禪

آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی – 52

آموزش CEH (هکر کلاه سفید): هکرها چگونه دیوارهای آتش را دور میزنند؟

متأسفانه، هیچ تکنیک پنهانی برای دور زدن دیوارهای آتش وجود ندارد. دیوارهای آتش به دلیل پیکربندی نادرست یا فهرستهای کنترل دسترسی که به اشتباه آماده شدهاند با شکست روبرو میشوند. از طرفی مهاجمان میتوانند اطلاعات را در لایههای مختلف مدل TCP / IP پنهان یا مبهم کنند. برای ایجاد ترافیک مخرب شبیه به بستههای عادی شبکه، میتوان از انواع تکنیکهای تونلزنی استفاده کرد.

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

Banner grabbing یکی از شناخته شدهترین و پر کاربردترین ابزارهای سرشمارسی است. اطلاعات جمعآوری شده توسط ابزار فوق به هکرها اجازه میدهد به دقیقترین شکل ممکن به شبکههای کامپیوتری حمله کنند. ابزار فوق سه سرویس اصلی در ارتباط با تلنت، FTP و وب ارائه میکند. برای این مدل حمله هیچ نوع ابزار خاصی نیاز نیست. فقط کافی است به آدرس آیپی تلنت کرده و شماره پورت موردنظر را وارد کنید. در اینجا مثالی با دیوار آتش قدیمی Eagle Raptor ارائه شده است:

```
telnet 192.168.13.254 21

(unknown) [192.168.13.254] 21 (21) open

220 Secure Gateway FTP server ready
```

اگر دیوارآتشی که در حال سرشماری آن هستید روتر سیسکو باشد، همیشه این احتمال وجود دارد که یک

درگاه Telnet یا Secure Shell (SSH) برای انجام یکسری فرآیندهای مدیریتی باز باشد . اکثر روترهای سیسکو دارای پنج خط ترمینال هستند ، بنابراین انجام تلنت به یکی از آنها ممکن است اطلاعات مفیدی در اختیارتان قرار دهد :

```
[root@mg /root]# telnet 192.168.13.1

Trying 192.168.13.1...

Connected to 192.168.13.1

Escape character is ‘^]’.

Your connected to router1

User Access Verification

Username:
```

Telnet امن نیست. علاوه بر حدس زدن گذرواژه نام کاربری، در برابر شنود نیز آسیبپذیر است . اگر چارهای جز استفاده از Telnet برای انجام یکسری فعالیتهای مدیریتی ندارید، حداقل بهتر است یک فهرست دسترسی آماده کنید تا افرادی که میتوانند به خطوط ترمینال مجازی (vty) دسترسی داشته باشند را محدود کنید . وبسرورها و سرورهای ایمیل نیز در دسترس ابزار banner grabbing قرار دارند . کافی است به آدرس وبسرور با تعیین پورت تلنت کرده و اطلاعات ارزشمندی به دست آورید .

دور زدن دیوارآتش

متأسفانه، هیچ تکنیک پنهانی برای دور زدن دیوارهای آتش وجود ندارد . دیوارهای آتش به دلیل پیکربندی نادرست یا فهرستهای کنترل دسترسی که به اشتباه آماده شدهاند با شکست روبرو میشوند . از طرفی مهاجمان میتوانند اطلاعات را در لایههای مختلف مدل TCP / IP پنهان یا مبهم کنند . برای ایجاد ترافیک مخرب شبیه به بستههای عادی شبکه، میتوان از انواع تکنیکهای تونلزنی استفاده کرد .

لایه اینترنت راهکارهای مختلفی برای تونلزنی شبکه در اختیار هکرها قرار میدهد . دو پروتکل معمول استفاده شده در ارتباط با تونلزنی IPv6 و ICMP است. IPv6 مانند تمامی پروتکلها میتواند برای دور زدن دیوارهای آتش دستکاری شود، زیرا این امکان وجود دارد که دیوارهای آتش و سامانههای تشخیص نفوذ برای تشخیص ترافیک IPv6 پیکربندی نشده باشند، در حالی که بیشتر سیستمعاملها از پروتکل فوق پشتیبانی میکنند . طبق گزارش US-CERT، سوء استفاده از این پروتکل در ویندوز به عوامل مختلفی به شرح زیر بستگی دارد :

پشتیبانی ناقص یا متناقض از IPv6

قابلیت پیکربندی خودکار IPv6

تونلزنی مخرب ترافیک : روشی برای انتقال دادههای اینترنتی که در آن از اینترنت عمومی برای رله دادههای شبکه خصوصی استفاده میشود.

دومین پروتکل لایه اینترنت که ممکن است برای دور زدن دیوارهای آتش استفاده شود، ICMP است. ICMP توسط سند RFC 792 بهطور کامل تشریح شده و به منظور پشتیبانی از خطاهای منطقی طراحی شده است. متداولترین پیام ICMP دستور ping است که از پیامهای نوع ICMP 8/0 برای آزمایش اتصال استفاده میکند . برخی از بخشهای سرآیند بسته ICMP ping □□□□Code ، Type، شناسه و دادهها حالت اختیاری دارند . ابزارهایی که برای تونلزنی روی ICMP از آنها استفاده میشود زیاد هستند که ICMPSend و Loki پر استفادهتر از نمونههای دیگر هستند . برای آنکه مانع استخراج اطلاعاتی از طریق ICMP شوید باید ترافیک ورودی ICMP را مسدود کنید .

لایه انتقال قابلیتهای بیشتری در اختیار مهاجمان برای دور زدن ترافیک شبکه فراهم میکند . حملات مبتنی بر این لایه بر مبنای پروتکلهای TCP و UDP انجام میشود . TCP فیلدهای مختلفی ارائه میدهد که توسط مهاجمان قابل دستکاری است که از آن جمله میتوان به فیلد TCP Options در سرآیند TCP و فیلد TCP Flag اشاره کرد . بهطور مثال، اگرچه بستههای SYN فقط در ابتدای یک نشست ایجاد میشوند، اما ممکن است هزاران بار ACK اتفاق بیفتد . به همین دستگاههای مبتنی بر فیلترینگ بسته قواعد خود را بر مبنای سگمنتهای SYN تنظیم میکنند . بیشتر سرپرستان شبکه فرض را بر این موضوع قرار میدهند که ACK فقط به عنوان بخشی از یک نشست انجام میشود.

به این ترتیب، از بستههای TCP ACK میتوان برای دور زدن فیلترهای بسته و دیوارهای آتش بدون حالت استفاده کرد . ابزارهایی شبیه به AckCmd برای این منظور ساخته شدهاند . AckCmd یک پوسته فرمان روی سیستمهای ویندوزی ارائه میدهد و تنها با استفاده از سگمنتهای TCP ACK اقدام به برقراری ارتباط میکند . به این ترتیب ، مؤلفه کلاینت را قادر است از طریق روترهایی با فهرستهای کنترل دسترسی موجود با مؤلفه سرور ارتباط برقرار کند تا ترافيك را مسدود کند . ابزار AckCmd را میتوانید از آدرس زیر دانلود کنید .

http://www.ntsecurance.nu/toolbox/ackcmd

UDP بدون حالت است و به همین ترتیب ممکن است در ارتباطات آن در دیوارآتش ثبت نشود . برخی از برنامههای مبتنی بر UDP مانند DNS معمولاً از طرف دیوارآتش مجاز شناخته میشوند و ممکن است توسط دیوارهای آتش و سامانههاش تخیص نفوذ به درستی بررسی نشوند. برخی از درگاهها، مانند UDP 53 به احتمال زیاد در جایی که DNS خدماتی را ارائه میکند باز هستند . این حرف بدان معنا است که برای مهاجمین این امکان وجود دارد تا آنرا به عنوان ابزاری بالقوه برای دور زدن دیوارهای آتش استفاده کنند . از جمله ابزارهای تونلزنی مبتنی بر UDP میتوان به Iodine و UDPTunnel اشاره کرد .

تونلزنی لایه کاربرد به مهاجمان قابلیت دیگری برای دور زدن دیوارهای آتش ارائه میدهد . بهطور مثال، ممکن است یک هکر به یک نشست روی درگاه 80 از طریق پورت SSH 22 تونلزنی کند . اینکار به راحتی امکانپذیر است، زیرا SSH اغلب از طریق دیوارهای آتش و دستگاههای لبه مجاز شناخته میشود . از آنجایی که SSH رمزگذاری شده، به سخی میتوان تفاوت میان یک نشست SSHمعتبر و یک تونل مخفی کخ برای ارسال دادهها به خارج از شبکه تعریف شده را تشخیص داد .

HTTP نیز میتواند برای تونلزنی ترافیک استفاده شود . اینکار به شکل گستردهای انجام میشود، زیرا اتصالهای درون شبکهای ممکن است به دقت مورد بررسی قرار نگیرند . Netcat ابزاری است که میتواند برای پیادهسازی یک تونل و استخراج دادهها از طریق HTTP استفاده شود . سرانجام، HTTP مبتنی بر SSL (HTTPS) وجود دارد . از بعضی جهات بهکارگیر پروتکل فوق برای هکرها سادهتر از هر روشی است، زیرا اجازه انتقال یک ترافیک رمزنگاری شده را میدهد که به راحتی کنترل نمیشود . در حالی که آدرسهای آیپی منبع و مقصد جلسه قابل مشاهده است، هکر از یک آدرس آیپی داخلی قابل اعتماد برای برقراری ارتباط با یک آدرس آیپی معتبر خارجی استفاده میکند . Cryptcat به نشانی https://sourceforge.net/projects/cryptcat/ برای این منظور استفاده میشود . مهاجمان همچنین میتوانند یک تونل SSL (Secure Sockets Layer) را با استفاده از stunnel یا اجرای یک مرورگر با HTTPS راهاندازی کرده و به مرورگر اجازه دهند به مدیریت ارتباط SSL و رمزنگاری دادهها بپردازد . هکرها محدود به ابزارهایی نیستند که به آنها اشاره شد و همچنین دیوارهای آتش نیز نمیتوانند به مقابله با تهدیداتی شبیه به ترافیک تونل شده، مهندسی اجتماعی، حمله از طریق ارتباط دوم، بهکارگیری سرورهای پروکسی، امنیت فیزیکی، خطمشیهای ضعیف یا اشتباه پیکربندی شده و هکهای داخلی بپردازند .

درست است که مرورگرهای وب آدرسهای اینترنتی که شامل کاراکترهای باینری یا هگزا هستند را تشخیص میدهند، اما برخی برنامههای فیلترینگ وبمحور قادر به انجام اینکار نیستند . به آدرس آیپی رمزگذاری شده باینری زیر دقت کنید :

آدرس http://8812120797/ عجیب و غریب به نظر میرسد؟ این آدرس اعشاری میتواند به یک آدرس آیپی قابل فهم تبدیل شود. کافی است آدرس را به مبنای هگزا ببریم، آنرا به چهار بخش دو رقمی تقسیم کنیم و در آخر هر مجموعه را به اعشار تبدیل کنید تا آدرس آیپی درست را پیدا کنیم . برای تبدیل آدرس IP به معادل دودویی آن باید مراحل زیر را انجام داد :

DMZ
Internal Network
Firewall
Honeypot
Packet Filter
Internet
Web Server
DMZ
Honeypot
Internal Network
Firewall
Packet Filter
Internet
Web Server

ظرفهای عسل میتوانند کاملا تعاملی یا نیمهتعاملی باشند . ظرفهای عسل نیمه تعاملی با تقلید از سرویسها و برنامههایی که در سامانههای منفرد پیدا میشوند کار میکنند . اگر مهاجم کاری را انجام دهد که ظرف عسل انتظار آنرا نداشته باشد، به سادگی خطایی ایجاد میکند .

سامانههای کاملا تعاملی عملکرد یک سامانه یا کامپیوترهای عضو شبکه را بهطور کامل تقلید میکنند . ایده این است که یک منطقه کنترل شده داشته باشیم که در آن مهاجمان بتوانند با آنچه که به نظر میرسد برنامهها و سرویسهای واقعی است در تعامل باشند . ظرفهای عسل کاملا تعاملی برای کنترل ترافیک به دستگاههای لبه تکیه میکنند تا مهاجمان بتوانند وارد شوند و فعالیت آنها به دقت کنترل شود . انواع مختلفی از ظرفهای عسل وجود دارد که برخی از آنها تجاری و برخی دیگر منبع باز هستند . از مهمترین این ابزارها به موارد زیر میتوان اشاره کرد :

- KFSensor
- NetBait
- PatriotBox
- Specter
- BackOfficer Friendly
- LaBrea Tarpit
- Honeyd
- Tiny Honeypot

ظرفهای عسلی شبیه به LaBrea Tarpit نمونههایی روشن از از سیاه چالهها هستند . این ظرفهای عسل چسبنده بهطور صریح ساخته شدهاند تا سرعت فعالیتهای مخرب را کاهش دهند. LaBrea Tarpit میتواند روی کامپیوترهای ویندوزی اجرا شود .

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 :
13:35 - 01/05/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - هک اخلاقی - دیوارآتش

نشانی
□□□□:https://www.shabakeh-mag.com/security/17103/%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%87%DA%A9%D8%B1%D9%87%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%AF%DB%8C%D9%88%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-

%D8%A2%D8%AA%D8%B4-%D8%B1%D8%A7-%D8%AF%D9%88%D8%B1-%D9%85%DB%8C%E2%80%8C%D8%B2%D9%86%D9%86%D8%AF%D8%9F