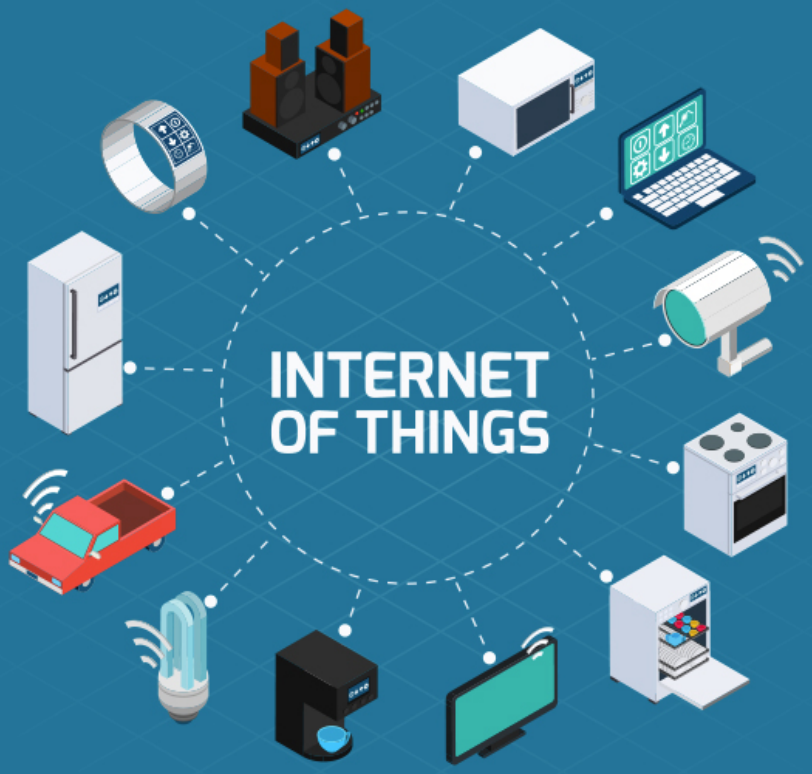

Preforming IOT Pentest

A Theorical Guide to Pentesting the Internet of Things

فهرست

مقدمه و تعریف IoT Pentest

مقدمه

اینترنت اشیاء (IoT) دیگر تنها یک مفهوم آینده‌نگرانه نیست؛ بلکه بخشی از زندگی روزمره ما شده است از دوربین‌های نظارتی خانگی گرفته تا سنسورهای صنعتی و دستگاه‌های پزشکی هوشمند، همه و همه زیرمجموعه‌ای از اکوسیستم عظیم IoT محسوب می‌شوند

اما همین گستردگی، به معنی سطح حمله (Attack Surface) وسیع‌تر و در نتیجه ریسک امنیتی بالاتر است به عنوان نمونه

- یک آسیب‌پذیری ساده در Firmware یک دوربین خانگی می‌تواند منجر به جاسوسی تصویری از کاربران شود

ضعف امنیتی در یک Hub خانگی ممکن است به مهاجم امکان دهد تا به شبکه خانگی و سایر دستگاه‌های متصل دسترسی پیدا کند

در حوزه صنعتی(IIoT) ، آسیب‌پذیری‌ها می‌توانند منجر به توقف خط تولید یا حتی خرابی فیزیکی تجهیزات شوند

در این شرایط IoT Penetration Test تست نفوذ IoT به عنوان یکی از ابزارهای کلیدی برای ارزیابی و تقویت امنیت دستگاه‌ها مطرح می‌شود

تعریف IoT Penetration Test

تست نفوذ IoT به معنی ارزیابی امنیتی جامع بر روی اجزای مختلف یک راهکار IoT است این تست تنها محدود به یک بخش مثلاً وب‌اپلیکیشن یا موبایل) نمی‌شود، بلکه تمامی مؤلفه‌ها را شامل می‌شود

- Embedded Devices – شامل سنسورها، گیت‌وی‌ها، میکروکنترلرها و...
- Firmware, Software & Applications – نرم‌افزار داخلی، اپلیکیشن‌های موبایل و وب، سرویس‌های ابری
- Radio Communications – ارتباطات بی‌سیم مانند Wi Fi, ZigBee, BLE, LoRa

تفاوت کلیدی IoT Pentest با تست نفوذ سنتی در همین چندلایه بودن است در حالی که تست وب یا موبایل بر روی یک لایه انجام می‌شود، در IoT باید تمام این لایه‌ها به صورت یکپارچه بررسی شوند

چالش‌های ویژه در IoT Pentest

تعدد پروتکل‌ها برخلاف وب که بیشتر حول HTTP/HTTPS است، در IoT پروتکل‌های متنوعی وجود دارند MQTT ، CoAP، ZigBee، BLE

دستگاه‌های فیزیکی تست ممکن است نیازمند باز کردن دستگاه، استفاده از ابزارهای سخت‌افزاری مثل JTAG یا SDR باشد

محدودیت منابع بسیاری از دستگاه‌های IoT منابع محدودی دارند CPU ، RAM، بنابراین استفاده از روش‌های معمولی امنیتی ممکن نیست

چالش‌های حریم خصوصی بسیاری از دستگاه‌های IoT داده‌های حساس کاربران را جمع‌آوری می‌کنند که علاوه بر امنیت، مسائل حریم خصوصی را هم مطرح می‌کند

نمونه واقعی (Real World Case)

در سال 2023، گروهی از پژوهشگران امنیتی موفق شدند آسیب‌پذیری‌های حیاتی در دستگاه‌های پزشکی هوشمند (Smart Infusion Pumps) شناسایی کنند که امکان تغییر دوز دارو از راه دور را فراهم می‌کرد این مثال نشان می‌دهد که IoT Pentest تنها یک تمرین آکادمیک نیست، بلکه می‌تواند مرز میان ایمنی و فاجعه باشد

بررسی Embedded Devices در معماری IoT

نقش کلیدی Embedded Devices در اکوسیستم IoT

دستگاه‌های تعبیه‌شده (Embedded Devices) مانند میکروکنترلرها، سنسورها، گیت‌وی‌ها و تجهیزات حساس نقش ستون فقرات را در معماری IoT ایفا می‌کنند این دستگاه‌ها داده‌ها را جمع‌آوری، ارسال و پردازش کرده و اغلب در محیط‌های حیاتی مثل پزشکی، صنعتی یا خانه‌های هوشمند استفاده می‌شوند بنابراین، آسیب‌پذیری در این بخش‌ها می‌تواند پیامدهای گسترده‌ای ایجاد کند، از اختلال در عملکرد تا تهدیدهای جدی امنیتی و خطر برای جان انسان‌ها

آسیب‌پذیری‌ها و تهدیدات رایج

منابع به‌روز نشان می‌دهند که سیستم‌های Embedded در برابر انواع تهدیدات مانند زیر آسیب‌پذیر هستند

- **حملات سخت‌افزاری و استخراج مستقیم** از طریق پروتکل‌هایی مانندJTAG ، Flash Dumpیا دسترسی از طریق پورت‌های سریال که امکان استخراج مستقیم Firmwareیا داده‌های داخلی را فراهم می‌کنند
- **نقص در امنیت سخت‌افزار** شامل نبود طراحی Secure by Default یا ضعف در سخت‌شدن فیزیکی (Physical Hardening) این نوع ضعف‌ها، به ویژه در دستگاه‌هایی که در محیط‌های عمومی یا دسترس هستند، خطر تزریق سخت‌افزاری یا manipulation را افزایش می‌دهند
- **معماری پیچیده و استفاده از اجزای کم‌منبع** این دستگاه‌ها اغلب محدودیت‌های قابل توجهی در پردازش و حافظه دارند، که اجرای مکانیسم‌های امنیتی استاندارد را دشوار می‌سازد

- **وابستگی به مؤلفه‌های جانبی ناامن** در بسیاری از Firmware ها از Third Party Components استفاده می‌شود که می‌توانند حامل آسیب‌پذیری‌های شناخته‌شده باشند یک مطالعه نشان داد که در بیش از 34 هزار Firmware ، تعداد زیادی Component آسیب‌پذیر وجود دارد که ناشی از استفاده از مؤلفه‌های سوم‌شخص به‌وجود آمده‌اند
- **حملات مبتنی بر حافظه (Memory)** در گیت‌وی‌های بی‌سیم، آسیب‌پذیری‌های امنیتی بر اساس حافظه مثل (buffer overflow) یکی از خطرناک‌ترین تهدیدات است؛ استفاده از تکنیک‌های Secure by Design مانند CHERI یا Rust می‌تواند کمک‌کننده باشد

بازنگری بر اساس منبع علمی

مطالعه‌ای جامع نیز به بررسی معماری Firmware ، روش‌های استخراج آن، و فریم‌ورک‌های مدرن تحلیل آسیب‌پذیری پرداخته است این مرور نشان می‌دهد برای شناسایی آسیب‌پذیری‌های Firmware ، ابزارهایی با توانایی‌های Static ، Dynamic و Hybrid Analysis کاربردی هستند همچنین به چالش‌هایی در تحلیل و نوت‌های مربوط به به‌روزرسانی‌های امن و استانداردسازی اشاره می‌شود

نمونه کاربردی(Case Study)

در یکی از مقاله‌های معتبر، دانشمندان با استفاده از آزمایش‌های خودکار روی دستگاه‌های مصرف‌کننده IoT در یک خانه هوشمند، حملاتی نظیر پرینت پورت‌ها، اسکن سیستم عامل و Flooding را انجام دادند نتایج نشان داد دستگاه‌ها به شدت آسیب‌پذیر بوده‌اند و مدل تست‌گذاری سیستماتیک برای بررسی امنیت دستگاه‌ها بسیار مؤثر است

Firmware ، Software و Applications در IoT

اهمیت Firmware در امنیت IoT

Firmware در واقع «روح» دستگاه IoT است؛ همان نرم‌افزاری که روی میکروکنترلر یا چیپ سخت‌افزاری اجرا می‌شود و کنترل همه اجزای دستگاه را بر عهده دارد هرگونه ضعف در Firmware می‌تواند معادل با در اختیار گرفتن کل دستگاه باشد

نمونه آسیب‌پذیری‌های Firmware

- **Ability to Modify Firmware** امکان تغییر Firmware و بارگذاری نسخه مخرب
- **Insecure Signature & Integrity Verification** نبود یا ضعف در فرآیند بررسی امضا دیجیتال و صحت فایل‌ها
- **Hardcoded Sensitive Values** ذخیره مستقیم API Keys ، پسوردها و گواهی‌نامه‌ها داخل کد
- **Private Certificates Exposure** دسترسی غیرمجاز به گواهی‌های SSL خصوصی
- **Outdated Components** استفاده از Kernel یا کتابخانه‌های قدیمی با آسیب‌پذیری شناخته‌شده

طبق پژوهش‌های اخیر، بیش از ۴۰٪ **Firmware های IoT حاوی کامپوننت‌های Third Party ناامن** هستند که به‌روز نشده‌اند و همین موضوع آن‌ها را در برابر حملات شناخته‌شده آسیب‌پذیر می‌کند

Applications Mobile + Web وSoftware

بخش نرم‌افزاری دستگاه‌های IoT معمولاً شامل **اپلیکیشن موبایل** Android/iOS، **وب‌اپلیکیشن** Dashboardهای مدیریتی و **سرویس‌های ابری** است

نمونه آسیب‌پذیری‌های Mobile Applications

- Reverse Engineeringکد و دسترسی به توابع حساس
- Insecure Authentication & Authorization
- Business Logic Flaws
- Side Channel Data Leakage
- استفاده ازSDK های قدیمی و ناامن

نمونه آسیب‌پذیری‌هایWeb Applications

- Client Side Injectionمانند XSS
- Insecure Direct Object Reference IDOR
- Cross Site Request Forgery CSRF
- دسترسی غیرمجاز به داده‌های کاربران دیگرUnauthorized Access

یک مطالعه جدید در **MDPI Sensors Journal 2024** نشان داد که اپلیکیشن‌های موبایل IoT همچنان بیشترین سهم از آسیب‌پذیری‌های امنیتی را دارند و در بیش از ۶۰٪ **تست‌های نفوذ IoT** به‌عنوان نقطه ورود اصلی حمله عمل کرده‌اند

چالش‌های امنیتی در API ها و پروتکل‌ها

بسیاری از دستگاه‌ها برای ارتباط میان Firmware ، اپ موبایل و وب از API ها و پروتکل‌های متنوع استفاده می‌کنند

- REST API
- SOAP
- MQTT
- CoAP

اگر این API ها به‌درستی ایمن‌سازی نشوند مانند استفاده از احراز هویت ضعیف، عدم اعتبارسنجی ورودی، یا ارسال داده بدون رمزنگاری، مهاجم می‌تواند **ارتباط بین دستگاه و Cloud**را شنود یا دستکاری کند

نمونه حمله واقعی در سال 2022، پژوهشگران امنیتی موفق شدند با بهره‌گیری از ضعف در **MQTT Authentication**به داده‌های زنده صدها دستگاه صنعتی متصل شوند

Structuring the Pentest in IoT

یکی از تفاوت‌های اصلی تست نفوذ در IoT با تست‌های سنتی، **چندبخشی بودن آن** است Pentestدر IoT فقط شناسایی و Exploitation یک اپلیکیشن وب یا موبایل نیست؛ بلکه باید به صورت **چندمرحله‌ای و ساختاریافته** پیش برود

چرا ساختاردهی اهمیت دارد؟

- **هماهنگی با مشتری** بسیاری از سازمان‌ها محدودیت زمانی و فنی دارند مثلاً تست فقط در شب انجام شود یا روی دستگاه‌هایStaging

- **پیچیدگی دستگاه‌ها** به دلیل وجود Embedded Devices ، Firmware، API، Cloud وRadio Communication ، لازم است تیم Pentest به صورت تقسیم وظایف کار کند
- **مستندسازی بهتر** ساختاردهی موجب می‌شود خروجی تست Report قابل درک، سازمان‌یافته و عملیاتی باشد

مراحل کلیدی در ساختار Pentest

Client Engagement and Initial Discussion Call

- اولین تماس با مشتری پس از درخواست Pentest
- تعیین محدوده تست کدام اجزا تست شوند؟ آیا تست **White Box / Black Box / Gray Box** خواهد بود؟
- مشخص کردن محدودیت‌ها مثلاً دستگاه‌های محدود، ساعت تست، قوانین Destroy/Non Destroy
- اهمیت این مرحله ایجاد شفافیت برای جلوگیری از اختلافات آتی

مثال در یک پروژه واقعی، تیم Pentest اجازه داشت Firmware دستگاه را Dump کند، اما اجازه **Destructive Testing** باز کردن چیپ‌ها داده نشد این توافق در همان جلسه اولیه مشخص شد

Additional Technical Discussion and Briefing Call

- بعد از امضای **NDA Non Disclosure Agreement**، مشتری جزئیات فنی دستگاه را به تیم می‌دهد

- Pentesters سؤالاتی درباره معماری دستگاه، فرآیند به‌روزرسانی Firmware ، مکانیزم Authentication ، و پروتکل‌های ارتباطی مطرح می‌کنند
- مشتری هم متدولوژی تست و روش گزارش‌دهی تیم را می‌بیند

طبق استانداردهای اخیر OWASP IoT Top 10 2024 ، در این مرحله باید تمرکز روی **Data Flow Diagram** و **Threat Modeling** باشد تا مسیر داده‌ها و نقاط حمله احتمالی مشخص شوند

Attacker Simulated Exploitation

- بخش اصلی تست که تیم نفوذگر مثل یک **هکر واقعی** عمل می‌کند
- تیم‌ها به صورت موازی کار می‌کنند
  - تیم Firmware ← آنالیز، استخراج، Reverse Engineering
  - تیم Embedded Devices ← سخت‌افزار، Serial/JTAG، Side Channel Attacks
  - تیم Software/Web/Mobile ← تست اپلیکیشن و API
  - تیم Radio ← شنود و Exploitation پروتکل‌های بی‌سیم Wi Fi, ZigBee, BLE, LoRa
- هدف شناسایی و Exploit کردن آسیب‌پذیری‌ها و تولید **Proof of Concept PoC**

مثال عملی در یک Pentest واقعی روی Smart Hub خانگی، تیم امنیتی توانستند از طریق یک **پورت Telnet بدون پسورد** وارد سیستم شوند و دسترسی Root بگیرند

Remediation

- پس از ارائه گزارش، تیم امنیتی با توسعه‌دهندگان همکاری می‌کند
- علاوه بر پیشنهادPatch ، جلسات مشترک برای آموزش تیم توسعه برگزار می‌شود تا همان خطا دوباره تکرار نشود
- در بسیاری از پروژه‌هایIoT ، توسعه‌دهندگان آشنایی کامل با امنیت ندارند؛ به همین دلیل، این مرحله **آموزشی + اصلاحی** است

Reassessment

- پس از رفع آسیب‌پذیری‌ها، تست مجدد روی دستگاه انجام می‌شود
- نکته مهم نباید فقط همان آسیب‌پذیری تست شود؛ زیرا ممکن است اصلاح کد باعث ایجاد **Bugجدید در بخش دیگر** شده باشد
- این مرحله باعث اطمینان می‌شود که دستگاه به نسخه امن ارتقا یافته است

تیم ایده‌آل برای IoT Pentest

طبق تجربه و تحقیقات جدید، تیم نفوذ IoT باید حداقل سه تخصص اصلی را پوشش دهد

1. **Hardware/Firmware Specialist**
2. **Software/Web/Mobile Specialist**
3. **Radio Communication Specialist**

بهترین نتیجه زمانی حاصل می‌شود که این تیم‌ها به صورت موازی روی بخش‌های مختلف کار کنند و یافته‌های خود را با هم به اشتراک بگذارند

با این ساختار، تست نفوذ IoT از یک فرآیند پراکنده به یک **چرخه منسجم** تبدیل می‌شود که شامل تعامل با مشتری، تحلیل فنی، شبیه‌سازی حمله، اصلاح و بازبینی است