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 سامانه‌های کنترل صنعتی)

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

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

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

انتشارات آوای قلم

سرشناسه	: اسمیت، پلSmith, Paul
عنوان و نام پدیدآور	: تست نفوذ سیستم‌های کنترل صنعتی: راهنمای هکرهای قانونمند برای تجزیه و تحلیل کاهش مخاطرات و ایمن‌سازی فرایندهای صنعتی/نوبسنده پل اسمیت؛ مترجمان پیام حاتم‌زاده ...[ودیگران].
مشخصات نشر	: تهران: آوای قلم، ۱۴۰۲. مشخصات ظاهری: ۴۲۰ص.
شابک	: ۹۷۸-۶۲۲-۷۶۵۲-۹۵-۶ 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.
یادداشت	: مترجمان پیام حاتم‌زاده ، آرش تابع ، کمیل صمدی ، محمدحسام تدین.
عنوان دیگر	: راهنمای هکرهای قانونمند برای تجزیه و تحلیل کاهش مخاطرات و ایمن‌سازی فرایندهای صنعتی.
موضوع	: 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 تجزیه‌وتحلیل، کاهش مخاطرات و ایمن‌سازی فرایندهای صنعتی

نویسنده:	پل اسمیت	**نوبت چاپ:**	اول
مترجمان:	پیام حاتم‌زاده- آرش تابع	**تاریخ نشر:**	۱۴۰۲
	کمیل صمدی- محمد حسام تدین	**شمارگان:**	۱۰۰ جلد
ناشر:	انتشارات آوای قلم	**شابک:**	۹۷۸-۶۲۲-۷۶۵۲-۹۵-۶
طراحی جلد:	انتشارات آوای قلم(مهران خانی)	**قیمت:**	۳۹۰۰۰۰ تومان
صفحه‌آرایی:	انتشارات آوای قلم(فاطمه دشتی)		

شماره تماس: ۶۶۵۹۱۵۰۴-۶۶۵۹۱۵۰۵ **همراه:** ۰۹۲۱۲۰۵۷۷۵۱

فروشگاه کتاب چاپی و الکترونیکی: www.avapublisher.com

فهرست مطالب

عنوان **صفحه**

بخش ۴: تسخیر پرچم‌ها و خاموش کردن چراغ‌ها

فهرست تصاویر

عنوان **صفحه**

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 به‌سوی 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، تقربش 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(صفحه آرایی) 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

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**[1] **(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[2] (OSINT) با ایجاد یک چشم‌انداز تهدید میزبان بالقوه، آن را هک کنید. گام‌به‌گام نحوه نصب و استفاده از تکنیک‌های تهاجمی مورداستفاده 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 تجزیه‌وتحلیل 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**[3] **(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، درحالی‌که مهندسین اتوماسیون/کنترل که می‌خواهند چشم‌انداز تهدیدات بالقوه خود را بهتر درک کنند، بیشتر در مورد جنبه‌های شبکه فناوری اطلاعات خواهند آموخت.

---

[1] Industrial Control System
[2] Open Source Intelligence
[3] Operational Technology

آنچه این کتاب پوشش می‌دهد:

فصل ۱، استفاده از مجازی‌سازی، از طریق بلوک‌های اصلی مجازی‌سازی و سپس ساخت یک هایپروایزر[1]، آزمایشگاه ICS مجازی را تشکیل خواهد داد.

فصل ۲، اتصال به سخت‌افزار فیزیکی، اصول راه‌اندازی یک کنترل‌کننده منطقی قابل‌برنامه‌ریزی[2] (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[3]، 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، تجزیه‌وتحلیل می‌کند.

فصل ۷، اسکن، با ساختن یک سیستم SCADA زنده[4] 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 تجزیه‌وتحلیل 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

---

[1] Hypervisor
[2] Programmable Logic Controller
[3] Open Source Ninja
[4] 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

قراردادهای مورداستفاده

تعدادی از قراردادهای متنی در سراسر این کتاب استفاده‌شده 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 توییتر را نشان می‌دهد. یک مثال در اینجا آمده است:

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

یک بلوک کد به‌صورت 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 به‌صورت 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 به‌صورت 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 به‌صورت 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.