راهنمای کاربردی

CompTIA Network+

Exam N10-009

به‌همراه ۸۰۰ سوال تمرینی با پاسخ تشریحی

ویرایش ششم

Todd Lammle

Jon Buhagiar

ترجمه: سید محمد متین روحانی راد

انتشارات پندار پارس

سرشناسه : لامل، تاد - Lammle, Todd
عنوان و نام پدیدآور : آموزش کاربردی +CompTIA Network به همراه ۸۰۰ سوال تمرینی با پاسخ تشریحی/[تاد لامل، جان باهیگیر] ؛ ترجمه سیدمحمدمتین روحانی‌راد.
مشخصات نشر : تهران : پندار پارس ، ۱۴۰۴.
مشخصات ظاهری : ۱۲۵۴ ص.: مصور.
شابک : 978-622-7785-45-6
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: Comptia Network+ deluxe study guide, sixth edition (exam : N10-009)
موضوع : شبکه‌های کامپیوتری - Computer networks؛ داده‌پردازی -- کارمندان -- گواهی و گواهی‌نامه‌ها
Electronic data processing personnel – Certification- مهندسان مخابرات -- گواهی و گواهی‌نامه‌ها - Telecommunications engineers -- Certification
شناسه افزوده : باهیگیر، جان
شناسه افزوده : Buhagiar, Jon
شناسه افزوده : روحانی‌راد، سید محمدمتین، ۱۳۷۶-، مترجم
رده بندی کنگره : QA۷۶/ ۳
رده بندی دیویی : ۰۰۴/ ۶
شماره کتابشناسی ملی : ۱۰۰۲۲۶۵۲
اطلاعات رکورد کتابشناسی : فیپا

انتشارات پندارپارس

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

تلفن: ۶۶۵۷۲۳۳۵ - ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۲۳۴۸ **info@pendarepars.com**

نام کتاب : **آموزش کاربردی +CompTIA Network (ویرایش ششم)، به‌همراه ۸۰۰ سوال تمرینی با پاسخ تشریحی**

ناشر : **انتشارات پندار پارس**

تالیف : **تد لامل، جان باهیگیر**

ترجمه : **سید محمد متین روحانی راد**

چاپ نخست : **اردیبهشت ۱۴۰۴**

شمارگان : **۲۰۰ نسخه**

طرح جلد : **رامین شکرالهی**

چاپ، صحافی : **روز**

قیمت : **۹۷۰.۰۰۰ تومان** **شابک : ۶-۴۵-۷۷۸۵-۶۲۲-۹۷۸**

فهرست

مقدمه

اگر مانند بسیاری از ما در جامعه شبکه هستید، احتمالاً یک یا چند گواهینامه شبکه دارید. اگر این چنین است، بسیار عاقلانه است که گواهینامه CompTIA Network+ (N10-009) را با افتخار به کارنامه خود اضافه کنید؛ زیرا این دستاورد، جایگاه شما را به عنوان یک شبکه‌کار، ارزشمندتر می‌کند.

در این دوران چالش برانگیز اقتصادی، پیشی‌گرفتن از رقبا (حتی در میان همکاران فعلی‌تان) می‌تواند تفاوت بزرگی در کسب ترفیع یا حفظ شغلتان ایجاد کند! یا شاید این اولین تلاش شما برای دریافت گواهینامه باشد؛ زیرا تصمیم گرفته‌اید وارد یک حرفه جدید در فناوری اطلاعات (IT) شوید. متوجه شده‌اید که ورود به حوزه فناوری اطلاعات راه خوبی برای پیمایش است؛ زیرا با پیشرفت عصر اطلاعات، تقاضا برای متخصصان آگاه در این زمینه پویا به طور چشمگیری افزایش می‌یابد.

در هر صورت، اگر در حرفه شبکه کار می‌کنید یا می‌خواهید وارد آن شوید، گرفتن گواهینامه یکی از بهترین کارهایی است که می‌توانید برای حرفه خود انجام دهید. زیرا ثابت می‌کند در مورد موضوعاتی که در مورد آن صحبت می‌کنید، اطلاعات کافی دارید. همچنین شما را به‌عنوان یک حرفه‌ای تأیید می‌کند، مانند پزشکی که در یک حوزه تخصصی خاص دارای بورد تخصصی است.

در این کتاب متوجه خواهید شد که آزمون CompTIA Network+ چیست؛ هر فصل بخشی از آزمون را پوشش می‌دهد. در پایان هر فصل "بررسی سوالات" را گنجانده‌ایم تا به یادگیری بیشتر اطلاعاتی که آموخته‌اید کمک کند و شما را برای آزمون آماده کند.

یک نکته جالب در مورد کار در حوزه IT این است که دائماً درحال تکامل است، بنابراین همیشه چیزهای جدیدی برای یادگیری وجود دارد و چالش‌های جدیدی برای تسلط برآن وجود دارد. هنگامی که گواهینامه Network+ خود را دریافت کردید و متوجه شدید که به آن علاقه‌مندید، با وارد شدن به شبکه‌های پیچیده‌تر (و کسب درآمد بیشتر) پیش بروید، گواهینامه Cisco CCNA قطعا گام بعدی شما خواهد بود. می‌توانید اطلاعاتی در مورد آن و حتی گواهینامه‌های دیگر در وبلاگ من (www.lammle.com) دریافت کنید.

> ***توجه:*** برای آموزش Network+ با Todd Lammle، چه توسط مربی و چه آنلاین، لطفاً به www.lammle.com مراجعه کنید.

گواهینامه Network+ چیست؟

گواهینامه Network+ توسط انجمن صنعت فناوری رایانه‌ای[1](CompTIA) ایجاد شده است که برای ارائه منابع و آموزش برای جامعه رایانه و فناوری وجود دارد. این همان ارگانی است که آزمون A+ را برای تکنسین‌های کامپیوتر توسعه داده است.

آزمون Network+ برای محک‌زدن مهارت تکنسین‌های شبکه با ۹ تا ۱۲ ماه سابقه در زمینه شبکه‌های فناوری اطلاعات طراحی شده است. این آزمون حوزه‌هایی از فناوری‌های شبکه، مانند تعریف یک پروتکل، مدل اتصال سامانه‌های باز[2](OSI) و لایه‌های آن و مفاهیم طراحی و پیاده‌سازی شبکه (حداقل دانش مورد نیاز برای کار بر روی یک شبکه و برخی از پیش‌نیازهای اساسی برای طراحی و پیاده سازی شبکه) را آزمایش می‌کند.

چرا باید گواهینامه Network+ را دریافت کنیم؟

از آنجایی که CompTIA یک توسعه‌دهنده معتبر گواهینامه‌های بی‌طرف صنعت شبکه است، دریافت گواهینامه Network+ نشان می‌دهد که شما در زمینه‌های خاص تحت پوشش اهداف آزمون Network+ مهارت دارید.

چهار مزیت عمده که با دریافت گواهینامه Network+ مرتبط است:

اثبات موفقیت حرفه‌ای: متخصصان شبکه در جمع‌آوری گواهینامه‌های بیشتر نسبت به همتایان خود در رقابت هستند. از آنجایی که گواهینامه Network+ به طور گسترده تمام حوزه شبکه را پوشش می‌دهد، تکنسین‌ها این گواهینامه را بسیار بیشتر از گواهینامه‌های مایکروسافت قبول دارند (Network+ بسیار معتبرتر و ارزشمندتر است). از آنجایی که به ندرت می‌توان با تلاش اندک چیزی به‌دست‌آورد که ارزش زیادی داشته باشد، صادقانه می‌گویم آماده شدن برای آزمون Network+ دقیقاً مانند روزی توام با بی‌حالی در ساحل نیست. (با این حال، سواحل واقعاً در لیست شخصی من از مکان‌های عالی برای مطالعه قرار دارند!) افرادی که در حوزه IT هستند می‌دانند که قبولی در آزمون Network+ کار آسانی نیست، بنابراین قطعاً به شما احترام بیشتری می‌گذارند و می‌دانند که شما به سطح مشخصی از تخصص در مورد موضوعات مرتبط با شبکه و مستقل از فروشنده دست یافته‌اید.

فرصتی برای پیشرفت: همه ما دوست داریم در شغل خود پیشرفت کنیم که مسئولیت و اعتبار بیشتری را به همراه دارد و این معمولاً به معنای حقوق بیشتر، فرصت‌های بیشتر و گزینه‌های اضافی است. در حوزه فناوری اطلاعات، یک راه عالی برای اطمینان از اینکه اتفاق‌های خوبی می‌افتد، کسب گواهینامه‌های فناوری زیاد از جمله Network+ است.

---

[1] Computing Technology Industry Association
[2] Open Systems Interconnection

برآورده کردن نیازهای آموزشی: +Network به دلیل پشتیبانی گسترده در صنعت، به عنوان پایه اطلاعات شبکه شناخته می‌شود. در واقع برخی از شرکت‌ها داشتن گواهینامه +Network را به‌عنوان یک شرط شغلی قبل از اینکه حتی به فکر استخدام شما باشند، مشخص می‌کنند، یا ممکن است به‌عنوان هدفی مشخص شود که باید پیش از بررسی شغلی بعدی شما محقق شود.

اعتماد مشتری: همانطور که شرکت‌ها مزیت CompTIA را کشف می‌کنند، بدون شک برای دستیابی به این گواهینامه‌ها به کارکنان واجد شرایط نیاز دارند. بسیاری از شرکت‌ها کار خود را به شرکت‌های مشاوره با تجربه کار با امنیت می‌سپارند. شرکت‌هایی که دارای کارکنان دارای گواهینامه هستند، نسبت به شرکت‌هایی که کارکنان بدون گواهینامه دارند، برتری قطعی دارند.

نحوه دریافت گواهینامه +Network

حین انتشار این کتاب، Pearson VUE تنها ارائه‌دهنده آزمون +Network است. در اینجا اطلاعات تماس و مشخصات لازم ویژه آزمون جهت ثبت نام آمده است. قیمت آزمون ممکن است با توجه به کشور یا عضویت CompTIA متفاوت باشد.

فروشنده: Pearson VUE

وب سایت: www.pearsonvue.com/comptia

شماره تلفن (آمریکا و کانادا): 877-551-PLUS (7587)

وقتی برای آزمون برنامه‌ریزی می‌کنید، دستورالعمل‌های مربوط به وقت ملاقات و انصراف، شناسایی الزامات و اطلاعات مربوط به محل مرکز آزمون را دریافت خواهید کرد. علاوه بر این، یک نامه تأیید ثبت نام و پرداخت دریافت خواهید کرد. آزمون‌ها می‌توانند تا شش هفته یا در روز بعد (یا در برخی موارد حتی در همان روز) برنامه‌ریزی شوند.

توجه: قیمت‌ها و کدهای آزمون ممکن است بر اساس کشوری که آزمون در آن برگزار می‌شود متفاوت باشد. برای اطلاع از قیمت دقیق و مراحل ثبت نام آزمون، به وب سایت CompTIA (www.comptia.org) مراجعه کنید.

پس از اینکه آزمون +Network خود را با موفقیت گذراندید، CompTIA به شما گواهینامه می‌دهد. در عرض چهار تا شش هفته پس از قبولی در آزمون، گواهینامه رسمی +CompTIA Network و کارت شناسایی خود را دریافت خواهید کرد. (اگر این موارد را ظرف هشت هفته پس از انجام آزمون دریافت نکردید، مستقیماً با استفاده از اطلاعات موجود در بسته ثبت نام خود با CompTIA تماس بگیرید.)

نکاتی برای شرکت در آزمون Network+

در اینجا چند نکته کلی برای شرکت و موفقیت در آزمون آورده شده است:

- دو فرم شناسایی همراه خود داشته باشید. یکی باید کارت شناسایی عکس‌دار باشد، مانند گواهینامه رانندگی، دیگری می‌تواند کارت اعتباری اصلی یا پاسپورت باشد. هر دو فرم باید دارای امضاء باشند.
- زودتر در مرکز آزمون حاضر شوید تا بتوانید استراحت کنید و مطالب درسی خود، به ویژه جدول‌ها و لیست‌های اطلاعات مربوط به آزمون را مرور کنید. پس از آماده‌شدن برای ورود به اتاق آزمون، باید همه چیز را بیرون بگذارید. شما نمی‌توانید هیچ وسیله‌ای را به محل آزمون بیاورید.
- سؤالات را با دقت بخوانید. وسوسه نشوید که زود به نتیجه برسید. مطمئن شوید که دقیقاً می‌دانید هر سؤال چه چیزی می‌پرسد.
- هیچ سؤالی را بی پاسخ نگذارید. سؤالات بی پاسخ امتیاز منفی دارند. سؤالاتی با چندین پاسخ صحیح وجود خواهد داشت. هنگامی که بیش از یک پاسخ صحیح وجود دارد، یک پیام در پایین صفحه از شما می‌خواهد که "دو مورد را انتخاب کنید" یا "همه مواردی که اعمال می‌شود را انتخاب کنید". حتما پیام‌های نمایش داده شده را بخوانید تا بدانید چه تعداد پاسخ صحیح را باید انتخاب کنید.
- هنگام پاسخ دادن به سؤالات چند گزینه‌ای که در مورد آنها مطمئن نیستید، از فرآیند حذف کردن استفاده کنید تا ابتدا از شر پاسخ‌هایی که آشکارا نادرست هستند خلاص شوید. اگر نیاز به حدس زدن دارید، انجام این کار شانس شما را بهبود می‌بخشد.
- در آزمون‌های مبتنی بر فرم (غیر انطباقی)، چون سؤالات سخت بیشترین زمان را خواهند گرفت، آنها را برای آخر نگه دارید. می‌توانید در طول آزمون به جلو و عقب بروید.

چه کسی باید این کتاب را بخواند؟

شما! اگر می‌خواهید در آزمون Network+ قبول شوید و آن را با اطمینان پشت سر بگذارید! این کتاب مملو از اطلاعات دقیقی است که نیاز دارید و مستقیماً اهداف آزمون Network+ را ترسیم می‌کند، بنابراین اگر از آن برای مطالعه در آزمون استفاده کنید، احتمال موفقیت شما افزایش می‌یابد.

علاوه بر گنجاندن هر ذره دانشی که برای گذراندن آزمون نیاز دارید، نکات بسیار عالی و محکمی برای مجهز کردن شما برای موفقیت در دنیای واقعی فناوری اطلاعات ارائه کرده‌ایم.

این کتاب چه چیزی را پوشش می‌دهد؟

این کتاب همه چیزهایی را که برای قبولی در آزمون CompTIA Network+ باید بدانید را پوشش می‌دهد. اما علاوه بر مطالعه کتاب، اگر می‌توانید، ایده خوبی است که در واقعیت در حوزه شبکه تمرین کنید.

در اینجا لیستی از ۲۱ فصل این کتاب آمده است:

فصل ۱، "مقدمه‌ای بر شبکه‌ها": این فصل شامل مقدمه‌ای بر شبکه‌ها و مروری بر رایج‌ترین توپولوژی‌های فیزیکی شبکه در شبکه‌های امروزی است.

فصل ۲، "مدل مرجع اتصال سامانه‌های باز (OSI)": این فصل مدل OSI، چیستی آن، آنچه در هریک از لایه‌های آن اتفاق می‌افتد و نحوه عملکرد هر لایه را پوشش می‌دهد.

فصل ۳، "کانکتورهای شبکه و استانداردهای سیم‌کشی": این فصل رسانه‌ها و توپولوژی‌های مختلف شبکه، به علاوه انواع و ویژگی‌های کابل مورد استفاده در شبکه‌های امروزی را پوشش می‌دهد.

فصل ۴، "مشخصات اترنت فعلی": این فصل نحوه عملکرد یک شبکه اترنت پایه را پوشش می‌دهد و مشخصات مختلف اترنت را توصیف و دسته‌بندی می‌کند.

فصل ۵، "دستگاه‌های شبکه": شما باید تمام دستگاه‌های مختلف مورد استفاده در شبکه‌های امروزی را بشناسید. این فصل نحوه عملکرد هاب‌ها، روترها، و سوئیچ‌ها و برخی دستگاه‌های دیگر در یک شبکه را شرح می‌دهد.

فصل ۶، "مقدمه‌ای بر پروتکل اینترنت": این مقدمه برای پشته پروتکل IP بسیار مهم است.

فصل ۷، "آدرس‌دهی IP": این فصل پس از پایان فصل ۶، ادامه خواهد یافت و به آدرس‌دهی IP منتقل می‌شود. همچنین حاوی اطلاعاتی در مورد آدرس‌دهی عمومی در مقابل خصوصی و DHCP است.

فصل ۸، "زیر شبکه IP، عیب‌یابی IP، و مقدمه‌ای بر NAT": پس از پایان فصل ۷ شروع می‌شود، در این فصل به زیرشبکه IP می‌پردازیم. اما جای نگرانی نیست (سخت تلاش کرده‌ایم تا این موضوع نه چندان محبوب و در عین حال حیاتی را تا حد امکان آسان کنیم).

فصل ۹، "مقدمه‌ای بر مسیریابی IP": این مقدمه اساساً برای مسیریابی آنچه روترها انجام می‌دهند و چگونگی انجام آنرا پوشش می‌دهد. این فصل، همراه با فصل‌های ۱۰ و ۱۱، مسیریابی و سوئیچینگ را با جزئیات بسیار بیشتر از آنچه برای دستیابی به اهداف CompTIA Network+ لازم است پوشش می‌دهد، زیرا درک این دانش هنگام کار با شبکه‌های امروزی بسیار حیاتی است.

فصل ۱۰، "پروتکل‌های مسیریابی": این فصل پروتکل‌هایی را که روی روترها اجرا می‌شوند و نحوه به‌روزرسانی جدول‌های مسیریابی برای ایجاد یک نقشه شبکه کارآمد را شرح می‌دهد.

فصل ۱۱، "سوئیچینگ و شبکه‌های محلی مجازی": این فصل سوئیچینگ در لایه ۲، پروتکل درخت پوشا (STP) و شبکه‌های محلی مجازی (vLANS) را پوشش می‌دهد. با فصل‌های مسیریابی، بیشتر از آنچه برای آزمون لازم است پیش رفتیم و سوئیچینگ و شبکه‌های محلی مجازی (که در شبکه‌های شرکتی امروزی نیز حیاتی هستند) را به طور کامل‌تر پوشش خواهیم داد.

فصل ۱۲، "شبکه بی‌سیم": از آنجایی که وایرلس امروزه برای شبکه‌های خانگی و تجاری بسیار ضروری است، در این فصل تمام اطلاعاتی که برای موفقیت در شبکه‌های بی‌سیم در خانه و محل کار نیاز دارید بارگذاری شده است.

فصل ۱۳، "دسترسی به شبکه از راه دور": در این فصل، با اهمیت فراهم کردن تحمل خطا و نیز دسترسی‌پذیری سطح بالا آشنا خواهید شد. همچنین با معماری VPN آشنا خواهید شد که عبارتند از: VPNهای سایت به سایت، VPNهای کلاینت به سایت، VPNهای بدون کلاینت، تونل تقسیم در مقابل VPN کامل، و VPNهای SSH.

فصل ۱۴، "استفاده از آمار و حسگرها برای اطمینان از در دسترس بودن شبکه": در این فصل، نوع داده‌هایی را که باید نظارت کنید و برخی از راه‌های انجام این کار را خواهید آموخت.

فصل ۱۵، "اسناد و خط مشیءهای سازمانی": در این فصل، خواهید آموخت که برنامه‌ها و رویه‌ها باید برای مدیریت مسائل عملیاتی مانند مدیریت تغییر، واکنش به حادثه، بازیابی فاجعه، تداوم کسب‌وکار و چرخه حیات سیستم، توسعه داده شوند. همچنین رویه‌های عملیاتی استانداردی را که باید برای هدایت هر یک از این فرآیندها ایجاد شوند، خواهید آموخت.

فصل ۱۶، "دسترسی سطح بالا و بازیابی حادثه": در این فصل، با مفاهیم افزونگی، تحمل خطا و فرآیند بازیابی حادثه آشنا خواهید شد.

فصل ۱۷، "معماری دیتاسنتر و مفاهیم ابری": در این فصل، در مورد جنبه‌های مستندسازی مدیریت شبکه صحبت خواهیم کرد. این فصل به طور منطقی به بحث در مورد نمودارهای فیزیکی و شماتیک‌ها و همچنین به مستندات مدیریت پیکربندی می‌پردازد. در مورد اهمیت این نمودارها، اشکال ساده تا پیچیده‌ای که می‌توانند داشته باشند و ابزارهای مورد استفاده برای ایجاد آنها (از مداد و کاغذ گرفته تا شماتیک‌های اتوکد با فناوری پیشرفته)، آشنا خواهید شد. همچنین چیزهای زیادی در مورد ایجاد و عملکرد خطوط مبنا خواهید یافت.

فصل ۱۸، "روش عیب‌یابی شبکه": در این فصل، در مورد همه موارد عیب‌یابی، مانند نحوه ردیابی و حل بسیاری از مشکلات شبکه، آشنا خواهید شد.

فصل ۱۹، "ابزارها و فرمان‌های نرم‌افزار شبکه": این فصل ابزارهای شبکه‌ای را که برای کمک به اجرای شبکه‌های خود استفاده خواهید کرد، معرفی می‌کند. کارهای تخصصی نیاز به ابزارهای تخصصی دارند و نصب اجزای شبکه نیز از این قاعده مستثنی نیست. ما هر روز از برخی از این ابزارها مانند اسکنرهای شبکه استفاده می‌کنیم.

فصل ۲۰، "مفاهیم امنیت شبکه": در این فصل، مفاهیم اساسی، اصطلاحات و اصولی را که همه متخصصان شبکه باید برای ایمن‌سازی شبکه سازمانی بدانند، خواهید آموخت.

فصل ۲۱، "انواع رایج حملات": در این فصل انواع رایج حملات را که همه متخصصان شبکه باید برای ایمن سازی شبکه سازمانی بدانند، خواهید آموخت.

آنچه در این کتاب گنجانده شده است

در سراسر کتاب چندین ابزار مطالعه را گنجانده‌ایم:

آزمون ارزیابی: در پایان این مقدمه یک آزمون سنجش وجود دارد که می‌توانید از آن برای بررسی آمادگی خود برای آزمون استفاده کنید. پیش از خواندن کتاب این تست را انجام دهید. این کار به شما کمک می‌کند تا بخش‌هایی را که ممکن است نیاز به تجدید معلومات خود داشته باشید، تعیین کنید. پاسخ سؤالات آزمون سنجش در صفحه‌ای جداگانه پس از آخرین سؤال آزمون قرار می‌گیرد. هر پاسخ شامل توضیح کاملی می‌باشد.

نقشه هدف و فهرست آغازین اهداف: در بخش‌های بعد این مقدمه یک نقشه هدف ارائه شده است که به شما نشان می‌دهد هر هدف برای امتحان در کجای این کتاب پوشش داده شده است. افزون بر این، هر فصل با فهرستی از اهداف امتحانی خود شروع می‌شود. از اینها برای مشاهده دقیق محل پوشش هر یک از مباحث امتحانی استفاده کنید.

الزامات امتحان: هر فصل شامل چندین مورد ضروری امتحان است. اینها موضوعات کلیدی هستند که باید از فصل مربوط به بخش‌هایی که هنگام آماده شدن برای امتحان روی آنها تمرکز کنید، استفاده کنید.

آزمایشگاه نوشتاری: هر فصل شامل یک آزمایشگاه نوشتاری است. اینها تمرینات کوتاهی هستند که با اهداف امتحانی هماهنگ است. پاسخ به این موارد را می‌توان در پیوست الف یافت.

بررسی سؤالات فصل: برای آزمایش دانش خود در حین پیشروی در کتاب، بررسی سؤالات در پایان هر فصل قرار دارند. همانطور که هر فصل را تمام می‌کنید، به بررسی سؤالات پاسخ دهید و سپس پاسخ‌های خود را بررسی کنید (پاسخ‌ها و توضیحات صحیح در پیوست ب آمده است). می‌توانید هر بخشی را با سؤالی که اشتباه کرده‌اید، بازخوانی کنید تا مطمئن شوید که دفعه بعد که مطالب را خواندید، به درستی پاسخ دهید.

محیط یادگیری آنلاین تعاملی و بانک نمونه سؤالات

محیط یادگیری آنلاین تعاملی همراه با CompTIA Network+ Study Guide: Exam N10-009 ویرایش ششم یک بانک نمونه سؤالات با ابزارهای مطالعه را فراهم می‌کند تا به شما کمک کند برای امتحان این گواهینامه آماده شوید و شانس خود را برای قبولی در اولین بار افزایش دهید! بانک نمونه سؤالات شامل ابزارهای زیر است:

نمونه سؤالات: تمام سؤالات این کتاب، از جمله آزمون سنجش که در پایان این مقدمه خواهید یافت و تست‌های فصل که شامل بررسی سؤالات در پایان هر فصل می‌شود ارائه شده است. علاوه بر این، دو آزمون عملی وجود دارد. از این سؤالات برای آزمایش دانش خود در مورد مطالب راهنمای مطالعه استفاده کنید. بانک نمونه سؤالات آنلاین بر روی چندین دستگاه اجرا می‌شود.

فلش کارت: تقریباً ۲۰۰ سؤال در فرمت فلش کارت دیجیتال ارائه شده است (یک سؤال و پاسخ صحیح آن). می‌توانید از فلش کارت‌ها برای تقویت یادگیری خود استفاده کنید وپیش از امتحان آمادگی تست لحظه آخری را انجام دهید.

واژه نامه: واژه نامه‌ای از اصطلاحات کلیدی این کتاب و تعاریف آنها به صورت PDF قابل جستجو در سایت انتشارات پندارپارس قابل دسترس است.

توجه: برای ثبت نام و دسترسی به این محیط یادگیری آنلاین تعاملی و بانک نمونه سؤالات با ابزارهای مطالعه، به www.wiley.com/go/netplustestprep بروید.

توجه: مانند همه امتحانات، گواهینامه CompTIA Network+ به طور دوره‌ای به‌روز می‌شود و ممکن است در نهایت از دور خارج شده یا جایگزین شود. در مقطعی پس از اینکه CompTIA دیگر این آزمون را ارائه ندهد، نسخه‌های قدیمی کتاب‌ها و ابزارهای آنلاین ما از رده خارج می‌شوند. اگر این کتاب را پس از از رده خارج شدن آزمون خریداری کرده‌اید یا می‌خواهید پس از آن آزمون، در محیط یادگیری آنلاین Sybex ثبت‌نام کنید، لطفاً بدانید که پس از در دسترس نبودن آزمون، ما هیچ تضمینی نمی‌دهیم که ابزارهای آنلاین Sybex این آزمون در دسترس باشد.

نحوه استفاده از این کتاب

اگر می‌خواهید برای آزمون Network+ تلاشی جدی کرده و آماده شوید، دیگر به دنبال آن نباشید، زیرا ما ساعت‌های بی‌شماری را صرف جمع‌آوری این کتاب کرده‌ایم تا به شما کمک کنیم در آن موفق شوید!

این کتاب مملو از اطلاعات ارزشمند است و اگر درک کنید که چگونه کتاب را کنار هم قرار داده‌ایم، بیشترین استفاده را از زمان مطالعه خود خواهید برد. در اینجا لیستی وجود دارد که نحوه مطالعه را شرح می‌دهد:

۱) بلافاصله پس از این مقدمه در آزمون ارزیابی شرکت کنید. (پاسخ‌ها در پایان آزمون هستند، اما به آنها نگاه نکنید!) اگر هیچ یک از پاسخ‌ها را نمی‌دانید اشکالی ندارد. این کتاب برای همین است. توضیح هر پاسخ اشتباه را با دقت بخوانید و فصلی را که در آن مطالب پوشش داده شده است را یادداشت کنید.

۲) هر فصل را با دقت مطالعه کنید و مطمئن شوید که اطلاعات و اهداف امتحانی که در ابتدای هر فصل ذکر شده است را کاملاً درک کرده‌اید. دوباره به فصلی که سؤالات آزمون ارزیابی‌اش را از دست داده‌اید، توجه ویژه‌ای داشته باشید.

۳) آزمایشگاه نوشتاری در پایان هر فصل را کامل کنید. این تمرین‌های نوشتاری را نادیده نگیرید، زیرا آنها مستقیماً اهداف CompTIA و آنچه که برای رسیدن به آنها نیاز دارید را نشان می‌دهند.

۴) به تمام بررسی سؤالات مربوط به هر فصل پاسخ دهید. به طور خاص هر سؤالی که شما را گیج می‌کند یادداشت کنید و بخش‌های مربوطه کتاب را دوباره مطالعه کنید و از این سؤالات عبور نکنید. مطمئن شوید که هر پاسخ را کاملاً درک کرده‌اید.

۵) توانایی خود را در امتحانات تمرینی محک بزنید. پیش از شرکت در آزمون، حتماً از وب سایت ما برای سؤالات، ویدیوها، فایل‌های صوتی و سایر اطلاعات مفید دیدن کنید.

۶) خود را با استفاده از تمام فلش کارت‌های الکترونیکی آزمایش کنید. این یک برنامه فلش کارت کاملاً جدید و به‌روز است که به شما کمک می‌کند برای آخرین امتحان CompTIA Network+ آماده شوید و یک ابزار مطالعه واقعاً عالی است.

ما با شما صادق هستیم! یادگیری تک تک مطالب این کتاب مستلزم آن است که خودتان را با معیارهای خوبی از نظم و انضباط به کار بگیرید. بنابراین سعی کنید هر روز یک بازه زمانی یکسان را برای مطالعه درنظر بگیرید و مکانی راحت و آرام را برای این کار انتخاب کنید. اگر سخت کار کنید، از سرعت یادگیری این مطالب شگفت‌زده خواهید شد.

اگر مراحل ذکر شده در اینجا را دنبال کنید و با بررسی سؤالات، امتحانات تمرینی، فلش کارت‌های الکترونیکی و تمام آزمایشگاه‌های نوشتاری را مطالعه کنید، مردود شدن در آزمون CompTIA Network+ کار سختی خواهد بود. با این حال، مطالعه برای آزمون Network+ مانند آموزش برای یک ماراتن است. اگر هر روز برای دویدن خوب تمرین نکنید، احتمالاً خیلی خوب به پایان نخواهید رسید.

اهداف امتحان N10-009

در مورد اهداف صحبت می‌کنیم، احتمالاً در مورد آنها بسیار کنجکاو هستید، درست است؟ CompTIA از گروه‌هایی از متخصصان فناوری اطلاعات خواست تا مهارت‌هایی را که احساس می‌کنند در شغل‌شان مهم است، رتبه‌بندی کنند و نتایج در اهداف امتحان گروه‌بندی و به پنج حوزه تقسیم شدند.

این جدول میزانی را بر حسب درصد به شما نشان می‌دهد که هر دامنه در بررسی واقعی نشان داده شده است.

هدف	درصد امتحان
مفاهیم شبکه	۲۳٪
پیاده سازی شبکه	۲۰٪
عملیات شبکه	۱۹٪
امنیت شبکه	۱۴٪
عیب‌یابی شبکه	۲۴٪

نقشه هدف

جدول زیر نشان می‌دهد که هر هدف در کدام بخش کتاب پوشش داده شده است.

شماره هدف	هدف	فصل
۱.۰	مفاهیم شبکه	
۱.۱	مفاهیم مربوط به مدل مرجع اتصال سامانه‌های باز (OSI).	فصل ۲، فصل ۶
۱.۲	مقایسه لوازم شبکه، برنامه‌های کاربردی و توابع.	فصل ۱۰
۱.۳	مفاهیم ابری و گزینه‌های اتصال.	فصل ۱۷
۱.۴	پورت‌های رایج شبکه، پروتکل‌ها، سرویس‌ها و انواع ترافیک.	فصل ۶، فصل ۸
۱.۵	مقایسه رسانه‌های انتقال و فرستنده و گیرنده.	فصل ۳، فصل ۴، فصل ۱۲
۱.۶	مقایسه توپولوژی‌ها، معماری‌ها و انواع شبکه.	فصل ۱
۱.۷	استفاده از آدرس‌دهی شبکه IPv4 مناسب با توجه به یک سناریو.	فصل ۷، فصل ۸
۱.۸	مورد کاربردی (Use case) درحال تکامل برای محیط‌های شبکه مدرن.	فصل ۷، فصل ۱۰، فصل ۱۷
۲.۰	پیاده سازی شبکه	
۲.۱	ویژگی‌های فناوری‌های مسیریابی.	فصل ۸، فصل ۹، فصل ۱۰
۲.۲	فناوری‌ها و ویژگی‌های سوئیچینگ با توجه به یک سناریو.	فصل ۱۱

شماره هدف	هدف	فصل
۲.۳	انتخاب پیکربندی دستگاه‌ها و فناوری‌های بی‌سیم با توجه به یک سناریو.	فصل ۵، فصل ۱۲
۲.۴	عوامل مهم تأسیسات فیزیکی.	فصل ۱۶
۳.۰	عملیات شبکه	
۳.۱	هدف فرآیندها و رویه‌های سازمانی را توضیح دهید.	فصل ۱۵
۳.۲	استفاده از فناوری‌های نظارت شبکه با توجه به یک سناریو.	فصل ۱۴
۳.۳	مفاهیم بازیابی از حادثه (DR) را توضیح دهید.	فصل ۱۶
۳.۴	با توجه به یک سناریو، سرویس شبکه IPv4 و IPv6 را پیاده‌سازی کنید.	فصل ۵، فصل ۷
۳.۵	مقایسه روش‌های مدیریت و دسترسی به شبکه.	فصل ۱۳
۴.۰	امنیت شبکه	
۴.۱	اهمیت مفاهیم مبنای امنیت شبکه را توضیح دهید.	فصل ۲۰، فصل ۲۱
۴.۲	انواع مختلف حملات و تأثیر آنها بر شبکه.	فصل ۲۱
۴.۳	با توجه به یک سناریو، ویژگی‌های امنیتی شبکه، تکنیک‌های دفاعی و راه حل‌ها را اعمال کنید.	فصل ۲۱
۵.۰	عیب‌یابی شبکه	
۵.۱	روش عیب‌یابی را توضیح دهید.	فصل ۱۸
۵.۲	با توجه به یک سناریو، مشکلات رایج کابل‌کشی و اینترفیس فیزیکی را عیب‌یابی کنید.	فصل ۳، فصل ۱۸
۵.۳	با توجه به یک سناریو، مشکلات رایج سرویس شبکه را عیب‌یابی کنید.	فصل ۱۱، فصل ۱۸
۵.۴	با توجه به یک سناریو، مشکلات رایج عملکرد را عیب‌یابی کنید.	فصل ۱۱، فصل ۱۸

شماره هدف	هدف	فصل
۵.۵	با توجه به یک سناریو، از ابزار یا پروتکل مناسب برای حل مشکلات شبکه استفاده کنید.	فصل ۱۹

نحوه تماس با ناشر

اگر فکر می‌کنید اشتباهی در این کتاب پیدا کرده‌اید، لطفاً آن را به ما اطلاع دهید. در John Wiley & Sons ما می‌دانیم که ارائه محتوای دقیق به مشتریانمان چقدر مهم است، اما با وجود تلاش زیاد ممکن است خطایی رخ دهد.

برای ارسال اشتباه احتمالی پیش آمده، لطفاً آن را با عنوان "ارسال اشتباه احتمالی کتاب" به تیم سرویس مشتری ما به آدرس wileysupport@wiley.com ایمیل کنید.

آزمون ارزیابی

۱) کدام معماری شبکه یک روش دسترسی دقیق را برای هاست‌های مختلف تعریف می‌کند؟

۱) همتا به همتا

۲) کلاینت سرور

۳) LAN

۴) توپولوژی ترکیبی

۲) برای اتصال دو مکان اداری باید یک توپولوژی را انتخاب کنید و انتظار ندارید در آینده مکان‌هایی را اضافه کنید. کدام توپولوژی را باید انتخاب کنید؟

۱) نقطه به نقطه

۲) نقطه به چند نقطه

۳) حلقه‌ای

۴) باس

۳) کدام پروتکل واحد داده (PDU) برای توصیف نوع داده‌ای که در لایه نمایش منتقل می‌شود، استفاده می‌شود؟

۱) بیت‌ها

۲) دیتاگرام‌های کاربر

۳) فریم‌ها

۴) قطعه‌ها

۴) کدام لایه وظیفه رمزگذاری و رمزگشایی را بر عهده دارد؟

۱) لایه اپلیکیشن

۲) لایه فیزیکی

۳) لایه جلسه

۴) لایه نمایش یا ارائه

۵) اگر بخواهید کابل UTP را با سرعت ۱۰ گیگابیت‌برثانیه با فاصله ۴۰ متر اجرا کنید، از کدام دسته‌بندی کابل باید استفاده کنید؟

۱) دسته ۵

۲) دسته 5e

۳) دسته ۶

۴) دسته ۳

۶) کدام عبارت، مسیر سیگنال‌دهی در کابل شبکه را توصیف می‌کند؟

۱) تضعیف (Attenuation)

۲) دوبلکس (Duplex)

۳) علامت‌گذاری (Demarcation)

۴) EMI

۷) با یک پیمانکار کار می‌کنید؛ آنها در حال کشیدن و تکمیل خطوط فیبر نوری هستند. خطوط فیبر نوری در مرکز خط تولید شما قرار خواهد گرفت. کدام انتهای کابل را توصیه می‌کنید که احتمال شل شدن کابل‌ها در اثر لرزش در کف تولیدی را کاهش دهد؟

۱) کانکتورهای SC

۲) کانکتورهای ST

۳) کانکتورهای LC

۴) کانکتورهای MTRJ

۸) کدام یک از گزینه‌های زیر دلیل رایج برای ازدحام LAN نیست؟

۱) برودکست[1]

۲) مولتی‌کست[2]

۳) اضافه کردن سوئیچ برای اتصال

۴) هاب‌های متعدد برای اتصال

۹) رایانه دریافت‌کننده، یک فریم Checksum را بررسی کرد. در حین انتقال آسیب دیده بود، بنابراین باید دور انداخته شود. در کدام لایه از OSI این اتفاق افتاده است؟

۱) لایه فیزیکی

۲) لایه پیوند داده

۳) لایه شبکه

۴) لایه جلسه

۱۰) دلیل اینکه یک مدیر شبکه، شبکه را با یک سوئیچ بخش‌بندی می‌کند چیست؟

۱) ایجاد دامنه‌های برودکست بیشتر

۲) ایجاد جداسازی از پیام‌های ARP

۳) ایجاد دامنه‌های برخورد کمتر

۴) جداسازی ترافیک بین قطعه‌ها

۱۱) بر اساس بهترین روش‌ها، محل قراردادن مناسب فایروال به چه صورت است؟

۱) فقط بین شبکه داخلی و اینترنت

۲) در مرزهای امنیتی کلیدی

۳) در DMZ

---

[1] Broadcast
[2] Multicast

۴) فقط بین DMZ و اینترنت

۱۲) روش مناقشه ۸۰۲.۱۱ شبکه بی‌سیم کدام است؟

۱) CSMA/CA

۲) CSMA/CD

۳) DSSS

۴) OFDM

۱۳) یک سرویس گیرنده DHCP از چه شکلی از ارتباط برای به‌دست‌آوردن یک آدرس IP در ابتدا استفاده می‌کند؟

۱) لایه ۳ برودکست

۲) لایه ۳ مولتی‌کست

۳) لایه ۳ از 802.1Q

۴) لایه ۳ یونیکست[1]

۱۴) کدام روش دسترسی مدیریت باید در دستگاه‌های شبکه برای رمزگذاری یک جلسه پیکربندی شود؟

۱) RADIUS

۲) HTTP

۳) SSH

۴) SFTP

۱۵) کدام پروتکل دسترسی از راه دور مایکروسافت اجازه می‌دهد تا درایوهای محلی به سیستم راه دور ارائه شوند؟

۱) VNC

۲) RDP

۳) SSH

۴) Telnet

۱۶) سیستم Syslog از کدام پروتکل و شماره پورت استفاده می‌کند؟

---

[1] Unicast

۱) UDP/161

۲) TCP/162

۳) UDP/162

۴) UDP/514

۱۷) کدام یک از موارد زیر محدوده IP شبکه کلاس B است؟

۱) ۱–۱۲۶

۲) ۱–۱۲۷

۳) ۱۲۸–۱۹۱

۴) ۱۹۲–۲۲۴

۱۸) کدام یک در مورد آدرس IP 135.20.255.255 درست است؟

۱) یک آدرس کلاس A است.

۲) آدرس برودکست است.

۳) آدرس Gateway پیش فرض است.

۴) دارای ماسک پیش فرض ۲۵۵.۰.۰.۰ است.

۱۹) دلیل اصلی استفاده از آدرس IP خصوصی چیست؟

۱) اجازه می‌دهد تا آدرس‌های IP عمومی را حفظ کنید.

۲) از آنجایی که آدرس‌های IP خصوصی در اینترنت قابل مسیریابی نیستند، ایمن هستند.

۳) ارتباطات را خصوصی نگه می‌دارد.

۴) راه‌اندازی آن آسان‌تر از آدرس‌های IP عمومی است.

۲۰) هنگام استفاده از آدرس‌های IP خصوصی برای برقراری ارتباط با هاست اینترنت چه چیزی لازم است؟

۱) روتر اینترنت

۲) تونل IPv4

۳) تونل VPN

۴) ترجمه آدرس شبکه

۲۱) کدام پروتکل مسیریابی یک پروتکل حالت پیوند[1] واقعی است؟

۱) RIP

۲) OSPF

۳) RIPv2

۴) EIGRP

۲۲) چرا در قسمت Age خروجی زیر خط تیره وجود دارد؟

```
Lab_A#sh ip arp
Protocol Address Age(min) Hardware Addr Type Interface
Internet 172.16.20.1 - 00d0.58ad.05f4 ARPA Ethernet1
Internet 172.16.20.2 3 0030.9492.a5dd ARPA Ethernet1
Internet 172.16.10.1 - 0015.0506.31b0 ARPA Ethernet0
```

۱) ورودی ARP کهنه است.

۲) ورودی ARP نامعتبر است.

۳) اینترفیس‌های فیزیکی هستند.

۴) اینترفیس‌های مجازی وجود دارد.

۲۳) تعریف مسیر AD چیست؟

۱) AD معیاری است که پروتکل‌های مسیریابی از آن برای انتخاب بهترین مسیر استفاده می‌کنند.

۲) AD مقداری است که توسط مدیران شبکه برای انتخاب مسیر اختصاص داده شده است.

۳) AD رتبه‌بندی اعتماد زمانی است که چندین مسیر به یک مقصد وجود داشته باشد.

۴) AD مقداری است که با هزینه رسیدن به مقصد مرتبط است.

۲۴) فرض کنید یک مسیر نمایش آی پی روی روتر انجام می‌دهید و چندین مسیر را با AD 90 می‌بینید. کدام پروتکل مسیریابی این فرمان‌های مسیر را ایجاد کرده است؟

۱) IGRP

۲) OSPF

۳) EIGRP

۴) RIP

---

[1] Link State

۲۵) کدام پروتکل مسیریابی از معیارهای بردار مسیر (Path-Vector) استفاده می‌کند؟

۱) BGP

۲) RIP

۳) OSPF

۴) EIGRP

۲۶) کدام پروتکل جایگزین ARP در IPv6 می‌شود؟

۱) NDP

۲) ARPv6

۳) GRE

۴) RA

۲۷) کدام حالت VTP اجازه نمی‌دهد سوئیچ در ترافیک VTP شرکت کند اما ترافیک VTP را ارسال می‌کند؟

۱) حالت سرور

۲) حالت شفاف (Transparent)

۳) حالت پراکسی

۴) حالت کلاینت

۲۸) کدام پروتکل از پروتکل اختصاصی سیسکو برای سوئیچ‌های ترانک استفاده می‌شود؟

۱) ISL

۲) 802.1Q

۳) VTP

۴) CDP

۲۹) کدام فناوری بر اساس احراز هویت، به شبکه، دسترسی انتخابی می‌دهد؟

۱) 802.1Q

۲) ACL

۳) 802.1X

۴) فایروال

۳۰) چند کانال غیر همپوشانی با 802.11a موجود است؟

۱) ۳

۲) ۱۲

۳) ۲۳

۴) ۴۰

۳۱) حداکثر نرخ داده برای استاندارد 802.11a چقدر است؟

۱) ۶ مگابیت بر ثانیه

۲) ۱۱ مگابیت بر ثانیه

۳) ۲۲ مگابیت بر ثانیه

۴) ۵۴ مگابیت بر ثانیه

۳۲) مزایای VPNهای سایت‌به‌سایت IPsec چیست؟

۱) نیاز به پهنای باند کمتر

۲) تأخیر کمتر

۳) مقیاس پذیری

۴) پشتیبانی از مولتی‌کست

۳۳) برای اتصال به پورت سریال روتر از چه کابلی باید استفاده کرد؟

۱) Cat 5e

۲) کابل رول شده

۳) کابل PuTTY

۴) SMF

۳۴) چه نوع پیام SNMP از NMS برای درخواست اطلاعات به عامل ارسال می‌شود؟

۱) پیام Get-request

۲) پیام Get-response

۳) پیام Set-request

۴) پیام Trap

۳۵) چه پروتکلی اطلاعات دقیقی در مورد جریان ترافیک بین نقاط پایانی ارائه می‌دهد؟

۱) Syslog

۲) SNMP

۳) NetFlow

۴) SPAN

۳۶) با یک ارائه دهنده سرویس جدید قرارداد بسته‌اید و در حال بررسی قرارداد سطح سرویس آنها (SLA) هستید. SLA بیان می‌کند که تعهد آنها به زمان کار ۹۹٪ است. زمان توقف مورد انتظار در سال چقدر است؟

۱) ۳.۶۵ روز

۲) ۸.۷۶ ساعت

۳) ۵۲.۵۶ دقیقه

۴) ۵.۲۹ دقیقه

۳۷) آیا باید مطمئن شوید که کاربران زمانی که رمز عبور آنها منقضی می‌شود و مجبور به تغییر آن هستند، از رمزهای عبور مجدد استفاده نمی‌کنند؟ در کدام یک از موارد زیر نیاز به تغییر دارید؟

۱) BYOD

۲) خط‌مشی رمز عبور

۳) DLP

۴) AUP

۳۸) کدام یک از موارد زیر معیاری است برای اینکه چقدر طول می‌کشد تا داده‌های شما قبل از حذف یا خرابی بازیابی شود؟

۱) RTO

۲) MTBF

۳) RPO

۴) MTTR

۳۹) بازیابی از نوار ۴ ساعت طول می‌کشد. این نمونه چیست؟

۱) هدف نقطه بازیابی (RPO)

۲) هدف زمان بازیابی (RTO)

۳) چرخش GFS

۴) پنجره پشتیبان‌گیری

۴۰) کدام سرویس ابری برای توسعه نرم‌افزار استفاده می‌شود؟

۱) SaaS

۲) IaaS

۳) PaaS

۴) DRaaS

۴۱) پروتکل مسیریابی در کدام سطح شبکه اجرا می‌شود؟

۱) سطح داده

۲) سطح کنترل

۳) سطح مدیریت

۴) سطح مسیریابی

۴۲) پس از تأیید یک نظریه، مرحله بعدی در حل مسئله چیست؟

۱) یک فرضیه ایجاد کنید.

۲) چندین رویکرد را درنظر بگیرید.

۳) یک برنامه اقدام تنظیم کنید.

۴) با مشکلات متعدد به صورت جداگانه برخورد کنید.

۴۳) مرحله نهایی برای حل یک مشکل در روش عیب‌یابی چیست؟

۱) راه حلی را اجرا کنید.

۲) اعتبار یک نظریه.

۳) یک برنامه اقدام تنظیم کنید.

۴) سند.

۴۴) کدام ابزار نرم‌افزاری به شما اجازه می‌دهد تا بررسی کنید که آیا یک برنامه وب در حال اجرا بر روی سرور آنلاین است؟

۱) ping
۲) nslookup
۳) Tracert/Traceroute
۴) Port scanner

۴۵) برای بررسی حداکثر واحد انتقال پیکربندی شده (MTU) در اینترفیس یک هاست لینوکس، از کدام فرمان باید استفاده کرد؟

۱) ipconfig
۲) ifconfig
۳) mtuconfig
۴) iptables

۴۶) کدام ابزار اجازه می‌دهد تا در سطح بسته[1] برای ترافیک مربوط به یک اپلیکیشن بررسی شود؟

۱) آنالیزگر پروتکل
۲) dig
۳) اسپکتروم آنالایزر (Spectrum analyzer)
۴) Nslookup

۴۷) کدام پروتکل، احراز هویت و حسابداری را در یک بسته TCP در پورت ۴۹ ترکیب می‌کند؟

۱) TACACS+
۲) RADIUS
۳) TLS
۴) LDAP

۴۸) کدام عامل احراز هویت، شما را ملزم به ارائه چیزی می‌کند که دارید؟

۱) رمز عبور
۲) امضاء

[1] Packet

۳) اثر انگشت

۴) توکن

۴۹) یک مدیر جوان با وحشت نزد شما می‌آید. پس از مشاهده فایل‌های گزارش، او متقاعد شده است که یک مهاجم تلاش می‌کند از یک آدرس IP قانونی برای ایجاد اختلال در دسترسی به نقاط دیگر شبکه استفاده کند. این کدام نوع حمله است؟

۱) جعل

۲) مهندسی اجتماعی

۳) کرم

۴) رمز عبور

۵۰) فرض کنید که مدیر یک شرکت بزرگ بطری‌سازی هستید. در پایان هر ماه، شما به طور معمول همه گزارش‌ها را مشاهده می‌کنید و به دنبال مغایرت می‌گردید. در این ماه، گزارش خطای سیستم ایمیل شما تعداد زیادی تلاش ناموفق برای ورود به سیستم را گزارش می‌دهد. واضح است که سرور ایمیل هدف قرار گرفته است. کدام نوع حمله به احتمال زیاد رخ می‌دهد؟

۱) بی رحمانه (Brute-force)

۲) درب پشتی (Backdoor)

۳) کرم

۴) جعل IP

پاسخ آزمون سنجش

۱) گزینه ۲. معماری شبکه کلاینت–سرور به طور دقیق هاست‌ها را تعریف می‌کند. کلاینت‌ها به اطلاعات دسترسی دارند و سرورها اطلاعات را به اشتراک می‌گذارند. همتابه‌همتا (Peer-to-Peer) یک معماری شبکه است که به یک هاست اجازه می‌دهد تا هم به منابع یک شبکه دسترسی داشته باشد و هم آنرا به اشتراک بگذارد. شبکه محلی (LAN) یک نوع شبکه است و به اشتراک‌گذاری اطلاعات مربوط نمی‌شود. توپولوژی ترکیبی، توپولوژی را توصیف می‌کند که دو یا چند توپولوژی را در خود جای داده است.

۲) گزینه ۱. اتصال نقطه‌به‌نقطه معمولاً برای اتصال دو اداره استفاده می‌شود که در آن گسترش مکان‌ها نگران‌کننده نیست. اگر یک اداره نیاز به اتصال به چندین مکان اداری دیگر داشته باشد، باید توپولوژی

نقطه‌به‌چندنقطه انتخاب شود. حلقه و باس، توپولوژی هستند و برای توصیف روش‌های اتصال WAN استفاده نمی‌شوند.

۳) گزینه ۲. دیتاگرام‌های کاربر، پروتکل واحدهای داده (PDUs) هستند که داده‌ها را در لایه نمایش توصیف می‌کنند. بیت‌ها، داده‌ها را در لایه فیزیکی توصیف می‌کنند. فریم‌ها داده‌ها را در لایه پیوند داده توصیف می‌کنند. قطعه‌ها داده‌ها را در لایه حمل توصیف می‌کنند.

۴) گزینه ۴. لایه نمایش، وظیفه رمزگذاری و رمزگشایی و همچنین فشرده‌سازی و رفع فشرده‌سازی را بر عهده دارد. لایه اپلیکیشن، مسئول دسترسی به اینترفیس برنامه‌نویسی کاربردی (API) و شروع فرآیند ارتباط شبکه است. لایه فیزیکی وظیفه انتقال داده‌ها از طریق نور، الکتریسیته و امواج هوا را بر عهده دارد. لایه جلسه، وظیفه تنظیم گفتگو بین دو هاست را بر عهده دارد.

۵) گزینه ۳. دسته ۶، قابلیت سرعت ۱۰ گیگابیت‌برثانیه تا حداکثر فاصله ۵۵ متری را دارد. دسته ۵، توانایی سرعت ۱۰۰ مگابیت‌برثانیه در فاصله ۱۰۰ متری را دارد. دسته 5e قادر به سرعت ۱ گیگابیت‌برثانیه در فاصله ۱۰۰ متری است. دسته ۳ تنها قادر به حداکثر سرعت ۱۰ مگابیت‌برثانیه است.

۶) گزینه ۲. Duplex به مسیر سیگنال‌دهی در کابل شبکه اشاره دارد. Attenuation، کاهش سیگنال با افزایش طول کابل است. Demarcation یا مرزبندی به نقطه مسئولیت یک ارائه دهنده شبکه اشاره دارد. تداخل الکترومغناطیسی (EMI) تداخلی است که از یک منبع خارجی به کابل شبکه القا می‌شود.

۷) گزینه ۲. کانکتور ST بهترین انتخاب برای نصب در نزدیکی منابع ارتعاش است. کانکتور SC یک کانکتور مربعی است که اغلب برای کابل چند حالته استفاده می‌شود. کانکتور ST دارای یک مهار فنری است که در برابر لرزش مقاومت می‌کند و به طور مثبت قفل می‌شود. اگرچه کانکتورهای LC و MTRJ دارای مکانیسم‌های مهارکننده هستند، ST دارای یک مهار فنری است تا از شل نشدن آن اطمینان حاصل کند.

۸) گزینه ۳. برودکست، مولتی‌کست و هاب‌های متعدد برای اتصال، همگی از علل شایع تراکم شبکه LAN هستند. افزودن سوئیچ برای اتصال، ارتباط مستقیمی با تراکم LAN ندارد، زیرا سوئیچ‌ها دامنه‌های برخورد ایجاد می‌کنند و پهنای باند مؤثر را افزایش می‌دهند.

۹) گزینه ۲. لایه پیوند داده، مسئول بررسی دنباله چک فریم (FCS)[1] است که Checksum فریم است. لایه فیزیکی مسئول انتقال داده‌ها از طریق برق، نور یا هوا است. لایه شبکه مسئول آدرس‌دهی منطقی و مسیریابی داده‌ها است. لایه جلسه وظیفه کنترل گفتگو را بر عهده دارد.

۱۰) گزینه ۴. یک سوئیچ، تقسیم‌بندی میکرو ایجاد می‌کند که به نوبه خود ترافیک بین دو رایانه مکالمه را از رایانه‌های دیگری که بخشی از ارتباطات نیستند جدا می‌کند. این به نوبه خود پهنای باند را برای رایانه‌هایی

[1] Frame Check Sequence

که بخشی از ارتباطات بین مکالمه دو رایانه نیستند افزایش می‌دهد. ایجاد دامنه‌های برودکست تنها با افزودن VLAN و روتر امکان‌پذیر است. جداسازی پیام‌های پروتکل حل آدرس (ARP) تنها با ایجاد دامنه‌های برودکست امکان‌پذیر است. تقسیم‌بندی با سوئیچ، دامنه‌های برخورد بیشتری ایجاد می‌کند، نه دامنه‌های برخورد کمتر.

۱۱) گزینه ۲. فایروال‌ها باید همیشه در مرزهای امنیتی کلیدی قرار گیرند که می‌تواند اینترنت و شبکه داخلی شما باشد. با این حال، قراردادن مناسب، منحصر به مرزهای اینترنت و شبکه‌های داخلی نیست. به عنوان مثال، می‌تواند بین دو شبکه داخلی مانند R&D و شبکه‌های مهمان قرار گیرد. شبکه منطقه غیرنظامی (DMZ[1]) که اکنون به عنوان یک زیرشبکه غربال شده نیز نامیده می‌شود، بخشی از فایروال است که در آن سرویس‌ها رو به روی اینترنت قرار می‌گیرند. فایروال‌ها معمولاً فقط بین DMZ و اینترنت قرار نمی‌گیرند زیرا اکثر شبکه‌ها دارای یک شبکه داخلی هستند.

۱۲) گزینه ۱. ۸۰۲.۱۱ از روش مناقشه‌ای استفاده می‌کند که شامل دسترسی چندگانه با قابلیت شنود سیگنال حامل/پیشگیری از حادثه (CSMA/CA[2]) است. ۸۰۲.۱۱ سازوکار Request-to-Send/Clear-to-Send را پیاده‌سازی می‌کند که از برخورد جلوگیری می‌کند. اترنت از یک روش مناقشه‌ای استفاده می‌کند که تشخیص برخورد/دسترسی چندگانه (CSMA/CD[3]) است. هر دو، طیف گسترده توالی مستقیم (DSSS)[4] و تقسیم فرکانس عمود برهم (OFDM)[5] مدولاسیون‌های بی‌سیم هستند که برای انتقال داده‌ها استفاده می‌شوند.

۱۳) گزینه ۱. DHCP از برودکست‌های لایه ۳ با ارسال بسته‌ها به ۲۵۵.۲۵۵.۲۵۵.۲۵۵ برای کشف اولیه DHCP استفاده می‌کند. مولتی‌کست لایه ۳ برای کلاینت‌های DHCP استفاده نمی‌شود. لایه ۳، 802.1Q پاسخ نادرستی است؛ زیرا 802.1Q برای سوئیچ ترانک استفاده می‌شود. یونیکست‌های لایه ۳ شکل ارتباطی است که کلاینت‌ها پس از به‌دست‌آوردن آدرس IP استفاده می‌کنند.

۱۴) گزینه ۳. پوسته امن[6] (SSH) یک روش شبیه‌سازی کنسول ایمن برای مدیریت دستگاه‌های شبکه است. این امکان را به فرستنده و گیرنده می‌دهد تا یک جلسه رمزگذاری شده ایجاد کنند تا داده‌ها قابل رهگیری نباشند. سیستم تأیید هویت کاربران جهت ورود از راه دور (RADIUS[7]) پروتکلی است که کاربران را احراز

---

[1] demilitarized zone
[2] Carrier Sense Multiple Access/Collision Avoidance
[3] Carrier Sense Multiple Access/Collision Detection
[4] Direct Sequence Spread Spectrum
[5] Orthogonal Frequency Division Multiplexing
[6] Secure Shell
[7] Remote Authentication Dial-In User Service

هویت می‌کند و رمزگذاری را ارائه نمی‌دهد. پروتکل انتقال ابرمتن (HTTP) روشی برای انتقال زبان نشانه‌گذاری ابرمتن (HTML) از سرور به هاست درخواست‌کننده است. رمزگذاری را ارائه نمی‌دهد. پروتکل انتقال فایل SSH (SFTP[1]) پروتکلی است که برای انتقال فایل رمزگذاری می‌کند، اما دسترسی مدیریتی را فراهم نمی‌کند.

۱۵) گزینه ۲. پروتکل ریموت دسکتاپ (RDP) اجازه می‌دهد تا درایوهای محلی در هنگام شروع جلسه RDP در دسترس دستگاه راه دور باشند. شبکه مجازی رایانه (VNC[2])، پوسته امن (SSH) و Telnet قادر به تغییر مسیر درایوها نیستند.

۱۶) گزینه ۴. روتر یا سوئیچ پیام‌های Syslog را به سرور Syslog در پورت ۵۱۴ با UDP ارسال می‌کند. عوامل SNMP به UDP/161 گوش می‌دهند. SNMP از TCP برای پیام‌رسانی استفاده نمی‌کند. SNMP تله‌ها را روی UDP/162 ارسال می‌کند.

۱۷) گزینه ۳. محدوده IP برای شبکه کلاس B، ۱۹۱–۱۲۸ است. آدرس‌دهی کلاس B به طور پیش فرض ۱۶ بیت آدرس‌دهی شبکه و ۱۶ بیت آدرس‌دهی هاست را فراهم می‌کند.

۱۸) گزینه ۲. آدرس IP 135.20.255.255 یک آدرس برودکست کلاس B است. این یک آدرس کلاس A نیست و همچنین آدرس Gateway پیش‌فرض نیست. ماسک پیش‌فرض یک آدرس کلاس B، 255.255.0.0 است.

۱۹) گزینه ۱. فضای آدرس IP خصوصی برای حفظ تعداد آدرس‌های IP عمومی ایجاد شده است. آدرس‌های IP خصوصی در اینترنت قابل مسیریابی نیستند، اما این امر باعث امنیت آنها نمی‌شود. آدرس‌های IP خصوصی، همانطور که از نامشان پیداست، ارتباطات را عمومی بیان نمی‌کنند. آدرس‌های IP خصوصی به صورت عمومی برای ارتباطات قابل آدرس‌دهی نیستند. راه‌اندازی آدرس‌های IP خصوصی آسان‌تر از آدرس‌های IP عمومی نیست.

۲۰) گزینه ۴. ترجمه آدرس شبکه (NAT) برای برقراری ارتباط از طریق اینترنت عمومی با آدرس‌های IP خصوصی مورد نیاز است. اگرچه روترهای اینترنت برای مسیریابی مورد نیاز هستند، اما به طور پیش‌فرض آدرس‌های IP خصوصی را به آدرس‌های IP عمومی هدایت نمی‌کنند. تونل IPv4 یا تونل VPN برای ارتباطات در اینترنت با آدرس‌های IP خصوصی مورد نیاز نیست.

۲۱) گزینه ۲. پروتکل نخستین کوتاه‌ترین مسیر باز یا OSPF[3] یک پروتکل حالت–پیوند است. پروتکل اطلاعات مسیریابی (RIP[1]) و RIPv2 هر دو پروتکل‌های برداری فاصله هستند. پروتکل مسیریابی گیت‌وی داخلی

---

[1] SSH File Transfer Protocol
[2] Virtual Network Computing
[3] Open Shortest Path First

پیشرفته (EIGRP[۲]) یک پروتکل مسیریابی ترکیبی است که بهترین ویژگی‌های بردار فاصله و حالت–پیوند را ترکیب می‌کند.

۲۲) گزینه ۳. هر ورودی پروتکل تفکیک آدرس (ARP[3]) یک زمان مشخص برای زندگی در حافظه پنهان ARP دارد. با این حال، اینترفیس‌های فیزیکی به طور دائم به حافظه پنهان ARP اضافه می‌شوند و با یک خط تیره زیر ستون Age مشخص می‌شوند. هنگامی که ورودی‌های ARP کهنه می‌شوند، ورودی از حافظه پنهان ARP حذف می‌شود. اگر ورودی ARP نامعتبر باشد، از حافظه پنهان ARP حذف خواهد شد.

۲۳) گزینه ۳. فاصله ادمینی (AD[۴]) رتبه‌بندی اعتماد بین پروتکل‌های مسیریابی مختلف و روش‌های مسیر است. این مقیاس اعتماد، زمانی مهم است که چندین مسیر به یک مقصد وجود داشته باشد. مسیرهای متصل مستقیم دارای فواصل ادمینی (AD) با بالاترین سطح اعتماد هستند. فرمان‌های مسیر پر شده توسط پروتکل مسیریابی پویا برای بهترین مسیر بر اساس اندازه‌های متریک و نه فاصله ادمینی آنها محاسبه می‌شود. فاصله ادمینی توسط مدیر برای انتخاب مسیر تعیین نشده است. مقدار فاصله ادمینی با هزینه تا مقصد مرتبط نیست، فقط اعتماد به یک بیانیه مسیر است.

۲۴) گزینه ۳. فاصله ادمینی یا اداری (AD) پروتکل مسیریابی گیت‌وی داخلی پیشرفته (EIGRP[۵])، ۹۰ است. رایج‌ترین ADها ۹۰ برای EIGRP، ۱۰۰ برای IGRP، ۱۱۰ برای OSPF، و ۱۲۰ برای RIP هستند. یادداشت "۹۰ *یاقوت بیضی هندی عجیب و غریب*" به شما کمک می‌کند ترتیب را به خاطر بسپارید. سپس با شروع EIGRP با مقدار ۹۰، مقادیر زیر ۱۰ را افزایش دهید.

۲۵) گزینه ۱. پروتکل گیت‌وی مرزی (BGP[۶]) یک پروتکل مسیریابی بردار مسیر است. پروتکل اطلاعات مسیریابی (RIP[۷]) یک پروتکل مسیریابی بردار فاصله است. OSPF یک پروتکل حالت–پیوند است. پروتکل مسیریابی گیت‌وی داخلی پیشرفته (EIGRP) یک پروتکل ترکیبی درنظر گرفته می‌شود که هم مکانیسم‌های بردار فاصله و هم سازوکار حالت پیوند را در بر می‌گیرد.

۲۶) گزینه ۱. پروتکل تفکیک آدرس (ARP) در IPv6 با پروتکل کشف شبکه (NDP[8]) جایگزین شده است. پروتکل NDP از درخواست همسایه (NS[۱]) و تبلیغات همسایه (NA[۲]) برای یادگیری همسایگان به جای

---

[1] Routing Information Protocol
[2] Enhanced Interior Gateway Routing Protocol
[3] Address Resolution Protocol
[4] Administrative Distance
[5] Enhanced Interior Gateway Routing Protocol
[6] Border Gateway Protocol
[7] Routing Information Protocol
[8] Network Discovery Protocol

برودکست ARP استفاده می‌کند. ARPv6 یک پروتکل واقعی نیست بنابراین یک پاسخ نامعتبر است. کپسوله‌سازی روتر عمومی (GRE[3]) یک پروتکل تونل‌سازی برای سایر پروتکل‌های شبکه است. یک بسته تبلیغاتی روتر (RA) از گیت‌وی بازگردانده می‌شود تا هاست، آدرس گیت‌وی را یاد بگیرد.

۲۷) گزینه ۲. سوئیچ در حالت شفاف VTP در VTP شرکت نخواهد کرد. با این حال، اگر VTP، v2 باشد، سوئیچ، تبلیغات VTP را ارسال و دریافت می‌کند. حالت سرور VTP به سوئیچ اجازه می‌دهد تا به عنوان یک Master برای دامنه VTP عمل کند. حالت پراکسی VTP یک حالت واقعی نیست. بنابراین، نادرست است. حالت سرویس‌گیرنده VTP به سوئیچ اجازه می‌دهد تا به عنوان یک Slave به سرور Master عمل کند.

۲۸) گزینه ۱. پیوند بین سوئیچ (ISL[4])، یک پروتکل اختصاصی است که برای ترانکینگ سوئیچ‌ها استفاده می‌شود. اگر نیاز به اتصال سوئیچ‌های غیر سیسکو به سوئیچ سیسکو دارید، باید از استاندارد IEEE 802.1Q استفاده کنید. VTP یک پروتکل ترانکینگ نیست. برای انطباق و سهولت در پیکربندی، به پرکردن VLANها در سوئیچ‌های سیسکو کمک می‌کند. پروتکل شناسایی سیسکو (CDP[5]) نیز یک پروتکل ترانکینگ نیست و از طریق قابلیت‌های قدرت برقراری ارتباط خود، با دستگاه‌های همسایه مذاکره می‌کند. همچنین امکان کشف همسایگان را فراهم می‌کند، اما CDP اختصاصی سیسکو است، بنابراین فقط با دستگاه‌های سیسکو می‌تواند ارتباط برقرار کند.

۲۹) گزینه ۳. 802.1X اجازه دسترسی انتخابی به شبکه در لایه ۲ را می‌دهد. این امکان را در سوئیچ فراهم می‌کند؛ زیرا سوئیچ به عنوان یک تأییدکننده برای یک سرور AAA عمل می‌کند و فقط پس از احراز هویت کاربر یا دستگاه، اجازه دسترسی را می‌دهد. 802.1Q یک پروتکل ترانکینگ است که برای انتقال چندین VLAN بر روی یک اتصال لایه ۲ استفاده می‌شود و احراز هویت را ارائه نمی‌دهد. لیست کنترل دسترسی (ACL[6]) یک شرط و عبارت عملی است که برای اجازه‌دادن، ردکردن یا ثبت ترافیک استفاده می‌شود. فایروال‌ها حاوی ACL و خط مشی‌هایی برای اجازه‌دادن، ردکردن و ثبت ترافیک هستند، اما معمولاً ترافیک را تأیید نمی‌کنند.

۳۰) گزینه ۲. استاندارد IEEE 802.11a تا ۱۲ کانال بدون همپوشانی یا اگر استاندارد 802.11h را اضافه کنید تا ۲۳ کانال را ارائه می‌دهد. همه پاسخ‌های دیگر نادرست است.

---

[1] neighbor solicitation
[2] neighbor advertisements
[3] Generic Router Encapsulation
[4] Inter-Switch Link
[5] Cisco Discovery Protocol
[6] Access Control List

۳۱) گزینه ۴. استاندارد IEEE 802.11a حداکثر سرعت داده تا ۵۴ مگابیت‌برثانیه را فراهم می‌کند. همه پاسخ‌های دیگر نادرست است.

۳۲) گزینه ۳. VPNهای IPsec سایت‌به‌سایت، مقیاس‌پذیری را به عنوان یک مزیت ارائه می‌دهند. این به این دلیل است که هر اداره راه دور فقط به اتصال اینترنت برای ایجاد یک تونل VPN به اداره اصلی نیاز دارد. هنگام استفاده از VPN، سربار خاصی وجود دارد. بنابراین، پس از استقرار VPNهای IPsec سایت‌به‌سایت ممکن است به پهنای باند بالاتری نیاز باشد. تأخیر، تحت تأثیر قرار می‌گیرد و به دلیل سطح رمزگذاری که هر بسته هنگام عبور از VPN سایت‌به‌سایت باید متحمل شود، بیشتر خواهد بود. پشتیبانی از مولتی‌کست مزیت رایج VPNهای IPsec سایت‌به‌سایت نیست.

۳۳) گزینه ۲. یک کابل رول شده برای ایجاد یک اتصال سریال از رایانه به روتر برای پیکربندی استفاده می‌شود. برای اتصال اترنت از کابل Cat 5e استفاده می‌شود. چیزی به نام کابل PuTTY وجود ندارد، اما PuTTY یک برنامه شبیه‌سازی ترمینال است که با کابل سریال استفاده می‌شود. فیبر تک حالته (SMF[1]) نوعی کابل فیبر نوری است که می‌تواند مسافت‌های طولانی را طی کند.

۳۴) گزینه ۱. پیام Get-Request توسط یک ایستگاه مدیریت شبکه (NMS[2]) برای درخواست اطلاعات از یک عامل SNMP استفاده می‌شود. پیام Get-Response پیامی است که پس از دریافت پیام Get-Request از کلاینت به NMS ارسال می‌شود. پیام Set-Request توسط NMS به سرویس‌گیرنده SNMP ارسال می‌شود و درخواست می‌کند یک شمارنده قابل نوشتن خاص روی مقدار مشخص شده تنظیم شود. پیام‌های Trap از دستگاه شبکه به ایستگاه مدیریت شبکه SNMP ارسال می‌شوند که رویدادی بیش از یک آستانه تعیین‌شده در دستگاه راه‌اندازی شود.

۳۵) گزینه ۳. استاندارد NetFlow اطلاعات جلسه شامل آدرس مبداء و مقصد، برنامه‌ها و حجم ترافیک را ارائه می‌دهد. Syslog روشی برای جمع‌آوری پیام‌های سیستمی برای شناسایی مشکلات است یا می‌توان از آن برای تجزیه‌وتحلیل پس از مرگ (Post-Mortem) استفاده کرد. پروتکل ساده مدیریت شبکه (SNMP[3]) پروتکلی است که برای ثبت آمار عملکرد سرورها، برنامه‌ها و دستگاه‌های شبکه استفاده می‌شود. آنالیزگر پورت سوئیچ (SPAN[4]) برای بازتاب ترافیک پورت استفاده می‌شود.

۳۶) گزینه ۱. یک SLA از دو نه ۳.۶۵ روز در سال از زمان توقف مورد انتظار است. این معادل ۷.۲ ساعت در ماه است که سرویس می‌تواند قطع شود. همه پاسخ‌های دیگر نادرست است.

---

[1] Single-mode fiber
[2] network management station
[3] Simple Network Management Protocol
[4] Switched Port Analyzer

۳۷) گزینه ۲. خط‌مشی رمز عبور، عمر، پیچیدگی، تاریخچه و پیچیدگی رمزهای عبور را در سازمان تعریف می‌کند. خط‌مشی (BYOD) نحوه استفاده از دستگاه‌های شخصی را در سازمان تعریف می‌کند. نرم‌افزار جلوگیری از فقدان داده (DLP) سعی می‌کند از کمبود داده‌ها جلوگیری کند. این کار را با حفظ آگاهی از اقداماتی انجام می‌دهد که می‌تواند و نمی‌توان آن را در رابطه با یک سند انجام داد. یک خط‌مشی استفاده قابل قبول (AUP[1])، استفاده قابل قبول از منابع سازمانی را تعریف می‌کند.

۳۸) گزینه ۱. هدف زمان بازیابی (RTO[2]) مدت زمان لازم برای بازیابی اطلاعات شما به هدف نقطه بازیابی (RPO[3]) است. RPO اندازه‌گیری زمان از یک شکست، فاجعه، یا یک رویداد زیان‌آور قابل مقایسه است. RPOها زمانی اندازه‌گیری می‌شوند که داده‌های شما در فرمت قابل استفاده معمولاً در آخرین نسخه پشتیبان ذخیره شده است. MTBF[4]، میانگین زمان بین خرابی‌ها است. MTTR[5] به معنی میانگین زمانی است که یک فروشنده برای تعمیر خرابی لازم دارد.

۳۹) گزینه ۲. هدف زمان بازیابی (RTO) اندازه‌گیری سرعتی است که می‌توانید از دست‌دادن داده‌ها را با استفاده از پشتیبان‌گیری بازیابی کنید. هدف نقطه بازیابی (RPO) نقطه زمانی است که در صورت وقوع فاجعه می‌توانید به آن بازگردید. چرخش Grandfather-Father-Son (GFS) یک روش سیستماتیک برای بایگانی کردن رسانه‌های پشتیبان است. پنجره پشتیبان‌گیری پنجره زمانی است که در آن می‌توان پشتیبان‌گیری را انجام داد.

۴۰) گزینه ۳. پلت‌فرم به عنوان یک سرویس (PaaS) معمولا توسط توسعه‌دهندگان نرم‌افزار استفاده می‌شود. این یک پلت‌فرم توسعه را فراهم می‌کند که توسعه‌دهنده نرم‌افزار می‌تواند از آن برای ایجاد برنامه‌های کاربردی استفاده کند. نمونه‌ای از آن، یک وب سرور با PHP و MySQL است که در فضای ابری میزبانی می‌شود. نرم‌افزار به عنوان سرویس (SaaS) یک محصول نرم‌افزاری مشابه ایمیل یا نرم‌افزار شبکه‌های اجتماعی است که در آن، از نرم‌افزار ارائه شده به عنوان سرویس استفاده می‌کنید. زیرساخت به عنوان یک سرویس (IaaS) به شما اجازه می‌دهد زیرساخت‌هایی مانند ماشین‌های مجازی (VM)، شبکه‌های مجازی یا حتی DNS را اجاره کنید. بازیابی فاجعه به عنوان یک سرویس (DRaaS[6]) یکی دیگر از سرویس‌های محبوب است. شما می‌توانید فضای ذخیره‌سازی را اجاره کنید و قدرت را محاسبه کنید تا یک سایت بازیابی فاجعه را تسهیل کنید.

---

[1] Acceptable Use Policy
[2] Recovery Time Objective
[3] Recovery Point Objective
[4] Mean Time Between Failures
[5] Mean Time To Repair
[6] Disaster recovery as a service