هو الحق

دانشکده‌ی مهندسی کامپیوتر

CE-40443 بهار ـ ۰۱

شبکه‌های کامپیوتری: تمرین سوم

مدرس: مهدی جعفری

۱

در خصوص شبکه‌های نرم‌افزار محور (SDN: Software Defined Network) تحقیق کرده و علل استفاده، انواع روش‌های پیاده‌سازی و مزایای آن‌ها را شرح دهید.

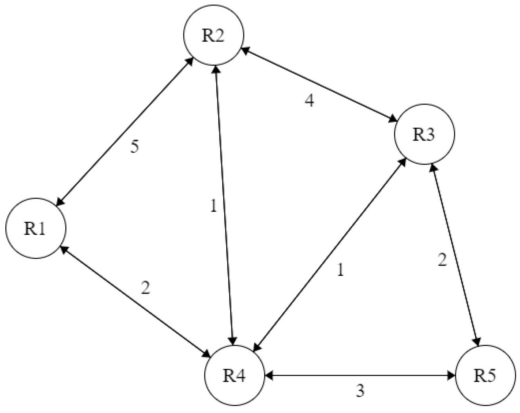
۲

۱. در خصوص تفاوت پیام عادی و Secret Chat تلگرام تحقیق کرده و تفاوت آن‌ها را بیان کنید. هر کدام از این پیام‌ها به چه صورت توسط سرور تلگرام تفسیر می‌شود و چگونه بین دو کاربر منتقل می‌شود؟

۲. تفاوت پیام در واتساپ که ادعا میکند P2P است با Secret Chat تلگرام چیست؟ توضیح دهید اگر پیام در واتساپ واقعاً P2P است چطور میتوان محتوای یک چت را هم در لپتاپ و هم در گوشی مشاهده کرد؟

۳

شبکه زیر با پنج مسیریاب را در نظر بگیرید. اعداد نوشته شده بر روی هریک از یال ها وزن هر لینک است:



۱. با استفاده از الگوریتم link state مرحله به مرحله هزینه رسیدن از مسیریاب ۱ به سایرین را مشخص کنید.

۲. حال الگوریتم بردار حالت را بروی آن اجرا کنید و توضیح دهید از تکنیک reverse poisoning چگونه میتوان برای حل مشکلاتی که ممکن است در این الگوریتم پیش بیاید، استفاده می‌شود.

۴

پنج مسیریاب با نام‌های A-E داریم که Table Forwarding آن‌ها پس از آنکه پروتکل RIP به وضعیت ایستا آمده است، در جدول‌های زیر آمده است. هزینه هر لینک را ۱ فرض کنید.

Forwarding Table For A		
Destination	Cost	Next Hop
A	۰	–
B	۱	B
C	۲	D
D	۱	D
E	۲	B
F	۳	B

Forwarding Table For B		
Destination	Cost	Next Hop
A	۱	A
B	۰	–
C	۳	E
D	۲	A
E	۱	E
F	۲	E

Forwarding Table For C		
Destination	Cost	Next Hop
A	۲	D
B	۳	F
C	۰	–
D	۱	D
E	۲	F
F	۱	F

Forwarding Table For D		
Destination	Cost	Next Hop
A	۱	A
B	۲	A
C	۱	C
D	۰	–
E	۳	A
F	۲	C

Forwarding Table For E		
Destination	Cost	Next Hop
A	۲	B
B	۱	B
C	۲	F
D	۳	B
E	۰	–
F	۱	F

Forwarding Table For F		
Destination	Cost	Next Hop
A	۳	C
B	۲	E
C	۱	C
D	۲	C
E	۱	E
F	۰	–

۱. اگر پیامی بخواهد از D به F برود چه مسیری را طی خواهد کرد؟

۲. اگر پیامی بخواهد از A به F برود چه مسیری را طی خواهد کرد؟

یک گراف شبکه ممکن برای این جداول ارایه دهید.

۵

در اکتبر ۲۰۲۱ برای Facebook مشکلی پیش آمده و Facebook, Instagram و دیگر سرویس‌های Facebook از دسترس خارج شدند. در خصوص علت ناپدید شدن Facebook از اینترنت سرچ کرده و آن را شرح دهید. همچنین در خصوص حمله‌های محتمل توضیح دهید و علت آن که در آن زمان IP Facebook از سمت ایران resolve می‌شد، تحقیق کنید.

۶ قسمت عملی

در این بخش قصد داریم ابزاری جهت مدیریت ترافیک شبکه طراحی کنیم که دستورات مدیر شبکه مبنی بر اعمال قوانین گوناگون را بر شبکه اعمال کند. بدین منظور لازم است با هسته اجرایی این دستورات آشنا شوید:
در ابتدا محبوب‌ترین بسته Firewall در لینوکس، ipchains بود که دارای کاستی‌هایی بود. برای اصلاح این کاستی‌ها، Netfilter تصمیم گرفت محصول جدیدی به نام iptables با بهبودهای زیر را توسعه دهد:

۱. ادغام بهتر با کرنل لینوکس با قابلیت بارگیری کرنل ماژول‌های مخصوص iptables که برای بهبود سرعت و افزایش قابلیت اطمینان طراحی شده اند.

۲. قابلیت stateful packet inspection که به این معناست که Firewall هر اتصال عبوری را از طریق آن ردیابی می کند و در موارد خاص محتوای جریان داده را مشاهده می کند تا تلاش بعدی پروتکل‌های خاص را پیش بینی کند. این یک ویژگی مهم در پشتیبانی از active FTP و DNS active و همچنین بسیاری از سرویس های شبکه است.

۳. فیلتر کردن بسته‌ها بر اساس آدرس MAC و Flag های هدر TCP که این امر در جلوگیری از حملات با استفاده از بسته‌های ناقص مفید است.

۴. قابلیت system logging که امکان تنظیم سطح گزارش‌گیری را فراهم می‌آورد.

۵. یک ویژگی محدود کردن نرخ که به iptables کمک می کند تا برخی از انواع حملات ممانعت از سرویس (DoS) را مسدود کند.

بدین صورت iptables با سرعت و ایمنی بالاتر در مقایسه با ipchains ، به Firewall پیش‌فرض توزیع‌های Ubuntu ، ،RedHat Debian و Fedora تبدیل شده است. در این تمرین از شما خواسته می‌شود تا یک Firewall پیشرفته را با استفاده از Firewall های پیشفرض سیستم‌عامل توسعه دهید که امکانات زیر را فراهم نماید:

◁ قابلیت مسدودسازی ترافیک ورودی و خروجی به ،IP ،Domain Regex URL و Port مورد نظر مدیر شبکه

◁ محدودسازی ترافیک ورودی و خروجی بر اساس تعداد، پروتکل و نوع درخواست

*نکته: در این بخش پروتکل‌های HTTPS HTTP DHCP DNS SMTP SSH FTP مدنظر می‌باشد. توجه کنید برای هر کدام باید با توجه به مفهوم آن پروتکل عمل کنید:

- در پروتکل FTP کاربر مدیر میتواند تنها اخذ فایل خاصی را محدود کند.
- در SSH اتصال نام کاربری خاصی میتواند محدود شود.
- در DNS درخواست URL خاصی میتواند فیلتر شود و Firewall باید بتواند درخواست را در صورتی که جهت resolve دامنه مشخصی است، بی‌پاسخ گذاشته و یا پاسخ خطای مناسب را خروجی دهد.
- در DHCP سامانه باید به‌گونه‌ای عمل کند که به MAC آدرس‌های مشخصی، جواب نداده و یا پاسخ خطای مناسب را خروجی دهد.
- در HTTPS HTTP باید بتوان محتوای ارسالی را فیلتر نمود و به صورت مشخص در HTTP در صورت وجود لغات و یا محتوای مدنظر مدیر، فیلتر صورت گیرد.

◁ قابلیت بررسی Header های درخواست و مسدود سازی Header با مقدار مورد نظر

*نکته: این قابلیت باید درخواست‌هایی که Header آن‌ها دارای مقادیر خاصی است را فیلتر کند.

◁ قابلیت ترکیبی حفاظت در برابر حملات منع سرویس (DoS) که باید علاوه بر حالت پیشفرض، به مدیر قابلیت تغییر در پارامترهای هشدار دهنده و پیشگیرانه را دهد.

*نکته: در این قسمت به صورت مشخص جهت مقابه در برابر DNS Flood ، Slowloris و SYN Flood راهکار ارائه دهید.

◁ بهره‌گیری از پایگاه داده و استفاده از آن در جهت بهبود عملکرد سامانه حفاظتی در برابر DoS

*نکته: در این بخش میتوانید از IP و مشخصات کاربران قبلی استفاده کنید تا از تاریخچه آن‌ها جهت تائید هویت آن‌ها استفاده کنید.

◁ مسدودسازی Port Scanner ها و قابلیت Port Knocking

*نکته: قابلیت Port knocking یک روش مخفی برای باز کردن هاییPort است که به طور پیش فرض توسط Firewall بسته نگه داشته شده است. هنگامی که توالی صحیح پورت "ضربه" (تلاش برای اتصال) دریافت میکنند، Firewall قانون خود را عوض کرده و Port مخفی شده را باز می کند تا اتصال برقرار شود. مزیت این کار این است که برای یک Port Scanner عادی، این هاPort بسته می‌ماند.
تحقیق کنید آیا یک مهاجم با قدرت پردازشی عادی، می تواند سیستم Port knocking را شکست دهد؟

برای این تمرین می‌توانید از Bash یا Python استفاده کنید هرچند توصیه می‌شود دستورات را ابتدا در ترمینال زده و سپس با استفاده از Python رابط کاربری و سازوکار دریافت ورودی را پیاده‌سازی کنید.

موفق باشید