درس ۹

کراکینگ پیشرفته: کراکینگ اینترنت (unix)

کراکینگ اینترنت: Firewalls

با هر شرکت جدیدی، که به «بزرگراه اطلاعـــاتی» متصـل میشـود, آخریـن کشـفیات جدیـد بـرای کراکرها به منظور جستجو و تحقیق صورت می گیرد. مدیـران سـایت (سـایتها) اقدامـات مختلـف امنیتی برای حفاظت از شبکه‌های داخلی‌شان، انجام داده‌اند.

یکی از این اقدامات، xinetd است. راه حل کلی تر، ایجـاد یـک اتصـال محتاطانـه میـان دو شـبکه نامتشابه بنام [Firewall] است، که مابین شبکه داخلی سایت و اینترنت عام و نامشخص اســت کـه ما بدنبال آن میگردیم. در حقیقت، تنها یک سوم از کل اینترنت متصــل کننـده دسـتگاهها، در حـال حاضر پشتیبان firewall هستند. اکثر سرویسهای اطلاع رسانی، با همان مشکلی که ما داریم مواجــه هستند: خارج شدن از طریق یک firewall داخلی یا ورود به یک سرویس از طریق firewall آنــها، راه حل کراک در اینجا هم مطرح می‌شود.

Firewall چیست؟

هدف اصلی یک firewall ممانعت از ورود غیرقانونی در بیــن شبکه‌هاســت. بطـور کلـی، ایـن بـه معنای حمایت از یک شبکه داخلی سایت اینترنت اســت. اگر سـایت، دارای یـک firewall باشـد،

تصمیماتی هم اتخاذ میشوند مبنی بر اینکه در firewall چه چیزی مجاز و چه چیزی غیرمجاز است.

این تصمیمات، همواره متفاوت و همیشه ناقص میباشند، و باعث چندگانگی اینترنت می شوند. همچنین، همیشه راههای گریزی هم وجود دارد که کراکر می‌تواند از آن سودجویی کند.

اساساً، firewall از طریق بررسی بسته‌های کوچک IP کار می‌کند که بین خدمات رسان و مشتری، ارتباط برقرار می سازند. این روش برای کنترل جریان اطلاعاتی برای هر سرویس از طریق آدرس IP، از طریق اتصال و به هر سمتی فراهم می‌کند.

یک firewall ، بیانگر یک «موضع» است. موضع یک firewall، بیان توازن بین حفاظت و سهلوت استفاده می‌باشد. موضع این فرم که هر آنچه که با صراحت جایز شمرده نشده ,ممنوع شده است، مستلزم آنست که هر سرویس جدیدی، بطور جداگانه مجاز شمرده شده و بندرت استفاده شود. بر عکس، این موضع «که هر چیزی که با صراحت ممنوع نشده، مجاز شمرده شده است، امنیت لازم برای راحتی بیشتر را فراهم نموده است.

حدس زدن موضع، هنگام اتخاذ تصمیم برای کراک کردن، بسیار مفید است.

Firewall ، یکسری وظایف کلی دارد که عبارت است از:

– اولین و مهمترین آن اینست که: اگر طبق خط مشی سایت، انجام اقدام خاصی مجاز دانسته نمیشود. Firewall باید اطمینان دهند که تمام سعی و تلاشها برای انجام آن عمل ناموفق خواهد ماند.

– Firewall باید وقایع شبهه برانگیز را ثبت نماید.

– Firewall باید به مسئولان داخلی تمام اقدامات کراکینگ هشدار دهد.

– برخی از firewallها استفاده از آمار کاربردی را نیز امکان‌پذیر می‌سازند.

انواع Firewall

به منظور اجتناب از حذف داده توسط هد، بهتر است تا قبل از تلاش جـهت اسـتفاده از firewall، توپولـوژی firewall خـود و محدودیتـهای آن را بلـد باشـید. در قسـمت ذیـل در مـورد دو تـا از توپولوژیهای معروف firewall بحث و تبادل نظر نموده‌ایم. گرچه انواع زیـادی از firewall وجـود دارد. اما دو نوع زیر، انواع اصلی هستند. سایر firewallهـای دیـگر، از مفـاهیم یکجـوری اسـتفاده نموده و ... خوشبختانه ـ محدودیتهای یکجوری دارند.

۱) اتصال دو شبکه نامتشابه به دو گانه سرویس گیرنده.

اتصال دو شبکه دوگانه سرویس گیرنده، firewall ی است کـه : متشـکل از یـک سیسـتم مجـزا و واحد با حداقل دو رابط شبکه می‌باشد. این سیستم، بطور عادی، به گونه‌ای طراحی شده اسـت کـه چنین بسته‌های کوچکی، مستقیماً از یک شبکه (اینترنت) به شبکه دیگر (شبکه داخلی که میخواهید کراک کنید). فرستاده نمی شوند. دستگاههای روی اینترنت میتواننـد بـا ایـن اتصـال گفتـگو کننـد، همانگونه که دستگاههای موجود در شبکه داخلی ایـن کـار را می‌کننـد، امـا ترافیـک مسـتقیم بیـن شبکه‌ها , بلوکه شده است.

در مبحث firewallها، این موضوع مورد پذیرش است که شما باید به شبکه داخلی بعنوان یـک دژ ابتدایی نگاه کنید. باستیان های(bastions) این دژ نقاط بحرانیی هستند که به دفاع می‌پردازند.

در توپولوژی اتصال دو شبکه نامتشابه دو گانـه سـرویس گیرنـده، خـود میزبـان سـرویس گیرنـده دوگانه، [میزبان باستیان] نامیده می‌شود.

عیب اصلی اتصال یک شبکه دوگانه سرویس گیرنده، از دیـدگاه اسـتفاده کننـده شـبکه، و احتمـالاً کراکرهای ما، در حقیقت اینست که این اتصال, ترافیک مستقیم IP در هر دو مسیر را بلوکه می‌کند. هر برنامه اجرا شده در شبکه داخلی که مستلزم یک مسیر فرستاده شده به ماشینهای خارجی اسـت،

در چنین محیطی، عمل نخواهد کرد. سرویسهای موجود در شبکه داخلـی مسـیر فرسـتاده شـده‌ای باین مراجعین خارجی ندارند. برای رفع چنین مشکلاتی، اتصال دو شبکه دوگانه سرویس گیرنـده، برنامه‌هایی اجرا می‌کند که [PROXEIS] نامیده می‌شود. تا بسته‌های کوچک بکار رفته بین شبکه‌ها را به آدرس جدید بفرستد. یک proxy، گفتگوی بین مراجع و پردازشهای خدمات رسان در محیـط firewall شده را کنترل می‌کند.

بعلاوه، در ارتباط بطور مستقیم، مراجع و خدمات رسان، هر دو با proxy خود گفتگو میکننـد، کـه معمولاً در خود میزبان باستیان اجرا می‌شود. معمولاً، proxy برای استفاده کنندگان، جای هیچ شـک و شبهه‌ای نمی‌گذارد.

یک proxy در میزبان باستیان، اجازه نمی دهد تا سرویسهای مشخص زمام امور را آزادانه در دست گیرند. اکثر نرم افزارهای proxy بگونه‌ای طراحی شده‌ندکه قـادرند بـر اسـاس منبـع یـا آدرسـهای مقصد یا اتصال، فورواردینگ را مجاز دانسته یا آن را ممنـوع کننـد. همچنیـن نمـایندگان بـه تـأیید متقاضیانی نیاز دارند که از سری کردن، یا سیستمهای بر اساس کلمه رمز استفاده می کنند.

استفاده از نرم افزار proxy در میزبان باستیان، بدین معناست که مسـئولان firewall، جایگزینـهایی برای مراجعان شبکه‌بندی استاندارد، کابوسی در محیطهای نامتجانس (سایتهایی با سیستم عاملـهای مختلف، صحنه‌ها، PC، HP, DEC, IBM, SUN...) و مسئولیتی سنگین بـرای مسـئولان و اسـتفاده کنندگان، فراهم نموده‌اند.

۲-اتصال میزبان انتخاب شده

اتصال میزبان انتخاب شده، یک firewall است که شامل حداقل یک روتر و یک میزبان باستیان بـا تداخل شبکه مجزا می‌باشد. روتر بطور خاصی طراحی شده تا تمام ترافیک موجود در شبکه داخلی را بلوکه کند، یک چنین میزبان باستیان تنها ماشینی است که از خارج میرسد. بر عکـس. در اتصـال

دو شبکه دوگانه سرویس گیرنده. یک اتصال میزبان انتخاب شده الزاماً، تمام ترافیک را بـــه زور بـه میزبان باستیان تحمیل نمی‌کند. از طریق طراحی روتر نمایش، میتوان "دریچه‌هایی" در firewall بـــه طرف ماشینهای دیگر در شبکه داخلی که میخواهید وارد آن شوید، باز کرد.

میزبان باستیان داخل firewall میزبان انتخاب شـــده، از ســوی یـک شـبکه خـارجی توسـط روتـر نمایش، حمایت می‌شود. روتر، کلاً بگونه‌ای طراحی شده تا ایجاد ترافیک فقط از ســوی مسـیرهای مخصوصی در میزبان باستیان، مجاز باشد. بعلاوه ممکن است امکانی فراهم آورد تا ترافیک فقـط از سوی میزبانهای خارجی خاص باشد. مثلاُ، ممکن است روتــر، بـه ترافیـک خبرهـای شـبکه مـورد استفاده اجازه دهد تا به میزبان باستیان دست یابد، در صورتیکه ترافیک، از سوی تهیه کننـــده اخبـار سایت ایجاد می‌شود. این عبور،براحتی کراک می‌شود: این بـــه آدرس IP یـک ماشـین کنـترل از راه دور بستگی دارد، که میتوان آن را جعل کرد.

روتر بیشتر سایتها، به گونه‌ای طراحی شده که به هر اتصالی (یا مجموعه‌ای از اتصالات مجـاز) کـه از شبکه داخلی آغاز شده، اجازه عبور میدهد. این کار از طریـق بررســی بیتـهای SYN و ACK از بسته‌های کوچک TCP صورت میگیرد: آغاز بسته کـوچـک اتصـال، دارای هـر دو مجموعـه بیـت خواهد بود. در صورتیکه، آدرس منبع این بسته‌های کوچک، داخلی بوده ... یا به نظر برسد داخلـــی است : =بسته کوچک، اجازه عبور دارد. این به استفاده کننده در شبکه داخلی اجازه میدهد تا بـدون سرویس‌رسانی proxy با اینترنت رابطه برقرار کند.

همانگونه که ذکر شد، این طرح همچنین اجازه میدهـد تـا دریچـه‌ها در firewall بـرای ماشـینهای موجود در شبکه داخلی باز باشند. در این حالت شما می توانید، نه تنها میزبان باستیان. بلکه ماشـین داخلی عرضه کننده سرویس را کراک کنید. اکثر این ماشینها، امنیتشان کمتر از میزبان باستیان است.

سرویسهای جدید، مثل سرویسهای جدید web (وب)، دارای اشکالات و موارد غیرقـانونی هسـتند که در گروههای شبکه مورد استفاده با آنها مواجه خواهید شد و اینکه شـــما میتوانیـد بـرای کـراک کردن ماشینهای داخلی با دریچه‌های firewall، از آنها آزادانه استفاده کنید.

Sendmail،مثال خوبی از چگونگی کراک کردن به این روش اسـت. قـاعده کلـی اینسـت: «بـزرگ خوب است». هرچه بسته نرم افزار، بزرگتر باشد، شانس اینکه بتوانیم برخی از اشکالات مربوط بـه محافظت را پیدا کنیم بیشتر است... و تمام این بسته‌ها، امروزه بسیار عظیم هستند.

سرانجام، به خاطر داشته باشید که ،LOGها(صورت عملیاتها) عمدتاً در میزبان باستیان نیستند!

اکثر مسئولان،آنها را از یک ماشین داخلی جمع آوری نموده‌اند نه از اینترنت.

LOG ها(صورت عملیتها)در یک مرحله اتوماتیک، به طور منظم، اسکن می‌شود و اطلاعات شـک برانگیز را گزارش می‌کند.

۳) سایر توپولوژی های firewall

اتصال دوگانه سرویس گیرنده(dual-homed gateway)و میزبان نمایش داده شده(screened host) احتمالاً از همه معروفتر هستند. سایر ترکیبها، شامل روتر ساده نمایشی (نـــه میزبـان باسـتیان)، زیـر شبکه یا شـــبکه فرعـی نمـایش داده شـده (دوروتـر نمایشـی و یـک میزبـان باسـتیان) و همچنیـن راه حلهای فروش تجاری می‌باشند.

چه نرم افزاری باید مطالعه کنیم؟

سـه راه حـل نـرم افـزاری معـروف unix بـه مراجـع اجـازه میدهـد تـا وارد firewall شـده و بـا خدمات‌رسان از بیرون رابطه برقرار کنند: خدمات رسان CERN web درSOCKS, proxy mode

و

TIS fairewall tolkit

۱) خدمات رسان CERN web، نه تنها HTTP، بلکه سایر پروتکلهایی که مراجعین استفاده میکنند را کنترل نموده و از راه دور، ارتباط برقرار نموده و اطلاعات را به وضوح به مراجع منتقل می‌کند. X-based mosaic را میتوان برای پروکسی مد براحتی بوسیله مشخص نمودن متغیرهای محیط طراحی نمود.

۲) بسته socks(که آزادانه برای ftp بدون ذکر نام از ftp.nec.com در فایل /pub/secrurity/socks. Cstc/socks.cstc.4.2.tar.gz قابل دسترس است) شامل یک پروکسی سرور(proxy server) است که بر روی میزبان باستیان یک firewall برنامه اجرا می‌کند. این بسته شامل جایگزینی‌هایی برای فراخوانیهای IP socks استاندارد از قبیل connect(), getsockname(), bind(), accept(), listen() و select() می‌باشد. در بسته، کتابخانه‌ای وجود دارد که از آن میتوانید برای socks کردن تحقیقات کراک خود استفاده کنید.

۳) firewall toolkit

تولکیت شامل ابزارهای مفیدی برای کراک کردن firewall و proxy server می‌باشد.

از netacl میتوان در inetd.conf برای مخفی نگاه داشتن درخواستهای جدیددر برابرجدول دستیابی استفاده نمود . قبل از آنکه httpd,ftpd یا سایر daemonهای قابل inetd بوجود آیند. Mail در ناحیه chroot()ed باستیان برای پردازش (غالباً از طریق sendmail)، ذخیره خواهد شد.

Toolkit در ftp بدون ذکر نام از ftp.tis.com در فایل /pub/firewalls/toolkit/fwtk.tar.z موجود است. راه حل معروف pc firewall، برای MS-windows عبارت است از:

"PC socks pack" که بصورت ftp.nec.com در دسترس است و شامل فایل winsock. Dll می‌باشد.

اقدامات کراکینگ باید پیرامون ftpd باشد که معمولاً در میزبان باستیان واقع شده است. این یک کاربرد عظیم است که لزوماً ftp بدون ذکر نام و از سوی شبکه داخلی و تمام اشکالات و موارد غیرمجاز، مجاز شمرده می‌شوند. معمولاً، در میزبان باستیان. Ftpd،در ناحیه chroot()ed واقع شده و بعنوان استفاده کننده بدون هیچ امتیازی عمل می‌کند. اگر محافظت از سوی یک ماشین داخلی صورت گیرد، میتوانید از امتیازات شبکه داخلی مخصوص آن در host.equiv یا rhosts. برخوردار شوید. اگر ماشین داخلی، به ماشین سرویس دهنده اعتماد کند، دیگر هیچ مشکلی نخواهید داشت.

روش دیگر، که واقعاً نتیجه بخش است، اینست که بدنه (جسم) کامپیوتر خود را در امتداد مسیر بین شبکه و سرویس دهنده archie قرار دهید و firewall را دست بیندازید تا باور کند که شما سرویس دهنده archie هستید. برای اینکار به کمک یک مزاحم کامپیوتری که دوستتان هم باشد نیاز دارید.

به خاطر داشته باشید که اگر از حق ویژه ناظر (مدیر) در یک ماشین برخوردار باشید، میتوانید بسته‌های کوچک خود را از اتصال ۲۰ بفرستید، و این در یک محیط نمایشی میزبان به جز اینکه FTP در پروکسی مد استفاده می‌شود، فیلترهای دستیابی اجازه میدهند تا غالب ارتباطات از سوی هر میزبان خارجی برقرار شود، اگراتصال منبع، ۲۰ بوده واتصال مقصد بیش از ۱۰۲۳ باشد.

به خاطر داشته باشید که NCSA MOSAIC از چند پروتکل استفاده می‌کند. که اتصال آنها باهم فرق می‌کند، و چنانچه در firewall سرویس دهنده proxy web (پروکسی وب) کار نکند، به هر پروتکلی باید بطور جداگانه پرداخت، همان چیزی که اغلب مسئولان تنبل بندرت آن را انجام میدهند.

به TRAPS(تله) دقت کنید: مراجعین شبکه بندی مثل شبکه مخابراتی و ftp با بی رحمی، جای خود را به برنامه‌هایی میدهند که مثل هم اسمهای خود عمل میکنند، اما در اصل به یک مدیر،

email میزنند. یک کراکر، بوسیله فرمان کنترل می‌شود تا تـأخیرات شـبکه را شبیه‌سـازی نمـوده و پیامهای خطای تصادفی را بدین منظور بیان کند. این کراکر یکبار مچ مرا گرفت و اینکار بـه انـدازه کافی برای من جذاب بود . داستان ترسناک Bill cheseick را بخوانید: غروبی با Ber ferd، کـه در آن یک دیوانه، به دام می‌افتد، سختی میکشد و در حین سختی مطالعه می‌کند.

طبق معمول، ممکن است هر نوع تله‌ای گذاشته شده و از طریق یک ذن ـ کراکینگ صحیح، کشـف شود:

شما باید حس کنید که برخی کدها (یا برخی از اعمال نرم افزار)، «واقعی» نیستند. امیدوارم بـه مـن اعتماد نموده و قبل از اقدام در رابطه با این نوع کراک، آن را یاد بگیرید.

چگونه میتوان firewall ها را کراک کرد؟

در مورد سؤال بالا، یک سری پیشنهاداتی شده، اما برای آموختن نحوه کراک کردن firewall به شما باید حداقل ٦ درس کامل آموزشـی، آن هـم بـرای کـراک کـردن سـاده و نـه چنـدان مـهم، بـه آن اختصاص داد، و شما باید بلافاصله، آنها را بدست آورید. باید باور کنیـد کـه میتوانیـد آن را بـدون آنکه هیچ چیزی در مورد آن بدانید،کراک کنید. خوب، من به خـاطر شـما، بـه شـما می‌آمـوزم کـه چگونه آن را یاد بگیرید، نه اینکه چگونه آن را انجام دهید (تفاوت جالبی بین این دو وجود دارد):

ابتدا متن، سپس نرم افزار مذکور، در مورد متن، ابتدا با مقاله مارکوس رانوم شروع می‌کنیم.

«تفکر در مورد firewall»،از ftp.tis.com در فـایل /pub/ firewall/ firewall.psz و یـک تحقیـق archie برای مقاله جدیدتر انجام دهید.

شما میتوانید، آزادانه در وب بدنبال نسخه‌ها (مدلها)ی اولیه نرم افزار proxy بگردیـد. آن را مطالعـه کنید، مطالعه کنید و باز هم آن را مطالعه کنید. اقدامات کراکینگ در نسخه‌ها یا کپـی هـای شـما، و ماشینهای شما، قبل از مبادرت به اقدام جدی،اجباری هستند.

در صورتیکه نخواهید، فوراً وارد اینترنت شوید، وقتی احساس کردیـــد کـه بـرای انجـام کراکینـگ جدی، آمادگی لازم را دارید، باید لزوماً با BBS کوچک شروع به کار کنیـد کـه از نسـخه یـا مـدل firewall استفاده می‌کند که بخوبی آن را مطالعه کرده‌اید. خیلـــی زود میتوانیـد بـه میزبـان باسـتیان دست یابید، مخدوش نمودن کـامل خـود firewall، قبـل از ورود بـه شـبکه داخلـی را بـه خـاطر بسپارید.

اگر احساس کردید که آمادگی دارید، و همه چیز رو به راه است ، وتمـام تواناییـهای ذن کراکینـگ کامل هستند . . .چند لحظه برای خودتان وقت بگذارید... خودتان را با کمـــی مـارتینی ودکـا آمـاده کنید، نفس عمیقـی بکشـید و دوبـاره از سـر بگیریـد! بعـداً خواهیـد توانسـت شـانس خـود را در سیبرنتیک، امتحان کنید.

کراکینگ اینترنت : XINETD

[xinetd] جایگزینی توسعه یافته موجود برای سرویس اینترنت daemon inetd، فقط به یک ســری استفاده کنندگان خاص اجازه میدهد، تا به FTP یا Telnet(شـبکه مخـابراتی) دسـت یـابند، بـدون دستیابی به شبکه جهانی، Xinetd فقط قادر است تا سیســتم را بـا کنـترل دسـتیابی اولیـه بـه اکـثر سرویسهای سیستم و از طریق ثبت فعالیتها، از مزاحمت، محافظت کند، بطوریکه بتوانید ,ورودیهای غیرقانونی به سیستم را کشف و شناسایی کنید. با این وجود، در حالیکه اتصال بـه سـرویس, مجـاز دانسته شده، xinetd. خارج از تصویر است.

این نمیتواند در برابر برنامه سرویس دهنده‌ای محافظت بعمـل آورد، کـه از درون، دارای مشـکلات امنیتی است. بعنوان مثال، خدمات رسان با دست، چند سال قبل، یک عیب داشته، یعنی به شـــخص باهوش، اجازه می داده تا بخشی از حافظه آن را با نوشتن مطا لعــه روی آن پـاک کنـد. ایـن بـرای

دستیابی به خیلی از سیستم‌هاست. حتی قرار گرفتن دست در زیر کنـــترل xinetd نمیتوانـد کمکـی بکند.

با در نظر گرفتن سیستم حفاظت شده firewall بعنوان یک دیوار محافظ:

هر سرویسی که برای اتصالات بعدی، فراهم شده باشد. می‌تواند بعنوان در یا پنجره این دیوارها در نظر گرفته شود. تمام این درها هم مطمئـــن نیســتند و قفلـهای مطمئنـی هـم ندارنـد. هـرچـه ایـن روزنه‌های موجود بیشتر باشند. فرصتهای بیشتری هم برای ما وجود دارد.

Xinetd چه کاری انجام میدهد

Xinetd به همه اتصالات سرویس فراهم شده گوش فرا داده و تنها امکان برقراری آن ارتباطهایی را فراهم می‌کند که به آنها اجازه داده شده است.

- پذیرفتن ارتباطات فقط از سوی آدرسهای IP مشخص
- پذیرفتن ارتباطات فقط از سوی استفاده کننده‌های مجاز
- نپذیرفتن (رد کردن) ارتباطات خارج از ساعتهای مجاز
- ثبت کردن سرویس انتخاب شده هنگامیکه ارتباطات پذیرفته یا نپذیرفته میشوند، و ثبت اطلاعات ذیل:
- آدرس میزبان از راه دور
- ID استفاده کننده از استفاده کننده راه دور (در برخی موارد)
- زمان ورود و خروج
- تایپ پایانی

سرویسهایی برای کراک کردن و Complice های داخلی اتفاقی بدین ترتیب، سرویسهای آسان:

FTP TELNET LOGIN(rlogin) SHELL(remd) EXEC

بدین ترتیب، سرویسهای مشکلتر:

Mount TFT Finger NFS(سیستم فایل شبکه)

به خاطر داشته باشید که sendmail(SMTP)، از طریق پیش فرض، پیامی را از سوی متقاضی ارتباط می‌پذیرد، فرستنده چنین پیامی میتواند آن را ظاهر کند .حال ادعای هویت(و در خواست) شما پذیرفته می‌شود. بدین ترتیب می‌توانید با مبتکر پیام دوستی برقرار کنید. اکثر دریافت کنندگان در شبکه حفاظت شده، درخواست شما را پذیرفته و تمام اطلاعات حساس که برای کراک کردن سیستم لازم دارید، را برایتان می‌فرستند. یافتن اتفاقی complices ، اغلب اوقات، ساده و جذاب است.

بنابراین. بهترین متد، برای xinetd ورودی، تهیه نسخه یا مدل واقعی از سوی panos @cs.Colorado.edu ،تغییر فایلهای سیستم به منظور یافتن یک سری موارد غیرمجاز، و سپس توزیع آنها به خدمات رسانهای در وب می‌باشد. هر دفعه که یک مدیر جدید، اطلاعات مدل xinedt شما را به سیستم بزرگتری منتقل می‌کند، شما میتوانید راحت به سیستم محافظت شده دست یابید.

مخفی نگاهداشتن هویت خود، در شبکه‌ها، حائز اهمیت است (اگر هویت خود را اعلام نکنید آنها سریعاً شما را پیدا خواهند کرد). بهترین روش، بدست آوردن آدرس IP یک ایستگاه کاری قانونی در طول ساعات معمول روز می‌باشد. سپس، شب هنگام، وقتیکه ارتباط ایستگاه کاری، قطع می‌شود یک ند مختلف روی شبکه بگونه‌ای طراحی می‌شود که بتوان از آدرس IP جعلی استفاده نمود. برای هر کسی در شبکه، مسلم است که استفاده کننده مجاز، فعال است. اگر از این استراتژی پیروی کنید، با بی خیالی هرچه تمام تر، عمل کراک کردن را انجام خواهید داد. برای کراکر، با وجود عدم اطمینان به مبتدی مشغول به کار، جستجو کردن هنوز هم ادامه خواهد داشت.

خب، این بود درس امروز. اما همه خودآموزهای من روی اینترنت نیستند، شما درسهایی را که فراموش کرده‌اید به من mail بزنید. شاید شما کلک‌هایی بلد باشید که من هنوز کشف نکرده‌ام. من همان قبلی‌ها را میدانم اما اگر چیز جدیدی باشد اعتبار شما را خیلی زیاد می‌کند. حتی اگر اینطور هم نباشد من می‌فهمم که شما خیلی روی موضوع کار کرده‌اید. در آنصورت من درسهای باقیمانده را برای شما خواهم فرستاد. انتقادات و پیشنهادات شما در مورد چرندیاتی که من نوشتم، همیشه برای من خوش‌آمد خواهد بود.

E-mail +ORC an526164@anon.penet.fi