firewall

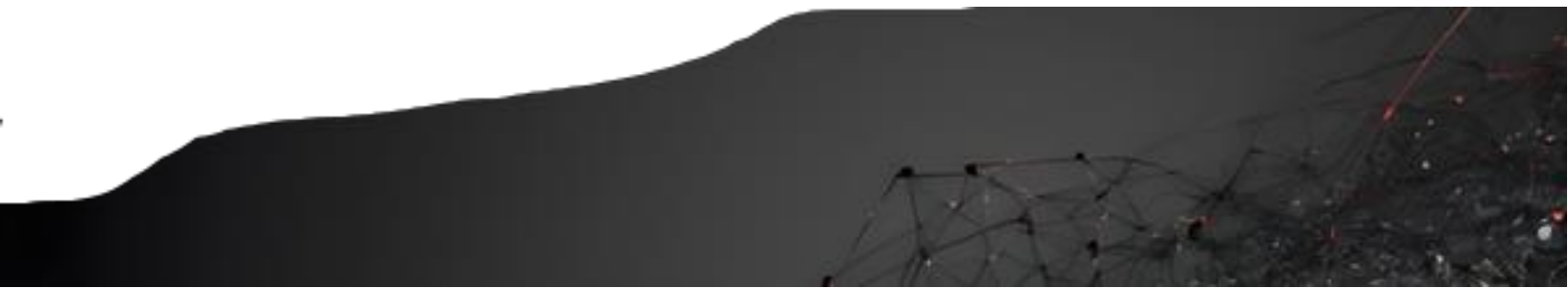
معرفی

DPI (Deep Packet Inspection) امنیت شبکه را با بررسی محتوای بسته های داده در حین عبور از یک ایست بازرسی افزایش می دهند که امکان تجزیه و تحلیل دقیق تری را در مقایسه با فیلتر کردن بسته های اولیه فراهم می کند و همجنین امکان شناسایی و جلوگیری از تهدیدات سایبری پیچیده را فراهم می کند. DPI می‌تواند ترافیک شبکه را در زمان واقعی (Real Time) شناسایی، دسته‌بندی و مدیریت کند که می‌تواند با افزودن تأخیر و نیاز به منابع محاسباتی قابل‌توجه بر عملکرد تأثیر بگذارد. با این حال، ابزارهای DPI مدرن برای تعادل بین امنیت و عملکرد بهینه شده اند.

انواع ابزارهای DPI

ابزارهای DPI را می توان بر اساس عملکردشان به چند نوع دسته بندی کرد:

- DPI مبتنی بر امضا (Signature-Based DPI): تهدیدات شناخته شده را با مقایسه محتویات بسته با پایگاه داده امضاهای تهدید شناسایی می کند.
- DPI مبتنی بر اکتشافی (Heuristic-Based DPI): از الگوریتم‌هایی برای شناسایی الگوها یا رفتارهای غیرعادی در ترافیک شبکه استفاده می‌کند که ممکن است تهدیدهای جدید یا ناشناخته را نشان دهد.
- DPI مبتنی بر رفتار (Behavioral-Based DPI): رفتار برنامه‌ها و کاربران را برای تشخیص ناهنجاری‌ها و نقض‌های امنیتی احتمالی نظارت می‌کند.
- DPI تجزیه و تحلیل پروتکل (Protocol Analysis DPI): پروتکل ها و انطباق آنها با استانداردها را برای شناسایی ناهنجاری ها و آسیب پذیری های احتمالی بررسی می کند.



برنامه های کاربردی(Applications)

ابزارهای DPI برای اهداف مختلفی در امنیت شبکه استفاده می شوند:

- تشخیص نفوذ و پیشگیری(Intrusion Detection and Prevention): شناسایی و مسدود کردن ترافیک مخرب در زمان واقعی.
- پیشگیری از نشت داده(Data Leak Prevention): نظارت و کنترل جریان اطلاعات حساس برای جلوگیری از دسترسی یا انتقال غیرمجاز.
- شکل دهی و مدیریت ترافیک(Traffic Shaping and Management): بهینه سازی و مدیریت ترافیک شبکه برای اطمینان از استفاده کارآمد از پهنای باند.
- فیلتر محتوا (Content Filtering): مسدود کردن دسترسی به محتوای نامناسب یا مضر با بازرسی بسته های داده.

فایروال یک دستگاه یا نرم افزار امنیتی شبکه است که ترافیک ورودی و خروجی شبکه را بر اساس قوانین امنیتی از پیش تعیین شده نظارت و کنترل می کند. هدف اصلی آن ایجاد مانعی بین یک شبکه داخلی قابل اعتماد و شبکه‌های خارجی غیرقابل اعتماد مانند اینترنت است تا از دسترسی غیرمجاز جلوگیری کند و در برابر تهدیدات سایبری مختلف محافظت کند.

فایروال ها را می توان به اشکال مختلف پیاده کرد که انواع آن به شرح زیر است:

از جمله ابزارهای سخت افزاری می‌توان به Bitdefender BOX، Cisco Firepower، Netgear ProSAFE و ... اشاره کرد.

از جمله ابزار های برنامه های کاربردی نرم افزاری می‌توان به ZoneAlarm ، Norton 360 ، Comodo Firewall و ... اشاره کرد.

از جمله ابزار های درون خود سیستم عامل می‌توان به Windows Defender Firewall ، MacOS Firewall ، iptables/nftables ، ufw (Uncomplicated Firewall) ، pf (Packet Filter) و ... اشاره کرد.

با استفاده از IPTables و Netfilter، مدیران می توانند راه حل های فایروال قوی را پیاده سازی کنند که به طور موثر از شبکه ها و سیستم ها در برابر دسترسی غیرمجاز، حملات مخرب و سایر خطرات امنیتی محافظت می کند. نهایتا، IPTables و Netfilter نقش مهمی در افزایش امنیت شبکه و تقویت دفاع از محیط‌های مدرن فناوری اطلاعات دارند.

IPTables: Packet Filtering، همراه با Netfilter، قابلیت‌های قدرتمندی برای فیلتر کردن بسته‌ها فراهم می‌کند و به مدیران این امکان را می‌دهد تا قوانینی را تعریف کنند که تعیین می‌کنند کدام بسته‌ها مجاز به عبور از سیستم هستند و کدام بسته‌ها مسدود شده‌اند. این قابلیت فایروال را قادر می سازد تا سیاست های کنترل دسترسی را بر اساس عواملی مانند آدرس های IP مبدا و مقصد، شماره پورت ها و پروتکل ها اعمال کند.

Netfilter: یک فریمورک فراهم شده توسط کرنل لینوکس است که اطلاعات ردیابی اتصال را برای اتصالات شبکه فعال تامین می‌کند و توانایی انجام تغییرات و عملیات های مرتبط با شبکه را به صورت شخصی سازی شده فراهم می کند. این فریمورک در لایه کرنل عمل می کند و کاربر دسترسی مستقیم به این لایه ندارد. در نتیجه برای ایجاد تغییرات دلخواه از ابزارهای لایه userspace مانند iptables استفاده می شود. این بدان معناست که IPTables می تواند به طور هوشمندانه وضعیت اتصالات شبکه را ارزیابی کنند و بر اساس زمینه هر بسته، تصمیمات فیلترینگ را اتخاذ کنند، مانند اینکه آیا بخشی از یک اتصال برقرار شده یا تلاش برای اتصال جدید است.

Network Address Translation(NAT): IPTables از ترجمه آدرس شبکه (NAT) پشتیبانی می کند و به فایروال اجازه می دهد آدرس های IP مبدا یا مقصد و شماره پورت ها را در سرصفحه های بسته تغییر دهد. NAT معمولاً برای اهدافی مانند مخفی کردن آدرس‌های IP داخلی از شبکه‌های خارجی، امکان اشتراک‌گذاری چندین دستگاه داخلی برای اشتراک‌گذاری یک آدرس IP عمومی یا تسهیل نگاشت سرویس‌های خارجی به میزبان‌های داخلی استفاده می‌شود.

- Iptables یک ابزار خط فرمان است که در userspace مورد استفاده قرار می گیرد (توسط کاربر قابل استفاده است و یک user program محسوب می شود) و اجازه می دهد که کاربران قوانین فیلترینگ خود را در فریمورک فیلترینگ netfilter اعمال کنند
- فریمورک netfilter در لایه کرنل عمل می کند و ابزارهای iptables/nftables وابسته به این فریمورک هستند. در نتیجه netfilter به نوعی زیرساخت اصلی سیستم فیلترینگ کرنل لینوکس است و ابزارهای iptables/nftables به کاربر توانایی استفاده از این فریمورک می دهند.

دانشگاه فردوسی مشهد

آزمایشگاه امنیت شبکه

تاریخ تحویل: ۱۴۰۳/۰۳/۲۹

هدف

هدف این تمرین ارائه تجربه عملی در پیکربندی، استقرار و ارزیابی راه حل های فایروال با استفاده از IPTables و درک عملکرد و اهمیت ابزارهای DPI(Deep Packet Inspection) در امنیت شبکه است.

درک اصول IPTables، که یک برنامه کاربردی فضای کاربر است که به مدیر سیستم اجازه می دهد تا جداول ارائه شده توسط فایروال هسته لینوکس (که در پروژه Netfilter پیاده سازی شده است) را پیکربندی کند. کاوش دقیق مدیریت بسته در سه حالت اصلی: ورودی(input)، خروجی(output) و فوروارد(forward).

فعالیت‌های درون کلاسی کار با IP-Tables

۱. مسئله

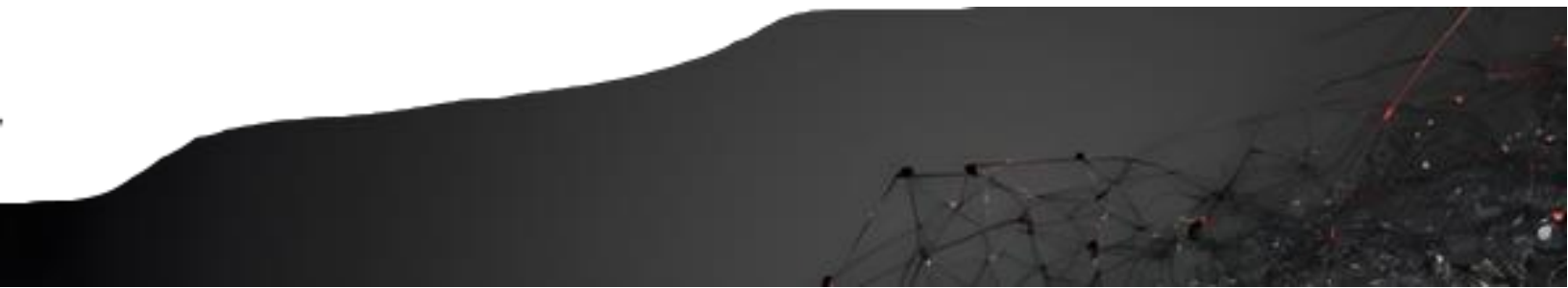
این قسمت به دو بخش تقسیم می‌شود که شرح هر یک به صورت زیر است:

بخش اول(مقدمه ای بر IPTables)

- سه حالت اولیه مدیریت بسته که بخش های پیشین اشاره شده را بررسی کنید (تعریف، دلایل استفاده و تفاوت هر یک)
- یک مثال دنیای واقعی از کاربرد هریک حالت ها را توضیح دهید.

بخش دوم (سه حالت اولیه مدیریت بسته)

- در ابدا یک IPTables در یک ماشین مجازی دارای نسخه لینوکس راه اندازی کنید.
- مرحله اول: نمایش قوانین IP Table فعلی
- مرحله دوم: افزودن یک/چند قانون جدید به واسطه دستور در خط فرمان و نمایش مجدد جدول قوانین
- مرحله سوم: ذخیره قوانین ایجاد شده در یک فایل
- مرحله سوم: حذف یک/چند قانون فعلی به واسطه دستور در خط فرمان و نمایش مجدد جدول قوانین
- مرحله چهارم: بازیابی قوانین ذخیره شده
- تمرین های عیب یابی(troubleshooting exercises) را برای تقویت درک رفتار IPTables انجام دهید.



۲. نیازمندی‌ها

درک اولیه CLI لینوکس و مفاهیم شبکه (استفاده از یک نسخه توزیع شده لینوکس)

تکلیف در منزل- کار با Snort

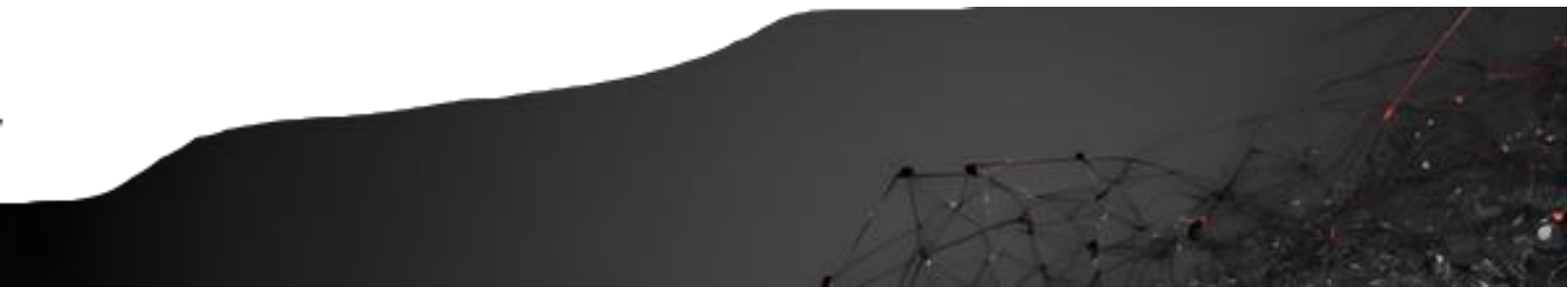
۱. مسئله

تئوری:

- معماری و عملکرد کلی DPI را شرح دهید.
- ابزارها و برنامه های DPI برای امنیت شبکه را لیست کرده، عملکرد، مزایا و معایب آنها را با هم مقایسه کنید
- معماری و عملکرد ابزار Snort را تحلیل و بررسی کنید.
- IPTables و Snort را از جنبه های مختلف مقایسه کنید
- نقش DAQ در فرآیند نصب ابزار Snort چیست؟

عملی:

- نصب و پیکربندی ابزار منبع باز DPI (Snort) را بر روی ماشین DUT انجام دهید.
- Snort را بر روی چند pcap فایل آلوده اجرا و نتایج حاصل از مطابقت بسته‌ها با signature های موجود در ابزار را در فایل های Log بیان کنید.
- مکان پیش فرض ذخیره سازی هشدار های ابزار Snort را مشخص کنید و به واسطه آن Log های موجود را نمایش دهید.
- ابزار Snort را به گونه‌ای پیکر بندی کنید که تمامی هشدار های تولیدی به ازای بسته های TCP دریافتی را به ماشین OUT بعنوان یک کارگزار SYSLOG راه دور ارسال شود.



- ارزیابی سرعت: با تولید ترافیک و ارسال آن به سمت ماشین DUT قدرت ابزار را در جهت تحلیل بسته های دریافتی اندازه گیری کنید. (تعداد بسته ها و میزان پهنای باند عبوری مطابقت داده شده را قبل و بعد ازتنظیم SYSLOG راه دور بررسی کنید.)
- ارزیابی دقت. تولید ترافیک آلوده

۲. نیازمندی‌ها

پیاده سازی و استفاده از سه ماشین IN، OUT و DUT و ابزار Snort

۳. نکات قابل توجه

- مهلت تحویل تکلیف، ساعت ۲۳:۵۵ روز سه‌شنبه مورخ ۱۴۰۳/۰۳/۲۹می‌باشد.
- دانشجویان گرامی تا تاریخ مشخص شده فرصت دارند تا فایل‌های زیر را در سامانه مجازی درس در آزمایش۷ آپلود نمایند. در غیر اینصورت، تاخیر در ارسال پاسخ مشمول کسر نمره خواهد شد.
- هر دو فایل کدهای اجرایی و پیاده‌سازی شده و ضبط صفحه همراه با توضیح تکلیف بایستی در قالب فشرده تحت عنوان StudentName_StudentID (به جای StudentName نام خانوادگی و به جای StudentID شماره دانشجویی خود را وارد نمایید.)
- این تکلیف به‌صورت فردی تعریف شده و قابل انجام است.

چه عواملی باعث می شود از این فعالیت نمره کسب نکنید:

- عدم تحویل فایل ها در سامانه vu
- فقط انجام بخش تئوری بدون انجام بخش عملی
- عدم ضبط ویدیو بر روی بخش عملی
- مشاهده شباهت بیش از حد معقول
- عدم تسلط به موضوع در جلسه ارائه سر کلاس

چه عواملی باعث می شود نصف نمره را کسب کنید؟

- تحویل فایل در سامانه vu، اما عدم ارائه در کلاس درس یا غیبت در روزی که ارائه باشد و نام فرد یا تیم برای ارائه تعیین شده باشد.
- عدم تحویل در زمان مقرر و تحویل با تاخیر.