



# تست نفوذ سیستم های کنترل صنعتی

راهنمای هکرهای قانونمند برای تجزیه و تحلیل، کاهش مخاطرات و ایمن سازی فرایندهای صنعتی

نویسنده:

پل اسمیت

مترجمان:

پیام حاتم زاده (کارشناس و مدرس امنیت شبکه و سامانه های کنترل صنعتی)

آرش تابع (مشاور، مدرس و کارشناس ارشد امنیت شبکه و سامانه های کنترل صنعتی)

کمیل صمدی (مشاور، مدرس و کارشناس ارشد امنیت شبکه و سامانه های کنترل صنعتی)

محمد حسام تدین (عضو هیات علمی پژوهشگاه ارتباطات و فناوری اطلاعات)



انتشارات آوای قلم

سرشناسه	: اسمیت، پل Smith, Paul
عنوان و نام پدیدآور	: تست نفوذ سیستم‌های کنترل صنعتی: راهنمای هکرهای قانونمند برای تجزیه و تحلیل کاهش مخاطرات و ایمن‌سازی فرایندهای صنعتی/نویسنده پل اسمیت؛ مترجمان پیام حاتم‌زاده...[و دیگران].
مشخصات نشر	: تهران: آوای قلم، ۱۴۰۲. مشخصات ظاهری: ۴۲۰ص.
شابک	: ۹۷۸-۶۲۲-۷۶۵۲-۹۵-۶
یادداشت	: وضعیت فهرست نویسی: فیپا
یادداشت	: عنوان اصلی: Pentesting industrial control systems : an ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes,2021.
عنوان دیگر	: مترجمان پیام حاتم‌زاده ، آرش تابع ، کمیل صمدی ، محمدحسام تدین.
موضوع	: راهنمای هکرهای قانونمند برای تجزیه و تحلیل کاهش مخاطرات و ایمن‌سازی فرایندهای صنعتی. آزمایش نفوذ ( ایمن‌سازی کامپیوتر) (Penetration testing (Computer security صنعت -- تدابیر ایمنی Industries -- Security measures شبکه‌های کامپیوتری -- تدابیر ایمنی Computer networks -- Security measures
شناسه افزوده	: حاتم‌زاده، پیام، ۱۳۶۴-
رده بندی کنگره	: QA۷۶/۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۹۴۰۶۲۷۶

### نام کتاب: تست نفوذ سیستم‌های کنترل صنعتی

راهنمای هکرهای قانونمند برای تجزیه و تحلیل، کاهش مخاطرات و ایمن‌سازی فرایندهای صنعتی

نویسنده:	پل اسمیت	نوبت چاپ:	اول
مترجمان:	پیام حاتم‌زاده- آرش تابع	تاریخ نشر:	۱۴۰۲
ناشر:	انتشارات آوای قلم	شمارگان:	۱۰۰ جلد
طراحی جلد:	انتشارات آوای قلم(مهران خانی)	قیمت:	۳۹۰۰۰۰ تومان
صفحه آرای:	انتشارات آوای قلم(فاطمه دشتی)		

شماره تماس: ۰۴-۶۶۵۹۱۵-۶۶۵۹۱۵۰۵ همراه: ۰۹۲۱۲۰۵۷۷۵۱

فروشگاه کتاب چاپی و الکترونیکی: [www.avapublisher.com](http://www.avapublisher.com)

این کتاب تحت داوری و حمایت مالی پژوهشگاه ارتباطات و فناوری اطلاعات به چاپ رسیده است

هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع و شرعاً حرام است.  
متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

## فهرست مطالب

صفحه	عنوان
۳۰	پیشگفتار
<b>بخش ۱: راه اندازی آزمایشگاه</b>	
۳۶	فصل ۱: استفاده از مجازی سازی
۳۷	الزامات فنی
۳۷	مجازی سازی چیست؟
۳۹	VMware چیست؟
۴۲	روشن کردن همه چیز
۶۳	راه اندازی شبکه آزمایشگاه مجازی
۷۲	فصل ۲: اتصال به سخت افزار فیزیکی
۷۳	الزامات فنی
۷۳	نصب نرم افزار Click
۸۲	راه اندازی Koyo Click
۸۷	پیگیری ارتباطات
۱۰۳	فصل ۳: راه اندازی آزمایشگاه
۱۰۴	الزامات فنی
۱۰۴	نوشتن و بارگیری اولین برنامه
۱۱۹	بازنویسی و اتصال ورودی/خروجی
۱۲۸	کنترل و تست
<b>بخش ۲: جمع آوری داده ها</b>	
۱۳۶	فصل ۴: نیجا منبع باز
۱۳۷	الزامات فنی
۱۳۷	درک Google-Fu
۱۴۰	جستجو در لینکدین
۱۴۳	Shodan.io
۱۴۹	بررسی پایگاه داده اکسپلویت ( exploit-db )

۱۵۲	..... پایگاه ملی آسیب‌پذیری NVD
۱۵۶	..... فصل ۵: نظارت ترافیک شبکه
۱۵۷	..... الزامات فنی
۱۵۷	..... نصب وایرشارک
۱۵۹	..... SPAN چیست و چگونه می‌توانیم آن را پیکربندی کنیم؟
۱۶۵	..... استفاده از TAP
۱۷۰	..... نظارت بر امنیت IDS
۱۷۵	..... فصل ۶: تحلیل عمیق پکت‌ها
۱۷۶	..... الزامات فنی
۱۷۶	..... بسته‌ها چگونه تشکیل می‌شوند؟
۱۸۳	..... ضبط بسته‌ها از روی رسانه
۱۸۹	..... تجزیه و تحلیل بسته‌ها برای اطلاعات کلیدی

### بخش ۳: من یک دزد دریایی هستم، صدای من را بشنو

۲۰۴	..... فصل ۷: اسکن
۲۰۵	..... الزامات فنی
۲۰۵	..... نصب و پیکربندی Ignition SCADA
۲۱۶	..... مقدمه‌ای بر NMAP
۲۲۰	..... اسکن پورت با RustScan
۲۲۱	..... نصب RustScan
۲۲۶	..... معرفی Gobuster
۲۲۷	..... نصب Gobuster
۲۲۸	..... فهرست کلمات
۲۳۱	..... تشخیص فایل
۲۳۱	..... اسکن وب اپلیکیشن با feroxbuster
۲۳۵	..... فصل ۸: پروتکل
۲۳۶	..... الزامات فنی
۲۳۶	..... پروتکل‌های صنعتی

۲۳۸	..... Modbus
۲۴۸	..... Ethernet/IP
۲۵۰	..... ایجاد سرور EthernetIP
۲۶۷	..... فصل ۹: نینجا
۲۶۸	..... الزامات فنی
۲۶۸	..... نصب FoxyProxy
۲۷۲	..... اجرای BurpSuite
۲۹۰	..... ساخت یک اسکریپت برای پروت فورس SCADA
۳۰۰	..... فصل ۱۰: من می توانم آن را انجام دهم ..
۳۰۱	..... الزامات فنی
۳۰۱	..... نصب عناصر محیطی سازمان
۳۰۳	..... نصب و پیکربندی دامین کنترلر
۳۱۴	..... افزودن و نصب سرور DNS
۳۱۸	..... افزودن و نصب سرور DHCP
۳۲۲	..... راه اندازی اشتراک فایل در شبکه
۳۲۳	..... پیکربندی Kerberos
۳۲۴	..... نصب و پیکربندی ایستگاه های کاری
۳۲۹	..... ابزارهای کالی لینوکس
۳۳۰	..... کشف و راه اندازی حملات
۳۳۷	..... گرفتن شل
۳۴۲	..... فصل ۱۱: من باید به عمق بروم ..
۳۴۳	..... الزامات فنی
۳۴۳	..... پیکربندی فایروال
۳۵۷	..... من یک شل دارم، حالا چی؟
۳۶۴	..... افزایش دسترسی
۳۶۸	..... اسکریپت های عالی جهت افزایش دسترسی ها در ویندوز
۳۷۰	..... pivoting

۳۷۳	.....Proxychains
۳۷۴	.....تونل SSH و پورت فورواردینگ
۳۷۶	.....Chisel

#### بخش ۴: تسخیر پرچم‌ها و خاموش کردن چراغ‌ها

۳۸۰	.....فصل ۱۲: من آینده را می‌بینم
۳۸۱	.....الزامات فنی
۳۸۱	.....تنظیمات آزمایشگاهی اضافی
۳۸۶	.....اتصال LDAP
۳۹۲	.....راه‌اندازی PHP
۳۹۴	.....کنترل رابط کاربری
۳۹۸	.....دسترسی به اسکریپت
۴۰۳	.....فصل ۱۳: متعجب اما با پشیمانی
۴۰۴	.....الزامات فنی
۴۰۴	.....تهیه گزارش تست نفوذ
۴۱۲	.....بستن شکاف امنیتی

## فهرست تصاویر

صفحه	عنوان
۴۱	شکل ۱-۱-۱- زیرساخت Vmware
۴۴	شکل ۱-۲-۱- لیست بارگیری Hypervisor
۴۵	شکل ۱-۳-۱- بررسی یکپارچگی فایل از طریق چکیده
۴۶	شکل ۱-۴-۱- جمع کنترلی SHA-1
۴۶	شکل ۱-۵-۱- انتخاب فایل برای ساخت USB راه‌انداز
۴۷	شکل ۱-۶-۱- هشدار پاک شدن جدول پارتیشن
۴۷	شکل ۱-۷-۱- پاکسازی USB
۴۸	شکل ۱-۸-۱- ورود به سیستم VMware ESXi
۴۸	شکل ۱-۹-۱- داشبورد VMware ESXi
۵۰	شکل ۱-۱۰-۱- بارگیری نرم‌افزار اوبونتو
۵۱	شکل ۱-۱۱-۱- ذخیره‌سازی داده‌ها
۵۱	شکل ۱-۱۲-۱- مرورگر مخزن داده
۵۲	شکل ۱-۱۳-۱- ایجاد یک شاخه جدید
۵۲	شکل ۱-۱۴-۱- بارگذاری در حال انجام است
۵۲	شکل ۱-۱۵-۱- ISO بارگذاری شده
۵۳	شکل ۱-۱۶-۱- داشبورد ماشین‌های مجازی
۵۳	شکل ۱-۱۷-۱- ایجاد یک ماشین مجازی
۵۴	شکل ۱-۱۸-۱- انتخاب سازگاری
۵۴	شکل ۱-۱۹-۱- محل ذخیره‌سازی را انتخاب کنید
۵۵	شکل ۱-۲۰-۱- سفارشی کردن تنظیمات
۵۶	شکل ۱-۲۱-۱- ماشین مجازی PLC
۵۶	شکل ۱-۲۲-۱- روشن کردن ماشین مجازی
۵۷	شکل ۱-۲۳-۱- صفحه ورود به سیستم PLC VM
۶۰	شکل ۱-۲۴-۱- ماشین مجازی ویندوز ۷
۶۱	شکل ۱-۲۵-۱- پیکربندی کالی لینوکس

شکل ۱-۲۶ - انتخاب نرم افزار	۶۱
شکل ۱-۲۷ - صفحه ورود به سیستم کالی لینوکس	۶۲
شکل ۱-۲۸ - ماشین های مجازی	۶۳
شکل ۱-۲۹ - داشبورد شبکه	۶۴
شکل ۱-۳۰ - پیکربندی سوئیچ مجازی	۶۵
شکل ۱-۳۱ - پیکربندی گروه پورت	۶۶
شکل ۱-۳۲ - داشبورد Port Groups	۶۶
شکل ۱-۳۳ - انتخاب گروه های پورت	۶۷
شکل ۱-۳۴ - تنظیمات شبکه	۶۷
شکل ۱-۳۵ - کارت شبکه سیمی	۶۸
شکل ۱-۳۶ - بررسی آدرس شبکه	۶۹
شکل ۱-۳۷ - پیکربندی دستی IP اوبونتو	۶۹
شکل ۱-۳۸ - پیکربندی دستی IP ویندوز ۷	۷۰
شکل ۱-۳۹ - بررسی ارتباط بین ماشین های مجازی	۷۱
شکل ۲-۱ - بارگیری نرم افزار را کلیک کنید	۷۴
شکل ۲-۲ - تأیید پست الکترونیک	۷۴
شکل ۲-۳ - راه اندازی وب سرور python3	۷۵
شکل ۲-۴ - کد پاسخ برای وضعیت موفقیت	۷۵
شکل ۲-۵ - فهرست دایرکتوری سرور HTTP پایتون	۷۵
شکل ۲-۶ - سی دی Koyo Click	۷۶
شکل ۲-۷ - نرم افزار کلیک را نصب کنید	۷۶
شکل ۲-۸ - تأیید اعتبار نصب UAC را بپذیرید	۷۶
شکل ۲-۹ - نرم افزار برنامه نویسی CLICK	۷۷
شکل ۲-۱۰ - روی InstallShield کلیک کنید	۷۷
شکل ۲-۱۱ - بررسی آنتی ویروس	۷۸
شکل ۲-۱۲ - موافقت نامه مجوز	۷۸
شکل ۲-۱۳ - پیکربندی اطلاعات مشتری	۷۹



شکل ۲-۱۴	مکان مقصد را انتخاب کنید	۷۹
شکل ۲-۱۵	برنامه را نصب کنید	۸۰
شکل ۲-۱۶	یک میان‌بر در دسکتاپ ایجاد کنید	۸۰
شکل ۲-۱۷	نصب را تمام کنید	۸۱
شکل ۲-۱۸	روی نماد نرم‌افزار برنامه‌نویسی کلیک کنید	۸۱
شکل ۲-۱۹	شروع یک پروژه جدید	۸۲
شکل ۲-۲۰	منبع تغذیه CO-01AC	۸۳
شکل ۲-۲۱	کنترل‌کننده	۸۴
شکل ۲-۲۲	دسترسی فایروال	۸۵
شکل ۲-۲۳	اتصال به PLC	۸۶
شکل ۲-۲۴	اجازه دسترسی فایروال	۸۶
شکل ۲-۲۵	خطای تطبیق زیر شبکه	۸۷
شکل ۲-۲۶	رابط شبکه ویندوز را پیکربندی کنید	۸۸
شکل ۲-۲۷	پروژه از قبل موجود در داخل PLC	۸۹
شکل ۲-۲۸	فایل پروژه را بخوانید	۹۰
شکل ۲-۲۹	راه‌اندازی پورت Com	۹۰
شکل ۲-۳۰	تنظیم پورت COM روی Koyo CLICK	۹۱
شکل ۲-۳۱	جزئیات راه‌اندازی پورت Com	۹۱
شکل ۲-۳۲	آدرس IP را تنظیم کنید	۹۲
شکل ۲-۳۳	پروژه را در PLC بنویسید	۹۳
شکل ۲-۳۴	خطای نحوی	۹۳
شکل ۲-۳۵	پنجره اشکال‌زدایی	۹۴
شکل ۲-۳۶	مشاهده انتخاب	۹۴
شکل ۲-۳۷	فهرست دستورالعمل	۹۴
شکل ۲-۳۸	منطق نردبان	۹۵
شکل ۲-۳۹	جایگزینی دستورالعمل	۹۵
شکل ۲-۴۰	جزئیات پروژه را تنظیم کنید	۹۶

۹۶	شکل ۲-۴۱- تأیید به روزرسانی
۹۷	شکل ۲-۴۲- جزئیات پروژه را بنویسید
۹۷	شکل ۲-۴۳- انتقال کامل شد
۹۸	شکل ۲-۴۴- اتصال PLC
۹۸	شکل ۲-۴۵- توپولوژی vSwitch
۹۹	شکل ۲-۴۶- تست اتصال پینگ
۹۹	شکل ۲-۴۷- افزودن Uplink
۹۹	شکل ۲-۴۸- PLC فیزیکی را به سوئیچ مجازی وصل کنید
۱۰۰	شکل ۲-۴۹- توپولوژی vSwitch با اتصال فیزیکی
۱۰۰	شکل ۲-۵۰- تست اتصال
۱۰۱	شکل ۲-۵۱- اتصال به PLC
۱۰۵	شکل ۳-۱- نرم افزار Koyo Click
۱۰۵	شکل ۳-۲- پروژه جدید
۱۰۶	شکل ۳-۳- شروع یک پروژه جدید
۱۰۶	شکل ۳-۴- انتخاب یک CPU آزمایشگاهی
۱۰۷	شکل ۳-۵- برنامه اصلی
۱۰۷	شکل ۳-۶- پیکربندی سیستم
۱۰۸	شکل ۳-۷- پنجره پیکربندی سیستم
۱۰۸	شکل ۳-۸- پنجره انتخاب منبع تغذیه
۱۰۹	شکل ۳-۹- پنجره به روز شده از پیکربندی سیستم
۱۱۰	شکل ۳-۱۰- قرار دادن یک مخاطب
۱۱۱	شکل ۳-۱۱- انتخاب گر آدرس
۱۱۱	شکل ۳-۱۲- آدرس انتخاب شده است
۱۱۱	شکل ۳-۱۳- تماس با X001
۱۱۲	شکل ۳-۱۴- خروجی کوپل
۱۱۲	شکل ۳-۱۵- خروجی
۱۱۳	شکل ۳-۱۶- آدرس کوپل

۱۱۳	شکل ۳-۱۷- انتخاب‌گر آدرس
۱۱۴	شکل ۳-۱۸- آدرس حافظه بی‌تی
۱۱۴	شکل ۳-۱۹- خروجی کوئل
۱۱۵	شکل ۳-۲۰- پین‌های ترمینال
۱۱۵	شکل ۳-۲۱- اضافه کردن یک تابع END
۱۱۶	شکل ۳-۲۲- بررسی نحو
۱۱۶	شکل ۳-۲۳- بررسی نحو
۱۱۷	شکل ۳-۲۴- نوشتن پروژه در PLC
۱۱۷	شکل ۳-۲۵- نوشتن پروژه در پنجره PLC
۱۱۸	شکل ۳-۲۶- انتقال کامل شد
۱۱۸	شکل ۳-۲۷- پنجره حالت‌های PLC
۱۱۹	شکل ۳-۲۸- نشانگرهای در حال اجرا
۱۲۰	شکل ۳-۲۹- انتخاب View Data
۱۲۰	شکل ۳-۳۰- ابزار مشاهده داده‌ها
۱۲۱	شکل ۳-۳۱- انتخاب‌گر آدرس
۱۲۱	شکل ۳-۳۲- آدرس X001 انتخاب شده است
۱۲۲	شکل ۳-۳۳- لغو
۱۲۳	شکل ۳-۳۴- لغو درگیر است
۱۲۳	شکل ۳-۳۵- کوئل برق‌دار
۱۲۴	شکل ۳-۳۶- Status Monitor
۱۲۴	شکل ۳-۳۷- ورودی خاموش است
۱۲۵	شکل ۳-۳۸- سوئیچ انتخاب‌گر
۱۲۵	شکل ۳-۳۹- نمودار سیمی
۱۲۶	شکل ۳-۴۰- سیم فیزیکی
۱۲۷	شکل ۳-۴۱- برج لامپ صنعتی
۱۲۷	شکل ۳-۴۲- سیم‌کشی خروجی به برج لامپ
۱۲۸	شکل ۳-۴۳- برنامه با سیم‌کشی چهار چراغ

۱۲۹.....	شکل ۳-۴۴- Data View
۱۲۹.....	شکل ۳-۴۵- نمای داده
۱۳۰.....	شکل ۳-۴۶- بازنویسی لامپ
۱۳۱.....	شکل ۳-۴۷- SCADA VM
۱۳۱.....	شکل ۳-۴۸- ابزار mbtget
۱۳۲.....	شکل ۳-۴۹- خروجی خواندن آدرس صفر
۱۳۳.....	شکل ۳-۵۰- نوشتن مقدار روی کویل
۱۳۳.....	شکل ۳-۵۱- خواندن آدرس کویل ۰
۱۳۸.....	شکل ۴-۱- GHDB
۱۳۸.....	شکل ۴-۲- جستجوی پیشرفته
۱۳۹.....	شکل ۴-۳- تابع پیچیده تر
۱۴۱.....	شکل ۴-۴- جستجوی شرکت
۱۴۲.....	شکل ۴-۵- جستجوی فرعی SCADA
۱۴۲.....	شکل ۴-۶- مجموعه مهارت های Telvent
۱۴۳.....	شکل ۴-۷- اطلاعات عمومی در مورد سیستم ها
۱۴۴.....	شکل ۴-۸- موتور جستجوی Shodan.io
۱۴۴.....	شکل ۴-۹- کاوش در Shodan.io
۱۴۵.....	شکل ۴-۱۰- سیستم های کنترل صنعتی
۱۴۵.....	شکل ۴-۱۱- پروتکل های عمومی
۱۴۷.....	شکل ۴-۱۲- DNP3 کشف شد
۱۴۸.....	شکل ۴-۱۳- Koyo CLICK را وارد کنید
۱۴۹.....	شکل ۴-۱۴- ExploitDB
۱۵۰.....	شکل ۴-۱۵- آسیب پذیری های SCADA
۱۵۱.....	شکل ۴-۱۶- بهره برداری راکول
۱۵۱.....	شکل ۴-۱۷- بهره برداری Rockwell SCADA
۱۵۲.....	شکل ۴-۱۸- NVD
۱۵۲.....	شکل ۴-۱۹- NVD CVE 2016-2279

۱۵۳	شکل ۴-۲۰- جزئیات CVE-2016-2279
۱۵۳	شکل ۴-۲۱- آسیب پذیری های راکول
۱۵۸	شکل ۵-۱- رابط های شبکه در وایر شارک
۱۶۰	شکل ۵-۲- ترافیک SPAN
۱۶۱	شکل ۵-۳- صفحه تنظیمات پورت
۱۶۲	شکل ۵-۴- صفحه آینه پورت
۱۶۲	شکل ۵-۵- Port Mirror را فعال کنید
۱۶۳	شکل ۵-۶- درگاه ۲ منعکس شده است
۱۶۳	شکل ۵-۷- پورت آینه پورت ۲ را تأیید کنید
۱۶۳	شکل ۵-۸- انتخاب رابط
۱۶۴	شکل ۵-۹- وایر شارک
۱۶۴	شکل ۵-۱۰- دستور Tcpdump
۱۶۵	شکل ۵-۱۱- خروجی Tcpdump
۱۶۷	شکل ۵-۱۲- پرتاب ستاره LAN TAP
۱۶۷	شکل ۵-۱۳- LAN TAP
۱۶۸	شکل ۵-۱۴- گرفتن بسته Tshark
۱۶۹	شکل ۵-۱۵- Packet Squirrel
۱۷۱	شکل ۵-۱۶- IDS
۱۷۷	شکل ۶-۱- مدل OSI
۱۷۹	شکل ۶-۲- یک بسته IPv4
۱۸۰	شکل ۶-۳- صفحه جزئیات بسته
۱۸۰	شکل ۶-۴- لایه اترنت
۱۸۱	شکل ۶-۵- لایه شبکه
۱۸۲	شکل ۶-۶- لایه انتقال
۱۸۲	شکل ۶-۷- لایه کاربرد
۱۸۲	شکل ۶-۸- صفحه بایت های بسته
۱۸۴	شکل ۶-۹- رابط Capture

شکل ۱۰-۶- ارتباط بین PLC و ایستگاه کاری	۱۸۶
شکل ۱۱-۶- فیلتر نمایش	۱۸۶
شکل ۱۲-۶- فیلتر نمایش http.authbasic	۱۹۰
شکل ۱۳-۶- CyberChef From Base64	۱۹۱
شکل ۱۴-۶- کمک بصری دسترسی HTTP	۱۹۲
شکل ۱۵-۶- درخواست‌های POST	۱۹۲
شکل ۱۶-۶- ستون اطلاعات	۱۹۳
شکل ۱۷-۶- درخواست POST /goform/svLogin	۱۹۳
شکل ۱۸-۶- فیلد کوکی	۱۹۴
شکل ۱۹-۶- شناسه چکیده	۱۹۵
شکل ۲۰-۶- crackstation.net MD5	۱۹۵
شکل ۲۱-۶- رمزهای عبور CrackStation پیدا شد	۱۹۶
شکل ۲۲-۶- دنبال کردن   جریان HTTP	۱۹۷
شکل ۲۳-۶- تغییر مسیر 302HTTP	۱۹۷
شکل ۲۴-۶- HTTP 200 OK	۱۹۸
شکل ۲۵-۶- تشخیص داده‌های HTTP	۱۹۸
شکل ۲۶-۶- ترافیک FTP	۱۹۹
شکل ۲۷-۶- دوربین شبکه 206AXIS	۱۹۹
شکل ۲۸-۶- پایگاه داده exploit-db	۲۰۰
شکل ۲۹-۶- سرور HTTP به دوربین شبکه AXIS	۲۰۰
شکل ۱-۷- نصب کننده	۲۰۵
شکل ۲-۷- محل نصب	۲۰۶
شکل ۳-۷- نصب معمولی	۲۰۶
شکل ۴-۷- نسخه‌های Ignition	۲۰۷
شکل ۵-۷- ایجاد یک کاربر	۲۰۷
شکل ۶-۷- پورت‌ها را پیکربندی کنید	۲۰۸
شکل ۷-۷- Start Gateway	۲۰۸

شکل ۷-۸- شروع سریع را فعال کنید	۲۰۹
شکل ۷-۹- ورود	۲۰۹
شکل ۷-۱۰- وضعیت	۲۱۰
شکل ۷-۱۱- دستگاه‌ها	۲۱۰
شکل ۷-۱۲- داشبورد دستگاه‌ها	۲۱۱
شکل ۷-۱۳- ایجاد دستگاه جدید	۲۱۱
شکل ۷-۱۴- Modbus TCP	۲۱۲
شکل ۷-۱۵- پیکربندی PLC	۲۱۲
شکل ۷-۱۶- آدرس‌دهی مبتنی بر صفر	۲۱۳
شکل ۷-۱۷- PLC متصل	۲۱۳
شکل ۷-۱۸- آدرس‌ها	۲۱۳
شکل ۷-۱۹- پیکربندی آدرس	۲۱۴
شکل ۷-۲۰- OPC Quick Client	۲۱۴
شکل ۷-۲۱- نگاشت برچسب OPC	۲۱۵
شکل ۷-۲۲- واسط شبکه دوم	۲۱۷
شکل ۷-۲۳- اسکن زیر شبکه	۲۱۸
شکل ۷-۲۴- اسکن ویندوز	۲۱۸
شکل ۷-۲۵- اسکن تهاجمی	۲۱۹
شکل ۷-۲۶- بسته‌های RustScan	۲۲۱
شکل ۷-۲۷- نصب RustScan	۲۲۲
شکل ۷-۲۸- راهنمای RustScan	۲۲۲
شکل ۷-۲۹- RustScan - ویندوز	۲۲۳
شکل ۷-۳۰- NMAP -A scan - RustScan	۲۲۴
شکل ۷-۳۱- سرویس‌های در حال اجرا	۲۲۴
شکل ۷-۳۲- اسکرپت modbus-discover	۲۲۵
شکل ۷-۳۳- modbus-discover SID	۲۲۶
شکل ۷-۳۴- Gobuster Help	۲۲۸

۲۳۰	..... Gobuster enumeration -۳۵-۷ شکل
۲۳۰	..... web enumeration -۳۶-۷ شکل
۲۳۲	.....feroxbuster -۳۷-۷ شکل
۲۳۳	..... Ferox اسکن SCADA جرقه‌زنی -۳۸-۷ شکل
۲۴۰	..... pymodbus سرور -۱-۸ شکل
۲۴۱	..... Modbus registers 10 -۲-۸ شکل
۲۴۱	..... ESXi vSwitch -۳-۸ شکل
۲۴۱	..... promiscuous حالت -۴-۸ شکل
۲۴۲	..... تنظیمات سوئیچ را ویرایش کنید -۵-۸ شکل
۲۴۳	..... Modbus گرفتن -۶-۸ شکل
۲۴۳	.....Decode As... -۷-۸ شکل
۲۴۴	..... TCP Modbus 5020 پورت -۸-۸ شکل
۲۴۴	..... Modbus درخواست -۹-۸ شکل
۲۴۵	..... Modbus پاسخ -۱۰-۸ شکل
۲۴۵	..... bit write ok -۱۱-۸ شکل
۲۴۵	..... Write Single Coil -۱۲-۸ شکل
۲۴۶	..... آدرس ۱ خاموش است -۱۳-۸ شکل
۲۴۶	..... آدرس پاسخ Modbus، 10 است -۱۴-۸ شکل
۲۴۷	..... Koyo CLICK خواندن mbtget -۱۵-۸ شکل
۲۵۰	..... enip پوشه -۱۶-۸ شکل
۲۵۱	..... سرور cpppo در حال اجرا است -۱۷-۸ شکل
۲۵۱	..... cpppo پاسخ -۱۸-۸ شکل
۲۵۲	..... Identity شی -۱۹-۸ شکل
۲۵۲	..... Success: Identity – Get Attributes All -۲۰-۸ شکل
۲۵۲	..... Identity جزئیات -۲۱-۸ شکل
۲۵۳	..... Koyo CLICK تنظیم -۲۲-۸ شکل
۲۵۴	..... Ethernet/IP راه‌اندازی آداپتور -۲۳-۸ شکل



۲۵۵	شکل ۸-۲۴- بلوک‌های داده ورودی
۲۵۵	شکل ۸-۲۵- انتخاب آدرس XD
۲۵۶	شکل ۸-۲۶- مجموعه آدرس بلوک ۱ ورودی XD
۲۵۶	شکل ۸-۲۷- مجموعه آدرس بلوک ۱ خروجی YD
۲۵۷	شکل ۸-۲۸- IP identity/Koyo CLICK Ethernet
۲۵۷	شکل ۸-۲۹- ضبط وایرشارک از Koyo CLICK ENIP
۲۵۹	شکل ۸-۳۰- برچسب Compressor_StationA
۲۵۹	شکل ۸-۳۱- Single attribute value
۲۵۹	شکل ۸-۳۲- تنظیم ویژگی
۲۶۰	شکل ۸-۳۳- Tag alias Get/Set attribute
۲۶۰	شکل ۸-۳۴- ورودی Class/Instance/Attribute
۲۶۱	شکل ۸-۳۵- خروجی Class/Instance/Attribute
۲۶۱	شکل ۸-۳۶- پیکربندی Data View
۲۶۲	شکل ۸-۳۷- Get attributes from Koyo CLICK
۲۶۲	شکل ۸-۳۸- X001 and X002 forced on
۲۶۳	شکل ۸-۳۹- XDO برابر با ۳ است
۲۶۳	شکل ۸-۴۰- Data View X001 and X002 forced on
۲۶۳	شکل ۸-۴۱- مقدار هگز ورودی ۳
۲۶۴	شکل ۸-۴۲- همه چراغ‌ها روشن هستند
۲۶۴	شکل ۸-۴۳- Y001-Y004 همه روشن هستند
۲۶۵	شکل ۸-۴۴- تشخیص وایرشارک
۲۶۵	شکل ۸-۴۵- CIP details Data: 0f00
۲۶۹	شکل ۹-۱- منوی کشویی
۲۶۹	شکل ۹-۲- پنجره جستجوی افزونه
۲۷۰	شکل ۹-۳- استاندارد FoxyProxy
۲۷۰	شکل ۹-۴- نصب FoxyProxy
۲۷۰	شکل ۹-۵- مجوزهای FoxyProxy

۲۷۱	شکل ۹-۶- پیکربندی FoxyProxy
۲۷۱	شکل ۹-۷- افزودن تنظیمات
۲۷۱	شکل ۹-۸- اولین تنظیمات پروکسی
۲۷۲	شکل ۹-۹- پروکسی BurpSuite
۲۷۳	شکل ۹-۱۰- گواهی CA
۲۷۳	شکل ۹-۱۱- ذخیره گواهی CA
۲۷۳	شکل ۹-۱۲- Preferences
۲۷۴	شکل ۹-۱۳- حریم خصوصی و امنیت
۲۷۴	شکل ۹-۱۴- گواهینامه‌ها
۲۷۴	شکل ۹-۱۵- وارد کردن گواهی
۲۷۵	شکل ۹-۱۶- تنظیم trust options
۲۷۵	شکل ۹-۱۷- گواهی PortSwigger
۲۷۶	شکل ۹-۱۸- پروژه موقت
۲۷۶	شکل ۹-۱۹- تنظیمات پیش فرض
۲۷۷	شکل ۹-۲۰- پروکسی
۲۷۷	شکل ۹-۲۱- Intercept روشن است
۲۷۸	شکل ۹-۲۲- صفحه ورود Ignition
۲۷۸	شکل ۹-۲۳- وقفه ورود
۲۸۰	شکل ۹-۲۴- اعتبارات admin:admin
۲۸۰	شکل ۹-۲۵- درخواست POST
۲۸۱	شکل ۹-۲۶- ارسال به Repeater
۲۸۱	شکل ۹-۲۷- ابزار Repeater
۲۸۲	شکل ۹-۲۸- Invalid token
۲۸۲	شکل ۹-۲۹- توکن CSRF
۲۸۲	شکل ۹-۳۰- تاریخچه HTTP
۲۸۳	شکل ۹-۳۱- درخواست POST
۲۸۳	شکل ۹-۳۲- next-challenge token

۲۸۴	شکل ۹-۳۳- ارسال مجدد رمز
۲۸۴	شکل ۹-۳۴- درخواست oidc GET
۲۸۵	شکل ۹-۳۵- خطای 302 OIDC
۲۸۵	شکل ۹-۳۶- نشانه OIDC next-challenge
۲۸۶	شکل ۹-۳۷- سه نشست Repeater
۲۸۶	شکل ۹-۳۸- تولید توکن OIDC
۲۸۶	شکل ۹-۳۹- جایگزینی توکن شکست خورده با یک توکن oidc جدید
۲۸۷	شکل ۹-۴۰- پاسخ ۲۰۰
۲۸۷	شکل ۹-۴۱- نام کاربری-رمز عبور چالش رمز جدید
۲۸۸	شکل ۹-۴۲- دور زدن توکن CSRF
۲۸۸	شکل ۹-۴۳- احراز هویت موفق
۲۸۹	شکل ۹-۴۴- نسخه حرفه‌ای - تولید CSRF PoC
۲۸۹	شکل ۹-۴۵- Custom Parameter Handler
۲۹۰	شکل ۹-۴۶- درخواست OIDC
۲۹۱	شکل ۹-۴۷- کلیک راست بر روی درخواست
۲۹۲	شکل ۹-۴۸- curl OIDC request
۲۹۲	شکل ۹-۴۹- اسکریپت توکن bash OIDC
۲۹۳	شکل ۹-۵۰- توکن OIDC ایجاد شد
۲۹۳	شکل ۹-۵۱- اسکریپت توکن next-challenge
۲۹۴	شکل ۹-۵۲- توکن next-challenge ایجاد شده است
۲۹۴	شکل ۹-۵۳- دستور auth
۲۹۴	شکل ۹-۵۴- احراز هویت موفق
۲۹۵	شکل ۹-۵۵- بازسازی اسکریپت
۲۹۵	شکل ۹-۵۶- refactor Post- test
۲۹۶	شکل ۹-۵۷- تابع test_auth
۲۹۷	شکل ۹-۵۸- پروت فورس نام کاربری و رمز عبور
۲۹۸	شکل ۹-۵۹- احراز هویت موفق

۳۰۲	شکل ۱۰-۱- طرح آزمایشگاه فعلی .....
۳۰۳	شکل ۱۰-۲- الحاقات آزمایشگاه .....
۳۰۴	شکل ۱۰-۳- به روزرسانی ویندوز .....
۳۰۴	شکل ۱۰-۴- رابط شبکه .....
۳۰۵	شکل ۱۰-۵- تغییر نام دستگاه .....
۳۰۵	شکل ۱۰-۶- Add roles and features .....
۳۰۵	شکل ۱۰-۷- نوع نصب را انتخاب کنید .....
۳۰۶	شکل ۱۰-۸- سرور مقصد را انتخاب کنید .....
۳۰۶	شکل ۱۰-۹- نقش‌های سرور را انتخاب کنید .....
۳۰۷	شکل ۱۰-۱۰- ویژگی‌ها را انتخاب کنید .....
۳۰۸	شکل ۱۰-۱۱- انتخاب‌های نصب را تأیید کنید .....
۳۰۸	شکل ۱۰-۱۲- ارتقای دامین کنترلر .....
۳۰۹	شکل ۱۰-۱۳- Deployment Configuration .....
۳۰۹	شکل ۱۰-۱۴- گزینه‌های دامین کنترلر .....
۳۱۰	شکل ۱۰-۱۵- بررسی پیش‌نیازها .....
۳۱۰	شکل ۱۰-۱۶- دامنه LABCORP .....
۳۱۱	شکل ۱۰-۱۷- کاربران و کامپیوترها .....
۳۱۱	شکل ۱۰-۱۸- مدیران دامین .....
۳۱۲	شکل ۱۰-۱۹- گروه‌های سازمانی .....
۳۱۲	شکل ۱۰-۲۰- گروه SCADA .....
۳۱۳	شکل ۱۰-۲۱- operator1 .....
۳۱۴	شکل ۱۰-۲۲- احراز هویت اولیه Kerberos را غیرفعال کنید .....
۳۱۵	شکل ۱۰-۲۳- سرور DNS .....
۳۱۵	شکل ۱۰-۲۴- DNS Manager .....
۳۱۶	شکل ۱۰-۲۵- New zone wizard .....
۳۱۶	شکل ۱۰-۲۶- Reverse Lookup Zone Name .....
۳۱۷	شکل ۱۰-۲۷- Scavenging for all zones .....

۳۱۷.....	شکل ۱۰-۲۸-Set Aging/Scavenging Properties
۳۱۸.....	شکل ۱۰-۲۹-پیکربندی سرور DHCP
۳۱۸.....	شکل ۱۰-۳۰-DHCP Manager
۳۱۹.....	شکل ۱۰-۳۱-منوی Authorize
۳۱۹.....	شکل ۱۰-۳۲-دامنه جدید IPv4
۳۲۰.....	شکل ۱۰-۳۳-محدوده آدرس IP
۳۲۰.....	شکل ۱۰-۳۴-نمایش سرورهای DNS
۳۲۱.....	شکل ۱۰-۳۵-پیکربندی کامل DHCP
۳۲۱.....	شکل ۱۰-۳۶-Authorization
۳۲۲.....	شکل ۱۰-۳۷-File and Storage Services
۳۲۲.....	شکل ۱۰-۳۸-انتخاب SMB and NFS share
۳۲۳.....	شکل ۱۰-۳۹-نام اشتراک را مشخص کنید
۳۲۴.....	شکل ۱۰-۴۰-تنظیم SPN
۳۲۴.....	شکل ۱۰-۴۱-About PC
۳۲۵.....	شکل ۱۰-۴۲-ویژگی‌های سیستم
۳۲۵.....	شکل ۱۰-۴۳-نام کامپیوتر و دامنه
۳۲۶.....	شکل ۱۰-۴۴-وارد کردن اعتبار مدیریت دامین
۳۲۶.....	شکل ۱۰-۴۵-labcorp.local
۳۲۷.....	شکل ۱۰-۴۶-ورود 1operator
۳۲۸.....	شکل ۱۰-۴۷-وضعیت سرویس
۳۲۸.....	شکل ۱۰-۴۸-گروه مدیریت از راه دور
۳۲۹.....	شکل ۱۰-۴۹-Windows Defender
۳۳۰.....	شکل ۱۰-۵۰-nbtscan
۳۳۱.....	شکل ۱۰-۵۱-enum4linux
۳۳۲.....	شکل ۱۰-۵۲-کاربران
۳۳۲.....	شکل ۱۰-۵۳-Impacket administrator check
۳۳۳.....	شکل ۱۰-۵۴-چکیده operator2

۳۳۳	شکل ۱۰-۵۵- رمز عبور operator2
۳۳۴	شکل ۱۰-۵۶- GetADUsers
۳۳۴	شکل ۱۰-۵۷- SPN
۳۳۵	شکل ۱۰-۵۸- رمز عبور شکسته 3operator
۳۳۵	شکل ۱۰-۵۹- پاسخ‌دهنده در حال اجرا
۳۳۶	شکل ۱۰-۶۰- تست
۳۳۶	شکل ۱۰-۶۱- چکیده NTLM
۳۳۶	شکل ۱۰-۶۲- رمز عبور 1operator
۳۳۷	شکل ۱۰-۶۳- Evil- WinRM شل
۳۳۸	شکل ۱۰-۶۴- منوی شل Evil-WinRM
۳۳۹	شکل ۱۰-۶۵- تنظیمات حفاظت از ویروس و تهدید
۳۳۹	شکل ۱۰-۶۶- پورت شنونده ۴۲۴۲
۳۴۰	شکل ۱۰-۶۷- PowerShell معکوس
۳۴۰	شکل ۱۰-۶۸- impacket-psexec
۳۴۴	شکل ۱۱-۱- پیکربندی فایروال
۳۴۴	شکل ۱۱-۲- EULA
۳۴۵	شکل ۱۱-۳- pfSense را نصب کنید
۳۴۵	شکل ۱۱-۴- زبان صفحه‌کلید
۳۴۶	شکل ۱۱-۵- پارتیشن‌بندی دیسک
۳۴۶	شکل ۱۱-۶- ترفندهای نهایی
۳۴۷	شکل ۱۱-۷- راه‌اندازی مجدد
۳۴۷	شکل ۱۱-۸- منوی کنسول
۳۴۸	شکل ۱۱-۹- ورود به سیستم pfSense
۳۴۸	شکل ۱۱-۱۰- Setup wizard
۳۴۹	شکل ۱۱-۱۱- General Information
۳۴۹	شکل ۱۱-۱۲- پیکربندی رابط WAN
۳۴۹	شکل ۱۱-۱۳- شبکه‌های 1918RFC

۳۵۰	..... شکل ۱۱-۱۴- رابط LAN
۳۵۰	..... شکل ۱۱-۱۵- داشبورد pfSense
۳۵۱	..... شکل ۱۱-۱۶- سرور DHCP
۳۵۱	..... شکل ۱۱-۱۷- سرور DHCP
۳۵۲	..... شکل ۱۱-۱۸- انتخاب NAT
۳۵۲	..... شکل ۱۱-۱۹- پورت فوروارد
۳۵۳	..... شکل ۱۱-۲۰- پورت فوروارد/ویرایش
۳۵۳	..... شکل ۱۱-۲۱- دکمه اعمال تغییرات
۳۵۳	..... شکل ۱۱-۲۲- قانون Port Forward
۳۵۴	..... شکل ۱۱-۲۳- حالت NAT خروجی
۳۵۴	..... شکل ۱۱-۲۴- قانون WAN
۳۵۵	..... شکل ۱۱-۲۵- سرور DNS
۳۵۵	..... شکل ۱۱-۲۶- تغییرات نام کامپیوتر/دامنه
۳۵۶	..... شکل ۱۱-۲۷- متصل به دامنه
۳۵۶	..... شکل ۱۱-۲۸- کاربران دامنه به‌عنوان Remote Desktop
۳۵۸	..... شکل ۱۱-۲۹- Empire
۳۵۸	..... شکل ۱۱-۳۰- uselistener http
۳۵۹	..... شکل ۱۱-۳۱- کد شل Stager
۳۶۰	..... شکل ۱۱-۳۲- تنظیمات OutFile
۳۶۰	..... شکل ۱۱-۳۳- generate کنید
۳۶۰	..... شکل ۱۱-۳۴- launcher.bat در ایستگاه کاری
۳۶۱	..... شکل ۱۱-۳۵- agentهای فعال
۳۶۱	..... شکل ۱۱-۳۶- تعامل با agent
۳۶۲	..... شکل ۱۱-۳۷- ماژول Seatbelt
۳۶۳	..... شکل ۱۱-۳۸- دسترسی مدیریتی
۳۶۳	..... شکل ۱۱-۳۹- جلسات RDP
۳۶۴	..... شکل ۱۱-۴۰- نصب agent operator1

۳۶۵	شکل ۱۱-۴۱- logonPasswords sekurlsa
۳۶۶	شکل ۱۱-۴۲- اعتبارنامه
۳۶۶	شکل ۱۱-۴۳- sekurlsa::tickets
۳۶۷	شکل ۱۱-۴۴- تیکت kirbi
۳۶۷	شکل ۱۱-۴۵- kerberos:: ptt - تیکت را پاس کنید
۳۶۷	شکل ۱۱-۴۶- تیکت های ذخیره شده
۳۶۸	شکل ۱۱-۴۷- اطلاعات سیستم پایه WinPEAS
۳۶۹	شکل ۱۱-۴۸- face های شبکه و میزبان های شناخته شده
۳۶۹	شکل ۱۱-۴۹- اتصالات RDP ذخیره شده
۳۷۰	شکل ۱۱-۵۰- تیکت kerberos
۳۷۱	شکل ۱۱-۵۱- نقشه شبکه
۳۷۱	شکل ۱۱-۵۲- سرور OpenSSH
۳۷۲	شکل ۱۱-۵۳- OpenSSH SSH Server
۳۷۲	شکل ۱۱-۵۴- SSH ویندوز ۱۰
۳۷۳	شکل ۱۱-۵۵- قوانین NAT
۳۷۳	شکل ۱۱-۵۶- خطای اتصال از راه دور
۳۷۴	شکل ۱۱-۵۷- proxychains.conf
۳۷۵	شکل ۵۸-۱۱- پورت فوروارد
۳۷۵	شکل ۱۱-۵۹- تونل SSH
۳۷۶	شکل ۱۱-۶۰- سرور Chisel
۳۷۷	شکل ۱۱-۶۱- پروکسی معکوس
۳۷۷	شکل ۱۱-۶۲- شنونده پروکسی معکوس
۳۷۷	شکل ۱۱-۶۳- شل معکوس Chisel با زنجیره های پروکسی
۳۸۱	شکل ۱۲-۱- آداپتور شبکه جدید
۳۸۱	شکل ۱۲-۲- Interfaces   Assignments
۳۸۲	شکل ۱۲-۳- پورت های شبکه موجود
۳۸۲	شکل ۱۲-۴- رابط OPT1



۳۸۳	شکل ۱۲-۵- رابط OPT1 جدید
۳۸۳	شکل ۱۲-۶- فعال کردن 4IPv ثابت
۳۸۴	شکل ۱۲-۷- آدرس IPv4 ثابت
۳۸۴	شکل ۱۲-۸- سرویس DHCP سرور
۳۸۴	شکل ۱۲-۹- سرور DHCP
۳۸۵	شکل ۱۲-۱۰- Firewall   Rules
۳۸۵	شکل ۱۲-۱۱- Any rule
۳۸۶	شکل ۱۲-۱۲- کاربران، نقش‌ها
۳۸۶	شکل ۱۲-۱۳- ایجاد منبع کاربری جدید
۳۸۷	شکل ۱۲-۱۴- منابع جدید
۳۸۸	شکل ۱۲-۱۵- ویژگی‌های اکتیو دایرکتوری
۳۸۹	شکل ۱۲-۱۶- کاربران دامنه
۳۸۹	شکل ۱۲-۱۷- نقش‌ها
۳۹۰	شکل ۱۲-۱۸- Identity Providers
۳۹۰	شکل ۱۲-۱۹- جزئیات اساسی
۳۹۱	شکل ۱۲-۲۰- ارائه‌دهنده هویت اضافه‌شده است
۳۹۱	شکل ۱۲-۲۱- Switching Identity Provider
۳۹۱	شکل ۱۲-۲۲- ورود Operator1
۳۹۵	شکل ۱۲-۲۳- مسیر حمله
۳۹۶	شکل ۱۲-۲۴- استفاده مجدد از اعتبار
۳۹۷	شکل ۱۲-۲۵- دسترسی به پیکربندی رابط کاربری
۳۹۸	شکل ۱۲-۲۶- اتصال FTP به SCADA
۳۹۹	شکل ۱۲-۲۷- دسترسی به پوشه pub
۳۹۹	شکل ۱۲-۲۸- شل‌های وب
۴۰۰	شکل ۱۲-۲۹- php-reverse- shell.php
۴۰۰	شکل ۱۲-۳۰- php-reverse- s hell.php را قرار دهید
۴۰۱	شکل ۱۲-۳۱- حرکت به شل معکوس

۴۰۱.....	شکل ۱۲-۳۲- شل معکوس جدید.....
۴۰۵.....	شکل ۱۳-۱- Change control.....
۴۰۸.....	شکل ۱۳-۲- اسکن NMAP از یک میزبان منفرد.....
۴۰۹.....	شکل ۱۳-۳- جزئیات آزمایشگاه NetworkMiner.....
۴۰۹.....	شکل ۱۳-۴- دسترسی اولیه به شبکه.....
۴۱۰.....	شکل ۱۳-۵- اسکن اولیه WinPEAS.....
۴۱۱.....	شکل ۱۳-۶- حرکت جانبی.....
۴۱۳.....	شکل ۱۳-۷- تاکتیک حرکت جانبی.....
۴۱۴.....	شکل ۱۳-۸- تکنیک حساب‌های معتبر.....
۴۱۴.....	شکل ۱۳-۹- تکنیک کاهش مخاطرات حساب معتبر.....
۴۱۷.....	شکل ۱۳-۱۰- راه‌حل معمولی نظارت بر OT.....
۴۱۹.....	شکل ۱۳-۱۱- نصب معمولی IDS.....

تقدیم به

انسان‌هایی که

به فردایی بهتر

می‌اندیشند.

#### مقدمه ناشر

سپاس بی‌کران پروردگار را که به انسان قدرت اندیشیدن بخشید، قدرتی که در مقایسه با سایر موجودات باعث شده است که انسان هرگز به امکانات محدود خود اکتفا نکند. مکاتب الهی، انسان را موجودی کمال‌طلب و پویا می‌دانند که جهت‌گیری او به سوی خالقش می‌باشد. از جمله راه‌های تقرب به خداوند علم است، علمی که زیبایی عقل است. علمی که در دریای بی‌کران آن، هر ذره نشانی از آفریدگار است و هر چه علم انسان افزون گردد، تقریبش بیشتر می‌شود. از این روست که به علم‌اندوزی و دانش‌آموزی توجهی بی‌نظیر مبذول گردیده است؛ اما علم‌آموزی به ابزاری نیاز دارد که مهم‌ترین آن کتاب است و انتشار نتیجه مطالعات پژوهشگران و اندیشمندان پاسخگوی این نیاز خواهد بود.

جهت تحقق این امر و گام برداشتن در جهت ارتقای پایه‌های علم و دانش و رشد و شکوفایی استعدادها، انتشار کتاب را یکی از اهداف خود قرار داده و انتظار داریم با حمایت‌های معنوی هم‌وطنان گرامی بتوانیم گام‌های مؤثر و ارزشمندی را برداریم. گرچه تلاش خواهد شد در حد دانش و تجربه اندکمان کارهایی بدون اشکال تقدیم حضورتان گردد، ولی اذعان داریم که راهنمایی‌های شما عزیزان می‌تواند ما را در ارتقای کیفی کتاب راهگشا باشد لذا همیشه منتظر پیشنهادات و راهنمایی‌های شما خواهیم بود.

در پایان از همه عزیزانی که در مراحل مختلف تهیه، تدوین و چاپ کتاب از همفکری و همکاری آن‌ها برخوردار بوده‌ام به‌خصوص آقایان پیام حاتم‌زاده، آرش تابع، کمیل صمدی و محمدحسام تدین (مترجمان)، خانم فاطمه دشتی رحمت آبادی (صفحه‌آرایی) و مهندس علی‌محمد خانی (مدیر فروش) سپاسگزاری نموده و موفقیت روزافزونشان را آرزومندم.

دکتر مهدی خانی

مدیرمسئول انتشارات آوای قلم

### تست نفوذ سیستم‌های کنترل صنعتی

ش تمامی حقوق محفوظ است. هیچ بخشی از این کتاب را نمی‌توان بدون اجازه کتبی قبلی ناشر تکثیر کرد، در یک سیستم ذخیره کرد، یا به هر شکل و یا به هر وسیله‌ای منتقل کرد، مگر در مورد نقل قول‌های مختصری که در مقالات انتقادی یا نقد گنجانده شده است. در تهیه این کتاب نهایت تلاش برای اطمینان از صحت اطلاعات ارائه شده صورت گرفته است. با این حال، اطلاعات موجود در این کتاب بدون ضمانت صحت، چه صریح یا ضمنی منتشر می‌شود. نه نویسنده، نه انتشارات یا فروشندگان و توزیع‌کنندگان آن، در قبال خسارات وارده یا ادعا شده که مستقیم یا غیرمستقیم توسط این کتاب ایجاد شده است، مسئول نیستند.

## مشارکت‌کنندگان

### درباره نویسنده

پل اسمیت نزدیک به ۲۰ سال را در فضای کنترل اتوماسیون گذرانده است و با مشکلات "شاه‌ماهی قرمز" که سر راه او قرار دارد، مقابله کرده است. او مسائل منحصر به فردی مانند عدم تعادل اندازه‌گیری ناشی از اشباع حسگر شعله‌ور، اشتباهات مهاجرت پایگاه‌داده و بسیاری موارد دیگر را مدیریت کرده است. این در نهایت منجر به تغییر حرفه او شد، جایی که او بیشتر وقت خود را در فضای امنیت سایبری صنعتی در استفاده از فناوری‌های جدید امنیتی در بخش‌های انرژی، ابزار و زیرساخت‌های حیاتی می‌گذراند.

کمک به توسعه استراتژی‌های امنیت سایبری از طریق استفاده از مشارکت‌های تیم قرمز/تست نفوذ، ارزیابی ریسک امنیت سایبری و انجام مانورهای رومیزی برای برخی از بزرگ‌ترین پیمانکاران دولتی، سازمان‌های صنعتی و شهرداری‌های جهان بخشی از فعالیت‌های وی می‌باشد.

"می‌خواهم از خانواده‌ام برای تشویق و انگیزه‌ای که برای نوشتن این کتاب نیاز داشتم تشکر کنم. تشکر ویژه از پدرم که اولین کامپیوترم را برایم خرید و به من اجازه داد آن را به سیستم تلفن وصل کنم. از گروهی از هکرها/فریکرها که برای هدایت من در این مسیر و در نهایت ایجاد حرفه من در این زمینه تلاش کردند و از کل تیم پکت، برای رسیدگی به برنامه‌ها و مشکلاتم، سپاسگزارم."

### درباره داور

دیمیتری خومنکو یک متخصص امنیت اطلاعات با بیش از ۱۰ سال تجربه در اتوماسیون صنعتی، فناوری اطلاعات و امنیت سایبری صنعتی است. او پروژه‌های توسعه امنیت سایبری اطلاعات OT/ICS را در بزرگ‌ترین شرکت‌های صنعتی روسیه مانند گازپروم، شرکت نفت روس، نوریلسک نیکل، گروه EuroChem و Metalloinvest طراحی، اجرا و پشتیبانی کرده است. در حال حاضر، او بنیان‌گذار و رئیس بخش امنیت اطلاعات بخش جدید خدمات امنیت اطلاعات در یک شرکت مهندسی است و با رهبران صنعت اتوماسیون صنعتی و شرکت‌های کلیدی صنعت استخراج روسیه همکاری می‌کند.

"می‌خواهم از همسرم الیزابت تشکر کنم که همیشه محبت خود را نشان می‌دهد و در تصمیم‌گیری‌ها و لحظات مهم زندگی‌ام از من حمایت می‌کند. از پسر کوچکم، ولادیسلاو، تشکر می‌کنم که با عشق و انرژی جوانی‌اش به من کمک نمود. از پدر و مادرم به خاطر سخنان صادقانه و حمایتشان بعد از اشتباهات زندگی و کاری تشکر می‌کنم. همه این‌ها به من کمک می‌کند تا بهتر شوم و به جلو بروم."

## پیشگفتار

امنیت سایبری سیستم‌های کنترل صنعتی<sup>۱</sup> (ICS) در سال‌های اخیر رشد چشمگیری داشته است. برای ایمن‌سازی واقعی زیرساخت‌های حیاتی امروزی، تیم‌های امنیتی باید به‌طور مداوم برای آزمایش و بهره‌برداری از یکپارچگی امنیتی افراد، فرایندها و محصولات یک شرکت به کار گرفته شوند. این کتاب به شما برای به دست آوردن تجربه عملی در مورد تجهیزاتی که در این زمینه با آن‌ها روبرو خواهید شد با رویکردی کمی متفاوت با سایر کتاب‌ها، کمک خواهد کرد. این کتاب به شما امکان می‌دهد بفهمید که چگونه تجهیزات کنترل صنعتی در یک محیط عملیاتی تعامل می‌کنند. این کتاب با درک اصول اولیه فرایندهای صنعتی آغاز می‌شود و سپس به شما نشان می‌دهد که چگونه فرایند ایجاد می‌شود و به شما کمک می‌کند تا به همراه جمع‌آوری اطلاعات منبع‌باز<sup>۲</sup> (OSINT) با ایجاد یک چشم‌انداز تهدید میزبان بالقوه، آن را هک کنید. گام‌به‌گام نحوه نصب و استفاده از تکنیک‌های تهاجمی مورد استفاده هکرهای حرفه‌ای را خواهید یافت. در این کتاب، آشنایی با تجهیزات سیستم‌های کنترل صنعتی، جمع‌آوری اطلاعات منبع‌باز، کشف پورت و سرویس، pivoting و در نهایت، راه‌اندازی حملات علیه سیستم‌ها در یک شبکه صنعتی را بررسی خواهیم کرد. در پایان این کتاب تست نفوذ، شما نه تنها نحوه تجزیه و تحلیل و پیمایش پیچیدگی‌های یک سیستم کنترل صنعتی را خواهید فهمید، بلکه مهارت‌های تهاجمی و دفاعی ضروری برای محافظت فعالانه از شبکه‌های صنعتی در برابر حملات سایبری مدرن را نیز به دست خواهید آورد.

### این کتاب برای چه کسی است؟

این کتاب در ابتدا به‌عنوان یک کتابچه راهنما، صرفاً برای تست نفوذ سیستم‌های کنترل صنعتی و برای افرادی که می‌خواستند در مورد تست نفوذ سیستم‌های کنترل صنعتی بیاموزند، طراحی شد. با این حال، در ادامه به یک تلاش دو جانبه تبدیل شد، زیرا افراد زیادی از من در مورد ورود به فضای امنیتی فناوری عملیاتی<sup>۳</sup> (OT) پرسیدند، لذا سعی خواهم کرد موضوعاتی را پوشش دهم که به هر دو موضوع OT و IT می‌پردازد. پرسنل امنیت فناوری اطلاعات که خواهان آشنایی عملی با تست نفوذ سیستم‌های کنترل صنعتی هستند، در مورد جنبه اتوماسیون و تست نفوذ یاد می‌گیرند، در حالی که مهندسين اتوماسیون/کنترل که می‌خواهند چشم‌انداز تهدیدات بالقوه خود را بهتر درک کنند، بیشتر در مورد جنبه‌های شبکه فناوری اطلاعات خواهند آموخت.

---

<sup>1</sup> Industrial Control System

<sup>2</sup> Open Source Intelligence

<sup>3</sup>Operational Technology

آنچه این کتاب پوشش می‌دهد:

**فصل ۱، استفاده از مجازی‌سازی،** از طریق بلوک‌های اصلی مجازی‌سازی و سپس ساخت یک هایپروایزر<sup>۱</sup>، آزمایشگاه ICS مجازی را تشکیل خواهد داد.

**فصل ۲، اتصال به سخت‌افزار فیزیکی،** اصول راه‌اندازی یک کنترل‌کننده منطقی قابل‌برنامه‌ریزی<sup>۲</sup> (PLC) را پوشش می‌دهد و سپس به اصول اتصال آن PLC به یک ماشین مجازی در هایپروایزر تازه ساخته‌شده، می‌پردازد.

**فصل ۳، پیکربندی آزمایشگاه،** مراحل نوشتن و بارگذاری اولین برنامه در PLC را شرح خواهد داد.

**فصل ۴، نینجا منبع‌باز<sup>۳</sup>،** قدرت Google-Fu، اشتراک‌گذاری اطلاعات در لینکدین، دستگاه‌های در معرض نمایش در Shodan.io، پیمایش ExploitDB و در نهایت استفاده از پایگاه داده آسیب‌پذیری ملی را به شما آموزش می‌دهد.

**فصل ۵، نظارت ترافیک شبکه،** SPAN ها و TAP ها و نحوه استفاده از آن‌ها در یک تعامل تست نفوذ را می‌آموزد و سپس به بررسی عمیق سیستم‌های تشخیص نفوذ خواهیم پرداخت.

**فصل ۶، تحلیل عمیق پکت‌ها،** ساختار یک بسته معمولی را بررسی می‌کند، به شما یاد می‌دهد که چگونه بسته‌ها را ضبط کنید و سپس آن‌ها را برای استخراج اطلاعات کلیدی، تجزیه و تحلیل می‌کند.

**فصل ۷، اسکن،** با ساختن یک سیستم SCADA زنده<sup>۴</sup> شروع می‌شود و سپس به استفاده از NMAP، RustScan، Gobuster و feroxbuster برای انجام تکنیک‌های اسکن در سیستم SCADA ادامه می‌دهد.

**فصل ۸، پروتکل‌ها،** به بررسی عمیق Modbus و Ethernet/IP و راه‌هایی می‌پردازد که ما می‌توانیم از این پروتکل‌ها برای انجام کارهای تست نفوذ در داخل ICS استفاده کنیم.

**فصل ۹، نینجا،** از FoxyProxy و Burp Suite برای تجزیه و تحلیل و حمله به رابط کاربری SCADA استفاده می‌کند.

**فصل ۱۰، من می‌توانم آن را انجام دهم،** با نصب و پیکربندی یک فایروال، راه‌اندازی آزمایشگاهی جامع‌تر شروع می‌شود. سپس، ما به اسکن، بهره‌برداری و سپس تزریق شل‌های معکوس خواهیم پرداخت.

**فصل ۱۱، من باید به عمق بروم،** اکنون که شل‌ها را داریم به اجرای ماژول‌های پس از نفوذ برای جمع‌آوری داده‌ها از داخل شبکه می‌پردازیم. ما دسترسی‌ها را برای ماشین‌هایی که به آن‌ها نفوذ

---

<sup>1</sup>Hypervisor

<sup>2</sup> Programmable Logic Controller

<sup>3</sup>Open Source Ninja

<sup>4</sup> Live

می‌کنیم، افزایش می‌دهیم و سپس به بخش‌های پایین‌تر شبکه می‌رویم.

**فصل ۱۲، من آینده را می‌بینم،** به خطرات استفاده مجدد از اعتبارنامه می‌پردازد و شما را با مراحل استفاده از اعتبارنامه‌های کشف‌شده در مراحل قبلی و سپس دسترسی به رابط SCADA برای کنترل نهایی سیستم، آشنا می‌کند.

**فصل ۱۳، متعجب اما با پشیمانی،** در مورد تحویل گزارش اصلی بحث می‌کند. اگر هیچ مدرکی وجود نداشته باشد، آیا واقعاً آزمایشی رخ داده است؟ ما یک الگو برای ارزیابی‌ها/آزمایش‌های آتی آماده می‌کنیم، سپس در مورد اطلاعات مهمی که در داخل گزارش قرار می‌گیرد بحث می‌کنیم و در نهایت، توصیه‌هایی را مستند می‌کنیم که می‌تواند توسط تیم بعدی برای محافظت از سیستم‌هایشان در آینده استفاده شود.

**چگونه می‌توانید بیشترین بهره را از این کتاب ببرید؟**

شما باید سعی کنید یک رایانه شخصی با ۳۲ گیگابایت رم و دارای حداقل دو پورت اترنت، در اختیار داشته باشید. Intel NUC، GigaByte BRIX و Zotac Z-Box نمونه‌هایی از دستگاه‌هایی هستند که برای اجرای مجازی‌سازی شما بسیار مفید هستند.

اگر از نسخه دیجیتال این کتاب استفاده می‌کنید، به شما توصیه می‌کنیم که کد را خودتان تایپ کنید یا از مخزن GitHub به آن دسترسی پیدا کنید (لینک در قسمت بعدی موجود است). انجام این کار به شما کمک می‌کند تا از هرگونه خطای احتمالی مربوط به کپی و چسباندن کد جلوگیری کنید.

**استفاده از کد در عمل**

ویدئوهای Code in Action این کتاب را می‌توانید در <https://bit.ly/3iZpT2f> و یا کانال <https://ble.ir/ptics> مشاهده کنید.

**بارگیری تصاویر رنگی**

فایل PDF زیر دارای تصاویر رنگی از شکل‌ها و نمودارهای استفاده‌شده در این کتاب است. می‌توانید آن را از لینک زیر بارگیری کنید:

[http://www.packtpub.com/sites/default/files/downloads/9781800202382\\_ColorImages.pdf](http://www.packtpub.com/sites/default/files/downloads/9781800202382_ColorImages.pdf)



## قراردادهای مورد استفاده

تعدادی از قراردادهای متنی در سراسر این کتاب استفاده شده است.

**کد در متن:** کلمات کد در متن، نام جدول پایگاه داده، نام پوشه، نام فایل، پسوند فایل، نام مسیر، URL ساختگی، ورودی کاربر و دسته‌های توییت را نشان می‌دهد. یک مثال در اینجا آمده است:

"بروید و فایل PCAP با برچسب 4SICS-GeekLounge151021.pcap را با ویرشارک باز کنید."

یک بلوک کد به صورت زیر تنظیم می‌شود:

```
def run_async_server():
    store = ModbusSlaveContext(
        di=ModbusSequentialDataBlock(0,[17]*100),
        co=ModbusSequentialDataBlock(0,[17]*100),
        hr=ModbusSequentialDataBlock(0,[17]*100))
```

وقتی می‌خواهیم توجه شما را به بخش خاصی از بلوک کد جلب کنیم، خطوط یا موارد مربوطه به صورت پررنگ تنظیم می‌شوند:

```
import logging
FORMAT = ('%(asctime)-15s %(threadName)-15s
%(levelname)-8s %(module)-15s:%(lineno)-8s (message)%')
logging.basicConfig(format=FORMAT)
log = logging.getLogger()
log.setLevel(logging.DEBUG)
```

ورودی یا خروجی خط فرمان به صورت زیر نوشته می‌شود:

```
tcpdump -i <interface> -v -X
```

**پررنگ:** عبارت جدید، کلمه مهم یا کلماتی را که روی صفحه می‌بینید را نشان می‌دهد. برای به‌عنوان مثال، کلمات در منوها یا کادرهای گفتگو به صورت پررنگ ظاهر می‌شوند. در اینجا یک مثال وجود دارد: "ما می‌خواهیم پورت mirroring را تنظیم کنیم، بنابراین گزینه **Monitoring** را از منوی سمت چپ انتخاب کنید و سپس **Port Mirror** را انتخاب کنید."

**نکته و یا نکات مهم:**

این‌گونه ظاهر می‌شوند.

در کانال <https://ble.ir/ptics> آماده دریافت هرگونه نظرات و پیشنهادات مخاطبین عزیز خواهیم بود.