دانشکده مهندسی کامپیوتر

پایان‌نامه دوره کارشناسی ارشد

شبکه ها کامپیوتری

عنوان پروژه:

پیاده‌سازی معماری شبکه بدون اعتماد (Zero Trust)

دانشجویان:

محمد طالبی، احمد فروغی، علیرضا کریمی

استاد:

دکتر کعبه یعقوبی

بهار 1404


بسم الله الرحمن الرحیم

چکیده

در این تحقیق، پیاده‌سازی معماری شبکه بدون اعتماد (Zero Trust) با استفاده از ابزارهای متن‌باز در شبکه دانشگاه صنعتی خواجه‌نصیرالدین طوسی بررسی شده است. در این مطالعه، ابتدا دلایل نیاز به معماری بدون اعتماد و چارچوب نظری آن شرح داده می‌شود. سپس فرآیند انتخاب، استقرار و پیکربندی Elastic SIEM برای نظارت و تشخیص تهدیدها و Keycloak برای مدیریت هویت و دسترسی ارائه می‌گردد. در ادامه، شبیه‌سازی حملات واقعی و استخراج قوانین تشخیص سفارشی برای کاهش موارد مثبت کاذب توضیح داده شده است. نتایج نشان می‌دهد که این پیاده‌سازی توانایی شناسایی رفتارهای مخرب در سطح شبکه و کنترل هویت کاربران را با کارایی بالا فراهم می‌کند.

واژگان کلیدی:

شبکه بدون اعتماد، SIEM، Keycloak، امنیت اطلاعات، نظارت بر رخدادها

مقدمه

با توجه به رشد روزافزون تهدیدات سایبری و پیچیدگی روزافزون زیرساخت‌های شبکه‌ای در دانشگاه‌ها، رویکردهای سنتی مبتنی بر "حلقه‌ای امن در پیرامون شبکه" (Perimeter Security) دیگر پاسخگوی نیازهای امنیتی نیستند.

معماری شبکه بدون اعتماد (Zero Trust Network Architecture) مبتنی بر اصل «هرگز اعتماد نکن، همیشه صحت‌سنج!» است که فرض را بر عدم اعتماد به هیچ کاربر یا سیستمی، چه درون شبکه و چه برون آن، می‌گذارد. این رویکرد، با تأکید بر کنترل دقیق دسترسی، نظارت لحظه‌ای بر ترافیک و اعتبارسنجی مداوم کاربران و دستگاه‌ها، می‌تواند سطح امنیت را به‌طور چشمگیری افزایش دهد.

در این مقاله، علاوه بر بیان مبانی نظری معماری بدون اعتماد، مراحل پیاده‌سازی عملی آن با استفاده از دو ابزار متن‌باز مطرح، یعنی Elastic SIEM برای نظارت و تشخیص تهدید و Keycloak برای مدیریت هویت و

دسترسی، در شبکه دانشگاه صنعتی خواجه‌نصیرالدین طوسی تشریح می‌شود. سپس نتایج شبیه‌سازی حملات و سنجش کارایی این ساختار ارائه می‌گردد.

---

۱. مبانی نظری و پیشینه تحقیق

مفهوم Zero Trust برای نخستین بار توسط جان کین (John Kindervag) در سال ۲۰۱۰ ارائه شد. در این مدل، شبکه به چندین بخش تقسیم می‌شود و کنترل دسترسی بر اساس هویت و سیاست‌های دسترسی پویا اعمال می‌گردد. مطالعه‌های متعددی نشان داده‌اند که استفاده از SIEM برای جمع‌آوری لاگ‌ها و تحلیل رخدادها در کنار IAM (مدیریت هویت و دسترسی) قوی، ضریب نفوذپذیری به حملات را کاهش می‌دهد.
همچنین پژوهش‌های دانشگاهی مختلف، چشم‌انداز و چالش‌های پیاده‌سازی Zero Trust را در محیط‌های دانشگاهی مورد بررسی قرار داده‌اند.
در این راستا، Elastic SIEM به عنوان یک راهکار جامع برای جمع‌آوری لاگ‌ها، تشخیص تهدیدات و مصورسازی داده‌های امنیتی شناخته شده است؛ و Keycloak به عنوان یک سرویس مدیریت هویت متن‌باز، امکانات SSO ، MFA و ادغام با LDAP/AD را فراهم می‌کند.

---

۲. ابزارها و فناوری‌های مورد استفاده

در این بخش ابزارها و فناوری‌های اصلی به کار رفته در پروژه معرفی و کاربرد هر یک توضیح داده می‌شود.

۲.۱ Elastic SIEM

یک بسته‌ی یکپارچه امنیتی بر پایه‌ی:

Elastic Stack (Elasticsearch, Kibana, Beats, Logstash)

قابلیت‌ها:

- جمع‌آوری لاگ از منابع متعدد (سرورها، فایروال‌ها، اپلیکیشن‌ها)
- تشخیص ناهنجاری‌ها و تهدیدهای زمان واقعی
- طراحی داشبوردهای سفارشی در Kibana برای نمایش رخدادها و الگوهای حملات

Keycloak۲.۲

توضیح Keycloak :یک راهکار مدیریت هویت و دسترسی متن‌باز است که امکانات زیر را ارائه می‌دهد:

- احراز هویت تک‌نقطه‌ای (SSO) برای چندین اپلیکیشن
- مدیریت کاربران، نقش‌ها و مجوزها
- پشتیبانی از پروتکل‌های OAuth 2.0 ، OpenID Connect وSAML
- ادغام با LDAP و Active Directory

---

۳. مراحل پیاده‌سازی

در این فصل، مراحل مختلف تحقیق و پیاده‌سازی به ترتیب ارائه می‌شوند:

۳.۱ تحقیق و برنامه‌ریزی

مقایسه‌ی راهکارها :پس از بررسی راهکارهای مرسوم SIEM وIAM ، Elastic SIEMو Keycloak به دلیل امکانات گسترده و جامعه‌ی کاربری فعال برگزیده شدند.

تهیه‌ی طرح کلی :تدوین اهداف تحقیق و تعریف شاخص‌های موفقیت (مانند میزان شناسایی حملات، تعداد مثبت کاذب).

۳.۲ استقرار اولیه

راه‌اندازی Elastic Stack:

1. نصب Elasticsearch با تنظیمات مربوط به امنیت داخلی
2. نصب Kibana و پیکربندی ارتباط باElasticsearch
3. نصب و راه‌اندازی Fleet Server برای مدیریتagent ها

نصب و پیکربندی:Keycloak

1. استقرار سرویس Keycloak بر روی یک ماشین مجازی یا کانتینر
2. پیکربندی Realm جدید و تعریف Client وRole های موردنظر

۳.۳ تنظیم نظارت امنیتی

نصب Elastic Agent: نصب agent بر روی چندین ماشین در شبکه دانشگاه (سرورهای لینوکسی و ویندوز) و اتصال آن‌ها به.Fleet Server

گردآوری لاگ‌ها: تعریف log sources شامل سیستم‌عامل، فایروال‌های سخت‌افزاری و اپلیکیشن‌های وب.

۳.۴ تعریف قوانین تشخیص

تهیه‌ی قوانین اولیه: بر اساس میانگین ترافیک عادی، قوانینی برای شناسایی فرآیندهای مشکوک و الگوهای غیرعادی نوشتیم.

کاهش مثبت کاذب: اعمال فیلتراسیون بر اساس لیست سفیدIP های داخلی و تعریف شرایط محدودکننده (مانند چندین تلاش ناموفق ورود پشت سر هم).

۳.۵ مدیریت احراز هویت

تعریف Realm وClient: درKeycloak ، یک Realm با نام KNTU_ZeroTrustایجاد و Clientهایی برای اپلیکیشن‌های شبیه‌سازی شده تعریف شد.

تخصیص Role و Policy: ساخت Roles مبتنی بر گروه‌های کاربری (دانشجو، هیئت علمی، ادمین) و ارتباط آن‌ها با سرویس‌های شبکه.

فعال‌سازی MFA: پیاده‌سازی تأیید هویت چندمرحله‌ای با استفاده از TOTP.

۳.۶ طراحی داشبوردها

داشبورد رخدادهای امنیتی :ایجاد داشبوردهای Kibana برای نمایش تعداد لاگ‌های ورود، هشدارهای تشخیص نفوذ و وضعیتagent ها.

داشبورد فعالیت‌های Keycloak: نمایش آمار ورودهای ناموفق، ورودهای موفق و درخواست‌های دسترسی غیرمجاز.

---

۴. شبیه‌سازی حملات

برای ارزیابی اثربخشی معماری بدون اعتماد، حملات زیر شبیه‌سازی شدند:

1. شبیه‌سازی شل معکوس(Reverse Shell): با استفاده از ابزارهای رایگان مانند netcat و اسکریپت‌های آماده درrevshells.com ، تلاش شد که ارتباط معکوس از شبکه به یک سرور خارج برقرار شود.

2. حملات اجرای فرآیندهای مخرب: اجرای فرآیندهای با نام غیرمعمول و ارسال بسته‌های مشکوک به شبکه.

3. تلاش‌های ناموفق ورود(Brute Force): شبیه‌سازی تلاش‌های ناموفق پی‌درپی برای دسترسی به حساب‌های کاربری.

نتایج تشخیص

- لاگ‌های Elastic SIEM: تمامی تلاش‌های ورود و اجرای فرآیندهای مخرب با قوانینی که تعریف شد شناسایی شده و در داشبوردها به نمایش درآمدند.

- شناسایی شل معکوس :نمونه‌ای از بسته‌های خروجی شناسایی گردید و هشدار مربوطه توسط Elastic SIEM تولید شد.

- گزارش Keycloak: تمامی تلاش‌های ناموفق ورود به درستی ثبت گردیدند و پس از چند تلاش متوالی، کاربر مسدود شد.

---

۵. بحث و تحلیل نتایج

تحلیل داده‌های به‌دست‌آمده نشان می‌دهد که:

- کفایت قوانین تشخیص: با تعریف دقیق شرایط (مثلاً حداقل تعداد تلاش‌های ناموفق)، تعداد مثبت‌های کاذب تا حدود ۱.۵٪ کاهش یافت.

- وجود نقص‌های احتمالی: برخی حملات پیچیده‌تر (مانند Exfiltration داده‌ها با نام ترافیک مجاز) شناسایی نشدند که نیازمند توسعه قوانین هستند.

- عملکرد Keycloak: سرعت پاسخ‌دهی در پردازش رخدادهای ورود در حد نیم‌ثانیه بود که برای یک محیط دانشگاهی قابل‌قبول ارزیابی شد.

- محدودیت‌ها: عدم وجود تحلیل کامل ترافیک رمزنگاری‌شده (TLS) در SIEM و نیاز به نصب SSL/TLS Inspectionدر فایروال.

نتیجه‌گیری:

در این پژوهش، چارچوب عملیاتی برای پیاده‌سازی معماری شبکه بدون اعتماد در محیط دانشگاهی ارائه شد. با استفاده از Elastic SIEM وKeycloak ، توانستیم نقاط زیر را به دست آوریم:

1. شناسایی و کشف تهدیدات: با تعریف قوانین سفارشی، حملات شبیه‌سازی‌شده به‌طور مؤثری شناسایی شدند.

2. کنترل دقیق دسترسی: با استقرار Keycloak و تعریف نقش‌های مبتنی بر سیاست، توانستیم سطح دسترسی کاربران را بر اساس هویت و نقش آن‌ها محدود کنیم.

3. گزارش‌دهی بلادرنگ: داشبوردهای پیاده‌سازی‌شده امکان نظارت لحظه‌ای بر رخدادهای امنیتی را فراهم کردند.

اگرچه این پیاده‌سازی در مقیاس یک شبکه دانشگاهی انجام شد، اما اصول و روش‌های ارائه‌شده قابل تعمیم به دیگر سازمان‌ها نیز خواهد بود. برای کارهای آتی، پیشنهاد می‌شود که ماژول‌های پیشرفته‌تر تحلیل ترافیک رمزنگاری‌شده به SIEM افزوده شود و سیاست‌های دقیق‌تری برای حفظ حریم خصوصی و تطابق با مقررات تدوین گردد.

مرجع:

Mtlbd & Pyhp2017 & alizk79 (2025). *Zero Trust Network Architecture Implementation*. GitHub repository.

(https://github.com/Mtlbd/zero-trust-network-kntu-master)
(https://github.com/pyhp2017/zero-trust-network-kntu-master)
(https://github.com/alizk79/zero-trust-network-kntu-master)

K. N. Toosi University of Technology

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of Master of Science (M.Sc.)
in Computer Networking.

Title:

Zero Trust Network Architecture Implementation

By:

Mohammad Talebi, Ahmad Foroughi, AliReza Karimi

Professor:

Dr. Kaebeh Yaeghoobi

Spring 2025