آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی – 36

آموزش CEH (هکر کلاه سفید): حملات DDoS و DoS چیستند و چگونه پیادهسازی میشوند؟

حمله دائمی انکار سرویس بهنام phlashing شناخته میشود. ایده phlashing این است که دستگاه یا سختافزار به شکل دائم غیرقابل استفاده شود . در حالی که چنین حملاتی عمدتاً نظری تلقی میشوند، اما ابزارهایی ساخته شدهاند که برای از بین بردن دائمی دادهها استفاده میشوند . به عنوان نمونه، هنگامی که سونی پیکچرز در سال 2014 هک شد، مهاجمان از بدافزارهایی برای ایجاد تغییرات سختافزاری در هارددیسکها استفاده کردند . در این حمله هرگونه دادهای روی دستگاههای هدف در معرض تهدید قرار میگیرند .

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

حملات سیلابی **SYN**

حملات سیلابی SYN با هدایت حجم زیادی از ترافیک به سمت یک سرویس شخصی روی یک ماشین هدف انجام میشود. برخلاف حمله پهنای باند، میتوان یک حمله سیلابی SYN را نوعی حمله مصرف سریع منابع توصیف کرد که تلاش میکند شود منابع یک سیستم واحد بیش از اندازه مصرف کند عملا عملکرد سیستم کند یا مختل شود. این حملات با تمرکز روی سامانههای انفرادی اصل دسترسپذیری را هدف قرار میدهند .

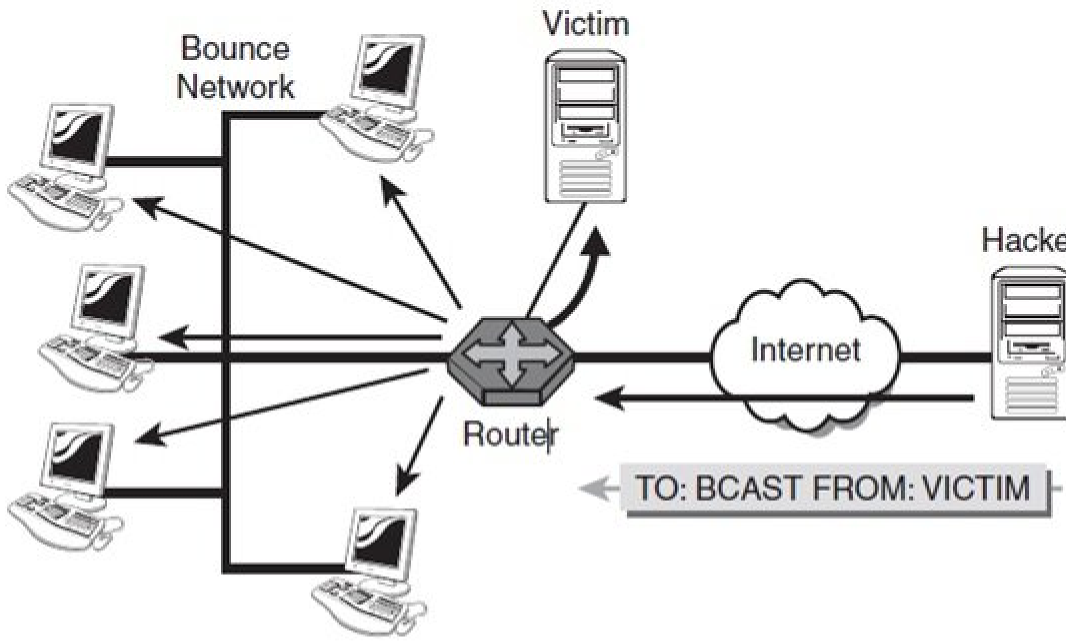
- SYN flood: یک حمله سیلابی SYN با ارسال تعداد زیادی بستههای جعلی از طریق TCP و مجموعهای از پرچمهای SYN پیادهسازی میشود. این تعداد زیاد از اتصالات TCP نیمه باز، بافر سیستم قربانی را پر میکند و مانع از دریافت ارتباطات معتبر میشود .. سیستمهای متصل به اینترنت که خدماتی مانند HTTP

[illegible] (SMTP) [illegible]. [illegible]
[illegible] SYN [illegible].

ICMP [illegible]

[illegible] ICMP [illegible] ICMP [illegible]. [illegible]
[illegible]
[illegible]. [illegible] Smurf [illegible] ICMP [illegible].

- Smurf: [illegible] ICMP [illegible]. [illegible]. [illegible] Smurf [illegible].



[illegible] ICMP [illegible] no ip directed-broadcast [illegible]
[illegible].

[illegible]

[illegible] (DC++) [illegible]. [illegible] Direct Connect [illegible]. [illegible] DC++ [illegible]. [illegible]. [illegible] P2P [illegible].

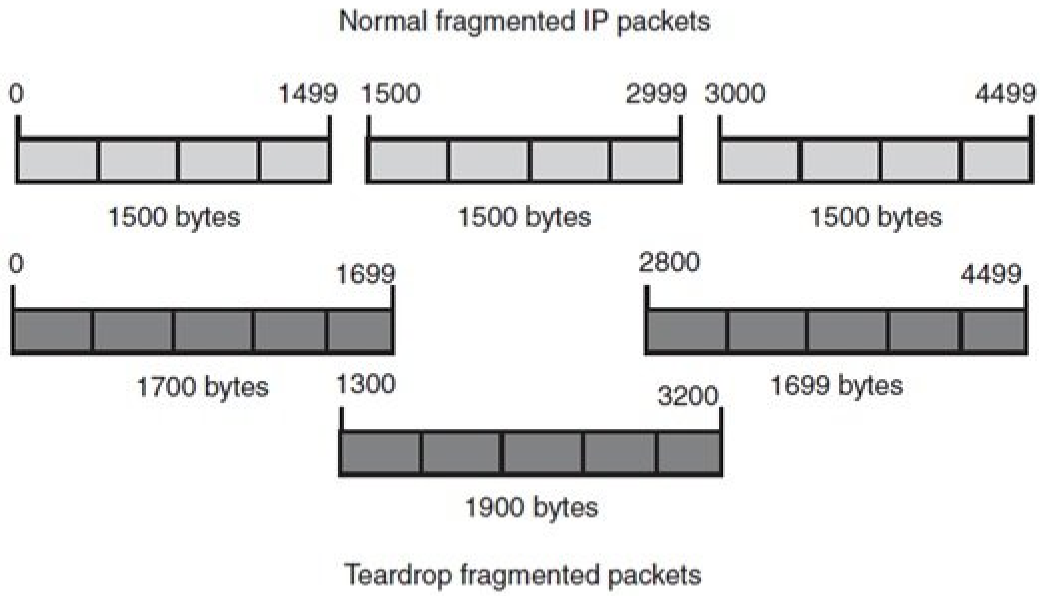
[illegible]

[illegible]:

- Ping of Death: [illegible]

است. سامانه هدف زمانی که بستهای که اندازهای از 65536 بایت دارد مجبور است این بسته را تکه تکه میکند، در این حالت سامانه ممکن است قفل کند یا مشکل سرزیربافر به وجود آید، زیرا سامانه دومرتبه مجبور میشود بستههای تکه تکه شده را سرهم کند .

- ■ Teardrop: این بردار حمله کمی متفاوت از Ping of Death عمل میکند، با این حال نتایج مشابهی را به همراه دارد، زیرا از پروتکل آیپی بهره میبرد . حمله Teardrop بستههای ناقصی میفرستد که مقدار افست تقسیم آنها دستکاری شده، به طوری که بستههای دریافتی با یکدیگر همپوشانی پیدا میکنند . سیستم قربانی نمیداند چگونه این بستههایی که با یکدیگر تداخل دارند را پردازش کند و در نتیجه دچار مشکل شده که عمدتا به صورت قفل شدن سیستم خود را نشان میدهند. این اتفاق در نهایت مشکل انکار سرویس را به وجود میآورد . شکل زیر نشان میدهد که این بستههای تکه تکه به چه شکلی به سمت سامانه هدف ارسال میشوند.



- ■ Land: در این بردار حمله بستهای با پورت منبع و مقصد و آدرس آیپی یکسان در یک بسته TCP SYN ارسال میشود. سیستم دریافتکننده بهطور معمول نمیداند چگونه این بستههای ناقص را مدیریت کند که در نهایت منجر قفل شدن سیستم شده و باعث انکار سرویس میشود. از آنجایی که سیستم نمیداند چگونه چنین ترافیکی را اداره کند، استفاده پردازنده در وضعیت کاری صد درصد قرار میگیرد .

حملات دائمی انکار سرویس

حمله دائمی انکار سرویس بهنام phlashing شناخته میشود. ایده phlashing این است که دستگاه یا سختافزار به شکل دائم غیرقابل استفاده شود . در حالی که چنین حملاتی عمدتاً نظری تلقی میشوند، اما ابزارهایی ساخته شدهاند که برای از بین بردن دائمی دادهها استفاده میشوند . به عنوان نمونه، هنگامی که سونی پیکچرز در سال 2014 هک شد، مهاجمان از بدافزارهایی برای ایجاد تغییرات سختافزاری در هارددیسکها استفاده کردند . در این حمله هرگونه دادهای روی دستگاههای هدف در معرض تهدید قرار میگیرند . در مثال دیگری، شرکت نفت عربستان سعودی (آرامکو) هنگام برخورد با بدافزار Shamoon نزدیک به 30،000 هارد دیسک را از دست داد. این اتفاق باعث شد تا سرویسدهی این شرکت نفتی برای چند ماه با مشکل همراه شود، حال اگر بدافزار فوق موفق میشد زیرساختهای تولیدی را هدف قرار دهد، وضعیت بغرنجتر میشد .

انکار سرویس توزیع شده

امروزه از حملات True DoS بیشتر به عنوان یک تاریخچهای از حملات انکار سرویس شناخته میشوند، زیرا امروزه هکرها از حملات انکار سرویس توزیع شده بر علیه سازمانها استفاده میکنند . تفاوت اصلی روش قدیمی و جدید این است که حملات انکار سرویس توزیع شده (DDoS) برای مخربتر کردن حملات

Client
Control messages
Master
Master
Master
Attack
messages
Zombie
Zombie
Zombie
Zombie
Zombie
Flood packets
Victim

- The zombie: سیستم فرعی که فرایند Daemon را اجرا میکند .

- The target: هدفی است که قرار است به آن حمله شود.

اکنون اجازه دهید به سراغ ابزارهایی برویم که برای پیادهسازی و اجرای حملات DDoS استفاده میشوند.

نکته : امروزه ابزارهای DDoS خالص به سختی پیدا میشوند، زیرا مهاجمان برای انجام این نوع حملات از شبکههای باتنت استفاده میکنند .

ابزارهای **DDoS**

یکسری ابزارها برای پیادهسازی حملات DDoS طراحی شدهاند که برخی از آنها به شکل گسترده استفاده میشوند.

- Tribal Flood Network: اولین ابزاری که برای پیادهسازی حملات انکار سرویس توزیع شده و مخصوص سیستمعاملهای یونیکسی طراحی شد TFN است. TFN میتواند حملات سیلآسای UDP ، Smurf ، ICMP و SYN را پیادهسازی کند . The master در ابزار فوق از پورت 31335 پروتکل UDP و پورت 27665 پورت TCP استفاده میکند . هنگامی که کلاینت به پورت 27665 متصل میشود، The master صبر میکند تا قبل از برگرداندن اطلاعات، گذرواژه ارسال شود .

- Trinoo: عملکرد خیلی نزدیکی به TFN دارد . ابزار فوق به کاربر اجازه میدهد تا یک حمله سیلآسای UDP را بر علیه قربانی ترتیب دهد . در این حالت قربانی با ترافیک بیش از اندازه روبرو میشود . یک حمله معمولی Trinoo فقط شامل چند سرور و تعداد زیادی کلاینت است که فرآیند Daemon Trinoo روی آنها در حال اجرا است . بهکارگیری Trinoo برای یک مهاجم ساده بوده، اما قدرت زیادی در اختیار او قرار میدهد، زیرا یک کامپیوتر میتواند به بسیاری از سرورهای Trinoo دستور دهد تا حمله DoS را علیه یک هدف خاص انجام دهند. دادههای به دست آمده از یک حمله Trinoo به شرح زیر هستند :

```
:Nov 23 10:03:14 snort[2270]: IDS197/trin00-master-to-daemon

192.168.13.100:27222 10.10.0.5:2976

:Nov 23 10:03:14 snort[2270]: IDS187/trin00-daemon-to-masterpong

10.10.0.5:31385 192.168.13.100:1025

:Nov 23 10:16:12 snort[2270]: IDS197/trin00-master-to-daemon

10.10.0.5:2986

192.168.13.100:27222

:Nov 23 10:16:12 snort[2270]: IDS187/trin00-daemon-to-masterpong

192.168.13.100:1027

10.10.0.5:31385
```

- Pandora: اجازه میدهد یک حمله انکار سرویس توزیع شده بر مبنای پنج حالت HTTP min، HTTP download، HTTP Combo، Socket connect و Max flood پیادهسازی شود.

- Dereil: یک ابزار DDoS است که میتواند از UDP ، TCP و HTTP استفاده کند .

- HOIC: امکان هدفگیری آسان هر آدرس آیپی را فراهم میکند و میتواند TCP و UDP را هدف قرار دهد .

■ HTTP DoS: [illegible] HTTP [illegible]

■ BangleDoS: [illegible] DDoS [illegible] HTTP [illegible]

■ LOIC: [illegible] DDoS [illegible] TCP [illegible] UDP [illegible]

[illegible] DoS [illegible] DDOS

[illegible] (IDS) [illegible] DoS [illegible] Activity profiling [illegible] (CUSUM) [illegible]

[illegible] DDoS [illegible] DoS [illegible] Replication [illegible]

[illegible] (Throttling) [illegible] black hole [illegible] DDoS [illegible] ISP [illegible] ISP [illegible] DoS [illegible]

[illegible] DoS [illegible] ISP [illegible] DoS [illegible] DoS [illegible]

[illegible]

[illegible] **CEH** [illegible]

[CEH [illegible]]

[illegible]:

[redacted]
[redacted]:[redacted]
[redacted]
[redacted]:[redacted]
05:25 - 26/03/1399
[redacted]:
[redacted] - CEH v10 [redacted] - [redacted] [redacted] [redacted] - CEH [redacted] [redacted] [redacted] - CEH [redacted] [redacted] - CEH [redacted] [redacted] - [redacted] [redacted] [redacted] [redacted] - ICMP [redacted] - SYN [redacted] [redacted] - [redacted] - [redacted] [redacted] - CEH10 [redacted] DDoS

[redacted]
[redacted]:https://www.shabakeh-mag.com/security/16956/%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-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-ddos-%D9%88-dos-%DA%86%DB%8C%D8%B3%D8%AA%D9%86%D8%AF-%D9%88-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF%D8%9F