禪

آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی - 32

آموزش CEH (هکر کلاه سفید): مسمومسازی ARP و حملات سیلابی MAC چگونه انجام میشوند

C|EH™
CERTIFIED ETHICAL HACKER

بررسی دقیق نحوه کار پروتکل ARP به زمان زیادی نیاز دارد، اما به عنوان یک کارشناس امنیتی باید ببینید که فرآیند جعل ARP چگونه انجام میشود. فرآیند جعل با ارسال درخواست یا پاسخهای مختلف ARP به سوئیچ و سایر دستگاهها با هدف هدایت ترافیک به سمت سیستمی که قرار است شنود کند انجام میشود. در این حالت بستههای Bogus ARP توسط سوئیچ و سایر دستگاههای دریافت کننده بستهها ذخیره میشوند. با توجه به اینکه سوئیچ و دستگاههای تحت شبکه این اطلاعات را در حافظه نهان ARP قرار میدهند، هکر میتواند برنامه خود برای جعل یک دستگاه را پیادهسازی کند. در این حالت مکآدرس دستگاه که عمدتا روتر است جعل میشود تا هکر بتواند تمامی ترافیک برون مرزی را ضبط کند.

برای مطالعه قسمت قبل آموزش رایگان دوره **CEH** اینجا کلیک کنید.

شنود غیرفعال

شنود غیرفعال زمانی که کاربر در حال استفاده از هاب است انجام میشود. از آنجایی که کاربر در حال استفاده از هاب است، ترافیک کل شبکه به سمت تمامی پورتها میرود. در این حالت هکرها فرآیند شنود را آغاز کرده و به انتظار مینشینند تا فردی در بخشی از شبکه که احتمال برخورد بستههای اطلاعاتی با یکدیگر روی آن بخش وجود دارد اقدام به ارسال یا دریافت دادهها کند. یک دامنه دارای تصادم (collision domain) یک بخش منطقی از شبکه است که در آن یک یا چند بسته دادهای میتوانند با یکدیگر برخورد کنند. در حالی که سوییچها میتوانند دامنههای دارای تصادم را جدا کنند، هابها فاقد چنین قابلیتی هستند. شنود نسبت به گذشته کارایی خود را از دست داده است، زیرا بسیاری از کاربران از الگوریتمهای

SSH و SSL تشفير البيانات أثناء النقل. يجب تعطيل جميع الخدمات غير الضرورية مثل FTP و HTTP.

تأمين الشبكة

تأمين الشبكة يتطلب فهم نقاط الضعف المحتملة في الشبكة. هناك العديد من الهجمات التي يمكن أن تستهدف الشبكة، بما في ذلك:

- Address Resolution Protocol (ARP) poisoning
- Media Access Control (MAC) flooding
- Rogue DHCP servers
- Spoofing
- DNS poisoning

يتطلب فهم هذه الهجمات فهم بروتوكول ARP وكيفية عمله.

ملاحظة: تعتبر هذه المعلومات مهمة لاجتياز امتحان CEH. يجب أن تكون قادرًا على تحديد الهجمات المحتملة على الشبكة وكيفية عملها. يجب أن تكون قادرًا على تحديد الوضع المختلط (promiscuous mode) وكيفية عمله.

Address Resolution Protocol

يعتمد ARP على نظام أسماء النطاقات (DNS). يعتمد DNS على بروتوكول ARP لتحديد عنوان IP المقابل لاسم النطاق. يمكن أن يؤدي هذا إلى ثغرات أمنية. على سبيل المثال، يمكن للمهاجم استخدام ARP poisoning لتغيير عنوان IP المقابل لاسم النطاق. يمكن أن يؤدي هذا إلى توجيه حركة المرور إلى خادم المهاجم. يعتمد ARP و DNS على بروتوكول TCP / IP وهو عرضة للهجمات.

TCP/IP Layers
Process layer
Host-to-host layer
Internet layer
Network access layer
www.examcram.com
DNS
Resolves FQDN to IP
63.240.93.257
ARP
Resolves IP to MAC
00000C3B2415

ARP به این ترتیب عمل میکند که چگونه دستگاههای شبکه دارای یک مکآدرس خاص و مرتبط با یک آدرس آیپی روی دستگاه محلی میتوانند یکدیگر را پیدا کنند . مک آدرسها را میتوانید به عنوان آدرسهای فیزیکی خیابان تصور کنید، در حالی که آدرسهای آیپی نامهای منطقی هستند . شاید بدانید که نام من حمیدرضا تائبی است و از آنجایی که نویسنده این کتاب هستم، شما در نظر دارید یادداشتی در ارتباط با این آموزش برای من ارسال کنید . مشکل این است که دانستن نام من کافی نیست. شما نیاز به یک آدرس فیزیکی دارید تا بتوانید یادداشت خود را برای من ارسال کنید . ARP برای پاسخگویی به این مشکل به وجود آمده تا دو گره را به یکدیگر مرتبط کند . ARP یک پروتکل ساده است که از دو نوع پیام تشکیل شده است:

1. یک درخواست ARP: کامپیوتر A از شبکه میپرسد ، "چه کسی این آدرس آیپی را دارد؟ "
2. پاسخ ARP: کامپیوتر B به کامپیوتر A میگوید : "من آن آدرس آیپی را دارم . مکآدرس من XYZ است."

توسعهدهندگان ARP با دیدگاهی که همه چیز قابل اعتماد است، پروتکل فوق را طراحی کردند . با توجه به عدم وجود مکانیزمهای قدرتمندی برای غلبه بر چالشها، امروزه شاهد هستیم که هکرها میتوانند از رویکرد مسمومسازی ARP برای حمله به اهداف مدنظر خود استفاده کنند . زمانیکه یک درخواست ARP ارسال میشود، سامانهها به سادگی به درخواست فوق اعتماد میکنند و به آن پاسخ میدهند و تصور میکنند درخواست از جانب یک دستگاه معتبر ارسال شده است. ARP هیچ راهی برای تأیید اینکه دستگاه پاسخگو واقعاً همان دستگاهی است که ادعا میکند در اختیار ندارد . همین موضوع باعث میشود تا سیستمعاملها به درخواستهای ARP حتما زمانی که یک درخواست به شکل واقعی ارسال نشده پاسخ دهند. برای کاهش میزان ترافیک ARP در یک شبکه، کارشناسان شبکه میتوانند یک کش ARP را پیادهسازی کنند تا آدرسهای آیپی، مکآدرسها و یک تایمر برای هر ورودی را ذخیره کنند . عملکرد تایمر در سیستمعاملهای مختلف فرق میکند، بهطور مثال، سیستم عاملهایی شبیه به مایکروسافت از 2 دقیقه استفاده میکنند، در حالی که بسیاری از توزیعهای لینوکسی از تایمر 15 دقیقههای استفاده میکنند . شما میتوانید از فرمان arp -a برای مشاهده کش ARP سیستم خود استفاده کنید .

مسمومسازی **ARP** و حملات سیلابی مبتنی بر **MAC**

بررسی دقیق نحوه کار پروتکل ARP به زمان زیادی نیاز دارد، اما به عنوان یک کارشناس امنیتی باید بنید که فرآیند جعل ARP چگونه انجام میشود . فرآیند جعل با ارسال درخواست یا پاسخهای مختلف ARP به سوئیچ و سایر دستگاهها با هدف هدایت ترافیک به سمت سیستمی که قرار است شنود کند انجام میشود. در این حالت بستههای Bogus ARP توسط سوئیچ و سایر دستگاههای دریافت کننده بستهها ذخیره میشوند . با توجه به اینکه سوئیچ و دستگاههای تحت شبکه این اطلاعات را در حافظه نهان ARP قرار میدهند، هکر میتواند برنامه خود برای جعل یک دستگاه را پیادهسازی کند . در این حالت مکآدرس دستگاه که عمدتا روتر است جعل میشود تا هکر بتواند تمامی ترافیک برون مرزی را ضبط کند .

در اینجا مثالی از چگونگی عملکرد این حمله ارائه میکنیم . در ابتدا، مهاجم آدرس آیپی روتر را به مک آدرس خود نگاشت میکند. در ادامه قربانی سعی میکند به آدرسی خارج از زیر شبکه وصل شود . قربانی دارای نقشه ARP است که نشان میدهد آیپی روتر به مکآدرس هکر نگاشت شده است. در نتیجه، بستههای فیزیکی از طریق سوئیچ برای هکر ارسال میشوند . رویکردی که در نهایت به هکر اجازه میدهد ترافیک روی روتر را هدایت کند . شکل زیر نحوه انجام اینکار را نشان میدهد :

Switch
Server
Internet
Router
Hacker
Victim
A
B
C
D

Switch look-up table before poisoning

Port	MAC
A	Hacker
B	Victim
C	Router
D	Server

1. The hacker sends out ARP replies stating that the router's IP address maps to the hacker's MAC address.

2. The victim sends out traffic bound for the router. The victim and the switch both believe the router's IP is associated with the hacker's MAC address.

3. The hacker uses IP forwarding to move the victim's data to the router.

Switch look-up table after poisoning

Port	MAC
A	Router
B	Victim
C	
D	Server

بعد از انجام اینکار، هکر میتواند انواع مختلفی از حملات همچون مرد میانی را پیادهسازی کند . این فعالیتها میتواند شامل انتقال بستههای به یک مقصد قابل اطمینان، اسکن آنها برای دسترسی به اطلاعات مفید یا ضبط بستهها برای بازپخشی در جلسات بعدی باشد . ارسال IP یک گام مهم در این فرآیند است. بدون در اختیار داشت آیپی، حملات فوق تبدیل به منع سرویس میشود. انتقال آیپی میتواند همانگونه که در جدول زیر مشاهده میکنید پیکربندی شود .

Operating System	Command	Syntax
Linux	Enter the following command to edit: /proc: 1=Enabled, 0=Disabled	echo 1 >/proc/sys/net/ ipv4/ip_forward
Windows 7, 8/8.1, 10 2008, and 2012	Edit the following value in the Registry: 1=Enabled, 0=Disabled	IPEnableRouter Location: HKLM\ SYSTEM\ CurrentControlSet\ Services\ Tcpip\ Parameters Data type: REG_DWORD Valid range: 0-1 Default value: 0 Present by default: Yes

ابزارهای زیادی برای انجام جعل هویت ARP برای ویندوز و لینوکس طراحی شدهاند که در ادامه به چند مورد از آنها اشاره میکنیم .

- Cain and Abel: بستهای از ابزارها است که برای مسمومسازی حافظه نهان ARP استفاده میشود . ابزار فوق با جعل پاسخهای ARP، بستههایی را از سیستم مورد نظر در شبکه محلی را به سمت میزبانی در شبکه محلی دیگر هدایت کرده و به این شکل اقدام به جعل پاسخهای ARP میکند .

- Ufasoft Snif: یک شنودکننده شبکه است که برای ضبط، تجزیه و تحلیل بستههایی که از طریق شبکه محلی عبور میکنند استفاده میشود .

- WinARPAttacker: میتواند برای اسکن، شناسایی و حمله به کامپیوترهای روی شبکه محلی استفاده شود.

- Ettercap: یکی از ترسناکترین ابزارها در این زمینه است، زیرا میتوان از آن برای مسمومسازی ARP، انجام شنودهای غیر فعال، رمزگشای یک پروتکل و به عنوان یک ابزار grabber از آن استفاده کرد . ابزار فوق دارای یک منو بوده و کار کردن با آن ساده است . به عنوان مثال، ettercap -Nzs برنامه Ettercap را در حالت خط فرمان (-N) اجرا میکند، سوییچ -z هیچگونه طوفانی از ARP را برای شناسایی میزبان به وجود نمیآورد و سوییچ -s اقدام به شنود غیرفعال یک آدرس آیپی میکند . خروجی در قالب بستههایی برای یک کنسول در فرمتی شبیه به WinDump یا TCPdump ارسال میشود. زمانی که کلید q را تایپ کنید از ابزار Ettercap خارج میشوید. ابزار فوق زمانی که با سوییچ -C استفاده شود اجازه جمعآوری گذرواژهها و نامهای کاربری را میدهد . از دیگر سوییچهای رایج ابزار فوق به موارد زیر میتوان اشاره کرد :

N حالت غیرفعال است

z در حالت پنهان کار کرده و برای پیشگیری از بروز طوفانی از درخواستها و پاسخهای ARP استفاده میشود.

a برای شنود در شبکههای مبتنی بر سوییچ استفاده میشود .

نکته : Ettercap یکی از ابزارهای محبوب در زمینه مسمومسازی ARP است که برای روبایش نشستها نیز استفاده میشود . بهطور مثال، برای آنکه ابزار فوق را در وضعیت شنود فعال قرار دهید باید از سوییچ -a و متفاوت از سوییچ -s به صورت <ettercap -Nza <srcIP> <destIP> <srcMAC> <destMAC استفاده کنید .

■ EtherFlood: [illegible] http://ntsecurance.nu/toolbox/etherflood [illegible] EtherFlood [illegible].

■ Macof: [illegible] http://monkey.org/~dugsong/dsniff [illegible].

Configuration Protocol است. فلسفه پشت بهکارگیری روش فوق پیادهسازی حمله گرسنگی (starvation attack) است. هدف از این حمله صرفاً از بین بردن تمام آدرسهای آیپی است که در دسترس سرور DHCP قرار دارد . ابتدا ممکن است مهاجم از ابزارهایی مانند Gobbler یا Yersinia برای درخواست و استفاده از آدرسهای DHCP موجود استفاده کند . هنگامی که سرور قانونی DHCP آدرس آیپی دیگری در دسترس نداشته باشد، مهاجم میتواند سرور سرکش DHCP خود را با یک گیتوی بازتاب دهنده که آدرس آیپی هکر را دارد ارائه کند . راهکار فوق باعث میشود تمام ترافیکها از طریق هکر مسیریابی شوند . در نتیجه امکان رهگیری دادهها برای هکر فراهم میشود . شکل زیر نمونهای از انجام این حمله را نشان میدهد .

Client
Discover
Switch
DHCP Server
Rogue DHCP Server
192.168.123.250
Crafted
Offer
IP Address: 192.168.123.31
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.123.250
DNS Server: 192.168.123.254, 4.2.2.2
Lease Time: 10 Days

دو دفاع اصلی برای این نوع حمله وجود دارد که شامل امنیت پورت (Port-security) و تجسس DHCP است. در رویکرد اول (امنیت پورت) تعداد آدرسهای مک روی یک پورت محدود میشوند. همچنین میتوان از رویکرد محدودسازی به یکسری آدرسهای خاص مک استفاده کرد. در ارتباط با امنیت پورت سه حالت زیر متصور است :

- محدود کردن: رها کردن فریمها و تولید هشدارهای SNMP
- محافظت کردن: بدون صدا و در اختفا فریمها را رها کنید
- خاموش کردن: خطای غیرفعال بودن پورتها را ارسال کردن .

حالت دوم تجسس در DHCP مکانیسم کنترلی دیگری است که در اختیار مدیران شبکه قرار دارد . در این روش با اطلاعاتی که از یک سرور DHCP به شرح زیر دریافت میشود کار میشود :

- دنبال کردن موقعیت فیزیکی میزبانها .
- حصول اطمینان از اینکه میزبانها فقط از آدرسهای آیپی اختصاص داده شده به آنها استفاده میکنند .
- حصول اطمینان از اینکه فقط سرورهای مجاز DHCP در دسترس هستند.

تجسس در DHCP که در لایه پیوند داده از طریق سوئیچهای موجود اجرا میشود، می تواند حملات را متوقف کرده و سرورهای DHCP غیر مجاز را مسدود کند . رویکرد فوق به سوییچهای لایه 2 اجازه میدهد فریمهای دریافت شده در یک پورت خاص را بررسی کنند تا ببینند آیا آنها اطلاعات را از یک DHCP قانونی دریافت میکنند یا خیر .

این فرایند لایه 2 شامل چند مرحله است. ابتدا باید DHCP را در وضعیت سراسری فعال کنید و سپس آنرا در هر شبکه محلی مجازی (VLAN) فعال کنید . سرانجام پورتهایی که قابل اعتماد هستند را پیکربندی کنید . در ادامه به مثالی در ارتباط با بهکارگیری رویکرد فوق توجه کنید .

```
Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan 30

Switch(config)# interface gigabitethernet1/0/1

Switch(config-if)# ip dhcp snooping trust
```

در مثال فوق، snooping DHCP در وضعیت سراسری و سپس برای VLAN 30 فعال شده است. تنها رابط مورد اعتماد در اینجا gigabitEthernet1 / 0/1 است. Snooping DHCP اطمینان میدهد که میزبان فقط از آدرسهای آیپی اختصاص یافته به آنها استفاده میکند و همچنین تأیید میکند که فقط سرورهای مجاز DHCP در دسترس هستند. پس از پیادهسازی رویکرد DHCP snooping پیامهای DHCP که از یک سرور DHCP غیرقابل اعتماد دریافت میشوند دورریخته میشوند .

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره **CEH**

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
13:20 - 17/03/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - هک اخلاقی - ویروس - مسمومسازی ARP - شنود غیرفعال - شنود فعال

نشانی:
https://www.shabakeh-mag.com/security/16924/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D9%85%D8%B3%D9%85%D9%88%D9%85%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-arp-%D9%88-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D8%B3%DB%8C%D9%84%D8%A7%D8%A8%DB%8C-mac-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF