KNO-1003-4105

نگاشت لایه های شبکه خارجی از طریق آسیب‌پذیری پروتکل های TCP/IP

حسین شادی[۱] ho3einshadi@gmail.com
یعقوب فرجامی[۲] farjami@gmail.com

[۱]فارغ الحصیل، کارسناسی ارشد، مهندسی فناوری اطلاعات، دانشگاه قم، ایران
[۲]استاد، دانشیار، مهندسی فناوری اطلاعات، دانشگاه قم، ایران

چکیده: برای نگاشت لایه دوم شبکه باید از آسیب پذیری پروتکل های مسیریابی داخلی استفاده کنیم تا بدانیم در داخل یک روتر چه سیستم هایی سرویس می‌گیرند، این آسیب پذیری ها برای پروتکل *RIP* روی پورت ۵۲۰ و برای *OSPF* روی پورت ۸۹ قابل مشخص می با شد و فقط کافی ست برای تعامل با این پروتکل ها با ا ستفاده از سرویس گیرنده آن که جزئیات بی شتر آن در کتابخانه *SCAPY* موجود می با شد یک برنامه بـ سازیم همچنین پروتکل دیگری که برای نگا شت و ار سال دیتاگرام به خارج شبکه مانند پروتکل های *ICMP* , *ARP* می باشد که در قطعه *UDP* استفاده می شوند بکار گرفته می‌شود.
در شـبکه برای کشـف میزبان ها در زیر لایه پیوند داده از سـرویس های احراز اصـالت و برای لایه شـبکه از پروتکل‌های مسـیریابی و همچنین برای لایه انتقال از نوع پروتکل‌های رمزنگاری برای احراز هویت میزبان ا ستفاده می کنیم ، که تمام موارد فوق در می تواند در جریان شنا سایی یک میزبان یا سی ستم به ما کمک کند و مهمترین مساله ار سال دیتاگرام به م سیر انتخابی و شنا سایی آ سیب پذیری‌های بسیاری که وجود دارد می‌تواند به ما در شناسایی رفتار یک سیستم کمک کند چرا که برای هر پورتی یک اسکریپت برای دور زدن فرایند احراز هویت وجود دارد ؛ در این مقاله به بررسی مجموعه تکنیک‌هایی که منجر به شناسایی *IP* هایی که از یک روتر ، سیستم یا مودم تغذیه می‌کنند می‌پردازیم. این روش می‌تواند در یک شبکه سراسری یا یک *NAT* مورد استفاده قرار بگیرد.

کلمات کلیدی: درخت تصمیم *NAT-SCAN* پویشگر[۹]شبکه ، نگاشت شبکه خارجی ، آسیب‌پذیری‌پروتکل‌های TCP/IP

[9] scan

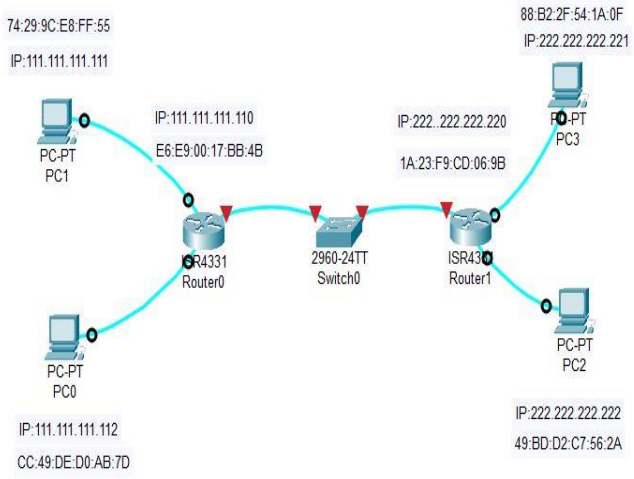
۱- مقدمه

یک شبکه اینترنت را در نظر بگیرید حال اگر بخواهیم به پایش لایه های شبکه بپردازیم اسکنرهای موجود تنها قادر به اسکن IP شبکه محلی می با شد حال اگر بخواهیم فرا سطح محلی در یک شبکه پایش کنیم و آدرس های یک NAT[1] را بدانیم باید DNS و TTL و مسیر روتر های شبکه را باید بدانیم؛ به عنوان مثال اگر از تهران بخواهیم بدانیم چه سیستم هایی در دانشگاه تبریز درحال سرویس دادن هستن کافی هست یک سناریو ساده ولی کاربردی کوچکی ساخته و آنرا تحلیل کنیم.

۲- ارسال دیتاگرام به خارج از زیرشبکه

وظیفه پروتکل ARP در شبکه اترنت پیدا کردن آدرس MAC مقصد از روی آدرس IP آن است. بنابراین ARP آدرس IP کامپیوتر مقصد را از پروتکل IP دریافت می‌کند؛ سپس پیامی را برای تمام ماشین‌های متصل به شبکه اترنت به صورت همه پخشی[1] ارسال می‌کند ولی بگذارید به موقعیت پیچیده‌تری نگاه کنیم که در آن یک میزبان می‌خواهد دیتاگرام خود را به میزبانی در زیر شبکه‌ی دیگر بفرستد، یعنی این دیتاگرام باید برای رسیدن به مقصد از یک مسیریاب عبور کند. در این مورد از شکل ۱ کمک می‌گیریم که در آن دو زیر شبکه با یک مسیریاب به یکدیگر متصل شده‌اند و شبکه‌ای ساده را به وجود آورده‌اند. نکته جالبی در شکل ۱ وجود دارد که باید به آن‌ها توجه‌ها توجه کنیم. هر میزبان فقط یک آداپتور شبکه با یک آدرس IP حد دارد ولی همان طور که می‌دانید یک مسیریاب برای هر واسط خود یک آدرس IP جداگانه دارد.

شکل ۱: سناریو تحلیلی پایش لایه فراسطحی شبکه



همچنین توجه کنید که زیر شبکه‌ی ۱ و زیرشبکه‌ی ۲ به ترتیب دارای آدرس شبکه‌ی ۱۱۱,۱۱۱,۱۱۱,۱۱۱/۲۴ و ۲۲۲,۲۲۲,۲۲۲,۲۲۲/۲۴هستند، پس تمامی واسط‌های متصل به زیر شبکه‌ی ۱ آدرس‌هایی به شکل آدرس همچون ۱۱۱,۱۱۱.XXX. ۱۱۱ دارند و تمامی واسط‌های متصل به زیر شبکه‌ی ۲ دارای آدرس‌هایی به شکل ۲۲۲,۲۲۲.XXX. ۲۲۲ هستند. اکنون یک میزبان روی زیر شبکه‌ی ۱ چگونه می‌تواند دیتاگرام خود را به میزبانی روی زیر شبکه‌ی ۲ بفرستد. به طور خاص، فرض کنید میزبان ۱۱۱,۱۱۱,۱۱۱,۱۱۱می‌خواهد یک دیتاگرام IP به ۲۲۲,۲۲۲. ۲۲۲,۲۲۲ بفرستد. فرستنده طبق معمول این دیتاگرام را به آداپتور خود تحویل می‌دهد؛ ولی این فریم باید آدرس MAC گیرنده را هم در خود داشته باشد. اما این آداپتور چه

[1] Network address translation [0]
[1] brodcast [1]

آدر سی را باید به کار ببرد؟ شاید تصور کنید که میزبان فر ستنده آدرس MAC میزبان ۲۲۲,۲۲۲,۲۲۲,۲۲۲ یعنی 49-BD-D2-C7-56-2A را در فریم خود درج کند؛ ولی این تصور اشتباه است. اگر میزبان فرستنده این آدرس MAC را در فریم خود قرار دهد، هیچ یک از میزبان‌های زیرشبکه‌ی ۱ به آن توجهی نخواهند کرد، (یعنی این دیتاگرام IP را به لایه‌ی شبکه‌ی خود نخواهند داد)، چون این آدرس با آدرس MAC هیچ یک از آن‌ها منطبق نیســت. در نتیجه این دیتاگرام پس از کمی چرخیدن در زیر شــبکه‌ی ۱ از بین خواهد رفت. اگر با دقت به شکل ۱ نگاه کنیم متوجه می شویم که اگر یک دیتاگرام بخواهد از میزبان ۱۱۱,۱۱۱. ۱۱۱,۱۱۱ به میزبانی در زیر شبکه‌ی ۲، برود باید اول به واسط ۱۱۱,۱۱۰. ۱۱۱,۱۱۱ مسیریاب آدرس IP مسیریاب اولین جهش در مسیر به سمت مقصد نهایی تحویل داده شود، بنابراین آدرس MAC مناسب برای این دیتاگرام آدرس MAC واسط ۱۱۱,۱۱۰. ۱۱۱,۱۱۱ مسیریاب، یعنی E6-E9-00-17-BB-4B است، اما میزبان فرستنده چگونه آدرس MAC واسط ۱۱۱,۱۱۰. ۱۱۱,۱۱۱ را پیدا می‌کند؟ معلوم است با ARP همین که آداپتور فرستنده آدرس MAC این واسط را به دست آورد یک فریم (شامل دیتاگرام مورد نظر به مقصد ۲۲۲,۲۲۲. ۲۲۲,۲۲۲) می‌سازد و آن را روی زیر شبکه‌ی ۱ می‌فرستد. وقتی آداپتور مسیریاب در سمت زیرشبکه‌ی ۱ این فریم را ببیند، (از آن جا که آدرس MAC مقصد این فریم آدرس MAC خودش است آن را بر می‌دارد) و به لایه‌ی شبکه‌ی مسیریاب تحویل می دهد. اکنون دیتاگرام IP با موفقیت از میزبان مبدأ به مسیریاب فرستاده شده است ولی کار هنوز تمام نیست، چون این دیتاگرام باید از مسیریاب به میزبان مقصد تحویل داده شود. در اولین گام مسیریاب باید تشخیص دهد که این دیتاگرام را به کدام واسط خروجی خود هدایت کند. همان طور که می‌دانیم مســیریاب برای این کار از جدول هدایت خود کمک می‌گیرد. در این مثال جدول هدایت به مســیریاب می‌گوید که باید دیتاگرام را به واسط ۲۲۲,۲۲۰، ۲۲۲,۲۲۲ بفرستد. واسط ۲۲۲,۲۲۰، ۲۲۲,۲۲۲ بعد از گرفتن این دیتاگرام از لایه‌ی شبکه‌ی مسیریاب آن را به آداپتور خود (آداپتوری که به زیر شبکه‌ی ۲ متصل است) تحویل می‌دهد که این آداپتور هم دیتاگرام را در یک فریم لایه‌ی پیوند می‌پیچد و روی زیر شبکه‌ی ۲ می‌فرستد. در پیوند لینک شبکه‌ی دسترسی و شبکه‌ی محلی این‌جا هم مسیریاب برای فرستادن فریم خود روی زیرشبکه‌ی ۲ به آدرس MAC میزبان ۲۲۲,۲۲۲,۲۲۲,۲۲۲ نیاز دارد و مسیریاب این آدرس MAC را کمک ARP بدست می‌آورد.

پروتکل ARP برای اترنت در RFC ۸۲۶ تعریف شده و در RFC۸۲۶ که به آموزش TCP/IP اختصاص دارد هم می‌توانید مطالب خوبی درباره ARP پیدا کرد.

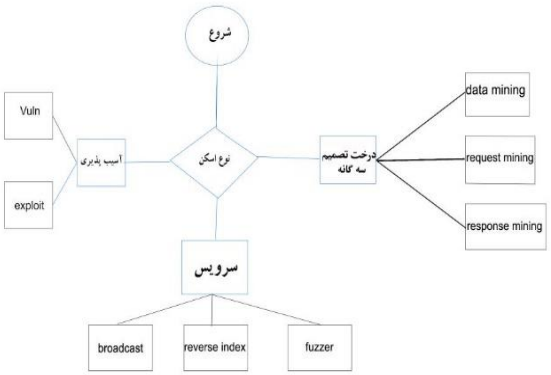
۳- الگوریتم Nat.scan

با استفاده از کتابخانه Nmap برای نگاشت درخت تصمیم با بررسی آسیب‌پذیری‌ها می پردازیم امروزه الگوریتم های بسیاری وجود دارند تا به ما برای ترسیم درخت تصمیم کمک کنند ولی ویژگی های مهم الگوریتم Nmap باعث شده تا ما نگاه ویژه ای به این الگوریتم داشته داشته باشیم . در طراحی الگوریتم بر سه طرح کشف ، نفوذ ، تخریب تقسیم می کنیم که اسکریت را به دو گروه soft ، malware قرار داده و بر اساس آن هر گروه بندی می کنیم تا از درصد ضرر آن‌ها به سیستم‌ها آگاه باشیم[۳۶]، در الگوریتم کشف که

در گروه اسکریپت‌های soft قرار دارد به چهار قسمت تقسیم می‌شوند که از جمله مهترین آن می‌توان کشف سرویس ، آسیب‌پذیری ، اطلاعات ، حساب کاربری نام برد.

در الگوریتم نفوذ که به سه قسمت تقسیم می‌شود از جمله نفوذ به حساب کاربری ، در دست گرفتن سرویس ، نفوذ به آسیب‌پذیری‌ها نام برد .

شکل۲: فلوچارت برنامه Nat-scan



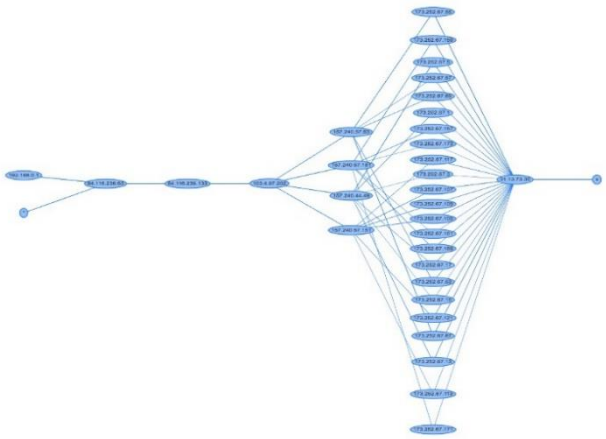
در الگوریتم تخرب که در گروه malware قرار دارند به منظور از کار انداختن ، قطع سرویس ، با استفاده از بد افزار ها معمولاً همراه می باشد به سه قسمت تقسیم می‌شود که از جمله: حملات از کار انداختن سرویس، کرش، بهرجو نام برد. این سه روش الگوریتم بر پایه کتابخانه برنامه Nmap و توسط (Gordon Lyon .2009) نوشته شده است [۱۲].

برای نگاشت نقشه ما باید رنج IP از شبکه های محلی یک NAT رو اسکن کنیم برای مثال: ۱۰,۱۰,۱۰,۱۰/۲۴ می توان بطور تقریبی گفت که در یک آدرس محلی هستند برنامه ما شروع به ارسال packet trace شروع به اسکن لیست IP کرده و بر اساس تعداد روتر مشترک رتبه بندی می کند و مشخص می کند که IP مشترک در یک ستون از جدول قرار بگیرند و همچنین بر اساس زمان دریافتی رتبه دهی به بسته‌ها برای تشخیص بهترین مسیر و همچنین نوع عملگرکه بر اساس گره های پر کاربرد یا کوتاه ترین مسیر یا طولانی ترین مسیر یا سریع ترین مسیر بوده تقسیم بندی کند که با استفاده از روش پرامتی برای ساخت ماتریس تصمیم و بهترین گره را بدست آورد.

```
Looking at Path ID 1 (src port:33453 , dst port:33452)
Looking at Path ID 2 (src port:33454 , dst port:33452)
Looking at Path ID 3 (src port:33455 , dst port:33452)
Looking at Path ID 4 (src port:33456 , dst port:33452)
TTL:          | 1              | 2              | 3              | 4
Path ID 1     | 192.168.0.1    | 84.116.236.63  | 84.116.239.133 | 62.115.172.136
Path ID 2     | 192.168.0.1    | 84.116.236.63  | 84.116.239.133 | 62.115.172.136
Path ID 3     | 192.168.0.1    | 84.116.236.63  | 84.116.239.133 | 62.115.172.136
Path ID 4     | 192.168.0.1    | 84.116.236.63  | 84.116.239.133 | 62.115.172.136
```

5	6	7	8	9
62.115.120.100	80.91.249.11	213.155.130.101	80.91.245.159	62.115.123.159
62.115.120.100	80.91.249.11	213.155.130.101	62.115.142.215	62.115.123.163
62.115.120.100	80.91.249.11	213.155.130.101	62.115.121.15	62.115.123.159
62.115.120.100	80.91.249.11	213.155.130.101	62.115.142.215	62.115.123.163

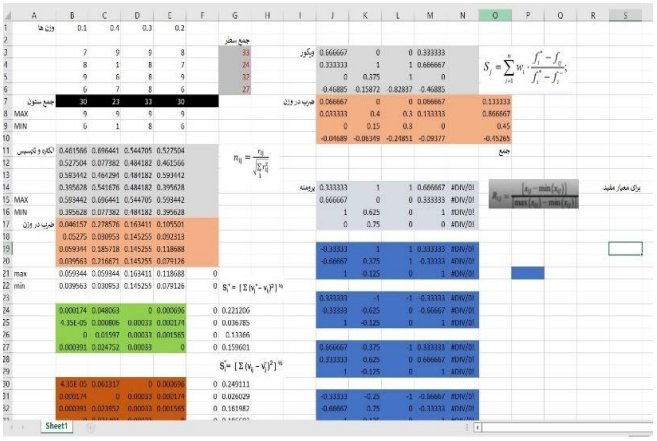
با توجه به نقشه بالا می توانیم حال ip ها را سازماندهی کنیم و آن ها را مطابق شکل ۲رسم کنیم.



شکل۳: نگاشت ساختار شبکه با استفاده از الگوریتم برنامه Nat.scan

ساخت ماتریس درخت تصمیم برای مقایسه و rank بندی بهترین مسیر می تواند به ما کمک فراوانی کند برای اینکه بدانیم در شبکه ما همیشه بهترین مسیر انتخاب می‌شود که باعث افزایش سرعت شبکه می‌شود درعملکرد شبکه تاثیر بسزایی دارد.

ویزگی دیگر طرح در چند سطحی و چند پخ شی[2]بودن آن ه ست که این قابلیت به ما امکان می دهد بر روی تمام شبکه‌های خارجی در مدل OSI پویش انجام دهیم.



شکل ۴: رتبه بندی گره ها با روش های الکتروه و تاپسیس و ویکور و پرامتی

همیشه مقایسه بهترین روش برای بهینه کردن یک شبکه می‌باشد روش های توصیفی و تحلیلی همواره جزو بهترین انتخاب های ما برای اکتشاف در شبکه هست برای کشف جریان های ناسازگار و سازگار مطالب زیادی در حال حاضر در دسترس نیست و در سلسله مراتب آینده جایگاه بالایی خواهد داشت زیرا رقابت شرکت‌ها در آینده در دست شرکتی خواهد بود که سرعت بالا با کمترین هزینه را ارائه کند.

٤- نگاشت لایه دوم شبکه

در مثالی می‌توان با استفاده از کتابخانه scapy نمونه بسته شبکه برای پیمایش شبکه جهت تشخیص نوع آسیب‌پذیری های شبکه ایجاد کرد ، برای پایش لایه دوم از پروتکل IARP , ARP استفاده می‌کنند به دین صورت که با فرض آدس همه پخشی روی آدرس MAC به صورتFF:FF:FF:FF:FF می باشد که از اسکنری که برای نگاشت لایه دوم استفاده می شود Angry ip می باشد. استفاده از پروتکل IARP به ما کمک می‌کنند با استفاده از آدرس IP همه پخشی که به صورت ۲۵۵:۲۵۵:۲۵۵:۲۵۵ می‌باشد.همچنین می‌توانیم

[1] multi cast , multi level [2]

با شنود در یک شبکه دانیم که چه تعداد ip دریک wlan درحال تعامل هستن برنامه ای همانند Bettercap , Ettercap از جمله برنامه بر:ای ضبط ترافیک یک شبکه می باشد که در خود برنامه بعضی امکانات برای رمزگشایی موجود می باشد و بعضی امکانات دیگر بصورت آنلاین می باشد. که این ویژگی در تمام لایه‌ها مشترک می باشد.

۵- نگاشت لایه سوم شبکه

در شبکه های خارجی بزرگ چالش ها انتخاب بهترین مسیر می باشد که استاندارد ها والگوریتم های بسیاری در مقالات جدید برای رفع این ضعف از جمله الگوریتم های ایستا و پویا وضع شده است که منابع مفیدی آن می‌توان جیمز کوروس[3]و همکاران [۵] اشاره کرد که در این مقاله به توضیع آن می‌پردازیم هر یک از الگوریتم های مسیر یابی دارای جدول و پورت مشخصی می باشند که می توان آنها را با ساخت برنامه سرویس گیرنده نگاشت کرد.

۴-۱ الگوریتم Distance Vector Or BellmanFord

یکی از مهم‌ترین الگوریتم های مسیریابی الگوریتم DV یا بلمن فورد است نام اینترنتی این الگوریتم قدیمی (RIP Information Routing Protocol) است . در حالت کلی این الگوریتم قادر است کوتاه‌ترین مسیر را در گراف‌هایی که دارای یال منفی می باشند را بر عکس دیج سترا که فقط برای یال‌های مثبت بود را به د ست بیاورد این الگوریتم خیلی شبیه دیج سترا ا ست با این تفاوت که از یک راس شروع شده و به تمامی نقاط مجاور اندیس می دهد با ادامه و نگه داشتن اندیس های کوچکتر کوتاه ترین فاصله از راس مبدا به تمامی نقاط گراف محاسبه می‌شود و در نتیجه کوتاه تریم مسیر بین مبدا و مقصد را مشخص می کند این الگوریتم که توزیع شده و پویا است هر مسیریاب یک جدول مسیریابی دارد که به ازای هر مسیریاب موجود در زیر شبکه یک شطر در آن وجود دراد و مراجعه به این جدول به کمک ایندکس صورت می گیرد در هر جدول دو فیلد وجود دراد یکی لینک خروجی منا سب برای ر سیدن به مقصد مورد نظر و دومی تخمینی از هزینه رسدن به آن مقصد است [۹].

۴-۲ آسیب‌پذیری پروتکل RIP[4]

در Routing protocol بین روتر بسته‌های update ارسال می‌شود که شامل اطلاعات مربوط شبکه‌هایی است که آن روتر در اختیار دارد. در RIP V1 بسته‌های update با خود Subnet mask حمل نمی‌کنند در نتیجه نسخه اول RIP از subnetting ، supernetting و VLSM پشتیبانی نمی‌کند و بسته‌های update به آدرس ۲۵۵,۲۵۵,۲۵۵,۲۵۵ ارسال می‌شود. در RIPv2 بسته‌های update با خود Subnet mask حمل می‌کنند پس بر خلاف نسخه اول ، این نسخه از subnetting ، supernettingو VLSM پشتیبانی می کند و بسته‌های update به آدرس ۲۲۴,۰,۰,۹ که یک آدرس از نوع multicast است، ارسال می‌شودUpdate RIP هر ۳۰ ثانیه یک باربه صورت Full ارسال می‌شود[۱].

أ. RIP V1 اهراز هویت (Authentication) ندارد.

ب. RIPv2 اهراز هویت (Authentication) دارد.

[1] James Koros [3]

[1] Routing Information Protocol [4]

به طور کلی RIP ، Convergence Timeبالایی دارد و دید به Topology Table شبکه ندارند در نتیجه مستعد Loop است به همین دلیل این Routing protocol[۱۵] روش هایی برای جلوگیری از Loop در اختیار دارد، در واقع پروتکلRIP یک نوع آسیب پذیری به حساب می آید و ما می توانی با ساخت برنامه گیرنده سرویس روی پورت۵۲۰که از پروتکل UDP استفاده می‌کند، اطلاعاتی از سرویس های داخل مسیریاب بدست بیاوریم. این سرویس برای شبکه شرکت سیسکو بصورت سفارشی جهت سهولت در ارتباط سیستم‌ها با یکدیگر ساخته شد.

۳-۴ الگوریتم Link State

در این پروتکل هر کدام از روترهایی که از پروتکل Link State بهره می‌برند.اطلاعات جامع در خصوص با روتر و لینک های مستقیم فراهم شده در آن و وضعیت لینک ها را در اختیار شبکه قرار می‌دهد.

این اطلاعات توسط پیام ها به همه روترهای موجود در شبکه جهانی وب ارسال می‌شود.بر خلاف پروتکل های مسیریابی Distance Vectorکه اینکار را به وسیله استفاده از فرآیند Broadcast انجام می دادند.

```
name = "RIP header"

fields_desc = [

ByteEnumField("cmd", 1, {1: "req", 2: "resp", 3:
"traceOn", 4: "traceOff", # noqa: E501

5: "sun", 6: "trigReq", 7: "trigResp", 8: "trigAck", #
noqa: E501

9: "updateReq", 10: "updateResp", 11:
"updateAck"}), # noqa: E501

ByteField("version", 1),

lass RIP(Packet):
```

سلسله مراتب مسیریابی این پروتکل به گونه ای است که با ایجاد شدن کوچک ترین تفاوتی در توپولوژی شبکه موجود، این تغییر بصورت Incrementalبرای سایر روتر ارسال می‌شود.

توپولوژی شبکه روی اکثر روترها باید بروز باشند. هر کدام از روترهای موجود در شبکه های Link State یک نوع کپی از این توپولوژی شبکه را در دست دارند و آن هیچ تغییری نمی‌کند.

بعد از اینکه آخرین تغییرات شبکه ها را دریافت کردند هر روتر بصورت کاملا مستقل به محاسبه بهترین مسیرها برای رسیدن به شبکه های مقصد می پردازد [۹]. این پروتکل ها در مسیریابی بر طبق الگوریتم است به نامShortest Path First نام دیگر این الگوریتم Dijkstraاست.

در الگوریتم SPF وقتی که وضعیت یک لینک ارتباط عوض می‌شود، و یک Routing Update که به عنوان Link-State Advertisementیا LSA شناخته می‌شود ایجاد می‌شود و در بین روترهای موجود تبادل اطلاعات صورت می گیرد و زمانیکه یک روتر LSA Routing Update را دریافت می‌کند، الگوریتم Link-State با استفاده از آن کوتاه ترین مسیر را برای رسیدن به مقصد مورد نظر محاسبه می‌کند.هر روتر برای خود یک نقشه کامل از شبکه ها ایجاد می کند. نمونه ای از پروتکل مسیریابی-Link Stateپروتکل ای به نام Open Shortest Path First یا OSPF است با وجود پروتکل flood در Link State Information ها دیگر جدید بودن آن ها از روی بزرگتر یا کوچکتر بودن مقدار Sequence Number قابل تشخیص دادن نیست.این Link State

[1] نیازمند [5]

Informationهمیشگی در درون دیتابیس بازنویسی شده و این عمل آنقدر تکرار می‌شود که بافر آن خطا داده و شبکه از دسترس خارج می‌شود.

۴-۴ ساختار پروتکل Link State

درباره ساختار این پروتکل می توان گفت که از یک ساختار و فرامینی استفاده می‌کنند که این ساختار باعث کم شدن اندازه ها و طول مسیرو نیاز کمتر به انتقال LSA ها می‌شود.این پروتکل ها از مکانیزم Multicast برای تقسیم کردن اطلاعات و داده مسیریاب استفاده می کنند، ولی تنها روترهایی که از این پروتکل‌هایLink State استفاده می کنند می‌توانند این Routing Update ها را پردازش کنند.پروتکل Link State ها فقط زمانی اطلاعات یا داده های هر روتر را ارسال کند، که در شبکه تغییری رخ دهد و صرفا همان تغییر را برای بقیه روترها ارسال می کنند.

نصب پروتکل‌های مسیریاب Link-State پیچیده‌تر و پرهزینه‌تر از پیاده‌سازی پروتکلDistance Vector است و پیچیده ترین و مهم ترین بخش عملکرد Link State ها مربوط می‌شود به جریان Link State Information ها در ساختار او است. برای این که این جریان درست انجام شود باید از دسته بندی های داخل فرمت Link State استفاده کرد.

۴-۵ آسیب پذیری پروتکل OSPF[۲]

پروتکل OSPF در دسته Link State قرار می گیرد یکی از وظایف پروتکل‌های Link State ایجاد یک دیتابیس از ساختار شبکه می‌باشد و برای پیدا کردن بهترین مسیر از الگوریتمی به نام SPF بهره می گیرد. پروتکل OSPF نسبت به سایر پروتکل های مسیریابی اطلاعات بیشتری در مورد ساختار شبکه بدست می‌آورد که باعث می‌شود تصمیم‌گیری بهتری برای مسیریابی داشته باشد.روترهایی که OSPF را اجرا می‌کنند بسته‌هایی تحت عنوان Hello را با روتر های مجاور خود[۱۷]تبادل می‌کنند و به این وسیله RID[۱۸] و Cost را بدست می‌آورد و اطلاعات بدست آمده را در جدول Neighbor خود نگه می دارد . سپس روتر اقدام به ایجاد LSA[۱۹] مناسب می کند این LSA شامل اطلاعات مانند RID ، Cost هر یک از همسایه می باشد. روتر این LSA را در اختیار همسایه های خود قرار می دهند همچنین روتر این اطلاعات را در جدولی به نام LSDB[۲۰] نگه داری می‌کنند و در نهایت با استفاده از الگوریتم SPF بهترین مسیرها را انتخاب می‌کنند [۲۳].

این پروتکل از احراز هویت پشتیبانی نمی کند و به راحتی می توان با جعل بسته آن اطلاعات آدرس های سیستم در داخل مسیریاب روی پورت ۸۹ بدست آورد، تنها کافیست بسته جعلی متناظر سرویس گیرنده را اجرا کنیم.

---

[1] Open Shortest Path First
[1] روتر همسایه
[1] روتر ID
[1] Link State Advertisements
[2] Link State Database

```
class OSPF_Hello(Packet):

name = "OSPF Hello"

fields_desc = [IPField("mask", "255.255.255.0"),

ShortField("hellointerval", 10),

OSPFOptionsField(),

ByteField("prio", 1),

IntField("deadinterval", 40),

IPField("روتر", "0.0.0.0"),

IPField("backup", "0.0.0.0"),

FieldListField("neighbors", [], IPField("",
"0.0.0.0"), length_from=lambda pkt:
(pkt.underlayer.len - 44) if pkt.underlayer else
None)] # noqa: E501
```

در زیر الگوریتم هـای مسـیریابی در حالـت اولیـه بایـد از ویژگی های زیر برخوردار باشند

أ. صحت عملکرد:(Correctness) الگوریتم باید صحیح عمل کند و پاسخ غلط تولید نکند.
ب. سادگی: (Simplicity) الگوریتم باید به سادگی قابل فهم و پیاده سازی باشد.
ج. سرعت:(Efficiency) الگوریتم باید به سرعت مسیر خود را پیدا کند.
د. پایداری:(Stability) الگوریتم باید به سمت پاسخ بهینه همگرا باشد و در حلقه ابدی گرفتار نشود.
ه. عدالت و مساوات:(Fairness) منابع باید به صورت عادلانه تقسیم شوند.
و. بهینه بودن: (Optimality) بهترین جواب یا جواب نزدیک به بهینه را بر اساس معیار های مورد نظر کاربرد

هر کدام از ویژگی های بالا به نسبت درصدی می تواند در الگوریتم های مورد نظر متفاوت باشد هر چند ممکن است که بعضی از این معیارها با یکدیگر در تضاد باشند مثلا مساوات با بهینگی در تضاد است و باید حالت موازنه برقرار باشد. در دسته بندی دیگر از الگوریتم های پویا می توان الگوریتم ها را به الگوریتم های متمرکز،توزیع شده تقسیم بندی کرد که الگوریتم ها می توانند در حالت‌های مختلف و دسته بندی های متفاوتی قرار بگیرند.

۵-۴ مقایسه الگوریتم های مسیریابی

پروتکل های Link State بر خلاف پروتکل های Distance Vector شبکه را در قالبHop Count و تعداد روترهای موجود در آن نمی‌بینند در عوض یک دیدگاه جامع و کامل در خصوص توپولوژی های مورد استفاده در شبکه ایجاد می کنند که همه جزئیات شبکه های موجود در توپولوژی را در خود دارد، تمامی روترها با Cost های آنها در این دید جامع و کامل وجود خواهند داشت [۹].

در پروتکل‌های Link State هر یک از روترهایی که از یکی از پروتکل‌های Link State استفاده می‌کند اطلاعات کاملی در خصوص خود روتر ، لینک‌های مستقیم متصل شده به آن و وضعیت آن لینک ها را در اختیار شبکه قرار می دهد. این اطلاعات توسط پیام های Multicastبه همه روترهای موجود در شبکه ارسال می‌شود دقیقا بر خلاف پروتکل های مسیریابیDistance Vectorکه اینکار را به وسیله استفاده از فرآیند Broadcast انجام می دادند.

فرآیند مسیریابی Link State به گونه ای است که با ایجاد شدن کوچکترین تغییری در توپولوژی شبکه های موجود بلافاصله این تغییر بصورت Incremental برای سایر روترها هم ارسال می‌شود تا توپولوژی شبکه روی همه روترها همیشه بروز باشد. هر کدام از روترهای موجود در شبکه های Link State یک کپی از این توپولوژی شبکه را در خود دارند و آن را تغییر نمی دهند، بعد از اینکه آخرین تغییرات شبکه ها را دریافت کردند هر روتر بصورت کاملا مستقل به محاسبه بهترین مسیرها برای رسیدن به شبکه های مقصد می پردازد.

پروتکل‌های مسیریابی Link State بر اساس الگوریتمی به نام Shortest Path First یا SFP برای پیدا کردن بهترین مسیر برای ر سیدن به مق صد پایه ریزی شده اند. نام دیگر این الگوریتمDijkstra ا ست. در الگوریتم Shortest Path First یا SPF زمانیکه وضعیت یک لینک ارتباطی تغییر می کند ، یک Routing Update که به عنوان Link-State Advertisement یا LSA شناخته می‌شود ایجاد می‌شود و بین تمامی روترهای موجود تبادل می‌شود.

زمانی‌که یک روتر LSA Routing Update را دریافت می‌کند، الگوریتم Link-State با استفاده از آن کوتاه ترین مسیر را برای رسیدن به مقصد مورد نظر محاسبه می کند. هر روتر برای خود یک نقشه کامل از شبکه ها ایجاد می کند. نمونه ای از پروتکل مسیریابی Link-State پروتکل‌ای به نامOpen

Shortest Path First یا OSPF است. چند واژه مهم در خصوص پروتکل‌های Link State وجود دارد.

Link-State AdvertisementیاLSA: یک Packet کوچک اطلاعاتی است که در آن اطلاعات مربوط به Routing بین روترها رد و بدل می‌شود.

Topological Database: مجموعه اطلاعاتی که از LSA ها دریافت می‌شود.

الگوریتم SPF یا : Dijkstra الگوریتمی است که محاسبات بر روی database های موجود در SPF Tree را انجام می دهد

Routing Table : یک لیست از مسیرها و Interface های شناسایی شده است.

پروتکل های مسیریابی Link State در عین اینکه به مدت زمان کمتری برای Converge شدن نسبت به پروتکل های مسیریابی Distance Vector برخوردارند در مقابل بوجود آمدنRouting Loop هم نسبت به Distance Vectorها مقاوم تر هستند و کمتر موردی پیش می آید کهRouting Loop در پروتکل های Link State ایجاد شود. اما از طرفی دیگر الگوریتم های مورد استفاده در پروتکل های Link State به قدرت پردازشی CPU و حافظه RAMبه نسبت پروتکل های Distance Vector نیاز دارند [۳۷].

پروتکل‌های Link State از یک ساختار سلسله مراتبی و موروثی استفاده می کنند که این ساختار باعث کاهش فاصله ها و نیاز کمتر به انتقال LSA ها می‌شود. پروتکل های Link State از مکانیزم Multicast برای اشتراک گذاری اطلاعات مسیریابی استفاده می کنند ، فقط روتری که از پروتکل های مسیریابی State Link استفاده می‌کنند Routing Update را پردازش می‌کنند. Link State ها فقط زمانی اطلاعات روتر را ارسال می کنند که در شبکه تغییری ایجاد شده باشد و صرفا همان تغییر را برای سایر روترها ارسال می کنند، پیاده‌سازی پروتکل‌های مسیریابی LinkStateپیچیده تر و پر هزینه تر از پیاده سازی پروتکل های Distance Vector می باشد و هزینه نگهداری آنها نیز به نسبت بیشتر است [۹]. برای تعیین کوتاه‌ترین مسیر از روش زیر برای استفاده می‌کنند به طوری که در صورت کمینه بودن هزینه هر مرحله مسیر به مرحله بعدی می‌رود.

$$D(A) = MIN\{c(x,y) + D(X)\}$$

$$D(B) = MIN\{c(x,y) + D(Y), c(x,z) + D(Z)\} \qquad (۱)$$

$$D(C) = MIN\{c(x,y) + D(X), c(x,z) + D(Z), c(x,v) + D(V)\}$$

$$D(G) = MIN\{c(x,y) + D(X) \dots\dots\dots\dots\dots\dots\dots\}$$

٦- نگاشت لایه چهارم

TCP Idle Scan توسط شخصی به نام Antirez طراحی و معرفی شد ، محقق و پژوهشگر حوزه امنیتی که ابزار hping2 را نیز به دنیا معرفی کرد. از این نوع اسکنر به عنوان پورت اسکن کاملا مخفی یا completely blind port scan نام برده می شود. مهاجم در این نوع اسکن کردن حتی یک بسته اطلاعاتی نیز به سمت هدف ارسال نمی کند که درصدی احتمال شناسایی مهاجم وجود داشته باشد. این سیستم Zombie هست که فرآیند پورت اسکن را در این حالت انجام می دهند و در هر مکانیزم Log برداری دیوارآتش یا سیستم تشخیص

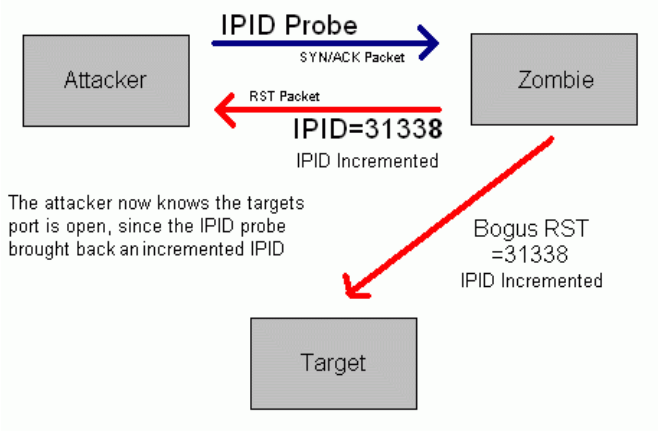
نفوذ ، آدرس Zombie ها ثبت و ضبط خواهد شد، یکی از دلایل محبوبیت این نوع پورت اسکن در میان هکرهای کلاه سیاه این است که می توانند اسکن ها را از کامپیوترهای Zombie انجام بدهند که در دایره اعتماد یا Trust سرور مقصد قرار دارند و بنابراین خیلی ساده‌تر می توان عملیات شناسایی را انجام داد.

یکی از روش‌های مر سومی که باز بودن یک پورت TCP را ت شخیص می دهد ار سال یک ب سته SYN برای برقراری ارتباط به پورت مورد نظر ا ست. اگر سیستم هدف در پا سخ ب سته SYN/ACK به منزله تایید برقرار ارتباط را بازگشت داد یعنی پورت مورد نظر باز ا ست و اگر در پا سخ ب سته RST برای ری ست کردن ارتباط ار سال کرد پورت مورد نظر ب سته ا ست، هر ما شینی که ب سته اطلاعاتی ناشناخته ای بصورت SYN/ACK دریافت کند با RST قطعاً پاسخ خواهد داد. هرگونه RST بی مورد در دیوارآتش‌ها نادیده گرفته می شود و هر ب سته اطلاعاتی از نوع IP در اینترنت برای خودش دارای یک Fragment Identification Number یا[۲] IP ID

[2] IP منحصر به فرد [1]

می باشد که شناسه منحصر به فرد آن سیستم یا بسته اطلاعاتی نیز خواهد بود. با توجه به اینکه اکثر سیستم عامل های امروزی از مکانیزم افزایش مقدار IP ID در ارسال بسته های اطلاعاتی خودشان استفاده می‌کنند ، با شنود کردن IPID سیستم های قربانی می توان تعداد بسته های اطلاعات و زمان و سایر اطلاعاتی از این قبیل را بدست آورد و در Idle Scan از این IPID برای اسکن کردن واسط استفاده می شود.

فرآیند Idle Scan یک فرآیند سه مرحله ای است که شامل همه مراحل برای اسکن کردن هر پورت بصورت مجزا می باشد ، یعنی برای اسکن کردن ده عدد پورت ، ده بار باید فرآیند زیر انجام شود که به شکل زیر می‌باشد.



شکل۵: فرآیند idelScam

باید بر روی سیستم قربانی Zombie به دنبال IP ID گشت و آن را ثبت کرد.

از طرف سیستم Zombie به سمت سیستم قربانی بر روی پورت مورد نظر یک بسته SYN ارسال کرد. بر حسب وضعیت پورت مورد نظر کامپیوتر هدف ممکن است باعث شود که IP ID بعدی اضافه شود یا نیازی به اضافه کردن آن نباشد و بدون تغییر بماند.

مجددا به دنبال IP ID جدید سیستم Zombie می‌گردیم و آن را ثبت می کنیم. برای بررسی کردن وضعیت پورت IP ID جدید را با IP ID قدیمی مقایسه کنیم و متوجه می شویم که وضعیت پورت مورد نظر چگونه است زیرا سیستم قربانی درخواست را به سمت Zombieهدایت کرده است. این فرآیند برای همه پورت مورد نظر مجددا از مرحله اول انجام می شود.

پس از اینکه این فرآیند انجام شد ، IP ID مربوط به Zombie بایستی یک یا دو عدد زیاد شده باشد. اضافه شدن یک عدد به این معنی است که Zombie بسته اطلاعاتی خاصی ارسال نکرده است و از آن Packet ای در واقع خارج نشده است ، مگر پاسخ آن به کامپیوتر مهاجم که ما هستیم.[۲]این کمبود بسته اطلاعاتی به منزله بسته بودن پورت مورد نظر است ، یعنی کامپیوتر هدف که اسکن شده است به سمت سیستم Zombie یک بسته ریست فقط ارسال کرده است که از طرف Zombie هم Ignore شده است؛ اما اگر عدد IP ID بیشتر زیاد شده باشد به منزله باز بودن پورت مورد نظر است زیرا سرور مقصد به سمت سیستم Zombie بسته اطلاعاتی بازگشتی داده است و درخواست برقراری ارتباط داده است؛ روش دیگر استفاده از بسته‌های ARP می‌باشد که بسیار کارآمدتر از روش

2 اسکنر 2

قبلی هست زیرا در این روش بسته‌های ARP توسط دیوار آتش مسدود نمی گردد ولی تنها معایبی که دارد این هست که IP شبکه های محلی و خصوصی را برمی‌گرداند.

```
def scan_now(start_port, end_port, victim_ip, zombie_ip,os_detection):
    if start_port < end_port:
        sys.stdout.write(GREEN + '\n\n'+' ' * 10 + 'PORT NO.     SERVICES' + '\n' + END)

        start_time = time.time()
        for port in range(start_port, end_port):
            try:

                # send SYN/ACK packet to zombie from attacker
                attack_zombie = sr1(IP(dst=zombie_ip)/TCP(dport=port,flags='SA'),timeout=2,verbose=0)

                # send SYN packet to victim from attacker
                attack_victim = sr1(IP(dst=victim_ip, src= zombie_ip)/TCP(dport=port,flags='S'),timeout=2,verbose=0)

                # send SYN/ACK packet to zombie from attacker again
                attack_zombie_again = sr1(IP(dst=zombie_ip)/TCP(dport=port,flags='SA'),timeout=2,verbose=0)

                # If ipid value after all operation is increased by 2, then port is open
                if attack_zombie_again[IP].id == (attack_zombie[IP].id + 2):
                    print(' ' * 10 + str(port) + ' /tcp' + '       ' + socket.getservbyport(port))

            except:
                pass
        # The time to leave ttl value of linux is less than 64 and window is more than 64.
        os_detection_response = sr1(IP(dst=victim_ip, src= zombie_ip)/TCP(dport=80,flags='S'),timeout=2,verbose=0)
        if os_detection.lower() == 'y':
            if os_detection_response[IP].ttl <= 64:
                print(' '*10 + 'Operating System : Linux/Unix')
            else:
                print(' '*10 + 'Operating System : Microsoft Windows')
        end_time = time.time()
        time_taken = round((end_time-start_time),2)
        print(' ' * 10 + 'Finished in {} seconds.'.format(time_taken))
```

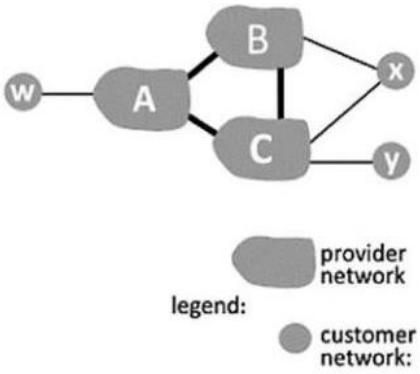
حداقل زمان زمان توضیع بسته های شبکه ، اگر F را تعداد پورت های پایش و d را آهنگ دریافت ، u آهنگ ارسال بسته بنامیم و N تعداد سیستم های پایش باشد آنگاه زمان توضیع بسته در شبکه از رابطه زیر بدست می آید.

$$D = MAX\{\frac{NF}{U} + \frac{F}{d}\} \qquad (۲)$$

۷- یافته ها

برای استفاده از پنل کنترل مودم،روتر یک شبکه غیر محلی دیگر با تنظیم dns برای خروجی هدایت شده الزامی می باشد ولی اگر هدف ما بصورت کور می‌باشد می توانیم از سایت shodan استفاده کنیم به طور مثال از یک مودم با آدرس 31.59.195.210 می خواهیم بدانیم چه تعداد وسیله متصل و با چه آدرس ip درآن قرار دارد بدین منظور با اسکریپت‌هایی که برای نفوذ با توجه به مدل و شرکت سازنده در دارک وب وجود می‌باشد می‌توانیم نتیجه آن را مشاهده کنیم.

در استفاده از شبکه محلی می توانیم با استفاده از تنظیمات network به اطلاعات یک سیستم دسترسی داشته باشیم که می توان از روش‌های مختلفی از جمله استفاده home group و work place نام برد. در بررسی فراسویه یک مودم و یا روتر می توانیم با پایش زامبی اسکن گامی در جهت اکتشاف IP هایی که از آن مودم سرویس می گیرند برداشته و لایه ها و پروتکل هایی که در پشت یک مودم یا روتر قرار دارند را شناسایی کنیم که این ویژگی منحصر به فرد وجه تمایز آن با سایر اسکنر ها و نرم افزار های جانبی می‌باشد در زامبی اسکن با استفاده از پیغام ack در پورت tcp جهت یافتن هدف مورد نظر بوده و ما می توانیم با همین روش به لایه های یک شبکه خصوصی مطابق شکل ۳ دسترسی پیدا کنیم.



شکل ۶ : شماتیک لایه یک شبکه محلی

با استفاده از آسیب‌پذیری های یک شبکه فرضا اگر ما x در شبکه باشیم می‌توانیم با زامبی اسکن یا idel اسکن به موجودیت A ، y ، B ، C پی ببریم هر چند اگر در شبکه دیوارآتشی فعال باشد که در این زمینه رویکرد دورزدن دیوارآتش و پنهان مانده در شبکه ضروری می باشد. همچنین قابلیت رهگیری بسته های شبکه بر اساس رفرنس جهت کشف مکان و مسیر ارتباطی آن استفاده می‌شود.

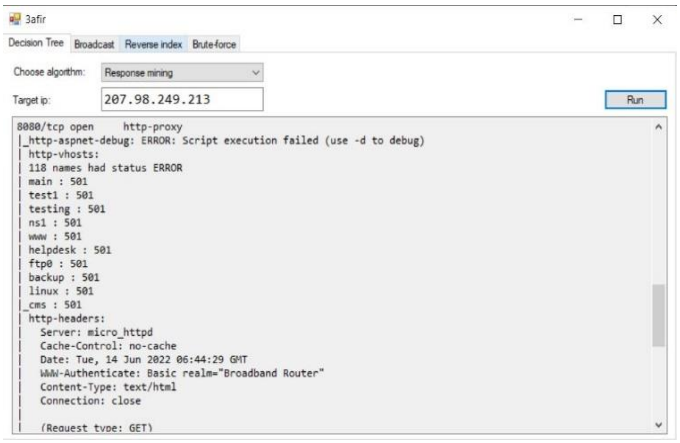
۸- برنامه Nat.scan

دسترسی سریع و آسان به منابع شبکه های مختلف، از جمله HTTP، HTTPS، FTP و پوشه های به اشتراک گذاری شده را فراهم می کند و همچنین امکانی برای تشخیص تمام دستگاه های شبکه اینترانت[۲۳] و اسکترانت[۲۴] از جمله دستگاه بیسیم و روتر را به کاربرانش ارائه می دهد.

برنامه براساس درخت تصمیم سه گانه بر مبنی data mining , request mining , response mining می باشد که برای بدست آوردن بر اساس پایش شبکه مبتنی بر اطلاعات پایگاه داده که اطلاعاتی از رفتار سیستم در گذشته به ما می دهد و روش مبتنی بر درخواست که درخواست های زیادی ارسال کرده و نتیجه را مستقیماً بر می گرداند و روش مبتنی بر پاسخ که به منظور کشف اطلاعات پروتکل‌ها و سرویس ها به ما بر می‌گرداند.

در هدر سه بخش دیگر نیز وجود دارند که شامل پایش broadcat که با استفاده از پروتکل ARP به کاوش می‌پردازد و reverse index که به کمک idel scan انجام می‌شود و بخش fuuzer که اسکن جدیدی مطابق حملات brout force می باشد که برای لایه اپلیکیشن بکار می‌رود. استفاده می‌کنیم، که می توانید در شکل ۷ برنامه ساخته شده را ببینید؛ البته تمام نکات و مزیت‌ها نسبت به دیگر پایشگرها در این مقاله قابل ذکر نیست و هدف ذکر الگوریتم‌ها و روش‌های استفاده در این برنامه هست که باعث برتری دادن به دیگر پایشگرها شده است.

[2] intranet
[2] extranet
[3]
[4]



شکل۷ : برنامه Nat.scan

۹- نتیجه گیری

امروزه با بالا رفتن فناوری و به وجود آمدن ابزارهای پیشـــرفته جهت شـــنود و دور زدن دیوار آتش و آنتی ویروس و اســـتفاده از crawler[۲۵] بروزتر جهت پیدا کردن آسـیب‌پذیری می توان نیاز ویژه ای برای شـناسـایی با اسـتفاده از تسـت نفوذ و سـاخت crawler برای پیدا کردن این آسیب‌پذیری قبل ایجاد فاجعه داشت .

در الگـوریتم برنامـه Nat.scan مـا بـا اسـتفاده از الگـوریتم فـرا ابتکـاری توانسـتیم بـا طبقـه بنـدی بـه سـه الگـوریتم پـردازش اطلاعات دیتـا و پـردازش درخواسـت و پـردازش پاسـخ دریـافتی از شـبکه بـا اسـتفاده از درخـت تصـمیم یـک چهـارچوب مناسـبی بسـازیم و در کنـار آن بتـوانیم بـا طبقـه بنـدی کـردن اسـکریپت هـا بتـوانیم یـک خروجـی مناسـب جهـت نگاشـت شـبکه بدسـت بیاوریم بسـیاری از دسـتگاه هـا ممکـن هسـت بـه روشـی از اسـکن کـردن حسـاس باشـند و آن را بـلاک کننـد بنـابراین بایـد از در کنار درخت تصمیم این قابلیت ایجاد شد که بتوانیم با درک رویکرد سیستم مطابق با آن سازگار رفتار کنیم.

در الگـوریتم مطـابق بـا مـاتریس تصـمیم پرامتـی بـرای نگاشـت شـبکه اسـتفاده شـد تـا بتـوانیم بـر اسـاس مـدت زمـان دریـافتی امتیاز دهی به بسته ها برای تشـخیص بهتـرین مسـیر و همچنـین نـوع عملگرکـه بـر اسـاس گـره هـای پـر کـاربرد یـا کوتـاه تـرین مسیر یا طولانی ترین مسیر یـا سـریع تـرین مسـیر بـوده تقسـیم بنـدی داشـته باشـیم و بـرای اینکـار بایـد ازغیـر رتبـه ای سـاخت مـاتریس تصـمیم و بهتـرین گـره را بدسـت آورد کـه علـت اسـتفاده از ایـن روش بـرای بدسـت آوردن توصـیف و تفسـیر از عملکـرد شبکه ما می باشد .

۱۰- مراجع

[1] K. Mishra and A. Kumar, "Performance-based Comparative Analysis of Open Source Vulnerability Testing Tools for Web Database Applications," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225324.

[2] ASABERE, Eunice Domfeh; PANFORD, Joseph Kobina; HAYFRON-ACQUAH, James Ben. Comparative Analysis Of Convergence Times Between OSPF, EIGRP, IS-IS and BGP Routing Protocols in a Network. International Journal of Computer Science and Information Security (IJCSIS), 2017, 15.12: 225.

[3] Automatic Inference of Environment Dependencies for Python Code Snippets , Eric Horton, Chris Parnin , NC State University , Raleigh, NC, USA

[4] BODENHEIM, Roland, et al. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection, 2014, 7.2: 114-123.

[5] Chen, Chen, et al. "TARANET: Traffic-analysis resistant anonymity at the network layer." 2018 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2018.

2 جستجوگر 5

[6] Dall'Asta, Luca, et al. "Exploring networks with traceroute-like probes: Theory and simulations." Theoretical Computer Science 355.1 (2006): 6-24.

[7] DOSHI, Mr Abhishek; SHARMA, Priyanka. Digital Forensics Analysis for Network Related Data. 2020.

[8] Ganzinger, Matthias, William J. Hymas, and Thomas Schutt. "Securing broadcast based ad hoc routing protocols." Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07). IEEE, 2007

[9] GHOURABI, Abdallah; ABBES, Tarek; BOUHOULA, Adel. Honeypot for routing protocols protection. In: 2009 Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS 2009). IEEE, 2009. p. 127-130.

[10] Goldschlag, David, Michael Reed, and Paul Syverson. "Onion routing." Communications of the ACM 42.2 (1999): 39-41

[11] https://docs.python-requests.org/en/latest

[12] https://nmap.readthedocs.io/en/latest/nmap.html for scan syn/ack

[13] https://rawsocket-python.readthedocs.io/en/latest/

[14] IZHAR, Mohd; SHAHID, Mohd; SINGH, V. R. Network Security Vulnerabilit Heading for Malicious Attack

[15] J. Mirkovic and E. Kissel, "Comparative Evaluation of Spoofing Defenses," in IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 218-232, March-April 2011, doi: 10.1109/TDSC.2009.

[16] Luckie, Matthew, Young Hyun, and Bradley Huffaker. "Traceroute probe method and forward IP path inference." Proceedings of the 8th ACM SIGCOMM conference on Internet measurement. 2008.

[17] MASRUROH, Siti Ummi, et al. Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP. In: 2017 International Conference on Innovative and Creative Information Technology (ICITech). IEEE, 2017. p. 1-7

[18] N. A. Noureldien and M. O. Hussein, "Block Spoofed Packets at Source (BSPS): A method for detecting and preventing all types of spoofed source IP packets and SYN flooding packets at source: A theoretical framework," 2009 Second International Conference on the Applications of Digital Information and Web Technologies, 2009, pp. 579-583, doi: 10.1109/ICADIWT.2009.5273927.

[19] Network Based Packet Watermarking using TCP/IP Protocol Suite Maitrik K. Shah, Samir B. Patel

[20] Network packet manipulation with Scapy. Hack.lu, October 15, 2005

[21] O. Ojagbule, H. Wimmer and R. J. Haddad, "Vulnerability Analysis of Content

[22] Management Systems to SQL Injection Using SQLMAP," SoutheastCon 2018, 2018, pp. 1-7, doi: 10.1109/SECON.2018.8479130.

[23] Packet generation and network based attacks with Scapy CanSecWest/core05, May 4-6, 2005

[24] Petr Stepanov , Galina Nikonova :Attack on the Address Resolution Protocol

[25] R. R. S, R. R, M. Moharir and S. G, "SCAPY- A powerful interactive packet

[26] manipulation program," 2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS), 2018, pp. 1-5, doi: 10.1109/ICNEWS.2018.8903954.

[27] R. S. Dewar, "The "triptych of cyber security": A classifi cation of active cyber defence," 2014 6th International Conference On Cyber Conflict (CyCon 2014), 2014, pp. 7-21, doi: 10.1109/CYCON.2014.6916392

[28] Rahman, Ashiqur, et al. "Advanced network scanning." American Journal of Engineering Research (AJER) 5.6 (2016): 38-42.

[29] S. Branigan, H. Burch, B. Cheswick and F. Wojcik, "What can you do with Traceroute?," in IEEE Internet Computing, vol. 5, no. 5, pp. 96-, Sept.-Oct. 2001, doi: 10.1109/4236.957902.

[30] Scapy document Built with Sphinx in scapy.readthedocs.io Philippe Biondi 2022

[31] Scapy–A Python Tool For Security Testing , Shipra Bansal and Nitin Bansal Department of Computer Applications, Lovely Professional University, Jalandhar, India

[32] Shah, Mujahid, et al. "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool." 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2019

[33] TAKAHASHI, Ryo; TASHIRO, Keiji; HIKIHARA, Takashi. روتر for power packet distribution network: Design and experimental verification. IEEE Transactions on Smart Grid, 2015, 6.2: 618-626.

[34] TAL, Oded; KNIGHT, Scott; DEAN, Tom. Syntax-based Vulnerability Testing of Frame-based Network Protocols. In: PST. 2004. p. 155-160.

[35] WAN, Tao. Securing routing protocols through information corroboration. 2006. PhD Thesis. Carleton University.

[36] Y. Ishikawa, N. Yamai, K. Okayama and M. Nakamura, "An Identification Method of PCs behind NAT Router with Proxy Authentication on HTTP Communication," 2011 IEEE/IPSJ International Symposium on Applications and the Internet, 2011, pp. 445-450, doi: 10.1109/SAINT.2011.83.

[۱] ارزیابی پروتکل های مسیریابی Open Shortest Path First و Routing Information Protocol و Internet Gatway Routing Protocol و Enhanced Internet Gateway Routing Protocol با استفاده از شبیه ساز OPNET Modeler علی اکبر اله دانه , پیام کیافر , ۱۳۹۵

[۲] پورنقدی. پدافند غیرعامل و بررسی تهدیدات نظم و امنیت در فضای سایبری. *فصلنامه دانش انتظامی کردستان*,۴-10.83 :3.11 ,2012

[۳] پوروهاب; مهران; ابراهیمی آتانی. بهره‌گیری از Port-Knocking بعنوان اولین لایه دفاعی در استراتژی دفاع در عمق با استفاده ترکیبی از ویژگی‌های پروتکل کنترل پیامهای اینترنتی، آدرس اینترنتی و تونل زنی .*پدافند الکترونیکی و سایبری*۲۰۱۵

[۴] کافی سعید. شاخص های دفاعی امنیتی فضای سایبری زیرساخت های حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکردهای پدافند غیرعامل.۱۳۹۷

[۵] شبکه های کامپیوتری رویکرد بالا به پایین جیمز کوروس . کیت راس مترجم احسان ملکیان . علیرضا زارع پور محمد گنجی چاپ سوم سال ۹۶

[۶] مهدی نژاد حسنعلی; رضایی ناصر. طراحی ساختاری و شبیه سازی انتقال بسته های IP از طریق ATM به روش.NHRP
[۷] نام کتاب : بررسی روتینگ پروتکل ها در شبکه های کامپیوتری ناشر طاهره پرادا۱۳۹۸