Brief Network Knowledge

for cybersecurity

Chaos Nexus Tech

فهرست

۱. مبانی شبکه

شبکه سازی چیست؟

شبکه‌سازی فرآیند اتصال دستگاه‌ها (کامپیوترها، تلفن‌ها، سرورها) برای تبادل داده‌ها و اشتراک‌گذاری منابع است. آن را به عنوان ساخت یک بزرگراه دیجیتال برای ارتباطات در نظر بگیرید.

اجزای کلیدی شبکه:

۱. **گره‌ها (Nodes)**: دستگاه‌هایی مانند رایانه‌ها و تلفن‌ها.

۲. **پیوندها(Links)**: مسیرهایی (کابل‌ها، وای‌فای) که دستگاه‌ها را به هم متصل می‌کنند.

۳. **انواع شبکه:**

- LAN: شبکه محلی (مثلاً خانه یا دفتر کار).
- WAN: شبکه گسترده (مثلاً اینترنت).
- MAN: شبکه شهری (شبکه‌های سراسری شهری).

II. آدرس دهی IP

آدرس IP چیست؟

آدرس IP یک شناسه منحصر به فرد برای یک دستگاه در یک شبکه است، مانند آدرس پستی منزل شما. این آدرس تضمین می‌کند که داده‌های ارسال شده از طریق شبکه به مقصد صحیح می‌رسند.

انواع آدرس‌های IP:

۱. IPv4: یک آدرس ۳۲ بیتی، مثلاً ۱۹۲.۱۶۸.۱.۱. ساده است اما تعداد محدودی دارد.

۲. IPv6: یک آدرس ۱۲۸ بیتی، مثلاً 2001:0db8:85a3:7334 . از تعداد زیادی دستگاه پشتیبانی می‌کند و شامل ویژگی‌های امنیتی داخلی است.

IP عمومی در مقابل IP خصوصی:

IP عمومی: قابل مشاهده در اینترنت؛ اختصاص داده شده توسط ارائه دهندگان خدمات اینترنتی.
IP خصوصی: در شبکه‌های محلی استفاده می‌شوند (مثلاً 193.186.x.x). این IP با استفاده از NAT (Network Address Translation) از اینترنت پنهان می‌شوند.

III. پروتکل‌ها و پورت‌های کلیدی شبکه

TCP (پروتکل کنترل انتقال – Transmission Control Protocol)

TCP با ایجاد اتصال قبل از ارسال داده، تحویل مطمئن داده‌ها را تضمین می‌کند. این مانند ارسال بسته‌ای با شماره پیگیری است.

چند پورت رایج TCP و مثال‌هایی از کاربردها:

۱. پورت ۸۰: HTTP (مرور وب).

۲. پورت ۴۴۳: HTTPS (مرور وب امن).

۳. پورت ۲۱: FTP (پروتکل انتقال فایل).

۴. پورت ۲۲: SSH (دسترسی امن از راه دور).

۵. پورت ۲۵: SMTP (ارسال ایمیل).

۶. پورت ۳۳۰۶: MySQL (ارتباط با پایگاه داده).

۷. پورت ۳۳۸۹: RDP (پروتکل دسکتاپ از راه دور).

UDP (پروتکل داده‌نگار کاربر – User Datagram Protocol)

UDP سریع‌تر است اما نسبت به TCP قابلیت اطمینان کمتری دارد. این پروتکل تأیید نمی‌کند که آیا داده‌ها دریافت شده‌اند یا خیر، و این آن را برای برنامه‌های بلادرنگ ایده‌آل می‌کند.

چند پورت رایج UDP و مثال‌هایی از کاربردها:

۱. پورت ۵۳: DNS (نام دامنه را به IP تبدیل می‌کند).

۲. پورت ۱۲۳: NTP (پروتکل زمان شبکه).

۳. پورت ۱۶۱: SNMP (نظارت بر دستگاه‌های شبکه).

۴. پورت ۶۹: TFTP (پروتکل انتقال فایل ساده).

۵. پورت ۵۰۰: IPsec (رمزگذاری VPN).

IV. توضیح ۲۰ پروتکل رایج شبکه

پروتکل‌های لایه Application

۱. HTTP (HyperText Transfer Protocol)

- هدف: انتقال صفحات وب و منابع.
- مثال: دسترسی به http://example.com.
- ارتباط با امنیت سایبری: آسیب‌پذیر در برابر حملات بدون HTTPS.

۲. HTTPS (HTTP Secure)

- هدف: امن‌سازی HTTP با استفاده از رمزگذاری SSL/TLS.
- مثال: بانکداری یا خرید آنلاین (مثلاً https://bank.com).
- مزایای امنیت سایبری: رمزگذاری داده‌ها در حین انتقال.

۳. FTP (File Transfer Protocol)

- هدف: انتقال فایل‌ها بین سیستم‌ها.
- مثال: آپلود فایل‌های وب‌سایت به سرور.
- نگرانی امنیت سایبری: انتقال داده‌ها به صورت متن ساده مگر اینکه با SFTP امن شده باشد.

۴. SFTP (Secure File Transfer Protocol)

- هدف: انتقال ایمن فایل‌ها با استفاده از SSH.
- مثال: ارسال پشتیبان‌های رمزگذاری شده.
- مزیت امنیت سایبری: جلوگیری از رهگیری داده‌ها.

۵. SMTP (Simple Mail Transfer Protocol)

- هدف: ارسال ایمیل از یک کلاینت به یک سرور.
- مثال: ارسال ایمیل از طریق Gmail.
- نگرانی امنیت سایبری: آسیب‌پذیر در برابر جعل بدون SPF/DKIM.

۶. IMAP (Internet Message Access Protocol)

- هدف: دسترسی و مدیریت ایمیل‌ها روی یک سرور.
- مثال: همگام‌سازی ایمیل‌ها بین دستگاه‌ها.
- مزیت امنیت سایبری: با رمزگذاری (SSL/TLS) کار می‌کند.

۷. DNS (Domain Name System)

- هدف: تبدیل نام دامنه به آدرس IP.
- مثال: google.com ← 142.250.190.14.
- نگرانی امنیت سایبری: آسیب‌پذیر در برابر جعل DNS.

۸. DHCP (Dynamic Host Configuration Protocol)

- هدف: اختصاص خودکار آدرس IP به دستگاه‌ها.
- مثال: لپ‌تاپ به Wi-Fi متصل می‌شود و یک IP دریافت می‌کند.
- خطر امنیت سایبری: سرورهای DHCP جعلی می‌توانند IPهای مخرب اختصاص دهند.

۹. SNMP (Simple Network Management Protocol)

- هدف: نظارت و مدیریت دستگاه‌های شبکه.
- مثال: مدیریت روترها و سوئیچ‌ها.
- نگرانی امنیت سایبری: رشته‌های اجتماعی ضعیف می‌توانند منجر به دسترسی غیرمجاز شوند.

۱۰. Telnet

- هدف: مدیریت دستگاه از راه دور (ناامن).
- مثال: پیکربندی دستگاه‌های شبکه.
- نگرانی امنیت سایبری: ارسال اعتبارنامه‌ها به صورت متن ساده.

پروتکل های لایه Transport

۱. TCP

- هدف: فراهم کردن ارتباط قابل اعتماد.
- مثال: مرور وب، دانلود فایل‌ها.
- نگرانی امنیت سایبری: جلسات TCP می‌توانند ربوده شوند.

۲. UDP

- هدف: ارتباط سریع‌تر بدون بررسی خطا.
- مثال: بازی آنلاین، پخش ویدئو.
- نگرانی امنیت سایبری: سیل UDP می‌تواند باعث DDoS شود.

پروتکل‌های لایه Network

۱. IP (پروتکل اینترنت)

- هدف: مسیریابی بسته‌های داده بین دستگاه‌ها.
- مثال: آدرس‌های IPv۴، IPv۶.
- نگرانی امنیت سایبری: حملات جعل IP.

۲. ICMP (پروتکل پیام کنترل اینترنت)

- هدف: ارسال پیام‌های خطا و تشخیصی.
- مثال: دستور پینگ.
- نگرانی امنیت سایبری: مورد سوءاستفاده در حملات DDoS.

پروتکل‌های لایه Data Link

۱. ARP (Address Resolution Protocol)

- هدف: تبدیل آدرس‌های IP به آدرس‌های MAC.
- مثال: تضمین مسیریابی صحیح در یک شبکه محلی.
- نگرانی امنیت سایبری: حملات جعل ARP.

۲. اترنت (Ethernet)

- هدف: تعریف ارتباطات سیمی شبکه محلی.
- مثال: شبکه‌های درون یک دفترکاری.
- نگرانی امنیت سایبری: استراق سمع ترافیک اترنت رمزگذاری نشده.

پروتکل‌های امنیتی

۱. SSL/TLS (Secure Sockets Layer/Transport Layer Security)

- هدف: رمزگذاری ارتباطات (مثلاً HTTPS).
- مثال: ایمن‌سازی تراکنش‌های آنلاین.
- مزایای امنیت سایبری: جلوگیری از حملات MITM.

۲. IPsec (امنیت پروتکل اینترنت)

- هدف: ایمن‌سازی ترافیک IP (مثلاً VPN).
- مثال: رمزگذاری ارتباط بین سایت‌ها.
- مزایای امنیت سایبری: فراهم کردن یکپارچگی و محرمانگی داده‌ها.

به اشتراک‌گذاری فایل و سرویس‌های دایرکتوری

۱. NFS (Network File System)

- هدف: اشتراک‌گذاری فایل‌ها از طریق شبکه.
- مثال: دسترسی به فایل‌های ذخیره شده در یک سرور از راه دور.
- نگرانی امنیت سایبری: نیاز به احراز هویت مناسب برای جلوگیری از دسترسی غیرمجاز.

۲. LDAP (Lightweight Directory Access Protocol)

- هدف: ارائه سرویس‌های دایرکتوری برای احراز هویت.
- مثال: سیستم‌های ورود متمرکز در سازمان‌ها. نگرانی امنیت سایبری: LDAP پیکربندی نشده می‌تواند امکان دسترسی غیرمجاز را فراهم کند.

V. نت (NAT) Network Address Translation

NAT به چندین دستگاه در یک شبکه خصوصی اجازه می‌دهد تا یک آدرس IP عمومی واحد را برای دسترسی به اینترنت به اشتراک بگذارند.

مثال: روتر وای‌فای خانگی شما از NAT استفاده می‌کند تا لپ‌تاپ، تلفن و تلویزیون شما با استفاده از یک IP عمومی به اینترنت متصل شوند.

ارتباط با امنیت سایبری: NAT آدرس‌های IP داخلی را پنهان می‌کند و یک لایه امنیتی اضافه می‌کند.

VI. دستگاه های کلیدی شبکه

۱. روتر

- هدف: اتصال شبکه‌های مختلف (مثلاً خانه و اینترنت).
- نقش امنیتی: مسدود کردن ترافیک غیرمجاز از طریق ACLها.

۲. سوئیچ

- هدف: اتصال دستگاه‌ها در یک شبکه محلی.
- ویژگی امنیتی: پشتیبانی از VLANها برای ایزوله کردن ترافیک.

۳. فایروال

- هدف: اجازه یا مسدود کردن ترافیک بر اساس قوانین.
- انواع: فایروال‌های فیلترینگ بسته، فایروال‌های حالت‌مند و فایروال‌های لایه کاربرد.

۴. نقاط دسترسی (AP - Access Points)

- هدف: اتصال بی‌سیم به دستگاه‌هایی مانند لپ‌تاپ، تلفن و تبلت را فراهم می‌کند.
- نگرانی امنیتی: رمزهای عبور ضعیف یا پیکربندی‌های ناامن می‌توانند امکان دسترسی غیرمجاز به شبکه را فراهم کنند. استفاده از رمزگذاری WPA3 برای امنیت بیشتر توصیه می‌شود.

۵. IDS/IPS (سیستم تشخیص نفوذ / سیستم پیشگیری از نفوذ)

Intrusion Detection System / Intrusion Prevention System

هدف:

- IDS: ترافیک شبکه را برای فعالیت‌های مشکوک رصد می‌کند و در صورت شناسایی الگوهای مخرب، هشدار ارسال می‌کند.
- IPS: به عنوان نسخه پیشگیرانه IDS عمل می‌کند و به طور فعال فعالیت‌های مخرب را بر اساس تشخیص بلادرنگ مسدود می‌کند.
- نقش امنیتی: هر دو سیستم با شناسایی و جلوگیری از حملاتی مانند بدافزار، تلاش‌های دسترسی غیرمجاز و ناهنجاری‌های ترافیکی، امنیت شبکه را افزایش می‌دهند.

VII. حملات رایج شبکه

۱. DDoS (Distributed Denial of Service)

- شرح: مهاجمان شبکه‌ای را با ترافیک بیش از حد از منابع مختلف پر می‌کنند، سرور یا سرویس را از کار می‌اندازند و آن را برای کاربران قانونی غیرقابل دسترس می‌کنند.
- مثال: وب‌سایتی که توسط سیلی از درخواست‌های جعلی از دسترس خارج می‌شود.
- راهکار کاهش خطرات سایبری: سرویس‌های محافظت از DDoS، فیلتر کردن ترافیک و محدود کردن سرعت می‌تواند به کاهش تأثیر کمک کند.

۲. MITM (Man-in-the-Middle)

- شرح: مهاجم ارتباط بین دو طرف (مثلاً یک کاربر و یک وب‌سایت) را برای سرقت داده‌ها یا تزریق محتوای مخرب قطع می‌کند.
- مثال: قطع ترافیک HTTP رمزگذاری نشده برای سرقت اعتبارنامه‌های ورود به سیستم.
- راهکار کاهش خطرات سایبری: استفاده از HTTPS، رمزگذاری و VPN های امن می‌تواند از حملات MITM جلوگیری کند.

۳. جعل ARP (ARP Spoofing)

- شرح: یک مهاجم پیام‌های ARP جعلی را در یک شبکه محلی ارسال می‌کند تا آدرس MAC خود را با آدرس IP دستگاه دیگری مرتبط کند و به آنها اجازه می‌دهد ترافیک را رهگیری یا دستکاری کنند.
- مثال: تغییر مسیر ترافیک شبکه که برای یک دروازه به سیستم مهاجم در نظر گرفته شده است.
- راهکار کاهش خطرات سایبری: ورودی‌های استاتیک ARP و استفاده از ابزارهای نظارت بر شبکه برای تشخیص ناهنجاری‌ها می‌تواند به دفاع در برابر جعل ARP کمک کند.

۴. جعل یا مسموم کردن DNS (DNS Spoofing - DNS Poisoning)

- شرح: مهاجم رکوردهای DNS را دستکاری می‌کند و کاربران را بدون اطلاع آنها به وب‌سایت‌های مخرب هدایت می‌کند.
- مثال: هدایت کاربرانی که سعی در بازدید از www.paypal.com به یک وب‌سایت جعلی برای سرقت جزئیات ورود به سیستم دارند.
- راهکار کاهش خطرات سایبری: DNSSEC (افزونه‌های امنیتی سیستم نام دامنه) و استفاده از سرویس‌های DNS معتبر می‌تواند از مسمومیت DNS جلوگیری کند.

۵. فیشینگ

- شرح: یک حمله مهندسی اجتماعی که در آن مهاجمان پیام‌های جعلی ارسال می‌کنند تا افراد را فریب دهند تا اطلاعات حساس مانند نام کاربری، رمز عبور یا داده‌های مالی را فاش کنند.
- مثال: یک ایمیل جعلی که به نظر می‌رسد از یک بانک ارسال شده و درخواست اطلاعات ورود به سیستم را دارد.
- راهکار کاهش خطرات سایبری: آموزش کاربر، فیلتر کردن ایمیل و احراز هویت چند عاملی (MFA) می‌تواند خطر فیشینگ را کاهش دهد.

VIII. بهترین شیوه‌های امنیت سایبری برای شبکه‌سازی

۱. استفاده از رمزگذاری:

اطمینان حاصل کنید که داده‌های حساس در حین انتقال رمزگذاری شده‌اند (مثلاً HTTPS، IPsec، VPN) تا از استراق سمع یا رهگیری توسط مهاجمان جلوگیری شود.

۲. اعمال احراز هویت قوی:

برای دسترسی به سیستم‌ها و شبکه‌های حیاتی از احراز هویت چند عاملی (MFA) استفاده کنید تا امنیت را افزایش دهید.

۳. نظارت بر ترافیک شبکه:

به طور مداوم ترافیک شبکه را با استفاده از ابزارهایی مانند Wireshark یا سیستم‌های نظارت بر شبکه (NMS) برای شناسایی ناهنجاری‌ها یا فعالیت‌های مشکوک نظارت کنید.

۴. بخش‌بندی شبکه‌ها:

پیاده‌سازی شبکه‌های محلی مجازی (VLAN) یا زیرشبکه‌ها برای جداسازی سیستم‌های حساس

و محدود کردن تأثیر حمله.

۵. به‌روزرسانی منظم دستگاه‌ها و نرم‌افزارها:

اعمال وصله‌های امنیتی و به‌روزرسانی‌ها بر روی دستگاه‌های شبکه، سرورها و برنامه‌ها برای رفع آسیب‌پذیری‌ها قبل از اینکه توسط مهاجمان مورد سوءاستفاده قرار گیرند.

۶. استفاده از فایروال‌ها و IDS/IPS:

فایروال‌ها را برای فیلتر کردن ترافیک و IDS/IPS را برای شناسایی و جلوگیری از فعالیت‌های مخرب مستقر کنید.

اطمینان حاصل کنید که این سیستم‌ها به طور منظم به‌روزرسانی و به درستی پیکربندی شده‌اند.

۷. پیاده‌سازی کنترل دسترسی:

دسترسی کاربران را فقط به سیستم‌ها و داده‌هایی که برای انجام کار خود نیاز دارند محدود کنید.

اصل حداقل امتیاز را اعمال کنید و در صورت امکان از کنترل دسترسی مبتنی بر نقش (RBAC) استفاده کنید.

۸. پشتیبان‌گیری از داده‌های حیاتی:

به طور منظم از داده‌های مهم پشتیبان‌گیری کنید و آنها را به طور ایمن ذخیره کنید تا در صورت حمله‌ای مانند باج‌افزار از دست دادن داده‌ها جلوگیری شود. ۹. آموزش کاربران:

به طور منظم به کارمندان یا کاربران شبکه، آموزش‌های امنیت سایبری در مورد خطرات فیشینگ، مهندسی اجتماعی و سایر تهدیدات ارائه دهید.

۱۰. شبکه‌های بی‌سیم امن:

از رمزگذاری قوی (مثلاً WPA3) برای شبکه‌های Wi-Fi استفاده کنید و از اعتبارنامه‌های پیش‌فرض برای ایمن‌سازی ارتباطات بی‌سیم در برابر دسترسی غیرمجاز خودداری کنید.

IX. اطلاعات تکمیلی

۱. مدل OSI چیست و آیا می‌توانید هر لایه را با جزئیات توضیح دهید؟

توضیح: مدل OSI یک چارچوب مفهومی است که برای درک تعاملات شبکه در هفت لایه استفاده می‌شود

۱. Physical - با انتقال سخت‌افزاری (مانند کابل‌ها، کارت‌های شبکه) سروکار دارد.

۲. Data Link - تشخیص خطا و آدرس‌های MAC (مانند Ethernet) را مدیریت می‌کند.

۳. Network - بسته‌ها را با استفاده از آدرس‌های IP مسیریابی می‌کند (مانند روترها).

۴. Transport - تحویل مطمئن داده‌ها را تضمین می‌کند (مانند TCP، UDP).

۵. Session - جلسات بین برنامه‌ها را مدیریت می‌کند (مانند NetBIOS).

۶. Presentation - ترجمه، رمزگذاری و فشرده‌سازی داده‌ها (مانند SSL/TLS).

۷. Application - پروتکل‌های کاربر نهایی (مانند HTTP، FTP).

سناریوی واقعی: یک session مرور وب را در نظر بگیرید. مرورگر از HTTP (لایه Application) استفاده می‌کند، داده‌ها از طریق TCP (لایه Transport) منتقل می‌شوند و روترها اطمینان حاصل می‌کنند که به مقصد صحیح می‌رسند (لایه Network). رمزگذاری، امنیت را تضمین می‌کند (لایه Presentation).

۲. تفاوت بین IPv۴ و IPv۶ چیست؟

توضیح: IPv4 دارای آدرس‌های ۳۲ بیتی است که حدود ۴.۳ میلیارد آدرس منحصر به فرد ارائه می‌دهد. از سوی دیگر، IPv6 دارای آدرس‌های ۱۲۸ بیتی است که تقریباً تعداد نامحدودی آدرس (۳۴۰ آندسیلیون) ارائه می‌دهد. IPv6 برای رسیدگی به کمبود آدرس‌های IPv4 طراحی شده است.

سناریوی واقعی: با افزایش تعداد دستگاه‌های متصل به اینترنت (به دستگاه‌های IOT، تلفن‌های هوشمند فکر کنید)، آدرس‌های IPv4 در حال اتمام هستند. اینجاست که IPv6 وارد می‌شود و به دستگاه‌هایی مانند یخچال‌های هوشمند، پوشیدنی‌ها و حسگرها اجازه می‌دهد آدرس‌های IP منحصر به فردی دریافت کنند.

۳. عملکرد روتر چیست و چه تفاوتی با سوئیچ دارد؟

توضیح: یک روتر چندین شبکه را به هم متصل می‌کند و داده‌ها را بین آنها با استفاده از آدرس‌های IP مسیریابی می‌کند، در حالی که یک سوئیچ دستگاه‌های درون یک شبکه را به هم متصل می‌کند و از آدرس‌های MAC برای ارسال داده‌ها استفاده می‌کند.

سناریوی واقعی: در یک دفتر کوچک، روتر شبکه محلی را به اینترنت متصل می‌کند. یک سوئیچ درون دفتر به رایانه‌های کارمندان اجازه می‌دهد تا با یکدیگر ارتباط برقرار کنند. روتر تضمین می‌کند که داده‌های ارسال شده از اینترنت به رایانه مناسب می‌رسد.

۴. آیا می‌توانید توضیح دهید که NAT چیست و چگونه کار می‌کند؟

توضیح: NAT به چندین دستگاه در یک شبکه محلی اجازه می‌دهد تا هنگام دسترسی به اینترنت، یک آدرس IP عمومی را به اشتراک بگذارند. این سرویس آدرس‌های IP خصوصی را به آدرس‌های عمومی و برعکس تبدیل می‌کند.

سناریوی واقعی: در یک شبکه خانگی، همه دستگاه‌ها (لپ‌تاپ، تلفن و غیره) از یک IP عمومی ارائه شده توسط ISP استفاده می‌کنند. روتر از NAT برای تمایز بین دستگاه‌ها استفاده می‌کند و اطمینان حاصل می‌کند که درخواست‌ها به دستگاه صحیح می‌رسند. بدون NAT، هر دستگاه به یک IP عمومی منحصر به فرد نیاز دارد.

۵. DNS چیست و چگونه کار می‌کند؟

توضیح: DNS (سیستم نام دامنه) نام‌های دامنه قابل خواندن توسط انسان (مانند www.google.com) را به آدرس‌های IP تبدیل می‌کند. این سیستم مانند یک دفترچه تلفن برای اینترنت عمل می‌کند.

سناریوی واقعی: وقتی نام یک وب‌سایت را در مرورگر خود تایپ می‌کنید، دستگاه شما با یک سرور DNS تماس می‌گیرد تا دامنه را به یک آدرس IP تبدیل کند و سپس به وب‌سایت متصل می‌شود. بدون DNS، باید آدرس‌های IP هر وب‌سایت را به خاطر بسپارید.

۶. ARP چیست و چگونه جعل ARP کار می‌کند؟

توضیح: ARP (پروتکل تفکیک آدرس) آدرس‌های IP را به آدرس‌های MAC در یک شبکه محلی نگاشت می‌کند. جعل ARP شامل ارسال پیام‌های ARP جعلی برای مرتبط کردن آدرس MAC مهاجم با یک IP قانونی، رهگیری یا تغییر مسیر ترافیک شبکه است.

سناریوی واقعی: اگر یک مهاجم جعل ARP را در یک شبکه شرکتی انجام دهد، می‌تواند با عمل کردن به عنوان "واسطه" بین قربانی و روتر، داده‌های حساس مانند اعتبارنامه‌های ورود به سیستم یا اطلاعات مالی را رهگیری کند.

۷. VLAN چیست و چگونه امنیت شبکه را افزایش می‌دهد؟

توضیح: VLAN (Virtual Local Area Network) یک شبکه فیزیکی را به چندین شبکه منطقی تقسیم می‌کند. این شبکه ترافیک را ایزوله می‌کند و عملکرد و امنیت را بهبود می‌بخشد.
سناریوی واقعی: در یک سازمان، بخش مالی می‌تواند به صورت مستقل در VLAN قرار گیرد تا دسترسی به داده‌های مالی حساس از بخش‌های دیگر مانند بازاریابی را محدود کرده و امنیت را افزایش دهد.

۸. VPN چیست و چگونه کار می‌کند؟

توضیح: یک شبکه خصوصی مجازی (VPN) یک تونل رمزگذاری شده بین دستگاه کاربر و یک سرور از راه دور ایجاد می‌کند و حریم خصوصی را در شبکه‌های ناامن مانند اینترنت تضمین می‌کند.

سناریوی واقعی: هنگام سفر به خارج از کشور، یک کارمند برای دسترسی ایمن به منابع داخلی به VPN شرکت متصل می‌شود. بدون VPN، اتصال کارمند در برابر هکرها در شبکه‌های Wi-Fi عمومی آسیب‌پذیر خواهد بود.

۹. تفاوت بین TCP و UDP چیست؟

توضیح: TCP اتصال‌گرا است و تحویل داده مطمئن را با بررسی خطا تضمین می‌کند، در حالی که UDP بدون اتصال و سریع‌تر است اما تحویل را تضمین نمی‌کند.

سناریوی واقعی: یک سرویس پخش ویدیو (مثلاً یوتیوب) از UDP برای تحویل سریع داده‌ها استفاده می‌کند، در حالی که یک برنامه انتقال فایل (مثلاً FTP) از TCP برای اطمینان از تحویل کامل و مطمئن فایل استفاده می‌کند.

۱۰. آیا می‌توانید تفاوت بین HTTP و HTTPS را توضیح دهید؟

توضیح: HTTP یک پروتکل رمزگذاری نشده برای انتقال داده‌ها است، در حالی که HTTPS (HTTP Secure) از رمزگذاری SSL/TLS برای ایمن‌سازی ارتباط، تضمین یکپارچگی داده‌ها و محرمانگی آنها استفاده می‌کند.

سناریوی واقعی: وقتی وارد حساب بانکی آنلاین خود می‌شوید، HTTPS ارتباط را رمزگذاری می‌کند و از اطلاعات حساس مانند رمزهای عبور و اطلاعات بانکی در برابر رهگیری محافظت می‌کند.

۱۱. فایروال چیست و چگونه از شبکه محافظت می‌کند؟

توضیح: فایروال ترافیک ورودی و خروجی را بر اساس قوانین امنیتی فیلتر می‌کند و دسترسی غیرمجاز و تهدیدات احتمالی را مسدود می‌کند.

سناریوی واقعی: در یک شبکه شرکتی، فایروال از دسترسی مهاجمان خارجی به سیستم‌های داخلی جلوگیری می‌کند. همچنین دسترسی به وب‌سایت‌ها یا پورت‌های غیرقابل اعتماد که به بدافزار مرتبط هستند را مسدود می‌کند.

۱۲. IDS و IPS چیستند؟

توضیح: یک IDS (سیستم تشخیص نفوذ) ترافیک شبکه را برای فعالیت‌های مشکوک رصد می‌کند و به مدیران هشدار می‌دهد. یک IPS (سیستم پیشگیری از نفوذ) با مسدود کردن فعال فعالیت‌های مخرب، یک قدم فراتر می‌رود.

سناریوی واقعی: یک IDS ممکن است در صورت شناسایی الگوهای ترافیکی غیرمعمول، مانند یک حمله DDoS بالقوه، به مدیر شبکه هشدار دهد. یک IPS به طور خودکار آدرس IP مخرب را مسدود می‌کند تا از آسیب بیشتر جلوگیری کند.

۱۳. حمله DDoS چیست و چگونه می‌توان آن را کاهش داد؟

توضیح: یک حمله DDoS شبکه یا سرور را با ترافیک از منابع مختلف اشباع می‌کند و آن را غیرقابل دسترس می‌سازد. تکنیک‌های کاهش شامل فیلتر کردن ترافیک، محدود کردن سرعت و استفاده از سرویس‌های محافظت DDoS است.

سناریوی واقعی: در طول یک رویداد آنلاین مهم، یک شرکت ممکن است یک حمله DDoS را تجربه کند که سعی در مختل کردن دسترسی به وب‌سایت خود دارد. آنها از محافظت DDoS مبتنی بر ابر برای جذب ترافیک و حفظ عملکرد وب‌سایت استفاده می‌کنند.

۱۴. برخی از شماره پورت‌های رایج و پروتکل‌های مرتبط با آنها چیست؟

پورت ۸۰: HTTP

پورت ۴۴۳: HTTPS

پورت ۲۱: FTP (پروتکل انتقال فایل)

پورت ۲۲: SSH (پوسته امن)

پورت ۲۵: SMTP (ایمیل)

سناریوی واقعی: یک مدیر شبکه ممکن است پورت ۲۲ را نظارت کند تا مطمئن شود که هیچ دسترسی SSH غیرمجازی به سرورهای امن وجود ندارد. به طور مشابه، اگر کاربران در دسترسی به یک وب‌سایت مشکل دارند، بررسی پورت ۸۰ و ۴۴۳ ممکن است به تشخیص مشکل کمک کند.

۱۵. IPsec چیست و چگونه در شبکه‌سازی استفاده می‌شود؟

توضیح: IPsec یک مجموعه پروتکل برای ایمن‌سازی ارتباطات IP با احراز هویت و رمزگذاری هر بسته IP در یک جلسه ارتباطی است. معمولاً در VPNها برای اطمینان از ارتباطات ایمن استفاده می‌شود.

سناریوی واقعی: یک شرکت به کارمندان از راه دور اجازه می‌دهد تا با اتصال به شبکه شرکتی از طریق IPsec VPN، به طور ایمن به منابع داخلی دسترسی پیدا کنند و از رمزگذاری تمام ارتباطات اطمینان حاصل شود.

۱۶. تفاوت بین IP عمومی و IP خصوصی چیست؟

توضیح: IP عمومی به دستگاهی اختصاص داده می‌شود که از طریق اینترنت قابل دسترسی است، در حالی که IP خصوصی در یک شبکه محلی استفاده می‌شود و در اینترنت قابل مسیریابی نیست.

سناریوی واقعی: به وب سرور یک شرکت یک IP عمومی اختصاص داده می‌شود که از طریق اینترنت قابل دسترسی است، در حالی که دستگاه‌های داخلی (مانند چاپگرها) از IPهای خصوصی استفاده می‌کنند که فقط در شبکه محلی قابل دسترسی هستند.

۱۷. هدف از سرور پروکسی چیست؟

توضیح: یک سرور پروکسی به عنوان واسطه‌ای بین کلاینت و اینترنت عمل می‌کند و اغلب برای امنیت، ذخیره‌سازی و فیلتر کردن محتوا استفاده می‌شود.

سناریوی واقعی: یک شرکت ممکن است از یک سرور پروکسی برای کنترل و نظارت بر دسترسی کارمندان به اینترنت استفاده کند و اطمینان حاصل کند که آنها از وب‌سایت‌های نامناسب بازدید نمی‌کنند یا از پهنای باند بیش از حد استفاده نمی‌کنند.

۱۸. انواع حملات شبکه چیست و چگونه می‌توان از آنها جلوگیری کرد؟

توضیح: حملات رایج شامل DDoS، MITM ، ARP spoofing، DNS poisoning و packet sniffng است. اقدامات پیشگیرانه شامل فایروال‌ها، رمزگذاری، سیستم‌های IDS/IPS و تقسیم‌بندی شبکه است.

سناریوی واقعی: برای جلوگیری از حملات MITM، یک سازمان ممکن است HTTPS را در همه جا پیاده‌سازی کند و اطمینان حاصل کند که حتی اگر ترافیک رهگیری شود، به راحتی قابل خواندن نیست.

۱۹. هدف DHCP چیست؟

توضیح: DHCP به طور خودکار آدرس‌های IP را به دستگاه‌های موجود در شبکه اختصاص می‌دهد و نیاز به پیکربندی دستی را کاهش می‌دهد و عدم تداخل آدرس‌های IP را تضمین می‌کند.

سناریوی واقعی: در یک دفتر بزرگ، DHCP تضمین می‌کند که لپ‌تاپ‌های کارمندان هنگام اتصال به شبکه Wi-Fi به طور خودکار یک آدرس IP موجود را بدون نیاز به مداخله IT دریافت می‌کنند.

۲۰. چگونه یک شبکه بی‌سیم را ایمن می‌کنید؟

توضیح: ایمن‌سازی یک شبکه بی‌سیم شامل استفاده از رمزگذاری قوی (WPA3)، غیرفعال کردن پخش SSID، استفاده از رمزهای عبور قوی، راه‌اندازی فایروال و اعمال لیست‌های کنترل دسترسی (ACL) است.

سناریوی واقعی: در یک کافه، برای محافظت در برابر دسترسی غیرمجاز، شبکه Wi-Fi با رمزگذاری WPA3 و یک رمز عبور قوی ایمن شده است و از اتصال آسان هکرها به شبکه و دسترسی به داده‌های حساس مشتری جلوگیری می‌کند.