulnerability window)نامیده می شود.

نشانی : تهران، خیابان شهید بهشتی، خیابان شهید صابونچی، نبش کوچه چهارم، شماره۲۰، ساختمان۳۴، طبقه۳، واحد۱۶ کدپستی: ۱۵۳۳۶۴۴۸۴۳
پست الکترونیکی: ensculine@gmail.com و Info@enscu.ir اینستاگرام: @enscunion سایت: www.enscu.ir
تلفن: ۸۸۷۳۳۱۸۰- ۸۸۷۳۱۸۰۹- ۸۸۷۳۲۴۵۰ تلفکس : ۸۸۷۳۱۷۶۱ تلفن‌همراه/شبکه‌های اجتماعی: ۰۹۱۲۹۵۸۴۳۵۰

جهت جلوگیری از این حمله می توان شرایط زیر را در سامانه اعمال نمود:

- ✓ کنترل دسترسی ها و محدودیت‌های مختلف از جمله شبکه‌های محلی مجازیLAN ، فایروال‌ها می‌توانند در برابر حملات روز صفر محافظت کنند.
- ✓ محدود کردن امتیازات برای حساب های کاربری این می تواند تأثیر هر گونه حملات احتمالی را کاهش دهد.
- ✓ **Windows Defender Exploit Guard:** یک ابزار امنیتی موجود در ویندوز ۲۰۱۰، که دارای چندین قابلیت است که می تواند به طور موثر در برابر حملات روز صفر ، سیستم را محافظت کند. این ابزار امنیتی می تواند اولین خط دفاعی در برابر حملات روز صفر باشد ، که نقاط انتهایی ویندوز را هدف قرار می دهند.
- ✓ مدیریت پچ : ایجاد یک فرآیند رسمی و پیاده‌سازی ابزارهای خودکار، می‌تواند به سازمان‌ها برای شناسایی سیستم‌هایی که نیاز به پچ دارند، کمک کنند، پچها را به‌دست آورند و به سرعت آن‌ها را مستقر کنند، قبل از اینکه مهاجمان بتوانند با یک حمله روز صفر حمله کنند.
- ✓ برنامه واکنش به حادثه : داشتن یک برنامه خاص متمرکز بر حملات روز صفر می تواند سردرگمی را کاهش دهد و شانس شناسایی و کاهش آسیب ناشی از حملات روز صفر را افزایش دهد.

۳- *حمله بروت فورس Brute forceچیست؟*

حمله **Brute Force** یکی از روشهای هکرها برای یافتن رمزهای عبور میباشد. معمولا این کار توسط نرم افزار های مخصوصی انجام میشود. در این حمله هکرها هیچ اقدامی برای رمزگشایی پسورد نمی کنند؛ بلکه با استفاده از نرم افزارهایی سعی در حدس زدن پسورد و بررسی تمام حالات ممکن برای یافتن پسورد صحیح مینماید. در صورتی که رمز پیچیده و طولانی باشد، این کار بسیار زمانبر خواهد شد. این نوع حملات به دو فاکتور زمان زیاد و قدرت پردازش بالا احتیاج دارد و خوشبختانه تا حدودی این دو مورد بازده هکرها را پایین آورده است.

قدرت پردازش بالا :فرایند رمزگشایی، عملیات محاسباتی پیچیده ای هستند و برای انجام آن، نیاز به قدرت بالای سیستم نرم افزاری کامپیوتر می باشد. از آنجا که کامپیوتر هایی با سخت افزار های بهتر و در نتیجه سرعت پردازش بیشتر روانه بازار شده اند، در نهایت این عملیات و حمله ها سریعتر و موثرتر واقع شده اند.

زمان زیاد :در این نوع حملات همه حالت های ممکن پسورد بصورت ترکیبی از کاراکتر ها شامل جایگشت های مختلف اعداد، حروف کوچک، بزرگ و کاراکترهای خاص بررسی میشود. این بررسی معمولا با یک کاراکتر شروع شده و پس از بررسی تمام حالات یک کاراکتری، بررسی تمامی موارد دو کاراکتری، سه کاراکتری و... شروع شده و این روند تا زمان کشف پسورد مربوطه، ادامه خواهد یافت. از نظر تئوری این روش در نهایت به جواب خواهد رسید، بطور مثال اگر پسورد مربوطه ۶ رقمی ۱۲۳۴۵۶ باشد، به راحتی طی زمان نسبتا کوتاهتری، توسط این روش قابل حدس زدن خواهد بود. اما تصور کنید که رمز مربوطه، بسیار طولانی و پیچیده باشد؛ در اینصورت این فرایند بسیار زمان بر و طولانی خواهد شد. این حملات می توانند به صورت آفلاین یا آنلاین صورت پذیرند.

۴- بهترین دفاع در برابر حملات brute force login کدام است؟

سه اقدام اساسی می توان جهت دفاع در برابر حمله **brute force login** انجام داد. در آغاز کار میتوان از قفل حساب کاربری **account lockout**بهره برد. حسابهای متخلف قفل می شوند تا موقعی که مدیر سیستم تصمیم به باز کردن دوباره آن بگیرد. در مرحله بعدی تاخیر در ورود قرار می گیرد. در اینجا، پس از انجام چند سعی ناموفق جهت ورود به حساب، حساب برای مدت معینی قفل می گردد. در انتها، آزمون پاسخ به چالش وجود دارد، که به شیوه هوشمندانه پرسش های اتوماتیک را در صفحه ورود به سیستم انجام می دهد.

۵- تنظیم امنیتی روی سوئیچ های دسترسی برای امن تر کردن سیستم نظارت تصویری را نام ببرید

- ✓ استفاده از پسوردهای امن: تا جای ممکن در روی تمامی سوئیچ ها و روترهای خود از دستور **enable secret** استفاده کرده و بدین ترتیب پسورد قدرتمندی را به محیط **privilege** دستگاه اختصاص دهید. همچنین اگر می توانید از ویژگی **AAA** برای بررسی هویت کلاینت هایی که از سوئیچ ها و یا روترها استفاده می نمایند استفاده کنید. در انتها باید از دستور **service password encryption**استفاده کنید تا تمامی پسوردهای نوشته شده در روی سوئیچ یا روتر از دید افراد مخفی شوند.
- ✓ تامین امنیت سرویس وب : در صورتی که از محیط وب برای مشاهده و مدیریت دستگاه استفاده نمی کنید، اقدام به غیرفعال کردن سرویس وب نمایید. اما در شرایطی که تمایل و یا نیاز به استفاده از محیط وب داشته باشید، سعی در بهره گیری از سرویس امن تر آن، یعنی **HTTPs** نمایید.پروتکل **HTTP** دارای نقاط ضعفی می باشد که امکان سوء استفاده از آن را فراهم ساخته است.
- ✓ امنیت پورت کنسول دستگاه را فراهم کنید: همیشه به یاد داشته باشید که اولین قدم در تامین امنیت دستگاه، محافظت آن از دسترسی فیزیکی افراد است. بنابراین سعی کنید تا پسورد قدرتمندی را بر روی پورت کنسول دستگاه اعمال کنید.
- ✓ امنیت اتصالات **telnet** یا همون پورت های **VTY** را تامین کنید: برای دسترسی به طریق **telnet** نیز باید پسوردی بر روی تمامی پورت های **VTY** دستگاه اعمال شود. همچنین باید آدرسهای **IP** افرادی که قادر به دسترسی به دستگاه از طریق **telnet**یا **SSH** می باشند را نیز محدود نمائید. برای این منظور می توان از یک **ACL** ساده استفاده کرد.
- ✓ تا جای ممکن از **SSH** استفاده کنید: اتصال **telnet** به راحتی قابل پیکربندی و استفاده است. اما این پروتکل امن نبوده و تمامی اطلاعاتی که از این طریق منتقل می شوند به صورت متون ساده فرستاده خواهند شد. بنابراین افراد هکر می توانند با شکار ترافیک انتقالی پی به نام های کاربری و پسوردها ببرند. برای برطرف کردن این خطر می توان از **SSH** به جای **telnet** استفاده کرد . این پروتکل از یک متد امنیتی بسیار قوی برای مخفی ساختن اطلاعات انتقالی استفاده می کند.
- ✓ تامین امنیت پورت های آزاد سوئیچ: تمامی پورتهای آزاد سوئیچ را غیرفعال کنید تا هیچکس بدون آگاهی شما قادر به متصل کردن دستگاهی دیگر به شبکه نباشد . علاوه بر این تمامی پورتهای آزاد سوئیچ را با استفاده از دستور switch port mode accessدر وضعیت **access** قرار دهید تا امکان ایجاد اتوماتیک اتصال **trunk** توسط افراد هکر در روی پورت های مزبور غیرممکن باشد. همچنین برای افزایش امنیت می توانید **VLAN** جدید ایجاد کرده و تمامی پورت های آزاد دستگاه

نشانی : تهران، خیابان شهید بهشتی، خیابان شهید صابونچی، نبش کوچه چهارم، شماره۲۰، ساختمان۳۴، طبقه۳، واحد۱۶ کدپستی: ۱۵۳۳۶۴۴۸۴۳
پست الکترونیکی: ensculine@gmail.com و Info@enscu.ir اینستاگرام: @enscunion سایت: www.enscu.ir
تلفن: ۸۸۷۳۳۱۸۰- ۸۸۷۳۱۸۰۹- ۸۸۷۳۲۴۵۰ تلفکس : ۸۸۷۳۱۷۶۱ تلفن‌همراه/شبکه‌های اجتماعی: ۰۹۱۲۹۵۸۴۳۵۰

را عضوی از این VLAN نمایید. در چنین وضعیتی حتی اگر فردی قادر به دسترسی به این پورت باشد نیز تنها به همان VLANدسترسی پیدا خواهد کرد.

- ✓ امنیت پروتکل STP را تامین کنید: افراد هکر می توانند دستگاه خود را به یکی از پورت های سوئیچ وصل کرده و پیامهای BPDUخود را ایجاد و ارسال نمایند. در این صورت می توانید از ویژگی BPDU Guard استفاده کنید تا پورتهای accessدستگاه در هنگام دریافت پیامهای BPDU غیرفعال گردند.
- ✓ امنیت پروتکل CDP را فراهم کنید: به صورت پیش فرض تمامی پورتهای سوئیچ در هر ۶۰ ثانیه یک بار اقدام به ارسال پیامهای (Cisco Discovery Protocol) CDP می کنند. با وجود آنکه این پروتکل می تواند در بسیاری از مواقع مفید باشد، اما برخی از افراد می توانند از اطلاعات منتشر شده توسط این پروتکل سوء استفاده کنند. بنابراین این پروتکل باید بر روی پورتهایی فعال باشد که به یک سوئیچ مطمئن دیگر متصل هستند. در این بین اگر پورتی از سوئیچ به تلفن های IP سیسکو متصل باشد، فعال بودن CDP در روی آن بسیار مفید خواهد بود .

۶- پروتکل SSL چیست و چگونه ایمن سازی ارتباطات را فراهم می سازد؟

این واژه مخفف Secure Socket Layer و به معنای لایه اتصال امن می باشد. به طور کلی این فناوری برای ایمن نگه داشتن اتصال به اینترنت و محافظت از هرگونه اطلاعات حساس است که بین دو سیستم ارسال می شود و از خواندن مجرمان و تغییر هرگونه اطلاعات منتقل شده توسط هکرها، از جمله جزئیات شخصی احتمالی جلوگیری می کند. این پروتکل باعث ایجاد ارتباط امن بین کاربر و سرور می‌شود و از لو رفتن اطلاعاتی همچون رمز عبور، اطلاعات بانکی و سایر اطلاعات محرمانه جلوگیری می‌کند. این فرآیند شامل سه مرحله برقراری ارتباط، تایید هویت و رمزنگاری داده‌ها است که با دریافت گواهی SSL این فرآیند آغاز می‌شود.

۷- پن تست یا تست نفوذ چیست؟

تست نفوذ (Penetration Testing) به فرآیند هک اخلاقی گفته می‌شود که شامل ارزیابی برنامه یا زیرساخت یک سازمان در برابر انواع مختلف تهدیدات می‌شود. این تست کمک می‌کند تا از آسیب پذیری‌های مختلف سیستم جلوگیری شود و دلایل احتمالی این آسیب پذیری‌ها مانند تنظیمات نادرست و طراحی ضعیف تشخیص داده شود. این تست در لایه های فیزیکی ، شبکه ، برنامه و وب انجام می پذیرد تا ضرایب نفوذ پذیری به سیستم مشخص گردد.

۸- پیامدهای احتمالی حمله به شبکه شامل چه مواردی است؟

- ✓ از دست دادن یا نقض امنیت اطلاعات حساس که برای بقا و موفقیت یک شرکت ضروری می باشد.
- ✓ از اعتبار و اعتماد بین مشتریان کاسته می شود.
- ✓ ارزش سهامداران کاهش می یابد.
- ✓ از ارزش نام تجاری کم می شود.
- ✓ سود شرکت کاهش می یابد.

۹- احراز هویت با استفاده از پروتکل kerberos را شرح دهید؟

روش کار در الگوریتم کربروس به این صورت است که وقتی کاربری به یک شبکه **Kerberos** وارد می شود، یک پیغام درخواست به سرور مربوط به نام و کلمه عبور حساب خود می فرستد. آن سرور با یک **TGT** که بر مبنای کلمه عبور سرویس گیرنده رمزنگاری شده است جواب می دهد. محض دریافت **TGT** از کاربر درخواست می شود که کلمه عبور خود را وارد کند و سپس از آن کلمه عبور برای رمزگشایی **TGT** استفاده می کند. چون در واقع فقط یک کاربر باید دارای کلمه عبور درست باشد، این روند به عنوان احراز هویت عمل می کند. اگر رمزگشایی **TGT** با موفقیت انجام شود، کاربر می تواند یک درخواست، حاوی یک کپی رمزنگاری شده از **TGT**به یک سرور**TGS** ، که الزاماً همان سرور احراز هویت اول نمی باشد، بفرستد و به منابع شبکه دسترسی پیدا کند. سرور **TGS**بعد از رمزگشایی **TGT** و تشخیص وضعیت کاربر یک بلیط سرور **(Server Ticket)** ایجاد می کند و به برای او می فرستد. این بلیط، کاربر را قادر می سازد برای مدت زمان محدودی به یک سرور مشخص دسترسی داشته باشد. این بلیط همچنین حاوی یک کلید نشست **(Session key)** می باشد که کاربر و سرور از آن می توانند برای رمزنگاری داده های در حال انتقال بین خود استفاده کنند. کاربر در صورت نیاز به یک منبع، بلیط سرور را به آن سرور می فرستد. سرور بعد از رمزگشایی آن بلیط، امکان دستیابی به منبع مورد نظر را فراهم می کند.

۱۰- تفاوت تهدید حمله و خسارت را در امنیت شبکه و اطلاعات بیان کنید.

تهدید امنیتی :هر عاملی که به طور بالقوه بتواند منجر به وقوع رخدادی خطرناک بشود یک تهدید امنیتی بشمار می آید.

حمله :هرگاه تهدیدی از قوه به فعل درآید اصطلاحاً یک حمله رخ داده است خواه آن حمله موجب خسارت به منابع بشود یا خواه یک تلاش نافرجام باشد.

تخریب یا خسارت :حمله ای که در اثر آن منابع شبکه از بین برود یا دست کاری شود یا اطلاعات و داده های محرمانه افشا شود و یا حریم خصوصی افراد مورد تعرض قرار گیرد یا به کمک جعل هویت و فریب کاری از خدمات معمول به شبکه سوء استفاده شود اصطلاحاً حمله به مرحله آسیب رسیده است.

۱۱- حملات فعال و غیرفعال شبکه را توضیح دهید.

حملات غیر فعال یا Passive: این نوع حملات شامل آنالیز ترافیک شبکه، شنود ارتباطات حفاظت نشده، رمزگشایی ترافیک های رمز شده ضعیف، و بدست آوردن اطلاعات معتبری همچون رمز عبور می باشد .رهگیری غیرفعال عملیات شبکه، می تواند اطلاعات لازم در خصوص عملیات قریب الوقوعی که قرار است در شبکه اتفاق افتند را به مهاجمان بدهد (مثلا قرار است از مسیر فوق در آینده محموله ای ارزشمند عبور داده شود). پیامدهای این نوع حملات، آشکارشدن اطلاعات و یا فایل های اطلاعاتی برای یک مهاجم، بدون رضایت و آگاهی کاربر خواهد بود.

حملات فعال یا Active: این نوع حملات شامل تلاش در جهت خنثی نمودن و یا حذف ویژگی های امنیتی، معرفی کدهای مخرب، سرقت و یا تغییر دادن اطلاعات می باشد .حملات فوق، می تواند از طریق ستون فقرات یک شبکه، سوء استفاده موقت اطلاعاتی، نفوذ الکترونیکی در یک قلمرو بسته و حفاظت شده و یا حمله به یک کاربر تایید شده در زمان اتصال به یک ناحیه بسته و حفاظت شده، بروز نماید. پیامد حملات فوق، افشای اطلاعات، اشاعه فایل های اطلاعاتی، عدم پذیرش سرویس و یا تغییر در داده ها خواهد بود.