禪

23 – [illegible] CEH [illegible]

[illegible] CEH [illegible]: [illegible]

[illegible] (rootkit) [illegible].

[illegible] CEH [illegible].

[illegible]

[illegible] (rootkit) [illegible].

[illegible] ls [illegible] ps ، ifconfig، inetd ، killall ، login ، netstat ، passwd ، pidof ، MD5Sum [illegible] Tripwire [illegible]:

■ Hypervisor: [illegible].

■ Hardware/firmware: [illegible]

■ Bootloader: [illegible] bootloader [illegible].

■ Library level: [illegible].

■ Application level: [illegible]

■ Loadable kernel level: [illegible].

[illegible] loadable kernel module [illegible] LKM [illegible]:

■ Avatar: [illegible] dropper [illegible] x86 [illegible].

■ Necurs: [illegible] 2011 [illegible] Gameover Zeus [illegible].

■ Azazel: [illegible] Jynx [illegible] userland [illegible].

■ Zeroaccess: [illegible] dropper [illegible].

[illegible]: [illegible] CEH [illegible].

[illegible]

■ Chkrootkit: [illegible].

■ RootKitRevealer: [illegible].

■ McAfee Rootkit Detective: [illegible].

■Trend Micro RootkitBuster: [illegible].

[illegible]

[illegible] NTFS ADSs [illegible] Hierarchical File System [illegible] (HFS) [illegible] ADS [illegible] FAT [illegible] ADS [illegible]:

Type certguide.zip > readme.txt:certguide.zip

[illegible] readme.txt [illegible] certguide.zip [illegible].

Erase certguide.zip

[illegible]:

Start c:\readme.txt:certguide.zip

[illegible] ADS [illegible]:

Streams: [illegible].

Sfind: [illegible].

LNS: [illegible] ntsecurity.nu [illegible]

شده است.

لینوکس از ADS پشتیبانی نمیکند، اگرچه ابزاری جالب بهنام Bmap در دسترس است که میتوانید آنرا از آدرس زیر دانلود کنید . http://www.securityfocus.com/tools/1359

این ابزار لینوکسی میتواند دادهها را درون فضای موجود و در دسترس قرار دهد . در نتیجه امکان پنهانسازی هر نوع محتوایی وجود دارد .

قدم نهایی برای مهاجم، دسترسی به خط فرمان روی سیستم قربانی است . دسترسی به خط فرمان به هکر اجازه میدهد تا کنترل کامل سیستم قربانی را بهدست آورد . ابزارهایی که به مهاجم اجازه دسترسی به خط فرمان را میدهد Remoxec ، Psexec و Netcat هستند. پس از اینکه مهاجم دسترسی به خط فرمان روی سیستم قربانی را بهدست آورد، به دنبال اهداف داخلی دیگری میگردد . در این مرحله متدولوژی حمله کامل شده و هکر همانند کاربر قانونی به سیستم او دسترسی دارد . در شکل زی چرخه کامل یک حمله موفقیتآمیز به یک سیستم را مشاهده میکنید:

جمعبندی کلی

همانگونه که مشاهده کردی سرشماری و هک هر دو سیستمعامل ویندوز و لینوکس را به یک اندازه در معرض خطر قرار میدهند . سرشماری سیستمهای ویندوزی میتواند با استفاده از روشهایی همچون SMB ، IPC$ SNMP ، SMTP ، share و DNS انجام شود . هر یک از روشهای فوق فرصتی در اختیار هکر قرار میدهند تا در مورد شبکه و سامانههایی که قرار است به آنها حمله کند اطلاعات بیشتری بهدست آورد . هدف از سرشماری، جمعآوری اطلاعات کافی برای ترسیم نقشه حمله به یک شبکه بر مبنای مجموعهای از نقاط ورودی بالقوه است . این نقطه ورودی ممکن است یک مشکل سرریز بافر، یک برنامه غیر ایمن مانند SNMPv1 یا 2 یا حتا یک رمز عبور ضعیف باشد که حدس زدن آن زمان زیادی را طلب نمیکند.

هک کردن سیستم نقطه عطف کار یک هکر است. در این نقطه هکر دیگر تحقیقی انجام نمیدهد و تمام تمرکزش روی حمله به یک سیستم و ورود به سیستم متمرکز است. هک کردن سیستم ممکن است با یک حساب کاربری سطح پایین شروع شود. یکی از مؤلفههای مهم هک سیستم، ترفیع امتیاز است که اشاره به بهرهبرداری از یک

[illegible]

[illegible] net [illegible] CEH [illegible]

net use \\ip address\ipc$ “” /u:””

net use * \\ip address\share * /u:username

net view \\ipaddress

NTFS [illegible]

[illegible] NTFS [illegible]

[illegible] LNS [illegible] NTFS [illegible]

/www.ntsecurity.nu/toolbox/lns

[illegible] test [illegible] NTFS [illegible]

[illegible] Notepad.exe [illegible] hack.exe [illegible] test [illegible]

[illegible] hello world [illegible] readme [illegible] readme.txt [illegible]

[illegible] hack.exe [illegible] test [illegible]

Type hack.exe > readme.txt:hack.exe

[illegible]

[illegible] hack.exe [illegible] readme.txt [illegible]

[illegible]:

```
Start c:\ test\ readme.txt:hack.exe
```

مرحله 10: آیا اتفاقی رخ داده است؟ فایل hack شما notepad.exe باید روی صفحه باز شده باشد. این فایل بهطور کامل پنهان است و پشت فایل readme.txt پنهان شده است.

مرحله 11: سرانجام LNS را از طریق خط فرمان اجرا کنید. برنامه باید بتواند فایل استریم شده hack.exe را شناسایی کند. استریم کردن فایل یکی از قدرتمندترین رشوهای برای پنهانسازی اطلاعات است که فرآیند تشخیص را مشکل میکند.

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 :
12:55 - 27/02/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - طبقهبندی مخاطرات امنیتی - هک اخلاقی - ترفیع امتیاز - Privilege Escalation

---

نشانی
□□□□: https://www.shabakeh-mag.com/security/16858/%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-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%B1%D9%88%D8%AA%E2%80%8C%DA%A9%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D9%85%D9%87%D8%A7%D8%AC%D9%85%D8%A7%D9%86-%D8%A8%D9%87-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7-%D8%B1%D8%A7-%D8%AA%D8%B6%D9%85%DB%8C%D9%86-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF