خبرنامه الکترونیکی ۶۶

مرکز تخصصی آپا دانشگاه سمنان

شماره شصت و ششم، سال ششم، آذر ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

آموزش حمله مرد میانی در پروتکل VRRP با استفاده از ابزار LOKI

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

بی اعتمادی و احتیاط، والدین امنیت هستند.

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

اجرای حملات تزریق کد از راه دور در سرورهای pfSense

pfSense یک فایروال و نرم‌افزار روتر Open Source محبوب است که امکان سفارشی‌سازی و انعطاف‌پذیری گسترده را فراهم می‌کند. در pfSense سه آسیب‌پذیری با شناسه‌های زیر کشف شده است:

- CVE-2023-42325 (Cross-Site Scripting – XSS شدت 5.4_)
- CVE-2023-42327 (Cross-Site Scripting - XSS) شدت 5.4_
- CVE-2023-42326 (Command Injection)_شدت 8.8

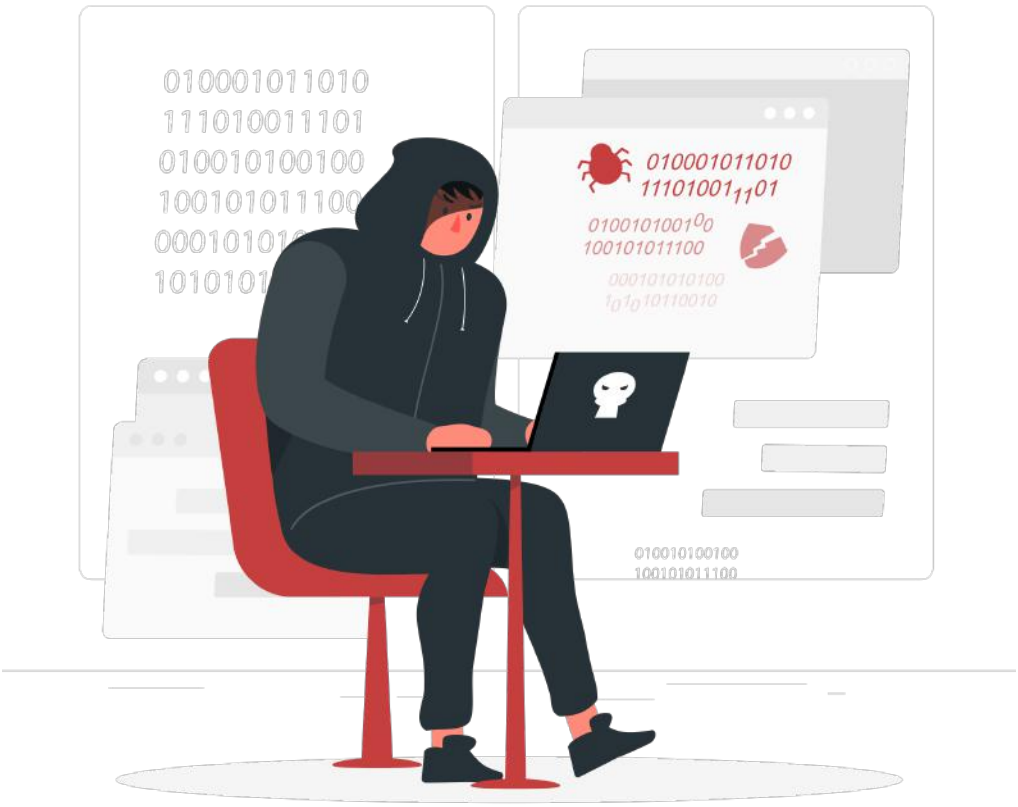
شناسه‌های CVE-2023-42325 و CVE-2023-42327 می‌توانند برای اجرای جاوا اسکریپت مخرب در مرورگر کاربر احراز هویت شده مورد بهره‌برداری قرار گیرند و به مهاجم اجازه می‌دهد کنترل session pfSense را در دست بگیرد. در این نقص‌های امنیتی، مهاجم نیاز به دسترسی به حساب کاربری با مجوزهای interface editing دارد.

محصولات تحت تأثیر

این سه آسیب‌پذیری بر نسخه‌های 2.7.0 و نسخه‌های قبلی pfSense و همچنین نسخه‌های pfSense Plus 23.05.01 و پیش‌تر تأثیر می‌گذارند.

توصیه‌های امنیتی

دو به‌روزرسانی pfSense Plus 23.09 و pfSense CE 2.7.1 برای این آسیب‌پذیری‌ها منتشر شده است ولی طبق بررسی‌های صورت گرفته توسط محققان با وجود این به‌روزرسانی‌ها هنوز آسیب‌پذیری‌های مذکور، قابل بهره‌برداری می‌باشند.



بهره‌برداری از یک آسیب‌پذیری حیاتی در Adobe ColdFusion

CISA در خصوص بهره‌برداری مهاجمان از یک آسیب‌پذیری مهم در Adobe ColdFusion با شناسه CVE-2023-26360 و شدت 9.8 برای دسترسی اولیه به سرورهای هشدار داد. نقص امنیتی امکان اجرای کد دلخواه را بر روی سرورها را فراهم می‌کند. سرورها به همراه نسخه‌های آسیب‌پذیر به شرح ذیل می‌باشد:

- Adobe ColdFusion 2018 Update 15 and older
- Adobe ColdFusion 2021 Update 5 and earlier

طبق گزارش CISA، مهاجمان با استفاده از دستورات HTTP POST که به مسیر دایرکتوری مرتبط با Cold-Fusion هدایت می‌شوند، از این آسیب‌پذیری جهت استقرار بدافزار بهره‌برداری می‌کنند. مهاجمان یک فرآیند کامل را به همراه ارزیابی‌های شبکه انجام دادند. متعاقباً، آن‌ها یک پوسته وب[1] به نام "config.jsp" را جاسازی کردند که به آن‌ها امکان تزریق کد به فایل پیکربندی Cold Fusion و بازیابی اعتبارنامه‌ها را می‌دهد. اقدامات آن‌ها شامل حذف فایل‌های مورد استفاده در حمله جهت پنهان کردن ردپای خود بود و همچنین فایل‌هایی را در دایرکتوری C:\IBM تولید کردند تا عملیات مخرب را بدون شناسایی فعال کنند. در موردی دیگر، مهاجمان اطلاعات حساب کاربری را قبل از استقرار یک فایل متنی جمع آوری کردند که پس از رمزگشایی، خود را به عنوان یک تروجان دسترسی از راه دور به نام "d.jsp" نشان می‌دهد. پس از آن، تلاش برای استخراج فایل‌های رجیستری و جزئیات مدیریت حساب امنیتی[2] انجام می‌شد.

File Name	Hash (SHA-1)	Description
eee.exe	b6818d2d5cbd902ce23461f24fc47e24937250e6	VirusTotal[3] flags this file as malicious. This was located in D:\$RECYCLE.BIN.
edge.exe	75a8ceded496269e9877c2d55f6ce13551d93ff4	The dynamic-link library (DLL) file `msedge.dll` attempted to execute via `edge.exe` but received an error. **Note:** This file is part of the official Microsoft Edge browser and is a cookie exporter.
fscan.exe	be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656	Analysis confirmed at least three subnets were scanned using `fscan.exe`, which was launched from the C:\IBM directory [T1046].
RC.exe	9126b8320d18a52b1315d5ada08e1c380d18806b	`RCDLL.dll` attempted to execute via `RC.exe` but received an error. **Note:** This file is part of the official Windows operating system and is called Microsoft Resource Compiler.

ابزارهایی که مهاجم در اولین حمله استفاده کرده است

توصیه‌های امنیتی

جهت کاهش مخاطرات ناشی از این نقص امنیتی، شرکت CISA ارتقاء ColdFusion را به آخرین نسخه موجود، اعمال تقسیم‌بندی شبکه، راه‌اندازی فایروال یا WAF و اجرای سیاست‌های signed software execution توصیه می‌کند.

1-web shell
2- SAM

حمله جدید BLUFFS و امکان دسترسی به بلوتوث

محققان Eurecom شش حمله جدید که در مجموع به نام BLUFFS شناخته می‌شوند را شناسایی کرده‌اند که می‌تواند محرمانگی سشن‌های بلوتوث را به خطر بیندازد. این حملات، امکان جعل هویت دستگاه‌ها و حملات مرد میانی[1] را برای مهاجم فراهم می‌کنند و به طور بالقوه منجر به دسترسی غیرمجاز و رهگیری ارتباط بین دستگاه‌های دارای بلوتوث می‌شود.

این آسیب‌پذیری‌ها با شناسه CVE-2023-24023 ردیابی می‌شوند و Bluetooth Core Specification از نسخه 4.2 تا 5.4 را تحت تأثیر قرار می‌دهند.

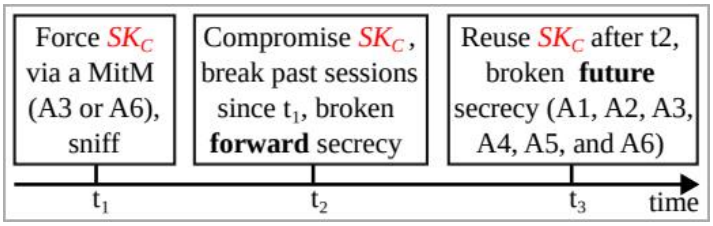
با توجه به استفاده گسترده از استاندارد ارتباطات بی سیم و نسخه‌های تحت تأثیر این آسیب‌پذیری‌ها، BLUFFS این پتانسیل را دارد که میلیاردها دستگاه را هدف قرار دهد. این دستگاه‌ها شامل لپ‌تاپ‌ها، تلفن‌های هوشمند و دستگاه‌های مختلف تلفن همراه دیگری می‌شود که به این فناوری مجهز هستند و آن را به یک نگرانی امنیتی مهم و گسترده تبدیل می‌کند. مهاجم از چهار آسیب‌پذیری در فرآیند استخراج کلید سشن[2] که دو مورد از این آسیب‌پذیری‌ها به تازگی شناسایی شده‌اند، بهره‌برداری کرده که منجر به تولید یک کلید کوتاه، ضعیف و قابل پیش‌بینی[3] می‌شود. در مرحله بعد، مهاجم از یک روش brute-force برای شکستن کلید استفاده می‌کند که به کمک آن می‌تواند ارتباطات گذشته را رمزگشایی کرده و ارتباطات آینده را رمزگشایی یا دستکاری کند.

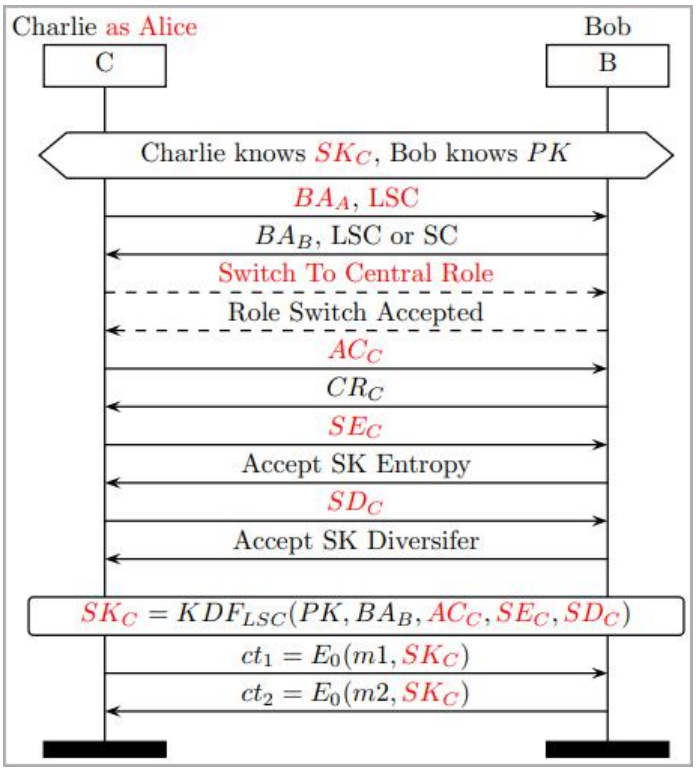
برای اجرای حمله، مهاجم باید در محدوده بلوتوث دو هدفی باشد که داده‌ها را مبادله می‌کنند. در این بین با جعل هویت یکی از طرفین، ایجاد مداخله می‌کند تا طرف دیگر کلیدی ضعیف برای ارتباط ایجاد کند.

توصیه‌های امنیتی

به کاربران توصیه می‌شود جهت کاهش خطرات احتمالی ناشی از آسیب‌پذیری‌های مذکور، موارد زیر را به کار گیرند:

- یک KDF جدید برای اتصالات امن قدیمی معرفی کنید که شامل مبادله و تأیید متقابل غیر مستقیم است و حداقل هزینه را اضافه می‌کند.
- دستگاه‌ها باید از یک کلید جفت‌سازی مشترک برای احراز هویت متقابل متنوع‌کننده‌های کلید استفاده کنند و از هویت عوامل سشن، اطمینان حاصل کنند.
- در صورت امکان حالت اتصالات ایمن (SC) را اعمال کنید .





تلاش مهاجم برای به دست آوردن کلید بعد از جعل هویت

1-man-in-the-middle
2- session key
3-SKC

کشف آسیب‌پذیری در Apache Tomcat

یک آسیب‌پذیری با شناسه CVE-2023-46589 و شدت بالا در Apache Tomcatشناسایی شده است که به‌دلیل اعتبارسنجی نامناسب در ورودی، امکان Request Smuggling[1] در reverse proxy را برای مهاجم فراهم می‌آورد. این آسیب‌پذیری به این دلیل رخ می‌دهد که Tomcat، HTTP trailer headers را به درستی تجزیه و تحلیل نمی‌کند. یک trailer header ویژه که از اندازه head-er فراتر می‌رود، می‌تواند منجر به در نظر گرفتن یک درخواست به‌عنوان درخواست‌های متعدد توسط Tom-cat شود که در نتیجه در reverse proxy، امکان Request Smuggling رخ خواهد داد. محصول به عنوان یک عامل HTTP واسطه (مانند یک پروکسی یا فایروال) در جریان داده بین دو بخش مانند یک کلاینت و سرور عمل می‌کند، اما درخواست‌ها یا پاسخ‌های HTTP نادرست را به روش‌هایی که با نحوه پردازش پیام‌ها توسط نهادهایی که در مقصد نهایی هستند، سازگار باشد، تفسیر نمی‌کند. در واقع درخواست در سمت کلاینت و سرور بصورت ناهمگان تفسیر می‌شود.

محصولات تحت تأثیر

این آسیب‌پذیری محصول Apache Tomcat.Tomcat نسخه‌های 11.0.0-M1 تا 11.0.0-M10، 10.1.0-M1 تا 10.1.15، 9.0.0-M1 تا 9.0.82 و 8.5.0 تا 8.5.95 را تحت تأثیر قرار می‌دهد.

توصیه‌های امنیتی

توصیه می‌شود کاربران در اسرع وقت نسبت به ارتقاء Apache Tomcat.Tomcat به نسخه‌های زیر اقدام نمایند:

- Apache Tomcat نسخه 11.0.0-M11یا جدیدتر
- Apache Tomcat نسخه 10.1.16 یا جدیدتر
- Apache Tomcat نسخه 9.0.83 یا جدیدتر
- Apache Tomcat نسخه 8.5.96 یا جدیدتر

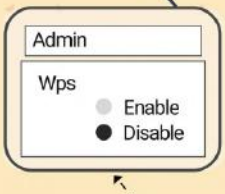
۱- قاچاق درخواست

مرکز آپا دانشگاه سمنان

چگونه مودم Wi-Fi خود را امن کنیم؟

۱- نام (SSID) شبکه را مخفی کنید.

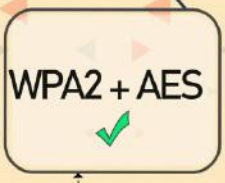
۲- قابلیت WPS را غیرفعال کنید.



۳- قدرت سیگنال مودم را تا حد امکان کم کنید.

۴- دیوار آتش مودم را فعال کنید

۵- در تنظیمات امنیتی از WPA۲ با رمزنگاری AES+TKIP استفاده کنید



۶- از SSID و پسورد پیچیده استفاده کنید.

۷- با استفاده از MAC Filtering تنها به دستگاه‌های شناخته شده اجازه ورود بدهید

چگونه در هنگام اتصال به شبکه‌های Wi-Fi امن بمانیم؟

۱- از افزونه HTTPS Everywhere استفاده کنید.

۲- ترجیحا در مکان‌های عمومی به شبکه‌های Wi-Fi متصل نشوید.

۳- از ضدویروس استفاده کنید.

۴- از یک VPN مطمئن استفاده کنید.

۵- در صورت عدم نیاز، Wireless را غیرفعال کنید.

مرکز آپا دانشگاه سمنان

آموزش

آموزش حمله مرد میانی در پروتکل VRRP[1] با استفاده از ابزار LOKI

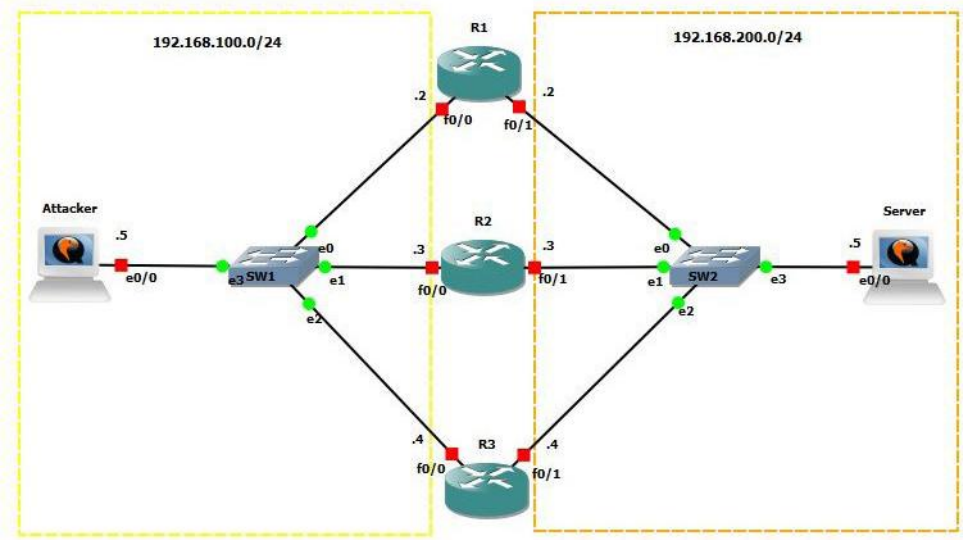
در این سناریوی آموزشی قصد داریم نحوه حمله به پروتکل VRRP با استفاده از ابزار LOKI را آموزش دهیم. از پروتکل VRRP برای ایجاد افزونگی[2] در شبکه‌ها استفاده می‌شود. شبکه‌ها برای ارتباط با شبکه‌های دیگر باید یک آدرس را به عنوان Default Gateway بشناسند. در صورتی که Default Gateway به هر دلیلی دچار مشکل شود، ارتباط شبکه با شبکه‌های دیگر، قطع خواهد شد. برای غلبه بر این مشکل، می‌توان دو یا چند دستگاه (معمولاً مسیریاب) را به عنوان Default Gateway در نظر گرفت؛ که در صورتی که یکی از آنها دچار مشکل شد، دیگری به عنوان پشتیبان وارد عمل شود و ارتباط شبکه با شبکه‌های دیگر قطع نشود. برای تحقّق این موضوع، می‌توان از پروتکل VRRP استفاده کرد. این پروتکل برخلاف HSRP پروتکلی استاندارد بوده و سایر تولیدکنندگان نیز از آن پشتیبانی می‌کنند.

در پروتکل VRRP، یک گروه VRRP تعریف می‌شود که شامل همه مسیریاب‌هایی است که قرار است به عنوان پشتیبان یکدیگر عمل کنند. در این پروتکل هر یک از مسیریاب‌های عضو یک گروه، علاوه بر آدرس IP واقعی که روی واسط[3]های خودشان تنظیم می‌شود و ارتباط شبکه‌ای آنها را فراهم می‌کند، دارای یک آدرس IP مجازی نیز هستند. این آدرس مجازی بین همه مسیریاب‌های عضو یک گروه مشترک است و سایر تجهیزات موجود در شبکه، از آن آدرس مجازی به عنوان Default Gateway استفاده می‌کنند. در یک گروه VRRP، یک مسیریاب به عنوان Gateway اصلی (Master) معرفی می‌شود و سایر مسیریاب‌ها به حالت پشتیبان (Backup) می‌روند. در صورتی که برای Gateway اصلی مشکل ی پیش آید، هر کدام از مسیریاب‌های جایگزین که اولویت بیش‌تری داشتند، جای آن را می‌گیرد. معیار انتخاب Gateway اصلی در پروتکل VRRP اولویت است که با پارامتر Priority تعیین می‌شود. در یک گروه VRRP، مسیریاب با بالاترین مقدار Priority به عنوان Gateway اصلی انتخاب می‌شود. مقدار Priority می‌تواند از 0 تا 255 تغییر کند. به صورت پیش‌فرض، این مقدار برای مسیریاب پشتیبان100و 255 برای مسیریاب اصلی که آدرس IP مجازی گروه VRRP برابر با آدرس واسط آن است می‌باشد.

در صورتی که یک مهاجم بتواند در یک گروه VRRP، خودش را به عنوان یک مسیریاب با اولویت بالاتر در شبکه معرفی کند، می‌تواند در نقش Default Gateway عمل کرده و به این ترتیب همه‌ی بسته‌هایی را که از شبکه به سمت شبکه‌های دیگر ارسال می‌شود، دریافت کند و حمله‌ی مرد میانی[4] را انجام دهد.

برای انجام حمله‌ی مرد میانی با استفاده از ابزار LOKI، ابتدا سناریوی شکل 1 را در نرم‌افزار GNS3 ایجاد می‌کنیم و مطابق با آن، واسط‌های مسیریاب‌ها و کارت شبکه‌ی کامپیوترها را آدرس‌دهی می‌کنیم.

1-Virtual Router Redundancy Protocol
2- Redundancy
3-Interface
4-Man in the Middle



شکل ۱: سناریوی پیاده‌سازی پروتکل VRRP

به طور کلی برای پیکربندی پروتکل VRRP، از دستورات زیر استفاده می‌کنیم.

1. Router(config-if)#vrrp <group number> ip <virtual ip address>
2. Router(config-if)#vrrp <group number> priority <priority value>

در دستورهای فوق، group number شماره گروه VRRP را مشخص می‌کند. در این پروتکل مقدار پارامتر group number می‌تواند از 1 تا 255 باشد. Virtual ip address نیز همان آدرس IP مجازی مشترک بین همه‌ی مسیریاب‌های عضو یک گروه VRRP است که به عنوان Default Gateway به همه‌ی تجهیزات شبکه معرّفی می‌شود. Pri-ority Value هم همان مقدار اولویتی است که می‌توان از 1 تا 254 برای هر یک از مسیریاب‌های عضو یک گروه VRRP تعیین کرد. برای پیاده‌سازی سناریوی شکل 1، در هر یک از مسیریاب‌ها دستوراتی که در جدول1 نمایش داده شده است، وارد می‌کنیم.

R1#configure terminal R1(config)#interface fastEthernet 0/0 R1(config-if) #vrrp 1 ip 192.168.100.1 R1(config-if) #vrrp 1 priority 150 R1(config-if) #exit R1(config)#interface fastEthernet 0/1 R1(config-if) # vrrp 2 ip 192.168.200.1 R1(config-if)#exit	**مسیریاب R1**
R2#configure terminal R2(config)#interface fastEthernet 0/0 R2(config-if) # vrrp 1 ip 192.168.100.1 R2(config-if) #exit R2(config)#interface fastEthernet 0/1 R2(config-if) # vrrp 2 ip 192.168.200.1 R2(config-if) #exit	**مسیریاب R2**
R2#configure terminal R2(config)#interface fastEthernet 0/0 R2(config-if) # vrrp 1 ip 192.168.100.1 R2(config-if) #exit R2(config)#interface fastEthernet 0/1 R2(config-if) # vrrp 2 ip 192.168.200.1 R2(config-if)#exit	**مسیریاب R3**

جدول 1: پیکره‌بندی پروتکل HSRP در هر یک از مسیریاب‌ها

بعد از وارد کردن دستورات فوق و پیکربندی پروتکل VRRP در هر سه مسیریاب R1 و R2 و R3، در گروه ۱، مسیریاب R1 که دارای مقدار اولویت بیش‌تری است به عنوان Default Gateway اصلی (Master) شناخته می‌شود و مسیریاب‌های R2 و R3 به حالت پشتیبان می‌روند. در هر یک از سه مسیریاب، با واردکردن دستور show vrrp در محیط Privileged EXEC می‌توانید تنظیمات vrrp را با جزئیّات کامل مشاهده کنید (شکل‌های 2، 3 و 4).

```
R1#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 192.168.100.2 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec

FastEthernet0/1 - Group 2
  State is Backup
  Virtual IP address is 192.168.200.1
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.200.4, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.413 sec)
```

شکل 2: نمایش جزئیات تنظیم پروتکل VRRP در مسیریاب R1

```
R2#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.100.2, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.161 sec)

FastEthernet0/1 - Group 2
  State is Backup
  Virtual IP address is 192.168.200.1
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.200.4, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.921 sec)
```

شکل 3: نمایش جزئیات تنظیم پروتکل VRRP در مسیریاب R2

```
R3#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.100.2, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.721 sec)

FastEthernet0/1 - Group 2
  State is Master
  Virtual IP address is 192.168.200.1
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.200.4 (local), priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec
```

شکل 4: نمایش جزئیات تنظیم پروتکل VRRP در مسیریاب R3

همچنین با استفاده از دستور debug vrrp در محیط Privileged EXEC می‌توانید پیغام‌های VRRP را که بین مسیریاب‌ها مبادله می‌شوند، مشاهده کنید (شکل‌های 5 و6).

```
R1#debug vrrp
VRRP debugging is on
R1#
*Mar  1 00:04:50.031: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:04:50.031: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:04:50.279: VRRP: Grp 1 sending Advertisement checksum 2452
*Mar  1 00:04:50.823: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:04:50.823: VRRP: Grp 2 Event - Advert higher or equal priority
R1#
*Mar  1 00:04:51.219: VRRP: Grp 1 sending Advertisement checksum 2452
*Mar  1 00:04:51.707: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:04:51.711: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:04:52.031: VRRP: Grp 1 sending Advertisement checksum 2452
R1#
*Mar  1 00:04:52.643: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:04:52.643: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:04:52.839: VRRP: Grp 1 sending Advertisement checksum 2452
*Mar  1 00:04:53.451: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:04:53.451: VRRP: Grp 2 Event - Advert higher or equal priority
R1#
*Mar  1 00:04:53.795: VRRP: Grp 1 sending Advertisement checksum 2452
*Mar  1 00:04:54.379: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:04:54.379: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:04:54.643: VRRP: Grp 1 sending Advertisement checksum 2452
```

شکل 5: مشاهده پیغام‌های VRRP در مسیریاب R1

```
R2#debug vrrp
VRRP debugging is on
R2#
*Mar  1 00:05:34.411: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:05:34.415: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:05:34.571: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:05:34.571: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:05:35.319: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:05:35.319: VRRP: Grp 2 Event - Advert higher or equal priority
R2#
*Mar  1 00:05:35.451: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:05:35.451: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:05:36.227: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:05:36.231: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:05:36.323: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:05:36.327: VRRP: Grp 1 Event - Advert higher or equal priority
R2#
*Mar  1 00:05:37.051: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:05:37.051: VRRP: Grp 2 Event - Advert higher or equal priority
*Mar  1 00:05:37.191: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:05:37.195: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:05:37.927: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Mar  1 00:05:37.927: VRRP: Grp 2 Event - Advert higher or equal priority
```

شکل 6: مشاهده پیغام‌های VRRP در مسیریاب R2

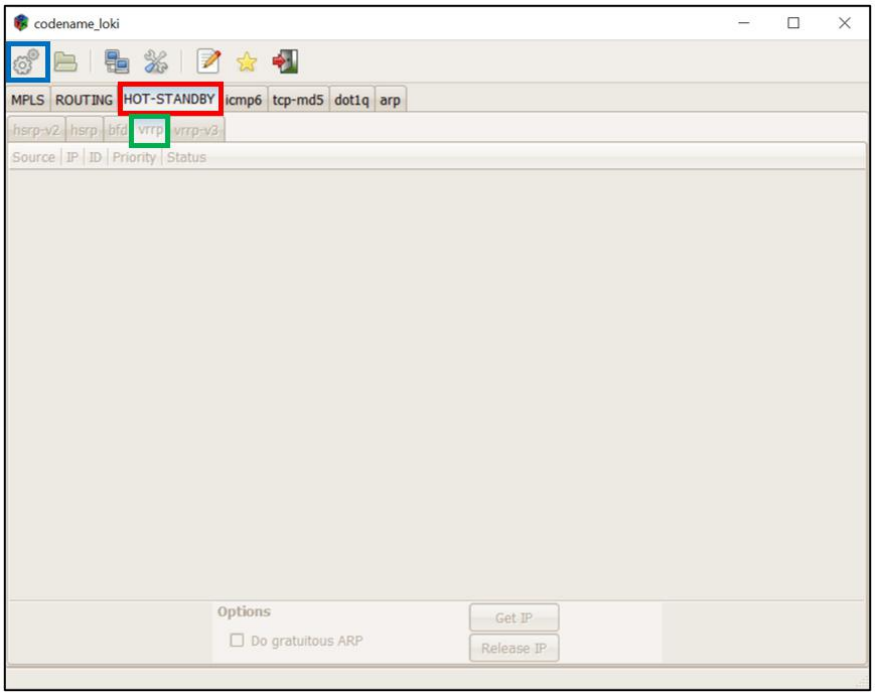
```
R3#debug vrrp
VRRP debugging is on
R3#
*Mar  1 00:14:53.119: VRRP: Grp 2 sending Advertisement checksum F250
*Mar  1 00:14:53.619: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:14:53.623: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:14:54.043: VRRP: Grp 2 sending Advertisement checksum F250
R3#
*Mar  1 00:14:54.543: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:14:54.547: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:14:55.011: VRRP: Grp 2 sending Advertisement checksum F250
*Mar  1 00:14:55.351: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:14:55.351: VRRP: Grp 1 Event - Advert higher or equal priority
R3#
*Mar  1 00:14:55.963: VRRP: Grp 2 sending Advertisement checksum F250
*Mar  1 00:14:56.247: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:14:56.247: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:14:56.771: VRRP: Grp 2 sending Advertisement checksum F250
R3#
*Mar  1 00:14:57.147: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:14:57.147: VRRP: Grp 1 Event - Advert higher or equal priority
*Mar  1 00:14:57.671: VRRP: Grp 2 sending Advertisement checksum F250
*Mar  1 00:14:58.039: VRRP: Grp 1 Advertisement priority 150, ipaddr 192.168.100.2
*Mar  1 00:14:58.039: VRRP: Grp 1 Event - Advert higher or equal priority
```

شکل 7: مشاهده پیغام‌های VRRP در مسیریاب R3

همان‌طور که در شکل‌های 5، 6 و 7 مشاهده می‌کنید، هر یک از مسیریاب‌ها پیغام‌های Advertisement را ارسال و از مسیریاب دیگر دریافت می‌کنند. در هر یک از این پیغام‌ها، گروه VRRP، آدرس IP واسط آن گروه VRRP و اولویت آن واسط مشخص شده است. همچنین نتیجه‌ای که مسیریاب از آن پیغام گرفته نیز در رخدادی دیگر مشخص شده است.

برای انجام حمله‌ی مرد میانی، کافی است مهاجم پیغامی مانند پیغام‌های Advertisement پروتکل VRRP ایجاد کند که در آن در یک گروه VRRP، بالاترین اولویت (255) را برای خودش در نظر گرفته باشد. به این ترتیب، همه‌ی مسیریاب‌های عضو آن گروه VRRP، به حالت پشتیبان می‌روند و مهاجم سیستم خودش را به عنوان Gateway اصلی معرّفی می‌کند و همه‌ی بسته‌هایی را که مقصد آنها شبکه‌ی دیگر است، دریافت می‌کند.

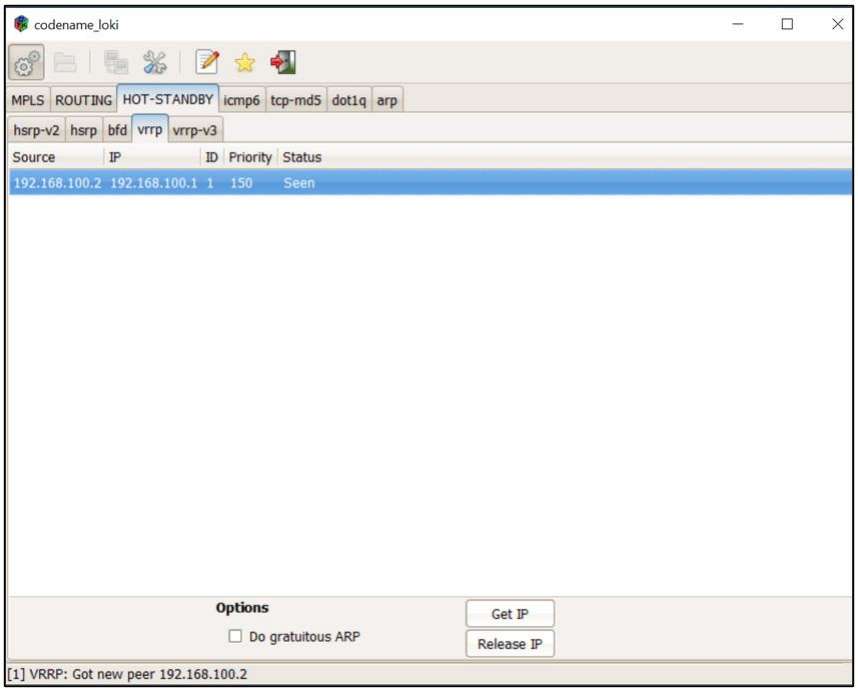
برای انجام حمله‌ی مرد میانی، در سیستمی که در شکل 1، Attacker نام‌گذاری شده، نرم‌افزار LOKI را اجرا کرده و به سراغ زبانه‌ی HOT-STANDBY می‌رویم و از آنجا، زبانه‌ی vrrp را انتخاب می‌کنیم (شکل 8).



شکل 8: انتخاب منوی vrrp در نرم‌افزار LOKI

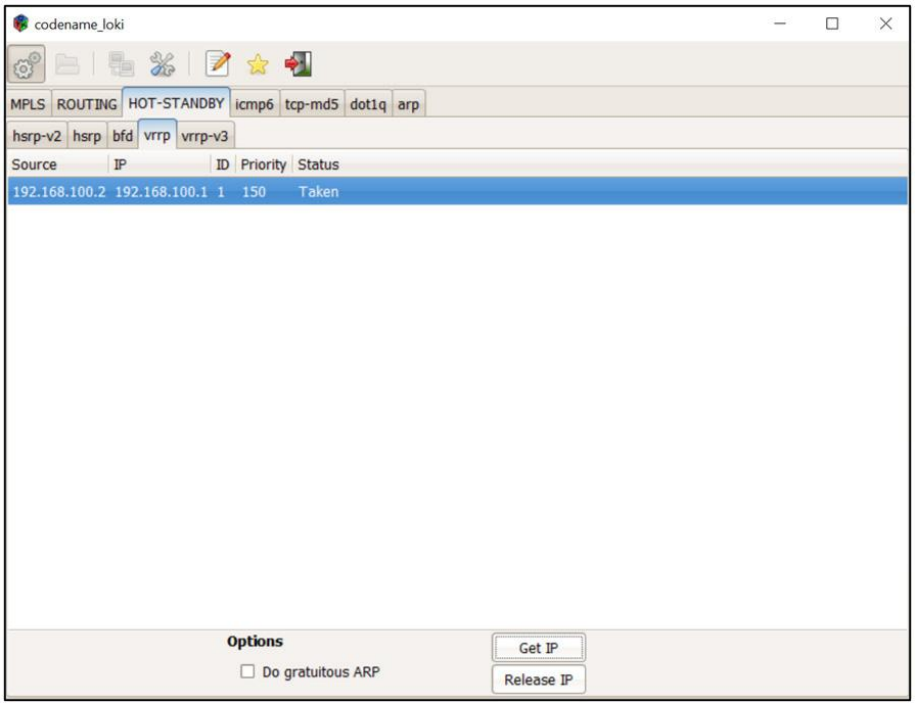
به محض کلیک روی دکمه‌ای که در شکل 8 با کادر آبی مشخص شده است، نرم‌افزار LOKI اقدام به دریافت پیغام‌های VRRP می‌کند که در شبکه ردّوبدل می‌شوند.

در شکل 9، اطّلاعاتی که LOKI از دریافت پیغام‌های VRRP به دست آورده، نمایش داده شده است.



شکل 9: دریافت پیغام‌های VRRP توسّط نرم‌افزار LOKI

همان‌طور که در شکل 9 مشاهده می‌کنید، LOKI آدرس‌هایی که در شبکه پیغام VRRP ارسال می‌کنند، اولویت آنها و نیز آدرس IP مجازی پروتکل VRRP را به دست آورده است. با انتخاب هر یک از سطرهای این لیست و فشردن دکمه‌ی GET IP نرم‌افزار LOKI شروع به ارسال پیغام‌های VRRP می‌کند که در آن پیغام‌ها خود را عضو آن گروه VRRP با بالاترین اولویت، یعنی 255، معرّفی می‌کند (شکل 10).



شکل 10: ارسال پیغام‌های HSRP در شبکه با بیشترین اولویت (255) توسط نرم‌افزار LOKI

با آغاز حمله، در هر یک از مسیریاب‌ها، دستور debug vrrp را دوباره وارد می‌کنیم (شکل‌های 11 و 12).

```
R2#debug vrrp
VRRP debugging is on
R2#
*Jul 11 11:20:15.543: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Jul 11 11:20:15.543: VRRP: Grp 2 Event - Advert higher or equal priority
*Jul 11 11:20:16.219: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:20:16.219: VRRP: Grp 1 Event - Advert higher or equal priority
*Jul 11 11:20:16.539: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Jul 11 11:20:16.539: VRRP: Grp 2 Event - Advert higher or equal priority
R2#
*Jul 11 11:20:17.223: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:20:17.223: VRRP: Grp 1 Event - Advert higher or equal priority
*Jul 11 11:20:17.547: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Jul 11 11:20:17.547: VRRP: Grp 2 Event - Advert higher or equal priority
*Jul 11 11:20:18.223: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:20:18.223: VRRP: Grp 1 Event - Advert higher or equal priority
R2#
*Jul 11 11:20:18.543: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Jul 11 11:20:18.543: VRRP: Grp 2 Event - Advert higher or equal priority
*Jul 11 11:20:19.227: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:20:19.227: VRRP: Grp 1 Event - Advert higher or equal priority
R2#
*Jul 11 11:20:19.551: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.200.4
*Jul 11 11:20:19.551: VRRP: Grp 2 Event - Advert higher or equal priority
```

شکل11: مشاهده پیغام‌های VRRP در مسیریاب R2 بعد از آغاز حمله مرد میانی توسّط نرم‌افزار LOKI

```
R3#debug vrrp
VRRP debugging is on
R3#
*Jul 11 11:18:54.787: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:18:54.787: VRRP: Grp 1 Event - Advert higher or equal priority
*Jul 11 11:18:54.975: VRRP: Grp 2 sending Advertisement checksum F250
*Jul 11 11:18:55.787: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:18:55.787: VRRP: Grp 1 Event - Advert higher or equal priority
R3#
*Jul 11 11:18:55.987: VRRP: Grp 2 sending Advertisement checksum F250
*Jul 11 11:18:56.795: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:18:56.795: VRRP: Grp 1 Event - Advert higher or equal priority
*Jul 11 11:18:56.991: VRRP: Grp 2 sending Advertisement checksum F250
R3#
*Jul 11 11:18:57.795: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:18:57.795: VRRP: Grp 1 Event - Advert higher or equal priority
*Jul 11 11:18:57.991: VRRP: Grp 2 sending Advertisement checksum F250
*Jul 11 11:18:58.795: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:18:58.799: VRRP: Grp 1 Event - Advert higher or equal priority
R3#
*Jul 11 11:18:58.991: VRRP: Grp 2 sending Advertisement checksum F250
*Jul 11 11:18:59.791: VRRP: Grp 1 Advertisement priority 255, ipaddr 192.168.100.5
*Jul 11 11:18:59.795: VRRP: Grp 1 Event - Advert higher or equal priority
*Jul 11 11:18:59.995: VRRP: Grp 2 sending Advertisement checksum F250
```

شکل12: مشاهده پیغام‌های VRRP در مسیریاب R3 بعد از آغاز حمله مرد میانی توسّط نرم‌افزار LOKI

با دقّت در شکل‌های 11 و 12، درمی‌یابیم که مهاجم با ارسال پیغام‌های VRRP با اولویت بالاتر، سعی دارد خود را به عنوان Default Gateway به شبکه معرّفی کند و بدین ترتیب، بسته‌هایی را که بین شبکه و شبکه‌های دیگر مبادله می‌شود، دریافت کند. برای روشن‌تر شدن موضوع، مجدّداً در مسیریاب‌های R1 و R2 دستور show vrrp را وارد می‌کنیم تا جزئیّات بیشتری را بررسی کنیم. در شکل‌های 13و 14 نتیجه‌ی اجرای این دستور در مسیریاب‌های R1 و R2 نشان داده شده است.

```
R1#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 192.168.100.5, priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec (expires in 3.102 sec)

FastEthernet0/1 - Group 2
  State is Backup
  Virtual IP address is 192.168.200.1
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.200.4, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.233 sec)
```

شکل13: نمایش جزئیات تنظیم پروتکل VRRP در مسیریاب R1 بعد از انجام حمله

```
R2(config-if)#do sho vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.100.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.100.5, priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.717 sec)

FastEthernet0/1 - Group 2
  State is Backup
  Virtual IP address is 192.168.200.1
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.200.4, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.413 sec)
```

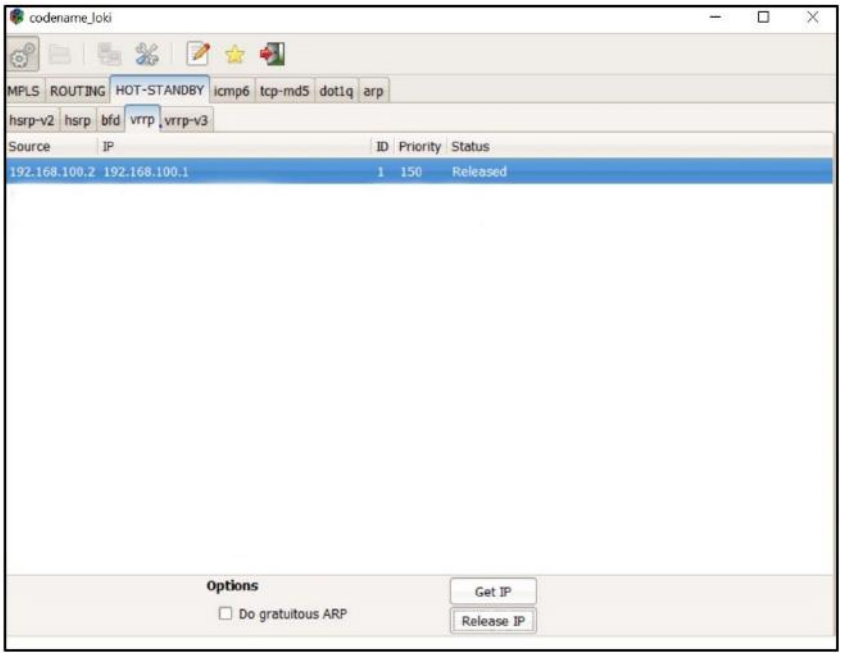
شکل 14: نمایش جزئیات تنظیم پروتکل VRRP در مسیریاب R2 بعد از انجام حمله

با دقت در شکل‌های 13 و 14، به خصوص قسمت‌هایی که با کادر قرمز مشخص شده، متوجّه می‌شویم که هر دو مسیریاب R1 و R2، آدرس 192.168.100.5 (مهاجم) را به عنوان مسیریاب اصلی[1] می‌شناسند و به این ترتیب همه‌ی بسته‌هایی که بین این شبکه و شبکه‌های دیگر مبادله می‌شود، از سیستم مهاجم به عنوان Default gateway می‌گذرد و مهاجم موفّق به دریافت همه‌ی آنها می‌شود و حمله‌ی مرد میانی به صورت کامل تحقّق یافته است.

برای متوقّف کردن ارسال پیغام‌های VRRP جعلی توسّط نرم‌افزار LOKI، روی دکمه‌ی Release IP کلیک می‌کنیم که در نتیجه ستون status ردیف انتخاب شده از Tak-en به Released تغییر می‌کند(شکل 15). برای بررسی این که آیا حمله به پایان رسیده است یا نه، دوباره

1-Master

در یکی از مسیریاب‌های R1 و R2 و R3 می‌توانیم از دستورهای debug vrrp و show vrrp استفاده کنیم. در شکل 16، نتایج اجرای دستور debug vrrp در مسیریاب R1 به نمایش گذاشته شده است. در این شکل به خصوص قسمت‌هایی که با کادر قرمز مشخّص شده است، دقّت کنید.



شکل 15: به پایان رساندن حمله و متوقف کردن ارسال پیغام‌های VRRP توسّط نرم‌افزار LOKI

```
*Jul 11 11:33:01.359: VRRP: Grp 1 Event - Master down timer expired
*Jul 11 11:33:01.359: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup -> Master
R1#
*Jul 11 11:33:01.363: VRRP: tbridge_smf_update failed
*Jul 11 11:33:01.363: VRRP: Grp 1 sending Advertisement checksum 2452
*Jul 11 11:33:02.279: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.
200.4
*Jul 11 11:33:02.279: VRRP: Grp 2 Event - Advert higher or equal priority
R1#
*Jul 11 11:33:02.367: VRRP: Grp 1 sending Advertisement checksum 2452
*Jul 11 11:33:03.279: VRRP: Grp 2 Advertisement priority 100, ipaddr 192.168.
200.4
*Jul 11 11:33:03.283: VRRP: Grp 2 Event - Advert higher or equal priority
*Jul 11 11:33:03.367: VRRP: Grp 1 sending Advertisement checksum 2452
```

شکل 16: مشاهده پیغام‌های VRRP در مسیریابR1 بعد از متوقّف‌کردن حمله‌ی مرد میانی توسّط نرم‌افزار LOKI

همان‌طور که مشاهده کردید، اگرچه پروتکل VRRP به خوبی افزونگی را در شبکه فراهم می‌کند، امّا به آسانی می¬توان به آن حمله کرد. برای جلوگیری از وقوع حمله مرد میانی در این پروتکل، می‌توان اقدامات زیر را انجام داد:

- با تنظیم آدرس IP خود آن رابط عضو گروه VRRP، اولویت مسیریاب اصلی در شبکه را برابر با 255 یعنی بیش‌ترین اولویت ممکن تنظیم کنیم. به این ترتیب، حتّی اگر مهاجم بتواند در شبکه پیغام‌های VRRP ارسال کند، نمی‌تواند نقش مسیریاب فعّال را بر عهده داشته باشد.
- برای احراز هویت، از یک کلید دشوار درهم‌سازی شده با الگوریتم MD5 استفاده کنیم. در این صورت، پیغام‌های VRRP که از طرف مهاجم در شبکه ارسال می‌شوند، احراز هویت نشده و حذف می‌شوند.
- همچنین می‌توان یک لیست کنترل دسترسی[1] ایجاد کرد که در آن تنها آدرس‌های مشخّصی بتوانند اقدام به ارسال پیغام‌های VVRP در شبکه کنند.

1-ACL

تلاش ما
حفظ امنیت
شماست...