آپا FUM Cert
آزمایشگاه تخصصی رسیدگی به حوادث رایانه‌ای
دانشگاه فردوسی مشهد

فناوری اطلاعات ۰۶۴

برادر گرامی جناب آقای مهندس خلیلی

مدیر محترم فناوری اطلاعات استانداری خراسان رضوی

با سلام و تحیات، بازگشت به نامه شماره ۳۸/۶۲/۲۰۶۹۹ مورخ ۱۳۸۹/۵/۲۶ به استحضار می‌رساند برنامه آزمایشگاه آپا جهت آزمون نفوذپذیری شبکه، پورتال و برنامه‌های کاربردی دستگاههای اجرایی به شرح زیر است:

۱. ارزیابی امنیتی و انجام آزمون نفوذپذیری
۲. ارائه گزارش آزمون نفوذپذیری
۳. رفع آسیب پذیری‌های ارائه‌شده در گزارش توسط سازمان ذیربط
۴. بررسی رفع آسیب پذیری‌ها

لازم به ذکر است که بررسی رفع آسیب پذیری‌ها تنها یک بار توسط آزمایشگاه آپا انجام خواهد شد و در صورت عدم رفع آسیب پذیری‌ها توسط سازمان ذیربط هیچ گونه مسوولیتی متوجه این آزمایشگاه نخواهد بود.

همچنین به پیوست راهنمای انجام آزمون نفوذپذیری شبکه برای اطلاع به سازمان‌های مربوطه ایفاد می‌گردد.

ورود به دبیرخانه استانداری
شماره ثبت: ۵۱۶۱۰
تاریخ ثبت: N 4
۱۳۸۹/۷/۱۴

محسن کلهانی
مدیر آزمایشگاه آپا

نشانی: مشهد، میدان آزادی، دانشگاه فردوسی مشهد، دانشکده مهندسی تلفن و نمابر: ۰۵۱۱-۸۷۸۴۱۷۷
پست الکترونیکی: cert@um.ac.ir وبگاه: http://cert.um.ac.ir

آزمایشگاه تخصصی آپا در حوزه امنیت سرویس‌های شبکه و تجهیزات بی‌سیم

cert@um.ac.ir

راهنمای سریع
آزمون نفوذپذیری شبکه

شهریورماه ۱۳۸۹

شماره سند: APA_FUM_M_PT_0005

آزمون نفوذپذیری شبکه سازمان‌های دولتی و شرکت‌های خصوصی در دو مرحله‌ی آزمون جعبه-سیاه و آزمون جعبه-سفید انجام می‌پذیرد. در ادامه هر یک از آزمون‌های فوق معرفی می‌شوند.

۱- آزمون جعبه-سیاه

در آزمون نفوذپذیری به صورت جعبه-سیاه، گروه آزمون نفوذپذیری از یک نقطه‌ی دسترسی به شبکه متصل گردیده و بدون آگاهی از جزییات سیستم‌ها، سرویس‌ها و شبکه‌ی سازمان مورد نظر و بدون دریافت هیچ‌گونه اطلاعات جانبی در مورد سیاست‌ها، تصمیمات و موارد مشابه، بررسی‌های لازم را در جهت کشف مشکلات امنیتی و نقاط آسیب‌پذیر آغاز می‌نماید. با توجه به این که سطح اختیارات و دسترسی به شبکه از نقاط مختلف متفاوت است، انتخاب نقطه‌ی اتصال به شبکه از نظر فیزیکی و از نظر سطح اختیارات و دسترسی‌ها به عهده‌ی سازمان متقاضی آزمون نفوذپذیری است. بدیهی است که انتخاب مذکور بایستی به شکلی صورت پذیرد که تأمین کننده‌ی نیازمندی‌های ذکر شده در جدول صفحه‌ی بعد باشد.

ردیف	هدف مرحله	بررسی‌ها و آزمون‌ها	نیازمندی‌ها	نتایج مورد انتظار
۱	• آشنایی با معماری و ساختار کلی شبکه • شناسایی محدوده‌های شبکه • کسب اطلاعات متفرقه و جانبی در مورد شبکه، سیستم‌ها و سرویس‌ها	• اتصال به شبکه‌ی داخلی از طریق یک کابل شبکه • اتصال به شبکه‌ی محلی بی‌سیم • بررسی آدرس‌های تخصیص یافته به سیستم‌های مختلف • ردیابی بسته‌های ارسالی به سیستم‌های مختلف • استراق‌سمع اطلاعات انتقالی روی شبکه	• امکان برقراری ارتباط ۲ الی ۵ عدد از سیستم‌های تیم آزمون نفوذپذیری با شبکه‌ی داخلی با تمامی شرایط در نظر گرفته شده برای نقطه‌ی دسترسی آزمون جعبه-سیاه • برقراری کلیه‌ی شرایط کاری عادی طی انجام این مرحله از آزمون از نظر پیکربندی تجهیزات و سیستم‌ها و همچنین اعمال انجام شده توسط کارکنان در وقت اداری	• شرح محدودیت‌های موجود و تشریح کامل شرایط در نظر گرفته شده برای آغاز آزمون نفوذپذیری جعبه-سیاه • فهرست آدرس‌های IP کشف شده • فهرست آدرس‌های فیزیکی کشف شده • حجم کافی از اطلاعات قابل دریافت از طریق استراق‌سمع
۲	• کسب اطلاعات بیشتر در مورد معماری، سطوح دسترسی و سگمنت‌های شبکه • شناسایی سیستم‌های موجود و قابل دسترس • شناسایی تجهیزات شبکه و پروتکل‌های مورد استفاده • شناسایی محدودیت‌های اعمالی احتمالی از سوی تجهیزات و یا دیواره‌های آتش	• تجزیه و تحلیل اطلاعات منتقل شده در شبکه • شناسایی گستره‌های IP موجود در شبکه • شناسایی سیستم‌های موجود در گستره‌های کشف شده • پویش پورت‌های سیستم‌های موجود به دو صورت اتصال کامل و اتصال ناقص و مقایسه نتایج • کشف آدرس فیزیکی سیستم‌های موجود در شبکه جهت شناسایی سخت‌افزارها	• حفظ کلیه‌ی شرایط در نظر گرفته شده برای نقطه‌ی دسترسی آزمون جعبه-سیاه و عدم برقراری هر گونه شرایط خاص و یا ایجاد هر گونه تغییر در معماری شبکه، پیکربندی تجهیزات و سیستم‌ها و اعمال انجام شده توسط کارکنان	• فهرست گستره‌های IP موجود در شبکه • فهرست آدرس‌های IP موجود در هر گستره • فهرست آدرس‌های فیزیکی مرتبط با هر آدرس IP • فهرست VLANها و سگمنت‌های کشف شده • نتایج خام عملیات پویش پورت‌ها

	• شناسایی سرویس‌های احتمالی موجود در شبکه			
۳	• شناسایی سرویس‌دهنده‌ها و سرویس‌های ارائه شده توسط هر یک از آن‌ها • شناسایی برنامه‌های مورد استفاده برای ایجاد و ارائه‌ی سرویس‌ها و نسخه‌های آن‌ها • شناسایی سیستم‌های عامل موجود در شبکه و نسخه‌های آن‌ها	• ارجاع متقابل و تجزیه و تحلیل نتایج پویش پورته نام سیستم‌های موجود در شبکه و سایر اطلاعات دریافتی از مراحل قبل • استفاده از روش‌های شناسایی سیستم‌های عامل برای تمامی سیستم‌ها و تجهیزات موجود در شبکه • جمع‌آوری بنرهای نرم‌افزارهای موجود در پورت‌های باز شناخته شده	• مشابه مرحله‌ی پیشین	• فهرست سرویس‌دهنده‌های موجود در شبکه به همراه آدرس IP، آدرس فیزیکی، سیستم عامل و سرویس‌های ارائه شده • فهرست نرم‌افزارهای سرویس‌دهنده سرویس ارائه شده توسط هر یک بنرها و نسخه‌های آن‌ها • فهرست سیستم‌های عامل موجود در شبکه
٤	• شناسایی بدافزارها • شناسایی آسیب‌پذیری‌های ناشی از عدم پیکربندی صحیح سیستم‌ها • شناسایی آسیب‌پذیری‌های ناشی از عدم به‌روز رسانی سیستم‌ها	• شناسایی پورت‌های باز غیرمعمول روی سیستم‌ها، ارجاع متقابل آن‌ها با فهرست بدافزارهای شناخته شده و تلاش برای کسب اطلاعات بیشتر در مورد این پورت‌ها • استفاده از پویشگرهای خودکار برای بررسی وجود یا عدم وجود آسیب‌پذیری‌های شناخته شده روی سرویس‌دهنده‌ها • استفاده از پویشگرهای خودکار برای پویش گستره‌های شناسایی شده و سیستم‌های موجود در شبکه	• مشابه مرحله‌ی پیشین	• فهرست بدافزارهای موجود روی هر یک از سیستم‌ها • فهرست پورت‌های باز ناشناخته موجود روی هر یک از سیستم‌ها • فهرست آسیب‌پذیری‌های تأیید شده‌ی مرتبط با هر یک از سیستم‌ها

		• تایید آسیب‌پذیری‌های گزارش شده توسط ابزارها و پویشگرها توسط بررسی دستی • تلاش برای شناسایی پیکربندی‌های پیش‌فرض خطرناک		
۵	• کشف کلیه‌ی مشکلات امنیتی ناشی از ضعف در ساختار شبکه • شناسایی مشکلات امنیتی ناشی از عدم پیکربندی صحیح تجهیزات شبکه • شناسایی آسیب‌پذیری‌های موجود در تجهیزات شبکه • شناسایی قابلیت‌های پیاده‌سازی شده توسط تجهیزات شبکه و پروتکل‌های مرتبط با مسیریابی و موارد مشابه	• تجزیه و تحلیل اطلاعات منتقل شده در شبکه • ارجاع متقابل فهرست تجهیزات شبکه‌ی شناسایی شده با نتایج پویش پورت‌ها و فهرست آدرس‌های فیزیکی • تلاش برای انجام حملات سمی‌سازی ARP، جعل آدرس‌های فیزیکی، انجام Firewalking و تغییر مقادیر TTL و موارد مشابه • آزمون تجهیزات شبکه در مقابل دریافت بسته‌های اطلاعاتی مختلفه بسته‌های بسیار کوچک و بسیار بزرگ و موارد مشابه • تلاش برای کسب اطلاعات مرتبط با پروتکل SNMP مانند Community Stringها و غیره با تجزیه و تحلیل نتایج حاصل از انجام حملاتی نظیر حمله‌ی Man-in-the-Middle و استراق‌سمع اطلاعات منتقل شده در شبکه	• مشابه مرحله‌ی پیشین	• فهرست تجهیزات شبکه به همراه آدرس IP و آدرس فیزیکی • شرح مشکلات موجود ناشی از ضعف در معماری شبکه • شرح مشکلات موجود ناشی از پیکربندی نادرست تجهیزات شبکه • فهرست حملات موفق و قابل انجام در شبکه • فهرست آسیب‌پذیری‌های موجود در تجهیزات شبکه به همراه روش‌های رفع آن‌ها

٦	• شناسایی دیوارهای آتش و سیستم‌های تشخیص نفوذ • بررسی خط‌مشی‌های اعمالی توسط دیوارهای آتش • کشف مشکلات امنیتی ناشی از عدم پیکربندی صحیح دیوارهای آتش	• مقایسه نتایج پویش پورت‌ها به دو صورت اتصال کامل و ناقص از خارج و داخل شبکه • تلاش برای کشف دیوارهای آتش احتمالی با تجزیه و تحلیل نتایج مراحل پیشین • شناسایی رفتار شبکه هنگام تغییر پورت‌های مبدأ و مقصد بسته‌های ارسالی از داخل و خارج شبکه • تلاش برای انجام حملاتی از قبیل Fragmentation، SYN-Flooding و برآورد قدرت دیواره‌ی آتش در برابر این حملات	• مشابه مرحله‌ی پیشین	• فهرست دیوارهای آتش کشف شده‌ی احتمالی • فهرست مشکلات موجود در انتخاب و یا پیکربندی دیوارهای آتش • فهرست حملات قابل انجام در شبکه برای دور زدن دیوارهای آتش
۷	• آزمون امنیت شبکه‌ی بی‌سیم	• استراق‌سمع اطلاعات ارسالی در شبکه‌ی بی‌سیم به روش‌های فعال و غیرفعال • شناسایی نقاط دسترسی و شبکه‌های بی‌سیم • شناسایی شبکه‌های قابل دسترس بدون کلید امنیتی • تلاش برای کشف یا شکستن کلیدهای امنیتی به روش‌های Brute Force و حملات واژه‌نامه	• فراهم‌آوردن امکان قرارگیری سیستم اعضای تیم آزمون نفوذپذیری در محدوده‌ی قابل پوشش توسط نقطه یا نقاط دسترسی شبکه‌های بی‌سیم	• فهرست شبکه‌های بی‌سیم موجود • فهرست پیکربندی‌های نالمن کشف شده • فهرست کلیدهای امنیتی ضعیف
۸	• آزمون شبکه و سیستم‌ها در برابر	• حدس و شناسایی نقاط آسیب‌پذیر احتمالی	• توافق با مسئول ذیربط در سازمان متقاضی	• فهرست گلوگاه‌ها و نقاط آسیب‌پذیر

	حملات جلوگیری از سرویس (DoS)	در برابر حملات جلوگیری از سرویس • آزمون نقاط شناسایی شده در برابر حملات جلوگیری از سرویس با توافق مسئول ذیربط در سازمان متقاضی	در مورد انجام یا عدم انجام حملات جلوگیری از سرویس با تحت بار قرار دادن شبکه • عدم ایجاد هرگونه مشکل ارتباطی در حین انجام حملات جلوگیری از سرویس شبیه-سازی شده • سایر موارد مشابه مراحل پیشین	شبکه در برابر حملات جلوگیری از سرویس • نتایج حاصل از انجام حملات جلوگیری از سرویس شبیه‌سازی شده
۹	• بررسی رفتار کارکنان در موارد مرتبط با امنیت اطلاعات • ارزیابی خط‌مشی‌ها و رویه‌کارهای عمومی و فیزیکی به کار گرفته شده برای حفظ امنیت اطلاعات • شناسایی گذرواژه‌های ضعیف	• زیر نظر داشتن رفتار و صحبت‌های میان کارکنان در خصوص موارد مرتبط با امنیت اطلاعات • تهیه‌ی فهرست مشکلات امنیتی کشف شده در مراحل قبل و مرتبط با رفتار عمومی کارکنان • تلاش برای استخراج گذرواژه‌ها یا درهم-سازی شده‌ی آن‌ها از طریق پرونده‌های قابل استخراج و یا نتایج استراق‌سمع • انجام حملات واژه‌نامه و بررسی استفاده‌ی احتمالی از گذرواژه‌های ساده و ضعیف در سراسر سیستم‌ها	• فراهم‌آوردن امکان تعامل کافی اعضای تیم آزمون نفوذپذیری با کارکنان • فراهم‌آوردن امکان تردد اعضای تیم آزمون نفوذپذیری در سطح مجاز تعریف شده برای کارکنان عادی	• تشریح محدودیت‌های موجود برای تردد و تعامل اعضای تیم نفوذپذیری با کارکنان • شرح خط‌مشی‌های کلی، موارد عمومی و فیزیکی خطرناک مشاهده شده توسط اعضای تیم آزمون نفوذپذیری • فهرست گذرواژه‌های ضعیف

۲- آزمون جعبه-سفید

در آزمون جعبه-سفید، تیم آزمون نفوذپذیری با آگاهی کامل از ساختار و معماری شبکه و با دسترسی کامل به سیستم‌ها و تجهیزات شبکه اقدام به بررسی مشکلات امنیتی موجود می‌نماید. بر اساس صلاح‌دید تیم آزمون نفوذپذیری، ترتیب انجام مراحل در این آزمون متغیر است.

ردیف	هدف	نیازمندی‌ها و دسترسی‌های لازم	نتایج مورد انتظار
۱	• بررسی رعایت نکات امنیتی در طراحی ساختار و معماری شبکه	• دسترسی به مستندات مرتبط با طراحی شبکه و ساختار آن شامل فهرست بخش‌هاو تجهیزات مورد استفاده و موارد مشابه	• فهرست ضعف‌های امنیتی موجود در معماری و طراحی شبکه
۲	• بررسی امنیت پیکربندی تجهیزات شبکه	• دسترسی کامل به تجهیزات شبکه شامل سوییچ‌ها، مسیریاب‌ها، دیواره‌های آتش و غیره برای بررسی پیکربندی آن‌ها	• فهرست مشکلات موجود در پیکربندی تجهیزات شبکه
۳	• بررسی امنیت سرویس‌های شبکه	• دسترسی به فهرست سرویس-دهنده‌های موجود در شبکه به همراه سیستم عامل و نسخه‌ی آن • دسترسی به فهرست سرویس‌های ارائه شده در شبکه به همراه نرم-افزارهای مورد استفاده و نسخه‌های آن‌ها • دسترسی به حساب مدیریتی سرویس‌دهنده‌ها و امکان بررسی پیکربندی سرویس‌دهنده‌ها و سایر نرم‌افزارهای مرتبط با سرویس‌های شبکه	• فهرست نسخه‌های قدیمی سیستم عامل‌ها و سایر نرم‌افزارهایی که احتیاج به به‌روز رسانی دارند • فهرست مشکلات موجود در پیکربندی سرویس‌دهنده‌ها و نرم‌افزارهای مرتبط با سرویس‌های شبکه اعم از مشکلات ناشی از عدم پیکربندی مناسب، آسیب-پذیری‌ها و غیره
٤	• بررسی امنیت سیستم‌های شبکه	• دسترسی به حساب مدیریتی سیستم‌ها و دامنه‌های موجود در	• فهرست آسیب‌پذیری‌های موجود در سیستم‌ها و سرویس‌دهنده‌ها

		شبکه با سطح اختیارات مورد نیاز • دسترسی به فهرست نرم‌افزارهای دیواره‌ی آتش، ضد ویروس و موارد مشابه و همچنین پیکربندی آن‌ها • امکان اجرای ابزارها و نرم‌افزارهای لازم روی برخی از سیستم‌های موجود در شبکه	• فهرست مشکلات امنیتی ناشی از عدم پیکربندی صحیح سیستم‌ها
۵	• بررسی امنیت خط‌مشی‌های عمومی و موارد مرتبط با عملکرد کارکنان	• امکان تعامل اعضای تیم آزمون نفوذپذیری با مسئولان ذیربط در سازمان متقاضی برای آگاهی از روندهای کاری و خط‌مشی‌های موجود در سازمان	• شرح خط‌مشی‌ها، عملکردها و سایر موضوعات عمومی که به جهت مشکلات امنیتی نیازمند تجدید نظر هستند