انجام عملیات پوششِ ردپا[1] روی سیستم های یونیکس

این مقاله به بررسی عمـــــــلیات پـوشش ردپـا (که با الفاظی مانند پاک کردن ردپا، پنهانی سازی اثـرات و ... نیـز بـه کـار می رود) یا Covering Track می پردازد و به دو بخش اصـلی تـقسیم می شود که اولین قسمت به بررسی تـئوری هـا و عملیـات پشت صحنه می پردازد و دومین قسمت یک عملیات تمرینی را حول این مبحث آشکار می سازد.

بخش اول: تئوری و پشت صحنه

۱- مقدمه
۲- روح
۳- موارد پایه ای
۴- موارد پیشرفته
۵- تحت سوء ظن و شَک
۶- برنامه ها

۱. مقدمه

این مقاله از دو فصل تشکیل شده که قسمت اول تئوری و پشت صحنه این فرآیند را نشان داده و فصل دوم در خـلال یـک روند آسان و گام به گام به شما بایدها و نبایدها را خواهد آموخت. اگر فرصت کافی برای خوانـدن تمـام ایـن مقالـه را نداریـد، مـی توانید به فصل دوم مراجعه کنید. مخاطب اصلی این مقاله، کاربران تـازه کـار یـونیکس مـی باشـد. اگـر فکـر مـی کنیـد کـه گـرفتن جدیدترین اکسپلویت ها مهم ترین چیزی است که باید تمام هم و غم خود را بـه آن جلـب کنیـد، سـخت در اشـتباهید. مهـم تـرین چیزی که یک هکر باید روی آن اصرار داشته باشد، مخفی ماندن می باشد، چرا که در بسیاری از اوقات، مخـصوصا اگـر شـما اولـین تجربه هک خود را روی یک سایت تجربه کنید و سایت مربوطه مقداری هوشیاری امنیتی به خرج دهد، اولین تجربه شما، مـی توانـد آخرین تجربه شما نیز باشد!!

[1] Covering Track

۲. روح

محتویات:

۲,۱ تحریک
۲,۲ چرا باید دیوانه بود!
۲,۳ چطور باید یک دیوانه شد!
۲,۴ چطور باید یک دیوانه ماند!

۲,۱ تحریک

جنبه روحی، کلید موفق شدن در هر چیزی است. این بسته به قدرت شماست که خود را برانگیخته سازید، با چیزی که به شما آسیب می رساند مبارزه کنید، به کار خود نظم دهید، دیوانه یا واقع گرا باشید، ریسک ها را به درستی محاسبه کنید و کارهایی که نمی خواهید انجام دهید!! اگر نمی توانید خودتان را برانگیزید تا ابزارهای مهمی برنامه نویسی کنید، دوره های بسیار سخت فرا خواهد رسید که در ضربه زدن به هدف هیچ چیز برای استفاده ندارید. یک هکر موفق باید این نیازهای روحی را در خود زنده سازد. در دنیای هک، بعضی از مسائل به عنوان Prevention یا اجتناب از انجام کارها مطرح می شوند (مثلا تا جای ممکن از deface کردن خود داری کنیم و ...). به هر حال، تا زمانی که شما نسبت به انجام این prevention ها یا حتی ایجاد کردن این prevention ها مبادرت می ورزید، حتی بهترین دانش هم به شما کمک نخواهد کرد.

۲,۲ چرا باید دیوانه بود!

این درست است که در حالت عادی دیوانه بودن چیزی نیست که زندگی شما را شادتر می سازد. به هر حال، اگر شما چشم داشتی بر بدترین ها نداشته باشید، هر چیزی می تواند تعادل روحی و شخصیتی شما را به هم زند و شما با کرده هاتان ریسک بسیار زیادی انجام می دهید.

در زندگی معمولی خود، شما احتیاجی به نگرانی راجع به پلیس ها، دزدان و ... ندارید. اما اگر در آن طرف هستید، به خاطر داشته باشید که شما برای مردم زندگی سخت درست می کنید و برای آنها کابوس و غم را بهمراه کار ارمغان می آورید و آنها می خواهند که شما را متوقف سازند.

حتی اگر احساس می کنید که جنایت مرتکب شدن را دوست ندارید – شما در عمل انجام خواهید داد. این یک چیز غمناک است: شما گناهکار هستید تا زمانی که غیر از آن ثابت شود!!

تا زمانی که شما دارای یک لکه ننگ باشید، یعنی در حقیقت هکر باشید (البته این نظریه در افراد دیگر می باشد)، هرگز نمی توانید آن لکه را پاک کنید. یک بار که یک پرونده پلیسی برای شما ساخته شود دیگر پیدا کردن کار برای شما سخت خواهد بود. به خصوص، هیچ شرکت نرم افزاری، یا کلا هر شرکتی که به کامپیوتر مربوط می شود شما را استخدام نخواهد کرد، آنها از مهارت های شما خواهند ترسید. هنگامی که افراد به زمین می خورند، تنها تعداد کمی از آنها می توانند مجددا برخیزند.

از خودتان محافظت کنید!

به خاطر داشته باشید که همه چیز را برای از بین بردن در دست دارید.

هرگز به فکر راه های احمقانه که بتوان بطور خارق العاده جلوی tracing را گرفت نیفتید!

هنگامی که شخصی به دیوانه بازی های شما می خندند، هرگز ناراحت نشوید!

هرگز برای دستکاری کردن log ها خسته و تنبل نباشید.

یک هکر باید کارش را تمام و کمال و ۱۰۰٪ انجام دهد.

۲,۳ چطور باید یک دیوانه شد!

اگر شما قسمت فوق را خوانده اید و فکر می کنید که درست می باشید، بسیار راحت است- شما از قبل دیوانه شده اید. اما آن باید یک بخش ذاتی از زندگی شما شود. اگر شما این کار را انجام دادید به یک هکر باهوش تبدیل خواهید شد و همیشه درباره اینکه به به چه کسی چه چیزی را باید بگوئید فکر خواهید کرد و قطعا به این نکته که شاید تماس های تلفنی و ایمیل های شما مانیتور شوند نیز فکر خواهید کرد. همیشه بند فوق را در ذهن خود به هنگام نفوذ کردن به یک سیستم و ... در خاطر داشته باشید و پیش خود مرور کنید.

اگر جملات فوق به شما هیچ کمکی نکرد، آنوقت در این باره فکر کنید که اگر شما را بگیرند چه اتفاقی خواهد افتاد. آیا دوستانتان با شما هستند؟ آیا می خواهید گریه والدین و ... را ببینید؟ می خواهید از کار / دانشگاه یا مدرسه خود اخراج شوید؟

هرگز به این موارد شانس رخ دادن ندهید.

اگر حتی این موارد برای تحریک کردن شما کافی نبود، در این صورت باید بگویم که: از هکینگ دوری کنید! شما برای کلِ جامعه هکینگ و دوستان هکرتان یک خطر به حساب می آئید!

۲,۴ چطور باید یک دیوانه ماند!

امیدوارم اکنون آموخته باشید که به چه دلیل دیوانه شدن مهم می باشد. بنابراین دیوانه بمانید! یک اشتباه یا غفلت در یک لحظه، ممکن است برای نابودی زندگی یا حرفه شما کافی باشد.

همیشه این انگیزه را برای انجام آن به خاطر بیاورید.

۳. موارد پایه ای

محتویات:

۳,۱ مقدمه
۳,۲ خودتان را ایمن سازید!
۳,۳ اکانت خودتان
۳,۴ LOG ها
۳,۵ اجازه Trace را ندهید!
۳,۶ چیزهایی که باید اجتناب کنید!

۳,۱ مقدمه

شما باید این را بدانید و قبل از شروع به اولین نفوذ و هکِ خود آنرا را تمرین کنید. اینها اساس و پایه های مطلق هستند، بدون آنها شما به زودی به دردسر خواهید افتاد. حتی یک هکر با تجربه نیز می توانید در این قسمت از مقاله اطلاعات و حقه های خاصی را بیاموزد.

۳,۲ خودتان را ایمن سازید!

اگر مدیر یک سیستم ایمیل های شما را بخواند چه می شود؟

اگر تماس های تلفنی شما توسط پلیس ضبط گردد چه می شود؟

اگر پلیس کامپیوتر شما را با تمام اطلاعات موجود در آن (که به هکینگ هم مربوط می شوند) توقیف کند چه می شود؟

اگر شما ایمیل های مشکوکی را دریافت نمی کنید، راجع به عملیات هکینگ و فریکینگ در تماس های تلفنی خود با دیگران صحبت نمی کنید و فایل های شخصی و حساس روی هارددیسک خود ندارید، احتیاجی به نگرانی نیست، اما به احتمال زیاد در این صورت شما هکر نیستید. هر هکر یا فریکر باید تماس با دیگران را متوقف ساخته و اطلاعات خود را در جایی ذخیره کند.

هر داده و اطلاعاتی که حساس می باشد، به صورت رمز در آورید (یا به اصطلاح Crypt کنید). Online-HardDisk-Crypter ها بسیار مهم و مفید هستند:

رمزگذار[2] های خوبی برای هارددیسک روی اینترنت به صورت رایگان وجود دارند که کاملا در سیستم عامل شما پنهان و مخفی رفتار می کنند. یعنی بسته هایی که در زیر لیست شده اند، تست گردیده و به عنوان یک انتخاب اول برای هکر توصیه می گردند.

- اگر از MS-Dos استفاده می کنید (این مورد برای کامل شدن مقاله بوده و به نظر من در این زمان هکرها بیشتر به لینوکس و ... گرایش دارند)، SFS v1.17 یا SecureDrive 1.4b را بگیرید.
- اگر از Amiga استفاده می کنید، EnigmaII v.1.5 را بگیرید.
- اگر از Unix استفاده می کنید، CFS v1.33 را بگیرید.

[2] Crypter

* رمزگذارهای فایل: شما می توانید از هر نرم افزاری برای این کار استفاده کنید، اما نرم افزار مربوطه باید به درستی شناخته شده باشد (یعنی از نظر کارکرد و مشهور بودن در سطح بالایی باشد) و از الگوریتم های ایمن و غیر public شده استفاده کند. هرگز از یک برنامه رمزگذاری که قابلیت export شدن را دارد، استفاده نکنید، چرا که طول کلیدهای[3] موثرِ آنها کاهش یافته است.

- Triple DES
- IDEA
- Blowfish (32 rounds)

* ایمیل های خود را رمزنگاری کنید:

PGP v2.6.x بیشترین استفاده را داشته است، بنابراین شما هم از آن استفاده کنید (یا اگر مورد مطمئن دیگری پیدا کردید، از آن استفاده کنید).

* تماس های تلفنی خود را در صورتی که می خواهید چیز مهمی بگوئید، رمزنگاری کنید (البته این مورد در ایران فکر نمی کنم قابلیت کارکرد داشته باشد):

Nautilus v1.5a تا کنون بهترین بوده است.

* هنگامی که به یک سیستم یونیکس متصل شده اید، جلسه های کاری ترمینال[4] خود را رمزنگاری کنید.

- یک نفر ممکن است خط تلفن شما را مانیتور یا اسنیف کند.
- SSH تا کنون ایمن ترین بوده است.
- DES-Login هم خوب می باشد.

از پسوردهای قوی که قابل حدس نباشند و در هیچ دیکشنری ای ذکر نشده باشند، استفاده کنید. پسوردهای شما باید تصادفی به نظر آیند و فقط خود شما باید بتوانید آنها را بیاد آورید. اگر keylength اجازه تجاوز بیشتر از ۱۰ کاراکتر را دارد، حتما این کار را بکنید و یک جمله از یک کتاب انتخاب کنید و مقداری آنرا تغییر دهید. حتما شماره تلفن های دوستان هکر خود را نیز رمزی کنید و در صورتی که نمی خواهید مکالمه را رمزی کنید، به آنها از طریق باجه های تلفن یا ... زنگ بزنید.

تازه کارها تنها به یک PGP نیاز دارند، یک رمزگذارِ فایل و یک online-harddisk-crypter. اگر شما واقعا می خواهید علم هکینگ را ادامه بدهید (و صرفا برای شما جنبه سرگرمی و ... ندارد)، پس همه چیز را رمزنگاری کنید.

از اطلاعات خود یک پشتیبان یا backup بگیرید (با استفاده از Zip-Drive، یک هارد اکسترنال و اضافی، CD یا ...) و البته آنها را قبل از انتقال به پیشتیبان حتما به صورت رمزی در آورید و سپس آنها را در جایی که با کامپیوتر هیچ رابطه ای ندارد و با شما رابطه نداشته، ذخیره کنید، مثل دوستان، اعضای خانواده و ... . بنابراین اگر یک کاستی، آتش سوزی یا قحطی رخ داد، از اطلاعات خود پشتیبان بگیرید.

در صورتی که واقعا به اطلاعاتی نیاز دارید از آنها یادداشت برداری کنید. آنها را در یک فایل رمزنگاری شده قرار دهید. برگه های حساس را در صورتی که دیگر به آنها احتیاجی نیست، بسوزانید. شما همچنین می توانید آنها را با یک الگوریتم رمزنگاری که فقط خودتان از آن الگوریتم اطلاع دارید بنویسید. به دیگران این الگوریتم را نگوئید و زیاد هم از این الگوریتم استفاده نکنید، چرا که در صورت استفاده زیاد از یک الگوریتم به راحتی می توان آنرا آنالیز کرده و شکست.

هکرهای فوق دیوانه (!) بایستی به پروژه TEMPEST پلیس ها ملاحظه کنند، جاسوسان و هکرها ممکن است تمام کرده های شما را مانیتور کنند. یک انسان مجهز می تواند هر چیزی که می خواهد داشته باشد:

---

[3] Key-Length
[4] Terminal Sessions

جریانِ[5] پالس الکترونیکی را می توان از ۱۰۰ ها متر دورتر گرفت و صفحه مانیتور خود را به یک فرد دیگر نشان داد، یک laserpoint را می توان برای پنجره شما برای شنیدن مکالمه های محرمانه نصب کرد، یا می توان سیگنال های تشخیص هویتِ hifrequency را برای چیزهای فشرده شده از keyboard به کار گرفت... بنابراین احتمالات همان طور که می بینید پایان ناپذیرند.

اجتناب های کم هزینه را می توان توسط پالس های الکترونیکیِ jammer انجام داد، اما به نظر می آید که این موارد برای دور نگه داشتن افراد کافی نباشد.

۳,۳ اکانت خودتان

بنابراین، بیائید درباره account خود شما صحبت کنیم. این account واقعی شماست که شما در محل کار و ... از آن استفاده می کنید و با نام شما به هم وابسته می باشند. هرگز فراموش نکنید که این قوانین را شکست دهید:

هرگز کارهای غیرقانونی یا مشکوک را با اکانت های واقعی خود انجام ندهید.

هرگز سعی بر telnet کردن به یک هاست هک شده نکنید.

Mailing list های امنیتی برای خواندن این اکانت صحیح می باشند.

اما هر چیزی که به نظر می آید با هکینگ مجبور به انجام آن هستید، یا باید رمزنگار شود یا در اولین فرصت پاک شود.

هرگز ابزاری امنیتی و .. را روی اکانت خود در هارددیسک رها نکنید.

اگر می توانید، از POP3 برای وصل شدن به یک mailserver استفاده کرده و ایمیل های خود را گرفته و بلافاصله آنها را پاک کنید (یا اگر با یونیکس به اندازه کافی آشنایی دارید، می توانید این کار را به هر صورتی که خود می دانید انجام دهید).

در صورتی که نام واقعی شما در فایل plan. یا/و فیلد geco وجود دارد، هرگز از ایمیل واقعی خود استفاده نکنید (دستور EXPN از sendmail را به خاطر داشته باشید ...). آن را تنها به افرادی که به آنها اعتماد دارید و از نظر امنیتی نیز در هوشیاری به سر می برند بدهید. چرا که اگر آنرا به افراد ناواردی بدهید، در صورتی که آنها را بگیرند شما هم بدنبال آن خواهند گرفت. ایمیل ها را با دیگر هکرها، تنها در زمانی مبادله کنید که رمزنگاری شده باشند (PGP). SysAdmin ها، اغلب دایرکتوری های کاربران را جاسوسی کرده و ایمیل های دیگران را می خوانند. همچنین ممکن است شخصی سایت شما را هک کرده و بخواهد چیزهای شما را بگیرد.

هرگز از اکانت خود در راهی که علاقه شما را به هکینگ نشان می دهد استفاده نکنید (همین جا استفاده از ID ها و ... که عناوینی مثل Hacker و ... استفاده می گردد، منع می شود). علاقه در امنیت صحیح است اما نه بیشتر !!

۳,۴ LOG ها

سه فایل مهم برای log ها وجود دارد:

WTMP – هر log on/off با زمان آن، بعلاوه TTY و هاست را در خود نگه می دارد.

UTMP – چه کسی در آن زمان online می باشد.

LASTLOG – login ها از کجا می آیند.

[5] Emanation

البته موارد دیگری هم وجود دارند که در اینجا از ذکر آنها خودداری کرده و در بخش بعدی این مقاله حول آنها بحث می کنیم. هر login به وسیله telnet، ftp، rlogin و روی بعضی سیستم rsh، در این log ها نوشته می شوند. در صورتی که در حال هک کردن یک سیستم و در اختیار گرفتن کنترل آن هستید، خیلی مهم است که اطلاعات مربوط به خود را از آن لاگ فایل ها پاک کنید، چرا که در غیر این صورت مسئولان هاست قربانی:

۱- می توانند ببینند که شما دقیقا چه زمانی عملیات هکینگ را شروع کرده اید.

۲- می توانند بازرسی کنند که از کدام سایت آمده اید.

۳- می توانند بفهمند که چه مدت آنلاین بوده اید و می توانند اثرگذاری شما را روی سیستم[6] محاسبه کنند.

هرگز لاگ ها را حذف نکنید! این راحت ترین راهی است که می توانید به مدیر نشان دهید که یک هکر روی ماشین آنها بوده است. یک برنامه خوب را برای تغییر و دستکاری لاگ ها بگیرید. ZAP (یا ZAP2) اغلب به عنوان بهترین ها ذکر می شوند- اما در حقیقت این چنین نیست. تنها کاری که این برنامه انجام می دهد این است که آخرین اطلاعات مربوط به لاگین کاربر را با صفرها جاینویسی (overwrite) می کند. CERT پیش از این برنامه های ساده ای منتشر کرده است که می توانند به دنبال entry های صفر شده گشته و آنها را بازرسی کنند. بنابراین استفاده از این ابزار نیز راهی ساده برای نمایان ساختن هکر بر مدیر می باشد. او درخواهد یافت که شخصی دستیابی root (ریشه) را هک کرده و آنوقت تمام کارهای شما بی بها و بی ارزش خواهند شد. نکته مهم دیگر راجع به ZAP این است که در صورتی که نتواند لاگ فایل ها را پیدا کند، هیچ گزارش یا اخطاری را اعلام نمی کند- بنابراین قبل از انجام کار مسیرها یا path ها را چک کنید.

یا یک برنامه ای بگیرید که داده ها (data) را تغییر می دهد (مانند CLOAK2) یا یک برنامه واقعا خوب بگیرید که entry ها را پاک کند (مانند CLEAR).

در حالت عادی شما باید برای دستکاری لاگ ها دستیابی ریشه ای (root) داشته باشید (به غیر از توزیع های[7] قدیمی که UTMP و WTMP قابل نوشتن بودند). اما اگر به صورت ریشه ای عملیات هکینگ را انجام نداده باشید، چه کاری می توانید بکنید؟

در جواب می توان گفت که به کامپیوتری که در حال حاضر روی آن سیطره خود را پهن کرده اید (!!!)، یک rlogin انجام داده و یک اطلاعات غیرمشکوک برای LASTLOG وارد کنید که این مورد هنگامی که owner (صاحب ماشین) در دفعه بعد، عملیات لاگین را انجام می دهد، برای او نمایش داده خواهد شد.

بنابراین اگر او "localhost" را ببیند، مشکوک و بدگمان نخواهد شد. بسیاری از توزیع های یونیکس، یک باگ با دستور login دارند. هنگامی که بعد از لاگین شدن به سیستم، مجددا آنرا اجرا می کنید، در این صورت این فایل فیلد Login-From را در UTMP (که هاستی که شما از آن عملیات لاگین را انجام داده اید نشان می دهد) با TTY فعلی شما جاینویسی یا overwrite می کند.

این لاگ فایل ها در حالت عادی در چه محلی قرار گرفته اند؟ در جواب باید گفت که این مورد بستگی به نسخه توزیع شده ی یونیکس شما دارد.

UTMP: /etc یا /var/adm یا /usr/adm یا /usr/var/adm یا /var/log

WTMP: /etc یا /var/adm یا /usr/adm یا /usr/var/adm یا /var/log

LASTLOG: /usr/var/adm یا /usr/adm یا /var/adm یا /var/log

---

[6] Impact
[7] Distribution

در بعضی از توزیع های قدیمی یونیکس اطلاعات LASTLOG در $HOME/.lastlog نوشته می شوند.

۳,۵ اجازه Trace را ندهید!

من با هکرهای بسیاری مواجه شده ام که خودشان را از لاگ ها پاک کرده اند اما فراموش کرده اند که دیگر چیزهایی که در ماشین ها از خود به جای گذاشته اند، پاک کنند: فایل های موجود در tmp/ و $HOME .

Shell History

بعضی از shell ها یک history file را با تمام دستورات تایپ شده، برجای می گذارند (بستگی به محیط پیکربندی شده دارد). این مورد برای یک هکر بسیار چالش ساز و بد می باشد. بهترین انتخاب این است که به عنوان اولین دستور خود بعد از لاگین کردن، یک shell جدید ایجاد کنید و دائما مراقب یک history file در $HOME باشید.

History File ها

sh_history : sh

history : csh

sh_history : ksh

bash_history : bash

history : zsh

Backup File ها:

dead letter ، *.bak ، *~

به بیان دیگر، قبل از ترک کردن خود، یک دستور "ls -altr" را اجرا کنید. در اینجا چهار دستور csh وجود دارد که بدون هیچ گونه trace و ردیابی، هنگامی که log out کردید، history. را پاک خواهند کرد.

۳,۶ چیزهایی که باید اجتناب کنید!

پسوردها را روی ماشین دیگری غیر از ماشین خود کرک نکنید و تنها روی یک بخش رمزنگاری شده این کار را انجام دهید. اگر شما آنها را برای مثال در دانشگاه کرک کنید و کاربر root ، پروسه شما را ببیند و آنرا بازرسی کند، نه تنها اکانت هکینگ شما را در history خواهد یافت، بلکه سایتی که فایل پسورد در آن است را نیز پیدا خواهد کرد و بنابراین دانشگاه با تمامی چشمان خود مراقب کارهای شما خواهد بود!!

اطلاعات passwd را دانلود کرده یا بدزدید و آنها را روی یک ماشین ثانویه یا در یک پروسه پشت صحنه کرک کنید. شما به اکانت های کرک شده زیادی احتیاج ندارید، تنها تعداد کمی از اکانت ها کفایت می کند.

اگر شما برنامه های مهمی مثل YPX، ISS، SATAN یا برنامه های اکسپلویتینگ را اداره کرده و آنها را قبل اجرا تغییر نام دهید یا از یک source معمول و کوچک برای تعویض فایل اجراشده در process list استفاده کنید ... حتی کاربر هوشیار به مسائل امنیتی (و البته مدیر) در صورتی که ۵ برنامه در حال اجرای YPX را در پشت صحنه ببیند، می فهمد که چه اتفاقی افتاده است... و البته اگر امکانش وجود داشت، در صورتی که برنامه یک حالت Interactive را پشتیبانی می کند (مثل netcat)، پارامترها را در command-line استفاده نکنید (یعنی به صورت مستقیم پارامترها را به برنامه انتقال ندهید – به زبان برنامه نویسی پارامترها

را به تابع main انتقال ندهید)، مثلا برای استفاده از تلنت به جای استفاده از telnet <target-host.com> ، ابتدا عبارت "telnet" را تایپ کرده و پس از فشردن کلید enter، عبارت "open <target-host.com> را وارد کنید و سپس enter را بفشارید که با اینکار target-host در process list به عنوان پارامتر نمایش داده نمی شود.

اگر شما یک سیستم را هک کردید – هیچ جای آن یک suid shell قرار ندهید!

به جای آن، سعی کنید چندین backdoor مانند، ping، quota یا login نصب کرده و در صورتی که احتمال دیگری پیش خود ندارید، از fix برای تصحیحِ atime و mtime فایل، استفاده کنید.

۴. موارد پیشرفته

محتویات:

۴,۱ مقدمه

۴,۲ از هر نوع از Tracing جلوگیری کنید

۴,۳ تمام لاگ فایل ها را پیدا کرده و دستکاری کنید

۴,۴ پیکربندی syslog و logfile را چک کنید

۴,۵ دنبال برنامه های امنیتی نصب شده بگردید

۴,۶ مدیرها را بازرسی کنید

۴,۷ چطور CHECKSUM را برای نرم افزار چک کننده "تصحیح" کنیم!

۴,۸ حقه های امنیتی کاربر (User Security Tricks)

۴,۹ موارد متفرقه

۴,۱ مقدمه

هنگامی که شما اولین sniffer خود را نصب کردید و شروع به هک کردن کردید، آنوقت بایستی این چک ها و تکنیک ها را بدانید و استفاده کنید! از نکاتی که در قسمت از مقاله استفاده کنید – در غیر این صورت فعالیت شما به زودی قطع خواهد شد.

۴,۲ از هر نوع از Tracing جلوگیری کنید

بعضی مواقع هک کردن شما آگهی داده خواهد شد. آن مشکل اصلی نخواهد بود – بعضی از سایت های شما، down خواهد شد اما چه کسی توجه دارد، موارد زیادی برای رسیدگی وجود دارند. چیزِ بسیار خطرناک، هنگامی است که آنها سعی بر trace کردن شما برای رسیدن به اصلیت شما انجام می دهند تا از این طریق با شما معامله کنند – برای شما مشکل ایجاد کنند یا ... ! این قسمت کوچک در این فصل به شما تمامی احتمالاتی که ممکن است آنها برای trace کردن شما مجبور به انجام آن باشند می گوید و در کنار آن به شما احتمالاتی که باید از آن دوری جوئید را نیز بازگو می کند.

* معمولا این نباید برای مدیر مسئله ای باشد که سیستمی که هکر از آن استفاده می کند را تشخیص هویت کند که این کار با انجام کارهای زیر ممکن می شود: در صورتی که هکر، تازه کار باشد، چک کردن entry های لاگ ها. نگاه کردن به خروجی

sniffer ای که هکر نصب کرده و خودش هم در آن است. استفاده از دیگر نرم افزارهای بازرسی[8] مانند loginlog، یا حتی در صورتی که هکر در حال حاضر آنلاین می باشد، نمایش تمامی ارتباطات فعال با "netcat" – در صورتی که آنها این موضوع را بدانند! به همین دلیل است که شما به یک Gateway Server احتیاج دارید.

* یک Gateway Server در میان است؟ آن چیست؟

آن یکی از سرورهای بسیاری است که شما روی آن اکانتی دارید که مطلاقا سیستم های ضعیف بوده و شما روی آنها دسترسی ریشه ای دارید. شما احتیاج به دستیابی ریشه ای دارید تا فایل های wtmp و lastlog را تغییر داده و همچنین ممکن است احتیاج باشد که چندین لاگ بازرسی (audit log) را که روی این ماشین کاری انجام نمی دهند، تغییر دهید!

شما باید استفاده از Gateway Server ها را روی یک پایه منطقی تغییر دهید، مثلا هر یک-دو هفته، و مجددا از آنها حداقل برای یک ماه استفاده نکنید.

با این رفتار بسیار غیرمحتمل می باشد که آنها بتوانند شما را trace کرده و به مبدا اصلی خود که دفعه بعد از آن استفاده می کنید، برسند: سروری که با آن هک می کنید که به صورت خلاصه از این به بعد آنرا، Hacking Server می نامیم.

* Hacking Server شما – اساس تمام فعالیت ها

از این سرورها شما هکینگ را شروع می کنید. Telnet (یا بهتر: remsh/rsh) به یک ماشینِ gateway و سپس به هدف. شما مجددا به دستیابی ریشه ای برای تغییر لاگ ها احتیاج دارید. شما بایستی Hacking Server خود را هر ۲ تا ۴ هفته عوض کنید.

* سرور باستیون (bastion)/ Dial-UP شما

این یک نقطه بحرانی است. یک بار که بتوانند شما را trace کنند و به ماشین dialup شما برسند، در آن صورت کار شما تمام خواهد بود! یک تماس به پلیس، یک خط trace و کامپیوتر شما که فعالیت های هکینگ را انجام می دهد – و شاید بقیه چیزها !

شما روی یک هاست باستیون احتیاج به دستیابی ریشه ای ندارید. به دلیل اینکه شما تنها بوسیله مودم به آن وصل می شوید، هیچ لاگی وجود ندارد که باید تغییر داده شود. شما بایستی هر روز از یک اکانت متفاوت برای لاگین کردن به سیستم استفاده کنید و سعی بر استفاده از آنهایی کنید که کم استفاده بوده اند.

سیستم را به هیچ وجه تغییر ندهید.

شما بایستی حداقل دو سیستم باستیون داشته باشید که بتواند به آن dialup کرده و هر ۱ یا ۲ ماه بین آنها سوئیچ کنید.

توجه: اگر این احتمال برای شما مسیر است که هر روز به سیستم های مختلفی dialup کنید (مثلا: blueboxing)، در این صورت این کار را انجام دهید. آنوقت شما احتیاج به یک Hacking Server نخواهید داشت.

موارد متفرقه

اگر می خواهید یک satan، iss، ypx، nfs یا ... اجرا کنید، آنوقت باید از یک سرور مخصوص برای این کار استفاده کنید. از آن در عمل برای telnet/rlogin به یک سیستم هدف استفاده نکنید، تنها از آن برای scanning استفاده کنید. به آن مثل حالتی که یک gateway server می باشد، وصل شوید.

---

[8] Audit

ابزاری وجود دارند که به یک پورت بخصوص bind می شود، و هنگامی که یک ارتباط با این پورت برقرار می گردد، به صورت اتوماتیک یک ارتباط را با یک سرور دیگر باز می کنند که به نوعی مانند یک shell روی سیستم عمل می کنند، بنابراین شما به این socket daemon نیز تلنت می کنید.

با یک چنین برنامه در حال اجرایی، اثرات شما در هیچ لاگی نوشته نخواهد شد بجز لاگ های فایروال ها. برنامه هایی وجود دارند که آن کار را برای شما انجام می دهند.

اگر امکانش وجود داشت، Hacking Server و/یا ماشینِ Gateway بایستی در یک کشور خارجی قرار داشته باشند! چرا که اگر تلاشِ نفوذ شما تشخیص داده شد و هاست اصلی شما تشخیص هویت داده شد، آنوقت بسیاری از مدیران گرایش به اذیت کردن منابع آن کشور خواهند! حتی اگر فدرال ها برای trace کردن شما بواسطه کشورهای مختلف تلاش کنند، یک وقفه برای اینکار بوجود می آید که حداقل بین ۲ تا ۱۰ هفته می باشد.

* راه حل: اگر شما چیز دیگری را از دانشگاه خود هک کردید، روش زیر را به کار گیرید. در زیر یک عکس کوچک وجود دارد که به شما کمک خواهد کرد.

```
+-------+    ~---------------->    +-------------+    +-----------+
|+-----+|    >hopefully     >    |one of at    |    |one of many|
|| YOU || --> >a trace-safe   > --> |least 3      | --> |hacking    |
|+-----+|    >dial possiblity>    |bastion hosts|    |server     |
+-------+    ~---------------->    +-------------+    +-----------+
                                  |
                                  |
                                  v
+-----------------+          +--------+    +-----------+
|maybe additional |          | the    |    |one hacked |
|server from      | ... <-- ... | main   | <-- |server as  |
|internal network |          | target |    |gateway    |
+-----------------+          +--------+    +-----------+
```

۴,۳ تمام لاگ فایل ها را پیدا کرده و دستکاری کنید

این نکته مهم است که شما تمامی لاگ فایل ها را بیابید – حتی آنهایی که مخفی هستند. برای پیدا کردن هر نوع از لاگ فایل ها، دو احتمال ساده وجود دارد:

۱- تمامی فایل های باز (open) را پیدا کنیم: به دلیل اینکه تمام لاگ فایل ها باید در جایی نوشته شوند، برنامه جذاب LSOF – که خلاصه عبارت LiSt Open Files می باشد – را گرفته تا فایل ها باز را ببینیم، چک کنیم و در صورت نیاز آنها را تصحیح کنیم.

۲- به دنبال تمام فایل هایی که بعد از لاگین شدنمان تغییر کرده اند، بگردیم: بعد از لاگین شدن خود، عبارت "touch /tmp/check" را اجرا کرده و کار خود را ادامه دهید. بعد از اتمام کارتان، عبارت "find / -newer /tmp/check –print" را اجرا کرده و بررسی کنید که آیا هر یک از آنها، audit file می باشند یا خیر. See => Check => Corret !! به خاطر داشته باشید که تمام نسخه های find، گزینه newer– را پشتیبانی می کنند. شما همچنین می توانید دستور "find / -ctime 0 -print" یا - "find / cmin 0 -print" را برای یافتن آنها انجام دهید.

تمام لاگ فایل هایی را که یافته اید چک کنید. معمولا آنها در /usr/adm ، /var/adm یا /var/log می باشند. اگر چیزها در loghost@، لاگینگ شده باشند، در این صورت به درد سر افتاده اید. چرا که نیاز دارید تا ماشین loghost را نیز هک کنید تا لاگ ها را در آنجا نیز دستکاری کنید.

برای دستکاری لاگ ها می توانید از چیزهایی مانند "grep -v" استفاده کنید یا از یک linecount با wc استفاده کنید و سپس ۱۰ خط آخر را با "head -LineNumbersMinus10" ببرید، یا از یک editor استفاده کنید یا ... .

اگر فایل های log/audit به صورت textfile نبوده و به صورت datarecord بودند، در این صورت نرم افزاری را که لاگ فایل ها را می نویسد تشخیص دهید. سپس source code را بگیرید و بعد هدر فایل های منطبق را که ساختار فایل را تعریف می کند، پیدا کنید. ZAP، CLEAR، CLOAK یا ... را بگیرید و آنرا با فایل هدر باز نویسی کنید تا از این نوع خاص از لاگ فایل استفاده کنید (و در صورتی که چنین رخدادی برای شما انجام شد، برنامه جدید خود را به جامعه هکرها بدهید تا دیگران در کارهایشان ایمن تر باشند).

اگرaccounting نصب می باشد، در این صورت شما می توانید acct-cleaner را از zhart مورد استفاده قرار دهید، همچنین در این انتشار، این مورد کارکرد داشته و بسیار عالی است!

در اینجا می خواهیم یک حیله کوچک را با هم بررسی کنیم: در صورتی که می خواهید WTMP را دستکاری کنید، اما نمی توانید یک سورس کد را کامپایل کنید هیچ perl و ... نصب نیست، در این صورت (روی SCO کارکرد داشته است اما روی لینوکس نه):

یک uuencode روی WTMP انجام دهید. vi را اجرا کنید، به انتهای فایل scroll down کنید و چهار خط آخر را که با "M" شروع می شوند پاک کنید ... سپس save+exit کرده و uudecode کنید. آنوقت، پنج entry آخر پاک شده است!!

اگر سیستم از WTMPX و نیز از UTMPX استفاده می کند، شما به دردسر افتاده اید! من هیچ cleaner ای تا کنون نمی شناسم که بتواند با آنها سروکله بزند.

۴,۵ پیکربندی syslog و logfile را چک کنید

بسیاری از برنامه ها از تابع syslog برای لاگ کردن هر چیز که بخواهند استفاده می کنند. بسیار مهم است که پیکربندی را چک کنیم که آیا syslog انواع خاصی را چاپ می کند یا خیر.

فایل پیکربندی[9] در /etc/syslog.conf بوده و اینجا نمی خواهیم بگوئیم که قالب این فایل چگونه بوده و چه entry هایی درون آن وجود دارند. می توانید روی اینترنت صفحات زیادی را راجع به آن بخوانید. انواعی که برای شما مهم هستند، kern.* و auth.* و authpriv.* هستند. به جایی که این فایل ها نوشته شده اند نگاه کنید: آیا فایل ها قابل تغییر هستند. اگر به هاست های دیگری فرستاده شده باشند، شما مجبور به هک کردن آن سیستم ها نیز هستید. اگر پیام ها به یک کاربر، TTYو/یا کنسل[10] فرستاده می شوند، می توانید یک حقه کوچک زده و پیام های لاگِ غلطی را تولید کنید، مثلا:

"echo 17:04 12-05-85 kernel sendmail[243]: can't resolve bla.bla.com > /dev/console"

یا می توانید هر وسیله ای[11] را که می خواهید Flood کنید، بطوریکه پیامی را که قصد دارید مخفی گردد، به سادگی در طوماری از پیام ها در صفحه گم خواهد شد (و به چشم نخواهد آمد). این لاگ فایل ها بسیار مهم هستند، بنابراین حتما آنها را چک کنید!

---

[9] Config
[10] Console
[11] Device

۴,۵ دنبال برنامه های امنیتی نصب شده بگردید

در بسیاری از سایت های آشنا به امور امنیتی، چک کننده هایی امنیتی[۱۲] وجود داشته که توسط Cron اجرا می گردند. دایرکتوری معمول برای crontabs در /var/spool/cron/crontabs می باشد. تمامی entry ها را چک کنید(مخصوصا فایل "root") و بازرسی کنید که چه فایل هایی را اجرا می کنند. برای تنها یک تحقیق سریع از crontabs برای نوع root[۱۳] می توانید از عبارت زیر استفاده کنید:

"crontab -l root"

بعضی از آن ابزار امنیتی در بیشتر اوقات روی اکانت های مدیرها نصب می گردند. بعضی از آنها (که ابزارهای کوچکی برای چک کردن WTMP هستند و نیز بازرسی می کنند که آیا یک sniffer روی ماشین نصب می باشد یا خیر)، در قسمت ~/bin از این اکانت ها قرار دارند. قسمت زیر را برای تشخیص دادن این مدیرهای بخصوص که در بالا ذکر شدند، بخوانید و دایرکتوری های آنها را چک کنید.

از نرم افزارهای چک کننده درونی می توان به tiger، cops، spi، tripwire، 15، binaudit، hobgoblin، s3 و ... اشاره کرد. شما باید آنها را بررسی کنید که چه چیزهایی گزارش می دهند و آیا چیزی گزارش می دهند که نشانه ای از نفوذ شما باشد یا خیر. اگر جواب مثبت بود، می توانید فایل های داده از checker را بروز رسانی کنید (learn mode)، بطوریکه آن نوع خاص را از این به بعد گزارش ندهد.

- می توانید نرم افزار را مجددا برنامه ریزی کنید/تغییر دهید بطوریکه آن نوع خاص را از این به بعد گزارش ندهد (من به شخصه برنامه ها تقلبی cpm را ترجیح می دهم).
- اگر امکانش وجود دارد، backdoor ای که نصب کرده اید را پاک کرده و سعی کنید که این کار را به روش دیگر انجام دهید.

۴,۶ مدیرها را بازرسی کنید

برای شما بسیار مهم است که گزینه های سیستمی (system options)[۱۴] را برای مقیاس های ضد امنیتی چک کنید. بنابراین ابتدا احتیاج به دانستن اینکه از کدام اکانت های معمولی استفاده می کنند دارید.می توانید فایل forward. از root و alias entry از root چک کنید. به sulog نگاهی انداخته و بخاطر بسپارید که کدام افراد یک su موفقیت آمیز به root داشته اند. Group file را دزدیده (!) و wheel و admin group (و هر گروه دیگری که در این فایل با مدیریت رابطه دارد) را بازرسی کنید. همچنین grep کردن فایل passwd برای "admin"، مدیرها یا administrator ها را آشکار خواهد ساخت.

اکنون شما بایستی دانسته باشید که مدیرهای اول تا ششم روی ماشین ها کدام ها هستند. به دایرکتوری های آنها بروید (در صورتی که root اجازه خواندن هیچ فایلی را نمی دهد، از chid.c یا changeid.c یا چیزی شبیه به آن استفاده کنید) و .history ، .sh_history و .bash_history مربوط به آنها را چک کنید تا ببینید که چه دستورهایی را معمولا تایپ می کنند. در

---

[12] Security Checker
[13] Root type
[14] که به صورت خلاصه sysops نامیده می شوند (نباید آنها را با سیساپ فرد راه انداز تابلوی های الکترونیکی اشتباه شود).

کنار آن فایل های .profile ، .login و .bash_profile مربوط به آنها را چک کنید تا ببینید چه alias هایی تنظیم شده اند[15] و آیا بازرسی ها و چک های auto-security یا log کردن انجام شده است یا خیر.

دایرکتوری ~/bin آنها را بازرسی کنید! بسیاری از مواقع برنامه های چک کننده امنیتی در آنجا قرار داده شده اند! و البته در کنار آن به همه دایرکتوری ها نظری بیفکنید!! آنها نزدیک آن قرار دارند (ls –aIR ~). اگر هر چیز مرتباط با امنیت پیدا کردید، قسمت های قبل را برای احتمالاتی که بتوان آن حفاظت ها را byspass کرد بخوانید.

۴,۷ چطور CHECKSUM را برای نرم افزار چک کننده "تصحیح" کنیم![16]

بعضی از مدیرها واقعا از هکرها می ترسند و نرم افزارهایی را برای تشخیصِ تغییرات در باینری های مقدار پذیر نصب می کنند. اگر با یک باینری مذاکرات پنهانی انجام دهید (tamper)، دفعه بعد که مدیر یک binary check انجام دهد، آن باینری تشخیص داده می شود.

بنابراین چگونه نخست می توان فهمید که آیا binary checker ها نصب شده اند یا خیر و دوما فهمید که چگونه آنها را دستکاری کنیم، بنابراین شما می توانید اسب تراوای خود را رشد (!!) دهید؟

به خاطر داشته باشید binary checker های بسیاری وجود دارند و نوشتن یکی از آنها هم بسیار ساده می باشد – در حدود ۱۵ دقیقه وقت می خواهد – و این کار را می توان توسط یک اسکریپت کوچک انجام داد. بنابراین بسیار دشوار می باشد که این چنین نرم افزارها را در صورت نصب بودن پیدا کنیم.

به خاطر داشته باشید که نرم افزارهای چک کننده امنیتی داخلی نیز این چنین بازرسی ها و چک ها (binary checking) را انجام می دهند. در زیر بعضی از آنهایی که به طور گسترده مورد استفاده قرار می گیرند می بینید:

نرم افزار : مسیر استاندارد : FileName های باینری

tripwire ، بانک های اطلاعاتی : **/usr/local/adm/tcheck** ، **/usr/adm/tcheck : Tripwire**

auditscan : /usr/local/adm/audit : binaudit

hobglobin : ~user/bin : hobgoblin

raudit.pl : ~user/bin : raudit

15 : compile directory : 15

اما همان طور که می بینید احتمالات زیادی می تواند وجود داشته باشد! نرم افزار یا بانک اطلاعاتی ممکن است حتی روی یک دیسک معولی mount نشده[17] یا قسمت NFS استخراج شده از یک هاست دیگر باشد. یا بانک اطلاعاتی checksum روی یک medium[18] که قابلیت Write-Protected روی آن اعمال شده است، باشد. احتمالات بسیار زیادی وجود دارد. اما در حالت عادی در صورتی که بسته های[19] فوق نصب شده اند و نمی خواهید باینری ها را مبادله کنید، می توانید تنها یک بازرسی و چک سریع انجام دهید. اگر شما آنها را پیدا نکردید، در حقیقت شما روی سایتی قرار دارید که بسیار خوب ایمن شده است و بنابراین شما نباید آنها را تحریف کنید!

---

[15] Set
[16] Correct Checksum Checking Software
[17] Unmounted
[18] در اینجا یعنی رسانه ای که امکان ذخیره و نمایش داده ها را به ما می دهد.
[19] Package

اما در حالتی که شما آن نرم افزار نصب شده را پیدا کردید و می توانید آنرا تغییر دهید (مثلا زمانی که روی یک رسانه write-protected، یا هر چیز که بتواند bypass شود- برای مثال unmount کردن دیسک و remount کردن به صورت writable – وجود دارد) چه باید بکنید؟

در این صورت شما ۲ احتمال پیش رو دارید:

- نخست اینکه شما می توانید تنها پارامترهای نرم افزار را چک کنید و یک "update" را روی باینری تغییر داده شده اجرا کنید. برای مثال برای tripwire به صورت "tripwire -update /bin/target" می باشد.
- دوم اینکه شما می توانید list file موجود برای چک کردن باینری ها را چک کنید و entry ای که روی آن عمل تعویض و جایگزینی (با چیز دیگری) انجام داده اید را پاک کنید.

به خاطر داشته باشید که بایستی همچنین چک کنید که آیا فایل بانک اطلاعاتی[20] خودش برای تغییرات چک می گردد یا خیر! اگر اینگونه بود، entry را نیز update/delete کنید.

۴,۸ حقه های امنیتی کاربر (User Security Tricks)

این مورد بسیار نادر است اما برای اینکه مقاله کامل باشد آنرا نیز ذکر می کنیم. بعضی کاربران، مانند مدیرها و هکرها دوست ندارند که اکانت هاشان توسط شخص دیگری استفاده گردد. به همین دلیل است که بعضی مواقع قابلیت های امنیتی را روی فایل هایشان در startup قرار می دهند.

بنابراین تمامی dotfile ها (.profile, .cshrc, .login, .logout و ...) را چک کنید که چه دستورهایی را اجرا می کنند، چه history logging و searchpath ای را تنظیم و set می کنند. برای مثال در مسیر جستجو (search path)، اگر $HOME/bin قبل از /bin بیاید، شما بایستی محتویات این دایرکتوری را چک کنید ... ممکن است برنامه ای با نام "ls" یا "w" نصب شده باشد که زمان اجرا (execution time) را log می کند و بعد از آن برنامه واقعی را اجرا می کند. بعضی ها هم ممکن است فایل های WTMP و LASTLOG را برای کاربرد ZAP، دستکاری .rhosts ، فایل های .Xauthority و sniffer های فعال و ... را به صورت اتوماتیک چک کنند. هرگز یا اکانتی که یک **Wizard** Unix با آن کار می کند، درگیر نشوید!

۴,۹ موارد متفرقه

کلاینت های telnet قدیمی، متغیر USER را استخراج (export) می کنند. مدیری که آنرا بداند و telnetd را تغییر دهید، می تواند تمامی user name ها را با آن دریافت کند و بنابراین یکبار که به شما اخطار دهد، اکانتی که شما از آن عملیات هک را انجام می دهید را نیز تشخیص هویت خواهد داد. کلاینت های جدید fix شدند – اما یک مدیر باهوش احتمال های دیگر برای تعیین هویت کاربر دارد: متغیرهای UID، MAIL و HOME هنوز استخراج می شوند و تعیین هویت اکانتی که توسط هکر مورد استفاده قرار گرفته است را آسان می گردانند. قبل از اینکه شما یک telnet انجام دهید، متغیر USER، UID، MAIL و HOME را تغییر دهید. حتی در صورتی که در دایرکتوری home هستید، ممکن است حتی نیاز به تغییرِ متغیرِ PWD نیز باشد.

روی HP-UX، v10 شما می توانید دایرکتوری ها را مخفی کنید. ما راجع به فایل های نقطه دار یا dotfile ها (dotfile =>) یا مشابه آن صحبت نمی کنیم بلکه راجع به یک فلگ بخصوص صحبت می کنیم. HP آنرا v9 معرفی کرد، اما از version 10

[20] DB File

حذف شد (چرا که آن تنها توسط هکرها مورد استفاده قرار می گرفت)! اگر شما یک "chmod +H directory" را انجام دهید، دایرکتوری مورد نظر برای "ls -al" نامعلوم یا invisible می باشد. برای دیدن دایرکتوری های مخفی شما احتیاج به اضافه کردن سوئیچ H– به ls دارید، یعنی از "ls -alH" برای دیدن همه چیز می توانید استفاده کنید.

هر وقت که شما احتیاج به تغییر تاریخ فایل داشتید، به خاطر داشته باشید که می توانید از دستور "touch" برای تنظیم کردن atime و mtime استفاده کنید. شما می توانید ctime را تنها با raw write ها روی هارددیسک تنظیم یا set کنید.

اگر شما یک sniffer نصب کنید و این برای شما یک سیستم مهم باشد، آنوقت حصور اطمینان کنید که خروجی sniffer را با یک الگوریتم، رمزنگاری کنید (ما اینجا درباره rot13 حرف نمی زنیم) یا اینکه به sniffer اجازه دهید تمامی داده های capture شده را به وسیله ICMP یا UDP به یک هاست خارجی تحت کنترل شما بفرستد. چرا آن؟ خوب، اگر مدیر به طریقی sniffer را پیدا کنید (cpm و دیگر نرم افزارهای بازرسی و چک برای sniffer ها)، نمی تواند در لاگ فایل تشخیص دهد که چه داده هایی sniff شده اند، بنابراین بنابراین نمی تواند به هاست هایی که توسط شما sniff شده اند هشدار دهد.

۵. تحت سوء ظن و شَک

هنگامی که تحت بدگمانی قرار گرفتید (توسط پلیس و/یا مدیر) بایستی اقدامات خاصی را انجام دهید تا نتوانند علیه شما مدرکی ارائه دهند.

توجه: اگر مدیرها فکر کنند که شما یک هکر هستید، شما در هر حالتی گناهکار خواهید بود تا خلاف آن ثابت گردد!

قوانین برای مدیرها هیچ معنی ندارد (بعضی مواقع من فکر می کنم که تفاوت بین یک هکر و یک مدیر تنها این است که کامپیوتر به آنها تعلق دارد!!!). هنگامی که آنها فکر کنند که شما یک هکر هستید شما حتی بدون فکر صحبت کردن یک وکیل و دفاع کردن از شما، گناهکار شناخته خواهید شد (این قوانین بشدت در ایران در حال اجرا می باشد). آنها شما، ایمیل های شما، فایل های شما را چک می کنند و در صورتی که نیاز باشد، کلیدهای فشرده شما (keystroke) را نیز چک می کنند.

هنگامی که خرابکاری شما سنگین بوده و فدرالی ها نیز درگیر کار شوند، خط تلفن شما مانیتور خواهد شد و به احتمالا یک یورش ناگهانی به شما نیز به زودی رخ خواهد داد.

اگر متوجه شدید یا بنابر اتفاق این ترس بر شما فائق شد که شما تحت سوء ظن و شک (بدگمانی) هستید، در این صورت باید مطلقا فعالیت های خود را کم نگه دارید! هیچ عمل تهاجمی که اشاره بر هکینگ داشته باشد نباید انجام شود.

بهترین راه این است که بمدت ۱ یا ۲ ماه صبر کرده و هیچ کار انجام ندهید (فرصت مناسبی برای مطالعه و ...). به دوستان خود هشدار دهید که به شما هیچ ایمیلی نفرستند. بعضی از افراد به اشتباه فکر می کنم که دوستان می توانند با رعایت اصول رمزنگاری مثلا PGP که در اوایل مقاله بحث شد، می توانند به آنها ایمیل بزنند، اما باید گفت که ایمیل های رمزنگاری شده با PGP و ... ، زنگ هشدار[۲۱] برای مانیتورینگ های مدیران و فدرال ها را به صدا در خواهد آورد. میتوان گفت که ایمیل های غیر تهاجمی از طرف دوستان، در این مورد بسیار به شما کمک خواهد کرد، مثلا می توانید به دوستان خود بگویید که برای شما ایمیل های معمولی و public را بفرستند. به هر حال با هر چیز باید قطع رابطه کنید. به هر حال برای این موقع می توانید مطالعه داشته باشید، به صورت local برنامه نویسی کنید، مقاله های دلخواه خود را بنویسید، از مطالب خوانده شده خود نت برداری کنید تا فراموش نشوند و ... . به خاطر داشته باشید که تمامی اطلاعات خود را رمزنگاری کنید و تمامی صفحاتی که حاوی اطلاعات اکانت شما، شماره

[21] Alarm Bell

های تلفن و ... هستند، پاک کنید. اینها مهم ترین چیزهایی هستند که فدرالی ها و پلیس ها بعد از یورش به شما بـه دنبالـــــــشان می گردند.

۶. برنامه ها

در زیر لیستی از برنامه های مورد نیاز که باید در حین کار داشته باشید را لیست کرده ام (بهترین). بـرای گـرفتن آنهـا بـه من پی ام یا ایمیل نزدید- بهترین راه سوال کردن از دکتر گوگل (www.google.com) است! به هر حـال در صـورتی کـه آنهـا را پیدا نکرده اید، در موقع مناسب برای شما آپلود خواهم کرد.

من تنها بهترین تغییر دهنده های log را معرفی کرده ام. برنامه های دیگری که اختیاری هستند، telnet redirector ها هستند.

در ابتدا واژه نامه ای از کلمات استفاده شده را در اینجا بیان می داریم:

دستکاری یا تغییر (Change): فلیدهای لاگ فایل را به هر چیزی که می خواهید تغییر می دهد.
حذف کردن یا پاک کردن (Delete): entry هایی که می خواهید را پاک می کند.
ویرایش (تغییر - Edit): ویراستار واقعی برای لاگ فایل.
Overwrite: تنها entry ها را با بایت هایی با ارزش صفر جاینویسی یا overwrite می کند.

از این چنین برنامه ها استفاده نکنید (برای مثال ZAP) – چرا که قابل تشخیص (detect) می باشد.

LOG MODIFIER

ah-1_0b.tar : entry های اطلاعات accounting را تغییر می دهد.
clear.c : entry ها را در UTMP، WTMP، LASTLOG و WTMPX پاک می کند.
cloak2.c : entry ها را در UTMP، WTMP و LASTLOG پاک می کند.
invisible.c : UTMP، WTMP و LASTLOG را با مقادیر از پیش تعریف شـده جاینویـسی مـی کنـد، بنـابراین از ZAP بهتـر است. مراقب باشید inv*.c های زیادی روی اینترنت وجود دارند!
marryv11.c !
wzap.c : entry ها را در WTMP پاک می کند.
wtmped.c : entry ها را در WTMP پاک می کند.
zap.c : UTMP، WTMP، LASTLOG را جاینویسی می کند – استفاده نکنید! قابل تشخیص است!

بخش دوم: عملیات تمرینی

۱. اولین دستور

اولین دستوری که بعد از لاگین شدن به یک اکانت هک شده کردید باید انجام دهید، یک shell متفاوت از shell ای که در حال حاضر با آن کار می کنید (که تحت عنوان Login Shell شناخته می شود) می باشد. هدف غیر فعال کردن ذخیره history از دستوراتی است که شما در حین هک کردن آنها را وارد می کنید. یک چک و بازرسیِ history توسط کاربر واقعی یا مدیرسیستم (sysadmin) حضورِ شما و کارهای انجام شده توسط شما را آشکار خواهد کرد. اگر شما در حال اجرای یک CSH هستید، آنوقت یک SH را اجرا کنید و برعکس.

$ – این اعلان[۲۲] برای SH می باشد.

% – این اعلان برای CSH می باشد.

اگر اعلان اولیه، شبیه اعلان های استاندارد نبود، در این صورت SH را اجرا کنید. اگر اعلان به همان صورت باقی می ماند، عبارت "exit" را وارد کرده و CSH را اجرا کنید ...

دلیل استفاده از این دو shell (نه bash هایی مانندKSH، ZSK و ...) این است که این خصوصیات ساده ای از خود نشان می دهند و هیچ گزینه اضافی که به صورت پیش فرض فعال شده باشد ندارند، که یکی از این گزینه های پیش فرض می تواند انجام عملیات " ذخیره سازی History " یا History Saving باشد.

۲. زمینه کاری LASTLOG

اگر اگر هنگامی که با اکانت هک شده لاگین شدید و نمی توانید root را هک کنید یا اصلا نمی خواهید لاگ های سیستمی را با پاک کردن اطلاعات منقطع (یا از هم گسیخته) و شک برانگیز سازید، و در این صورت با یک فایل متنی مانند "Last successful login from alpha.master.mil" مواجه شدید، آنوقت دستور زیر را اجرا کنید و مجددا در صورت لزوم پسورد اکانت هک شده را وارد سازید:

"rlogin <the_host_you_are_on>"

بعد از دیدن اعلان مربوط به shell، عبارت exit را تایپ کرده تا به مکان اولیه خود برگردید. با انجام دستور فوق، عبارت متنیِ فوق به:

"Last successful login from <Current-Host>"

یا

"Last successful login from <LocalHost>"

تغییر خواهد کرد که این حالت از حالت قبلی یعنی "Last successful login from alpha.master.mil" کمتر شک برانگیز می باشد. البته شما تنها هنگامی نیاز به این کار دارید که هاست اصلی شما ممکن است برای کاربر و/یا مدیر سیستم جلب توجه داشته باشد.

---

[22] Prompt

۳. زمینه کاری WHO

بعد از انجام قسمت های ۱ و ۲ در فوق، عبارت "w" را تایپ کنید ... تمامی کاربران فعلیِ آنلاین را به همراه آدرسی که از آنجا لاگین کرده اند، خواهید دید. مجددا باید گفت که در صورتی که سایت مورد نظر شما در آمریکا قرار دارد، چیزی مانند هاست اصلی شما که در ایران هست برای کاربران و/یا مدیر (root) بسیار شک برانگیز خواهد بود.

اگر نمی توانید root را هک کنید یا همان طور که ذکر شد نمی خواهید با لاگ فایل ها دست به گریبان شوید، می توانید باگی را که هنوز روی خیلی از توزیع های یونیکس کار می کند امتحان کنید: فقط کافی است، "login" را با همان login+password ای که در حال حاضر با آن لاگین کرده اید، وارد کنید. مجددا "w" را وارد کنید و در صورتی که کار کرد، مبدا اصلیِ شما (هاست اصلیِ شما) به چیزی شبیه به "tty04" تغییر خواهد کرد.

البته مجددا باید گفت که تنها در صورتی نیاز به انجام این کار خواهد بود که هاست اصلی شما امکان جلب توجه برای کاربران و/یا مدیر سیستم را داشته باشد.

۴. اجرای برنامه ها

برنامه ها را با نام های شک برانگیز اجرا نکنید. برای مثال ISS و YPX بسیار شک برانگیز هستند و یک مدیر با تجربه اگر ببیند یک کاربر "loadmodule SandraBullok" را روی Sun او اجرا می کند، از قضایای پشت پرده سر در خواهد آورد!

به هر حال یا دستورات را کپی کرده و rename کنید یا از منابعی (sources) استفاده کنید که نام دستورات را در لیست پروسه ها عوض می کنند.

لیست پروسه را می توان بوسیله "ps -ef" یا "ps -auxwww" چک کرد و همچنین می توان دستور فعلی که هر کاربر با "w" اجرا می کند و نیز میزان استفاده ی پروسه ها از CPU در برنامه هایی که کاربران در حال اجرای آنها هستند را چک کرد.

۵. اجرای Telnet

تنها دو نکته در استفاده تلنت برای موارد هکینگ وجود دارد (مثلا انجام یک تلنت به هدف بعدی).

اولا – همان طور که در قبل ذکر شد، هرگز دستور "telnet target.host.com" را اجرا نکنید، بلکه ابتدا "telnet" را تایپ کرده و کلید enter را بزنید و این بار عبارت "open target.host.com" را نوشته و مجددا کلید enter را بزنید[۲۳] که با این کار به عنوان یک پارامتر در لیست پروسه ها ظاهر نمی شود.

ثانیا – بعضی از کلاینت های telnet متغیرهای محیطی[۲۴] را استخراج می کنند (export). و به این صورت اگر هکینگِ شما تشخیص داده شد و توانستند شما را trace کنند و به هاست اصلی شما برسند، در این صورت خواهند توانست اکانتی که شما برای هکینگ روی هاست اصلی استفاده کردید را نیز بدست آوردند. بنابراین قبل از انجام عملیات telnet، rlogin یا مشابه آنها، متغیرهای محیطی زیر را به هر چیزی که می خواهید تغییر دهید:

---

[23] همان طور که در قبل ذکر کردم، این مورد از خاصیت Interactive بودن Telnet سرچشمه می گیرد.

[24] Environment Variable

USER، LOGNAME، UID، HOME، MAIL – ممکن است این الزام وجود داشته باشد تا یک دستور "cd /tmp" را نیز انجام دهید تا متغیر PWD را نیز تغییر دهید.

برای تغییر این متغیرها به صورت زیر عمل کنید:

ساختار: SH: <variable>=<new_value>;export <variable>

مثال: **USER=nobody;export USER**

ساختار: CSH: setenv <variable> <new_value>

مثال: **setenv USER nobody**

در اینجا باید به یک نکته واضح اشاره کرد:

اگر بعد از عملیاتِ telnet خواستید از سیستم خارج شوید و به اصطلاح log out کنید، ولی احیانا خواستید قبل از log out کردن با اکانت هک شده (که متغیرهای در رابطه به آن در حال حاضر تغییر یافته اند) کاری انجام دهید، فراموش نکنید که حتما متغیرها را reset کنید.

۶. فایل های خود را پاک کنید!

اکسپلویت هایی را که روی سیستم امتحان کردید، چه در صورتی موفق بودن و چه در صورت موفق نبودن، به سرعت پاک کنید – مخصوصا اگر مکان امتحان کردن آنها در tmp/ بوده است!

هیچ چیز جالب تر از این نیست که در دایرکتوری tmp/ جاسوسی و تجسس کنیم تا ببینیم دیگر کاربران چه می کنند. اگر واقعا نیاز به انجام کاری روی دایرکتوری TEMP هستید، (به دلیل اینکه SUID در دایرکتوریِ home شما مخفی شده و حضور دارد[۲۵]) در این صورت یک دایرکتوری معمولی مانند ".X11" بسازید و به آن permission های 711 را بدهید.

به خاطر داشته باشید: اگر شخصی به جاسوسی روی دایرکتوری ها بپردازد و احیانا این کار او با زمانی مصادف باشد که شما به هک مشغول هستید یا ارتباط را منتفی[۲۶] کرده اید و نمی توانید relogin کنید یا اصلا این موضوع را فراموش کرده اید (جاسوسی شخصی روی دایرکتوری ها)، در این صورت به دردسر خطرناکی افتاده اید.

دو نکته زیر تنها با دستیابیِ root احتمال پذیر هستند:

۶,۱ دستکاری LOG ها

لاگ فایل های مهم، LASTLOG، WTMP و UTMP هستند. اگر در هک کردن root موفق بودید، در اینصورت آنها را تغییر دهید. آنها را معمولا در /etc ، /var/adm یا /var/log پیدا خواهید کرد. در مکان آنها تفاوت وجود دارد، تنها صفحات اصلی را چک کنید. چه ابزاری را باید استفاده کنید؟ ZAP (یا ZAP2) خوب هستند، اما شما را از لاگ ها پاک نمی کند، بلکه entry ها را با مقادیر صفر جاینویسی و overwrite می کند (که به هر حال در قبل حول آن صحبت شد). CERT قبلا ابزاری را منتشر ساخته که به راحتی لاگ فایل ها را برای entry های جاینویسی شده پاک می کند. و هنگامی که این اتفاق (جاینویسی مقادیر با صفر و ...)

[25] Squash
[26] Loose

روی یک سیستم رخ دهد و مدیر سیستم با آن مواجه شود، اولـــین فـــــــکری که به ذهنش می رسد این است که "یک هکر بـا دسترسی root روی سیستم می باشد" !!

نکته مهمی که در صورت استفاده از ZAP باید آنرا به خاطر بسپارید: مسیرها یا path های تعریف شده در منـابع را بـرای لاگ ها چک کنید!

CLOAK2 را امتحان کنید که می توانید داده های موجود در فیلدهای داده مهم را تغییر دهد. اما نکته نهفته این است کـه روی هیچ یک از نسخه های یونیکس کامپایل نمی گردد.

شما همچنین می توانید CLEAR را که در این مقاله آورده شده است امتحان کنید که واقعا entry ها را پاک می کند.

۶,۲ SYSLOG و LASTCOMM

شما بایستی همچنین لاگ فایلِ پیام های سیستمیِ لاگ[۲۷] را نیز چک کنید چرا که ممکن است entry هایی بـا اکانـت هـک شده شما یا هاست اصلی شما در آن وجود داشته باشد. این فایل معمولا در /var/adm یا /var/log قـرار گرفتـه اسـت و بـسیاری از اوقات پیام ها یا "message" ها نامیده می شود، اما مجددا باید گفت که بین این دو لفظ باید تفاوت قائل شد – و همچنین باید گفت که در کنار این مورد، دیگر لاگ فایل ها که بوسیله پیام های *.auth یا *.authpriv تولید شـده انـد، و البتـه xferlog را نیـز چـک کنید.

فایلِ /etc/syslog.conf را چک کنید تا فایل صحیح و درست را ببینید و بازدیـد کنیـد کـه چـه چیزهـایی بـه کـدام فایـل، برنامه، mail، کاربر لاگ شده اند.

اگر چیزی شبیه به "@loghost"[۲۸] می بینید و هاست اصلی خود را در فایل پیام ها پیدا کردید، در این صورت بـه مـشکل برخورده اید! چرا که هاست اصلی شما همچنین در سایتِ دیگری که در بسیاری از اوقات به صورت remote قابل دسترس نیـست، لاگ شده است. اما سعی بر نصب یک sniffer کنید (قسمت بعدی را ببینید) و چک کنید که آیا یک root یک لاگین موفقیت آمیـز به loghost انجام می دهد یا خیر و در صورتی که لاگین توسط root به loghost انجام شد، در این صورت شما یـک پـسورد بـرای آن هاست (loghost) در اختیار دارید و می توانید با مشکل پیش آمده دست و پنجه نرم کنید.

برای حذفِ مثلا hostname خود از لاگ فایلِ پیام ها (messages) دستور زیر را اجرا کنید:

"grep -v evil.host.com messages > /tmp/tmpfile; mv /tmp/tmpfile messages"

LASTCOME (از accton)، ابزاری است که تمامی دستورات اجرا شده را لاگ می کند و در صورتی که فایلِ اجـرا شـده با فلگ SUID تنظیم شده باشد و یا یک دستور توسط root اجرا شود، یک flag به آن اضافه می شود. شما می توانید این لاگ فایل را در همان دایرکتوری که فایل syslog وجود دارد، پیدا کنید. ایـن ابـزار واقعـا یـک دشـمن اصـلی بـرای هکرهـا مـی باشـد، امـا – خوشبختانه! – اکثر اوقات نصب نشده است! اما در حال حاضر دیگر نیازی نیـست از آن بترسـید (!)، ابـزار عـالیِ ACCT Cleaner (برای **Zhart**) را بگیرید و آزادی را احساس کنید !!!

۶,۳ نصب کردن اسب های تراوا

هنگامی که یک sniffer را نصب می کنید، به خاطر داشته باشید که هر کسی میتواند "ifconfig –a" را اجرا کند تـا چـک کنید که آیا کارت در حالت Promiscious Mode می باشد یا خیر. یک rootkit برای سیستم عامل یونیکس خود بگیرید و بـا آن

---

[27] Syslog Message Logfile

[28] لازم به تذکر است که loghost تنها یک عبارت کلیشه ای می باشد و جای آن هر چیزی می تواند باشد!

تعویض کنید. فایل fixer.c را روی آن با checksumِ صحیح و date/timeِ صحیح اجرا کنید؛ اما ابتدا اکانت root را چک کنید که شاید tripwire یا دیگر نرم افزارهای Binary Checker نصب شده باشند! این نکته (یعنی عملیات Binary Checking یا کلا نرم افزارهای Binary Checker) را هر هنگامی که یک باینری را تعویض (replace) می کنید به خاطر آورید. اگر باینری در یک دایرکتوری بود که به صورت NFS Mounted بود و امکان remount شدن آن در حالت Write Mode وجود نداشت، در این صورت شما باید ابتدا هاستِ NFS (NFS Host) را هک کنید – به هر حال زندگی بعضی از اوقات راحت نیست!! این حقه ها را به خاطر بسپارید. اگر شخصی می خواهد در این مطالب، نکاتی را تصحیح کند یا توضیحی بیفزاید، یا احتیاج به اطلاعات بیشتری روی یک موضوع دارد یا حتی فکر می کند جایی از این مطالب اشتباه است – می تواند با من در ارتباط بگذارد!

به هر حال، هرگز تنبل نباشید. هر کار باید کامل و ۱۰۰٪ انجام شود– در غیر این صورت با عواقب و پیامدها نیز باید روبرو شد!

تالیف: سعید بیکی (cephexin@secumania.net)

Secumania Security & Vulnerability Research Lab
www.secumania.net