فهرست محتوای دوره جامع امنیت (مقدماتی)

CompTIA Security+

ساینت: آموزش تخصصی امنیت و شبکه

بهار ۹۹

HTTPS://CYNETCO.COM

۱	مقدمه	۰۲:۴۲
۲	تجهیزات امنیتی زیرساخت	۲۵:۳۷
۳	تجهیزات امنیتی زیرساخت (قسمت دوم)	۰۷:۲۰
۴	جداسازی شبکه با VLAN	۰۹:۲۱
۵	فناوری هایی برای بهبود امنیت	۱۰:۵۱
۶	کاربرد عملی ACL	۱۴:۴۱
۷	اجزاء مورد استفاده در طراحی شبکه امن	۱۵:۵۳
۸	اعمال بهروشها ، چارچوبها و دستورالعملهای امنیتی	۰۴:۲۰
۹	ترجمه IP	۱۱:۴۱
۱۰	متدهای امنیتی فایروال و سوییچ	۱۹:۲۶
۱۱	مروری بر مجازی سازی	۱۰:۱۸
۱۲	تانل امن IP و Portهای شناخته شده	۰۶:۳۸
۱۳	پروتکل ICMP و چند پروتکل دیگر	۰۸:۳۵
۱۴	بررسی و استفاده از پروتکل های ایمن	۰۷:۵۹
۱۵	امنیت شبکه های بیسیم	۲۲:۴۹
۱۶	امنیت موبایلها	۰۶:۲۶
۱۷	تکنولوژی و ابزارهای امنیتی	۱۲:۲۷
۱۸	ریسک	۱۳:۱۸
۱۹	محاسبه ریسک	۱۹:۳۲
۲۰	روشهای حمله، مدیریت ریسک ، ریکاوری	۱۴:۲۲
۲۱	یکپارچه سازی و اتصال به شرکتهای دیگر	۱۱:۰۵
۲۲	مدیریت تغییرات و ممیزی اکانت ها	۱۸:۵۹
۲۳	سیستم جلوگیری از نشت داده ها DLP	۰۹:۲۴
۲۴	جرم شناسی کامپیوتری	۱۶:۱۱
۲۵	پاسخ به رخداد	۱۰:۱۷
۲۶	آگاهی رسانی امنیتی	۰۸:۵۳
۲۷	پسوردها	۱۰:۳۷
۲۸	کنترل های محیطی	۱۰:۲۹
۲۹	امنیت فیزیکی	۰۶:۴۷
۳۰	استمرار کسب و کار	۱۲:۲۹
۳۱	برنامه ریزی برای امنیت	۱۳:۰۹
۳۲	قابلیت تحمل خطا FT	۱۶:۵۹
۳۳	کنترل محرمانگی	۰۸:۳۰

۳۴	یکپارچگی داده ها	۱۶:۵۸
۳۵	دردسترس بودن	۰۴:۱۰
۳۶	بدافزارها: ویروس ، جاسوس افزار ، تبلیغ افزار	۱۶:۰۷
۳۷	بدافزارها: تروجان، بک دور ، باج افزار	۱۴:۱۳
۳۸	انواع حملات : MITM و DDOS و	۱۷:۰۳
۳۹	انواع حملات : سمت کلاینت	۱۳:۰۰
۴۰	حملات پسورد	۱۱:۰۳
۴۱	مهندسی اجتماعی	۱۳:۱۶
۴۲	Vishing	۰۸:۰۳
۴۳	حملات شبکه بیسیم	۰۸:۵۳
۴۴	حملات برنامه ها	۱۴:۲۹
۴۵	حملات برنامه ها (قسمت دوم)	۱۳:۰۷
۴۶	مانیتورینگ و Hardening	۱۴:۱۹
۴۷	دسترسی شبکه و امنیت داده ها	۱۵:۲۵
۴۸	اصول اولیه	۰۷:۲۷
۴۹	آنالایزر و اسکنرها	۱۶:۱۷
۵۰	ابزارهای ارزیابی امنیت	۱۰:۰۱
۵۱	ارزیابی و کشف تهدیدات	۱۰:۱۷
۵۲	تست نفوذ	۱۶:۵۳
۵۳	روشهایی برای امنیت برنامه ها	۰۸:۰۷
۵۴	کنترل های امنیتی برنامه ها	۱۰:۵۴
۵۵	اصول توسعه و استقرار برنامه ها	۰۷:۲۹
۵۶	امنیت تجهیزات موبایل سازمانی	۰۸:۱۲
۵۷	سیاست های امنیتی برای تجهیزات موبایل	۰۴:۴۹
۵۸	مزایای سیاست های امنیتی	۰۸:۴۸
۵۹	امنیت موبایل و پاکسازی خودکار	۰۵:۰۴
۶۰	ملاحضات امنیتی موبایل ها	۰۳:۱۹
۶۱	امنیت Hostهای شبکه	۰۷:۳۲
۶۲	امنیت سخت افزار و مجازی سازی	۰۹:۰۵
۶۳	استراتژی کاهش ریسک	۰۸:۱۵
۶۴	امنیت داده ها	۱۱:۴۹
۶۵	امن سازی داده ها با کنترل های سخت افزاری	۰۸:۳۷
۶۶	امنیت اجزاء مختلف سیستم	۰۸:۲۶

۶۷	امنیت سیستم های کنترل صنعتی SCADA	۰۷:۵۲
۶۸	مفاهیم AAA	۰۶:۵۵
۶۹	سرویسها و پروتکل های احراز هویت	۱۳:۵۳
۷۰	احراز هویت چند عاملی	۱۲:۳۴
۷۱	کنترل احراز هویت	۱۱:۴۴
۷۲	مدیریت و کنترل دسترسی	۰۸:۴۷
۷۳	کنترل دسترسی با اعتبارسنجی	۰۷:۳۵
۷۴	مدیریت اکانتها	۱۷:۳۷
۷۵	رمزنگاری: متقارن و نامتقارن	۱۷:۴۰
۷۶	الزامات رمزنگاری	۱۲:۳۱
۷۷	مدیریت کلیدهای رمزنگاری	۱۸:۴۵
۷۸	Hashing و پروتکل های رمزنگاری	۱۶:۰۰
۷۹	مقایسه روشهای مختلف رمزنگاری	۱۶:۰۳
۸۰	PKI و کاربرد آن در رمزنگاری	۱۵:۲۶
۸۱	PKI و گواهی دیجیتال	۰۶:۵۷
۸۲	دفاع در عمق	۱۰:۲۵
۸۳	انواع حملات	۰۹:۲۱
۸۴	حملات Amplification و متد Salting	۱۰:۲۹
۸۵	اخطارهای گواهی دیجیتال و مدل اعتماد	۰۵:۵۶
۸۶	انواع هکرها	۰۵:۵۸
۸۷	جمع آوری اطلاعات	۲۰:۱۷
۸۸	اصطلاحات مربوط به هک	۰۹:۴۵
۸۹	مفاهیم بدافزار	۰۸:۵۰
۹۰	یک سیستم آلوده	۰۴:۲۸
۹۱	اسکن شبکه	۰۶:۵۱
۹۲	الزام اسکن و مدیریت آسیب پذیری	۰۷:۰۰
۹۳	بررسی تروجان ها و کار عملی	۱۳:۳۸
۹۴	حلات لایه ۲ و port-security	۱۵:۱۰
۹۵	انواع اسکن شبکه	۱۱:۵۰
۹۶	بررسی تست آسیب پذیری	۱۱:۳۴
۹۷	Sniffing	۱۰:۲۱
۹۸	نصب و راه اندازی Nessus	۱۳:۵۳
۹۹	کندی شبکه!!!	۱۳:۱۹

۱۰۰	پایان دوره+مهندسی اجتماعی+ آرزوی موفقیت	۱۱:۴۷