**** اخطار! ****

این جزوه تاییدیه استاد را ندارد و جزوه ای شخصی است.

این جزوه میتواند ناقص و یا اشتباه باشد.

تهیه این جزوه یک کار داوطلبانه بوده است

و حضور نداشتن شما در کلاس، مسئولیتی را برای بنده ایجاد نمیکند

امنیت سیستم ها و شبکه های کامپیوتری

کار غیراخلاقی در حیطه کامپیوتر و شبکه مانند دستبرد به اطلاعات، دسترسی غیرمجاز به داده ها، جارو کردن اطلاعات، گوش کردن به جریان اطلاعات

دو مورد اصلی در هک :: دانش فنی: برنامه نویسی / ابزار

دانش اولیه در سال های ۱۹۵۹ تا ۱۹۹۵ فقط متکی بر برنامه نویسی بود اما از سال ۱۹۹۵ به بعد بیشتر تمرکز بر روی ابزار بود.

در بحث امنیت موارد زیر مطرح میشود:

۱- **تعریف نقاط و اصطلاحات فنی**
۲- **مقدمه ای بر سیستم جمع اوری اطلاعات و مهندسی اجتماعی**
۳- **به کار گیری ابزار و راه حل های از پیش تعریف شده در به دست اوردن اطلاعات و دسترسی غیرمجاز به اطلاعات**
۴- **نحوه به کار گیری و ارتباط ویروس ها با سیستم های امن**
۵- **شناسایی سیستم عامل ها و نقاط آسیب پذیر آنها**
۶- **به دست آوردن اطلاعات از نقاط ناامن بانک های اطلاعاتی**
۷- **عملیات برهم زننده ساختارهای داده**
۸- **عملیات برهم زننده و پیدا کننده نقاط ضعف در ساختار مهندسی نرم افزار**
۹- **تفکیک عملیات روی شبکه های وایرلس و شبکه های کابلی**
۱۰- **امنیت فیزیکی و تجهیزات** Physical Security

تمامی موارد بالا میشود اصول تست و نفوذ.

مفهوم امنیت

امنیت، نفوذ و هک، همه کارهایی غیراخلاقی هستند که در جهت حفظ داده های امانت داده شده به ما سمت و سو میگیرند. این عملیات شامل دستبرد به شبکه ها و بانک های اطلاعاتی، از بین بردن آنها. دسترسی غیر مجاز به محتوای سایت ها و اطلاعات ذخیره شده در آنها. جارو کردن اطلاعات، گوش کردن به خط ارتباطی داده ها و دزدیدن پسورد ها و دزدیدن بسته های اطلاعاتی در راه شبکه که همگی مسائل غیراخلاقی در IT است، منجر به انجام مدیریت بهتر و در جهت رفع نقص موارد برنامه نویسی و شبکه ای میشود که به آن هک قانونمند یا اخلاقی میگویند.

****جلسه دوم****

مفاهیم مهم در امنیت

۱- **مفهوم تهدید:** تهدید شرایطی است یا حالتی است که میتواند امنیت را مختل کند. یعنی در اثر این شرایط و حالت عملی انجام میشود که امنیت را بهم میریزد. تهدید را سطح بندی میکنند و بر مبنای آن مشخص می کنند که چه خطراتی برای سیستم ها میتوانند داشته باشند.

۲- Exploite : Script یا Macro ای است که به کمک آن میتوانیم نقاط ضعف سیستم ها را به دست آوریم و در اثر این نقاط ضعف یا آسیب پذیر که درون برنامه وجود دارد به برنامه مورد نظر حمله کنیم.
معمولا در نرم افزارهای تحت وب یا تحت شبکه ایرادهای برنامه نویسی موجب Exploite میشود و دو دسته هستند.
Remote یا خارجی یا از راه دور و دیگری داخلی یا درون سیستمی. معمولا برنامه های موجود دارای ساختارهای غلط طراحی و ساختمان داده نادرست هستند. این روش نقاط آسیب پذیر آنها را از درون خود نرم افزار بروز میدهد.

۳- آسیب پذیری و نقاط آسیب پذیری: بعضی از سیستم ها نقاط ضعفشان طوری است که به کمک یکسری ابزار یا الگوریتم کمکی به برنامه مربوطه ضربه هایی را وارد میکند تا در مواقع ناخوشایند و غیر منتظره امنیت سیستم را به هم بزنند و یک رویداد خاص را انجام دهند. در این صورت میگوییم سیستم مورد نظر دارای نقاط آسیب پذیری است. مثل نقاط آسیب پذیری در بافر یا نوع سیستم عامل و سرویس پک های آن و یا باگ های کلی در سیستم ها و نرم افزارها.

۴- حمله یا Attack: حمله زمانی رخ میدهد که سیستم در اثر آسیب پذیری دچار مشکل شود و اتفاقات ناگواری برای آن رقم بخورد. معمولا حمله از تهدیدهای هوشمند شکل میگیرد.

۵- تعاریف تکنولوژی های هک: آندسته از الگوریتم ها که تحت عنوان خاصی یا تحت نام ابزار خاصی نقاط آسیب پذیر و نقاط مشکل ساز سیستم را هدف قرار میدهند یا از سیستم اطلاعاتی به دست می آورند را تکنولوژی هک میگویند.
مثلا: SQL Injection – Backdoor – Sniff
عملیاتی مانند ربایش پکت ها، جعل هویت، سرریزی بافر، جمع آوری پکت ها در هنگام عبور از مسیر، عملیات تزریق و عملیات سمی کردن پکت ها، همه از تکنولوژی های مربوط به هک میباشد.
Backdoor ها نیز از تکنولوژی های هک میباشد اما بعضی مواقع وجود آنها برای حمله نیست، مثل SQL Admin در SQL SERVER

سوال: ابزارهای هک چگونه و از چه ضعف هایی استفاده میکنند؟
چهارروش زیر دست هکر را برای حمله باز میگذارد
۱- نصب سیستم عامل ها به صورت تنظیمات پیش فرض
۲- عدم تست برنامه نویس ها روی برنامه نوشته شده خودشان و یا رفع نکردن باگ برنامه و همچنین عدم به کارگیری صحیح تکنولوژی ها
۳- استفاده از ماکروها و برنامه های کاربردی در پس زمینه سیستم هایی مثل word، Photoshop و غیره
۴- پیکربندی نادرست دسترسی های کاربردی در سیستم عامل ها و بانک های اطلاعاتی و role نویسی های غلط در سیستم های سرور

تذکر: در سیستم های هک عموما دودسته حمله وجود دارد: فعال و غیرفعال
حمله های فعال، تغییر حالت و تغییر وضعیت ایجاد میکنند و دگرگونی سیستم را به وجود می آورند. اما حملات Passive یا غیرفعال عمدتا روی جمع آوری Data عمل میکنند.

تذکر: در سازمان ها و شرکت ها معمولا دو دسته حمله وجود دارد: داخلی و خارجی
داخلی توسط کارمندان و یا مراجعین انجام میشود.
خارجی توسط رقبا، دشمنان و غیره

الگوریتم هک چیست؟

این الگوریتم شامل مراحل زیر است که منجر به یک نوع حمله میشود و احتمال خرابکاری نیز در آن میرود.

مرحله یک: شناسایی
در شناسایی غیر فعال جمع آوری اطلاعات بدون دانش انجام میشود. معمولا روش های مهندسی تکنولوژی مثل استراق سمع، به دست آوردن مسیر IP ها، Monitoring، شناسایی ترافیک از نوع غیرفعال است.

در نوع فعال از مهندسی اجتماعی استفاده میکنیم، مانند آشغال گردی، استفاده از متکدیان
در شناسایی فعال ریسک بالاتر است چون احتمال لو رفتن وجود دارد. معمولا در شناسایی فعال جمع آوری اطلاعات تعامل مستقیم با هدف دارد، اما شناسایی غیرفعال تعامل غیر مستقیم با هدف دارد.

مرحله دوم: اسکن
نرم افزارها و عملیات پوشش و ربات هایی برای پویش در سیستم ها استفاده میشود.
مثل IP Scanner، Port Scanner، Password Scanner، Sweepers
عملیات اسکن نقشه شبکه یا Network Mapper ها هم از نوع اسکن هستند.

مرحله سوم: ایجاد دسترسی
وقتی آسیب پذیری شناخته شد و توانستیم به مراحل بالاتر هک برسیم، یعنی پسوردها را به دست آوردیم یا User Control را تغییر دادیم یا Session را دزدیدیم یا پکت ها را بدزدیم. در این صورت مالک کامپیوتر طرف مقابل خواهیم شد، پس میتوانیم به آن دسترسی داشته باشیم.

مرحله چهارم: حفظ ارتباط
وقتی هکر دسترسی پیدا کرد زیرساخت ارتباط خود را در کامپیوتر هدف دنبال میکند و بنا میگذارد.

استفاده از Backdoor، Agent، rootkit و Zombie (با استفاده از سیستم به سیستم های دیگر حمله کردن) ، برای ذخیره سازی لاگ ها و مدیریت جمع آوری اطلاعات و ارائه گزارش های لحظه ای تغییرات از کامپیوتر هدف به حمله کننده برای حملات بعدی و گسترده.

مرحله پنجم: از بین بردن ردپا
چه هکر اخلاقی و چه هکر غیراخلاقی، زماتی که عملیات هک را انجام داده اند باید ردپای خود را از فایل های لاگ و همچنین سیستم پیام رسان IDS پاک کنند و همچنین مسیرهای مربوط به آنها را نیز از بین ببرند که به این کار استگانوگرافی میگویند.

Hacktivism چیست؟

مکتبی است در رشته IT که انگیزه های اجتماعی و سیاسی و فعالیت های دفاعی را در بر میگیرد. پیروان این مکتب دارای تفکرات تحلیلی و ایده آل گرایی در IT هستند و به واقعیت نزدیکترند.

این افراد معمولا در آژانس های دولتی و خصوصی اقدام به پیاده سازی بخش های دفاعی و امنیتی میکنند، این بخش ها را پدافند غیرعامل میگویند. آنها بیشتر افراد با اخلاقی هستند که منافع عمومی و مضار عمومی را در سیستم های IT تشخیص میدهد و به همین دلیل به آنها هکر اخلاقی میگویند.

**** هفته سوم ****

تفاوت هکر و Cracker:

هکر نفوذ غیرقانونی و دستیابی غیر مجاز به سیستم ها دارد، او دنبال هدف خاصی است و میداند که کارایی حمله و ابزار آن در چه سطحی است. اما Cracker یک هکر مجرم است که قصد اون نابودی است، بر هم زننده نظم در سیستم است و مبنای کار او جرم، جنایت علیه بشریت، دزدی و انهدام است. به این افراد Criminal Hacker گفته میشود.

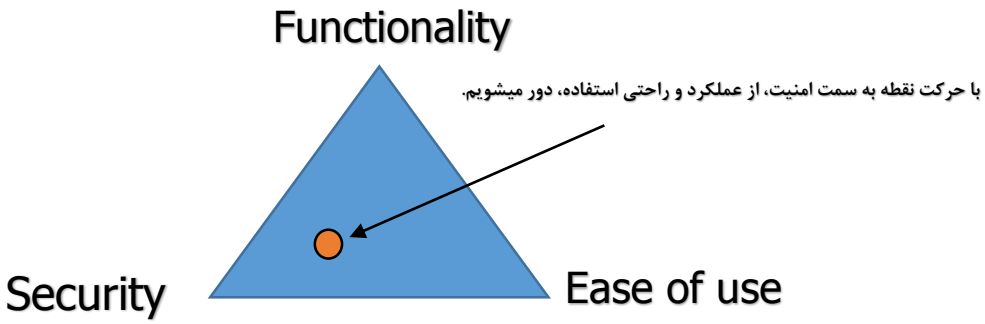
مثلث امنیت و تعریف آن:

امنیت شامل سه ضلع :

- **محرمانگی** Confidentiality
- **یکپارچگی** Integrity
- **در دسترس بودن** Availibility

این سه ضلع هر کدام دچار لغزش شود چهارچوب امنیت شکسته میشود. هکر معمولا این سه ضلع را مورد حمله قرار میدهد.

هکرها میتوانند با انواع حملات مختلف به پیکره این سه ضلع سیستم ها را دچار نابودی یا تست نابودی نمایند. بر مبنای سه ضلع امنیت مثلث دیگری به وجود می آید، که در این مثلث اگر به هر سمتی کشیده شویم. سمت های دیگر دچار لغزش می شود و این خود آسیب جدی را به پیکره امنیت وارد میکند.



در مثلث فوق Security یک ضلع را دارد، ولی باید بین آن و بقیه اجزا تعادل برقرار کرد.

برای یافتن تعادل به چند مورد زیر باید توجه کرد:

۱- **اهداف سازمان**
۲- **تعریف امنیت**
۳- **پیدا کردن تهدیدات**

تذکر: اگر امنیت زیاد مورد توجه قرار بگیرد، و زیاد به آن بها داده شود، خود یک تهدید است، چون نادیده گرفته میشود.

تذکر۲ : وقتی امنیت را مطالع میکنیم، بیشتر دنبال آسیب پذیری و نفوذ پذیری میگردیم. چون در نفوذ پذیری همه حالت های امنیتی تعریف میشود. سایت های زیر به شما کمک میکند تا میزان نفوذ پذیری و آسیب پذیری سیستم خود را پیدا کنید.

www.Nvd.nist.gov
www.Securitytracker.com

www.Microsoft.com/security
www.securiteam.com
www.packetstormsecurity.com
www.hackerstorm.com
www.hackerwatch.org
www.securityfocous.com
www.securitymagazine.com

در هنگام پیدا کردن نقاط ضـعف، باید یک سـازمان دهی وجود داشـته باشـد، این سـازمان دهی را سـر ممیزی امنیتی میگویند. برای سـرممیزی کردن یا بازرسـی کردن متخصـص امنیت، به سـازمان مورد نظر مراجعه میکند و شـش مرحله زیر را انجام میدهد، در آخرین مرحله گزارشـی به مشـتری داده میشود، در پروژه های مهم این گزارش که غالبا تعداد صفحات آن بیش از هزار است در یک فرمت چهل صفحه ای خلاصه میشود و به کمیته ای به نام، شام داده میشود. این کمیته زیر نظر شورای عالی امنیت ملی است.

این کمیته شامل موارد و دستگاه های زیر است:

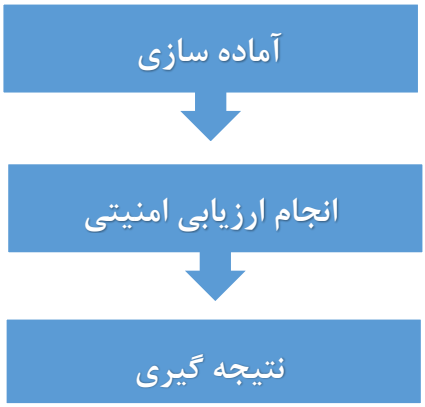
- **نماینده کمیسیون امنیت ملی مجلس**
- **نماینده وزارت ICT**
- **نماینده بخش امنیتی و اطلاعاتی وزارت اطلاعات**
- **نماینده گروه امنیت دانشگاه شریف یا امیرکبیر**
- **نماینده پدافند سایبری و جرائم رایانه ای**

مدیریت کمیته بر عهده نماینده پدافند غیرعامل است.

مراحل انجام ممیزی شامل موارد زیر است:

۱- **تماس با مشتری و بحث با او در مورد نیازهایی که در تست باید مورد توجه قرار گیرند.**
۲- **آماده سازی و امضای تعهدنامه منع افشاری اطلاعات (NDA) با مشتری**
۳- **سازمان دهی تیم هک و آماده سازی برنامه برای تست**
۴- **انجام تست**
۵- **تحلیل نتایج تست و آماده سازی گزارش**
۶- **ارائه گزارش به مشتری**

ارزیاب امنیت، مراحل زیر را برای تست و نفوذ انجام میدهد.



سوال: در تست و نفوذ معمولا چه نوع حملاتی انجام میشود؟

۱- **حمله از راه شبکه دور دست و یا از طریق سرور دور دست به صورت شبکه ای و یا تلفنی:** با این حمله ها میتوانیم، از طریق چند سرور یا چند کامپیوتر به سرور مورد نظر درخواست اتصال دهیم و با اطلاعاتی که از قبل جمع آوری کردیم ورود غیرمجاز کنیم.

۲- **حمله از طریق شبکه داخلی سرور:** از داخل شبکه یک سازمان، مثل کامپیوتر کارمندان یا مدیران، به آن سازمان حمله میکنیم.

۳- **سرقت تجهیزات:** در بعضی مواقع لپ تاپ ها نام کاربری و پسورد، اجزای شبکه، از یک شبکه ربوده میشود تا طراحان IT آن سازمان، مورد کنترل امنیتی قرار گیرند.

۴- **ورود فیزیکی یا حمله فیزیکی:** در این حالت که مرتبط با حالت سوم است، به محل کار کارکنان حمله میشود. نصب Rootkit ها و Logger ها یکی از عوامل مهم ورود فیزیکی است.

۵- **مهندسی اجتماعی یا حمله روانشناسی شده:** در این سیستم با برقراری ارتباط با طراحان و مدیران IT میتوانیم راز سازمان دهی آنها را روی شبکه و برنامه ها به دست آوریم. بعضی مواقع بهتر است که از جانب مدیران IT اطلاعات نادرست و غیرکاربردی در سطح جامعه منتشر شود.

انواع تست را نام ببرید و هر یک را تعریف کنید:

۱- **تست سیاه یا تست کور یا تست بدون دانش:** تست کننده هیچ گونه اطلاعاتی از مورد حمله ندارد. یکی از مهمترین تست های امنیت است. این تست، تستی پر هزینه و خارج از سازمان است. طولانی است و هکرهای زیادی را میطلبد.

۲- **تست با دانش یا تست سفید:** اطلاعات کامل از مورد حمله وجود دارد. معمولا حمله از متولیان IT صورت میگیرد و عموما جواب خوبی هم نمیدهد، چون هرکس کار خودش را ارزیابی میکند.

۳- **تست خاکستری یا تست با دانش جزئی:** این تست از درون سیستم و برخی از سطوح پایین IT انجام میشود.

گزارش هکر قانونمند یا ارزیاب یا ممیز شامل چه مواردی است؟

این مستند طبق استاندارد های مستند سازی است. قابل فهم و ردگیری است. شامل بخش های زیر است:

۱- صفحه عنوان

۲- فهرست

۳- مقدمه

۴- فصل های مربوط به کارهای انجام شده، در حال انجام و انجام نشده

۵- نتایج کارها و فصل های مربوط به آنها

۶- Solution

۷- Troubleshooting

۸- Proposal & maintenance

**** جلسه چهارم ****

امنیت و مهندسی اجتماعی

در بحث امنیت، در مهندسی اجتماعی پیش فرض هایی، وجود دارد که به کمک آن میتوانیم، ارزیابی ها و حمله ها را طبق یک اسلوب یا روش برنامه ریزی شده جلو ببریم.

مهمترین بحث در مهندسی اجتماعی، جمع آوری اطلاعات یا footprint است که نود درصد از کار امنیت را شامل میشود. در واقع footprint یک نقشه و یک ساختار است که از قبل برنامه ریزی میشود و شامل سیستم های فیزیکی و نرم افزاری هدف می باشد.

شروع به کار footprint از جستجو در سایت هایی مثل گوگل، گروه های یاهو، فیس بوک و غیره می باشد.

برای به دست آوردن اطلاعات افراد از سایت های زیر استفاده میکنیم:

groups.google.com
intellius.com
people.yahoo.com

در سایت گوگل با دستورات زیر میتوانیم از افراد و سازمان ها و همچنین افراد مرتبط با آنها و همچنین اطلاعات خاص در صفحات وب آن ها با خبر شویم:

Site: داخل سایت یا دامین را جستجو میکند، وب سایت یا دامنه مورد جستجو بعد از کولن بنویسید

Filetype: جستجو را فقط برای نوع خاصی از فایل انجام میدهد، باید نوع فایل را بعد از کولن بنویسید

Link: داخل hyperlink، یک کلمه را جستجو و صفحات لینک شده را شناسایی میکند

Cache: نسخه یک صفحه وب را مشخص میکند، آدرس سایت را باید بعد از کولن ذکر کنید

Intitle: به دنبال کلمه ای در داخل عنوان یک فایل میگردد

Inurl: تنها داخل آدرس یک فایل جستجو میکند، باید کلمه مورد جستجو را بعد از کولن ذکر کنید.

برای مثال هکر میتواند از دستور زیر برای شناسایی انواع مشخص آسیبپذیری های برنامه های وب استفاده

inurl: ["parameter="] with Filetype:[ext] and inurl:[scriptname]

در footprint این چنین اطلاعاتی باعث پیدا کردن اطلاعات ریزتر در سیستم های کامپیوتری میشود.

چگونگی جمع آوری اطلاعات

برای به دست آوردن اطلاعات، دو راه مهم وجود دارد.

۱- به دست آوردن اطلاعات اولیه

۲- شناسایی شبکه هدف

در شناسایی شبکه موارد زیر مورد استفاده قرار میگیرد:

- تعیین ماشین های فعال
- شناسایی پورت های باز
- شناسایی سیستم عامل ها
- شناسایی سرویس های روی پورت ها

- ترسیم نقشه شبکه

- سیستم عامل و نوع آن
- سیستم بافرینگ سیستم عامل
- کشینگ سیستم عامل
- قرارگیری سرویس ها روی سیستم عامل
- نحوه قرارگیری و دسترسی به سرویس بانک اطلاعاتی
- مدیریت وب و سرویس ها آن
- مدیریت فایل در سیستم عامل

در هنگام استفاده از ابزارهای footprint میتوانیم اطلاعات خاصی را به صورت طبقه بندی شده از foot ها بیرون بکشیم، این ابزارها شامل موارد زیر هستند:

- Whois
- NSlookup
- ARIN
- NEO Trace
- Visual Route Trace
- Smart Whois
- eMail Tracker Pro
- website watcher
- Google Earth
- GEO Spider
- HTTrack Web Coppier
- Email Spider

ابزاری مانند whois میتواند اطلاعاتی در رابطه با DNS، ثبت کننده و آدرس های خاص شبکه را به ما بدهد.

ممکن است در جمع آوری اطلاعات ابزاری مانند NSlookup به دست آید که اطلاعات کلی سیستم ها، DNS ها و IP ها را به ما بدهد. این ابزار جداول مربوط به DNS ها و IP مربوط به آن ها را به ما نشان میدهد.

معمولا در dnslookup جدول دامین ها و آی پی ها نمایش داده میشود. اما در whois و ARIN دامین های مربوط به سایت ها و اطلاعات اساسی سایت ها نمایش داده میشود، اگر سایتی دامنه ir. داشته باشد، به جای استفاده از whois.com از irnic استفاده میکنیم.

سایت ها و بانک های اطلاعاتی فوق به ما کمک میکند تا عملیات شناسایی سایت های اینترنتی را انجام دهیم و اطلاعات لازم را به دست آوریم.

تحلیل خروجی Whois

وقتی روی سایتی whois میگیریم اطلاعات آن به دست می آید:

۱- ID دامنه

۲- نام دامنه

۳- زمان ایجاد

۴- آخرین آپدیت

۵- زمان انقضا

۶- نام ثبت کننده یا اسپانسر

۷- وضعیت در حال فعالیت است یا خیر

۸- ID ثبت کننده

۹- نام ثبت کننده

۱۰- سازمان ثبت کننده

۱۱- آدرس ثابت کننده

۱۲- شهر و ایالت ثبت کننده

۱۳- تلفن ثبت کننده

۱۴- فکس و ایمیل ثبت کننده

۱۵- Admin ID

۱۶- نام ادمین

۱۷- کمپانی که ادمین را معرفی کرده است

۱۸- آدرس و تلفن و شهر کمپانی ادمین

۱۹- ایمیل ادمین

۲۰- شناسه تکنسین ها و یا کمپانی معرفی کننده آنها

۲۱- نام تکنسین

۲۲- آدرس کامل معرفی کننده تکنسین

۲۳- ایمیل کمپانی

۲۴- نام سرورهای تامین کننده DNS و تعداد و محل آنها

ابزارهایی که درون whois قرار دارند شامل موارد زیر است:

- Wikto Footprinting Tool
- Whois Lookup
- Smart whois
- Active whois
- Lan whois
- Country Whois
- WhereisIP
- Ip2country
- CallerIP
- Web Data Extractor

پیدا کردن آدرس ها در شبکه

با استفاده از دستور عمل های مربوط به مسیریابی میتوانیم آدرس Gateway ها و همچنین آدرس IP ها و همین طور Subnet Mask را پیدا کنیم. این عملیات با دستور Trace انجام میشود. در سیستم عامل ویندوز و لینوکس دستورهای زیر به صورت پیش فرض در سیستم عامل وجود دارد. Traceroute یا Tracert این دستور عمل ها مسیر عبور بسته و همچنین گذر از مسیریاب ها در شبکه را مشخص میکنند که عموما برای استفاده بهتر میتوانیم از نرم افزارهای Visual Route یا NeoTrace استفاده کنیم. این دستور عمل ها به صورت گرافیکی میتواند محل قرار گیری کامپیوترها و محل قرار گیری فیزیکی روترها و سوییچ ها را نشان دهد. IP های درونی ماشین ها مثل IP های ماشین های مجازی و IP های سرورهای مجازی و پورت های آنها را نیز مشخص کنند.

معمولا از DNS چه اطلاعاتی به دست می آید؟

رکوردهایی که از DNS بیرون می آید و قابل تفسیر میباشد شامل موارد ذیل است:

۱- A: تبدیل نام به آدرس IP

۲- SOA: مشخص کننده سرور DNS مسئول برای اطلاعات دامین

۳- CNAME: اسامی اضافی یا مستعار برای رکوردها میدهد.

۴- MX: مشخص کننده سرور ایمیل

۵- SRV: سرویس هایی از قبیل Directory Server را مشخص میکند

۶- PTR: تبدیل آدرس های IP به اسم

۷- NS: دیگر Name Server های شبکه را مشخص میکند

TraceRoute میتواند بسته های ICMP را نیز در مسیر حرکت دهد و از روی آنها روترها را از شمارش TTL شناسایی کند. اگر فایروال TraceRoute را ببیند، به هکر یا اخطار میدهد یا TTL را به صورت نامشخص تبدیل میکند. در ابزارهای جدیدتر Trace میتوان فایروال را نیز دور زد. مانند Spade

برای پیدا کردن یک آدرس مثل دامین یاهو میتوانیم دستور زیر را بدهیم. این دستور باعث میشود به ترتیب اول آدرس Virtual Machine آدرس کامپیوتر شما، آدرس کامپیوتر ISP و بعد طبق مسیر آدرس کامپیوتر مقصد اعلام شود. اطلاعات موجود در این دستور آدرس فیزیکی سرورها و روترها را نیز مشخص میکند.

ابزارهای مهمی که در زمینه Trace استفاده میشوند موارد زیر هستند:

- 3D Traceroute
- NeoTrace
- VisualRoute Trace
- Path Analyzer Pro
- Maltego

چگونگی Trace کردن ایمیل ها:

ایمیل ها را میتوان با ارسال پیام و پیوست یک نامه آلوده به ویروس یا Rootkit مورد دستیابی قرار داد، بدین صورت که در داخل ایمیل

ارسالی برای فرد گیرنده یک لینک قرار دهیم که این لینک یا یک تصویر باشد یا یک فایل مستند باشد و یا آدرس یک سایت. در آن صورت با باز کردن این لینک Log های کامپیوتر فرد مورد حمله برای ارسال کننده فرستاده میشود.

ابزارهای Email Tracking شامل موارد زیر هستند:
eMail tracker Pro ، VisualRoute Mail Tracker

نقش Spider در ایمیل و وب چیست؟
اسپایدر ها صفحات وب را میخوانند و هر آنچه که آدرس ایمیل باشد و در آن کلمه @ باشد جمع آوری میکنند. آنها میتوانند آدرس های ایمیل را از صفحه وب شناسایی کنند و آنها را در بانک قرار دهند. در این ابزار رباتی وجود دارد که کارش خواندن لیست ایمیل ها و فهرست مربوط به آنهاست.

چگونه الگوریتم FootPrint را اجرا کنیم

۱- پیدا کردن آدرس های داخلی و خارجی شرکت
۲- انجام جستجوی Whois برای جزئیات شخصی
۳- استخراج اطلاعات DNS
۴- جستجو به دنبال اسامی در وب سایت
۵- استخراج آرشیو وب سایت
۶- جستجو از طریق گوگل برای اخبار مربوط به شرکت
۷- استفاده از People Search برای یافتن اطلاعات شخصی پرسنل
۸- یافتن مکان فیزیکی وب سرور با استفاده از ابزار NeoTracer
۹- تحلیل جزئیات زیرساخت شرکت با استفاده از فرصت های شغلی
۱۰- ردیابی ایمیل با استفاده از Readnotify.com

تمرین شب عید: ده مرحله فوق را روی یک سیستم عامل که روی VirtualBox قرار گرفته است نصب کنید و اجرا کنید.

جلسه پنجم

مهندسی اجتماعی بر مبنای انسان شامل چند دسته زیر است:

۱- خود را جای شخص دیگری جا زدن یا در نقاب فرد دیگری پنهان شدن: در این صورت هکر وانمود میکند، کارمند یا کاربر قانونی یک سیستم است و در سیستم های کنترلی و حفاظتی، آن سیستم ورود پیدا میکند و در آن سازمان، جا برای کار پیدا خواهد کرد

۲- خود را به عنوان شخص مهم وانمود کردن: هکر میتواند در یک سازمان، پایین دستی، وارد شود و خود را جای مدیر ارشد قرار دهد و به کارمندان پایین دست دستور عمل های خاصی را انجام دهد

۳- استفاده از شخص سوم: در این روش، هکر خودش را از سازمان خاصی معرفی میکند و میگوید مجوز ورود به سازمان را دارد. این حمله یکی از موثر ترین حمله های انسانی است.

۴- تماس با پشتیبان فنی: معمولا هکر ها با Help Desk یا به جای او عملیات خود را انجام میدهند.

۵- ایستادن کنار کاربر: در این نوع حمله ها تحت عنوان دوست، مدیر بالایی، بازرس از کنار کاربر، میتواند اطلاعات محرمانه را بیرون بکشد.

۶- آشغال گردی dumpster Diving: در این حالت که یکی از تخصص های IT است، افراد متخصص آشغال ها را از کاغذ ها، دست نوشته ها و یا اطلاعات محرمانه دیگر جستجو میکنند. در حال حاضر افرادی که اطلاعات محرمانه را روی کاغذ ها قرار میدهند، موقع دور اندازی آنها، از کاغذ پودر کن استفاده میکنند. هکر میتواند، کاغذ های رشته شده را بر حسب سنگینی و سبکی و نوع برش و نوع خط نوشته شده روی آن در کنار هم بچیند و باز گرداند.

مهندسی اجتماعی بر مبنای کامپیوتر:

در این حالت، سه عملیات مختلف ایجاد میشود:

۱- ضمیمه های ایمیل که شامل فایل هایی است که میتواند توانایی اجرا ماکروها را داشته باشد

۲- وب سایت های جعلی: وب سایت هایی است که جایگزین وب سایت اصلی میشود با همان رنگ و نگاره

۳- پنجره ها یا منوی های popup: این پنجره ها دارای اسکریپ هایی هستند که ممکن است، اطلاعات خاصی را از سیستم شما جمع آوری کند

تذکر۱: اگر هیچ یک از این حملات کارساز نبود، از حملات درونی استفاده میکنیم. مثلا نفوذ به کارمندان سازمان که با استفاده از تطمیع، تحدید تقریب و ترغیب انجام میشود. حملات دیگری نیز مطرح میشود که به آنها حملات phishing گویند. این حملات، جا زدن کارت اعتباری، جا زدن وب سایت بانک و یا موسسه را شامل میشود.

تذکر۲: در ضمیمه های ایمیل، کد های مخرب یا ابزارهای خودکاری وجود دارد که میتواند، روی کامپیوتر طرف نصب شود و پسورد ها را از روی بانک اطلاعاتی موقت، مرورگرها و Temporary ها به دست آورد.

تذکر۳: دزدی یا جعل کردن آدرس های URL (url obfuscation) : در این صورت، یک آدرس url مخفی یا غیر قانونی، نوشته میشود و در آن یک کلمه یا نام یک سایت معتبر نیز قرار میگیرد. کاربر چون توجهی به آدرس بار نمیکند با زدن این آدرس، به سایت جعلی مراجعه میکند.

تذکر۴: برای پیشگیری از مهندسی اجتماعی، معمولا باید بخش ها را از یکدیگر جدا کرد. همچنین آموزش های فراگیر در جهت استانداردهای امنیت در رده های کاری مختلف ارائه داد. این کار با کلاس های ضمن خدمت و مسائل فرهنگی مثل خبرنامه ها، هفته نامه، روزنامه ها و بخش نامه های داخلی سازمان انجام میشود. جا به جا کردن افراد، در بخش های IT و استفاده از مستندات آنها بسیار مهم است.

اسکن و مدل های آن: در عملیات هک یکی از مهمترین قسمت ها اسکن میباشد. اسکن به سه قسم میباشد:

۱- اسکن پورت

۲- اسکن شبکه

۳- اسکن نقاط آسیب پذیر

در مورد اول، پورت ها و سرویس ها مورد بررسی قرار میگیرند. در دومی آدرس های IP و شبکه، در قسمت سوم، سیستم عامل، نقاط ضعف سیستم برنامه نویسی، مهندسی نرم افزار، معماری نرم افزار، اشکالات فنی فایروال، اشکالات نرم افزاری سوییچ و غیره بررسی میشود.

تذکر ۱: اسکن پورت روی مجموعه خانواده TCP/IP انجام میشود، برای دستیابی به پورت ها،در سیستم عامل ویندوز، مسیر زیر را بروید

System32/drivers/etc/service

تذکر ۲: وقتی اسکن انجام میدهید، فایروال و IDS الگوریتم اسکن شما را شناسایی میکند و در مقابل اسکن می ایستد.

متدولوژی اسکن:
برای انجام این فرایند، پس از جمع آوری همه اطلاعات، مراحل زیر یک به یک به ترتیب انجام میشود

۱- بررسی سیستم های فعال

۲- بررسی پورت های باز

۳- شناسایی سیستم ها

۴- شناسایی سیستم عامل ها

۵- پیدا کردن نقاط آسیب پذیری

۶- ترسیم نقشه، از سیستم های آسیب پذیر

۷- آماده سازی پراکسی ها برای عبور از نقاط خاص و یا رد گم کردن آی پی ها

یکی از مهمترین عملیات اسکن ping sweep می باشد که روی بازه ای از آدرس های آی.پی عمل میکند و اسکن ICMP انجام میشود. در این صورت در کنار این عمل میتوانیم روی بازه های آی.پی، عملیات موازی دیگری نیز انجام دهیم. Ping sweep همزمان روی چند دستگاه کار میکند و به کمک فایروال و IDS شناسایی میشود.

تذکر: IDS یعنی شناسایی کننده حمله و نفوذ و مزاحمت، IPS مبارزه کننده یا محافظت کننده از نفوذ و مزاحمت

برای پینگ و اسکن IP ها ابزارهای دیگری نیز وجود دارد، مثل ws ping pro و یا Angry IP Scanner، Friendly IP Scanner، Friendly ping که عموما اسکن ICMP انجام میدهند.

چگونگی تشخیص، ping sweep ها از طریق، proxy server ها، Firewall ها و IPS و IDS ها انجام میشوند.

معمولا وقتی، به ping sweep پاسخ داده میشود، یعنی ممانعت کننده ای در کار نیست. اگر ماشینی فعال باشد ولی ping sweep دچار مشکل timeout شود و پاسخ ندهد یعنی باید نوع اسکن را عوض کرد. برای این منظور، میتوانیم اسکن پورت ها و شناسایی سرویس ها را نیز طبق یک استاندارد اسکن دیگری انجام دهیم.

سوال: چگونه با اسکن پورت و سرویس های شبکه مقابله کنیم:

۱- معماری امنیتی صحیح (یعنی جایدهی وسایلی مثل IDS، IPS، Firewall، Server و بقیه اجزا طبق معماری لایه ای شبکه معماری امنیتی چیده شود)

۲- امکان تست فایروال به صورت مطلق و تست فایروال به صورت، کلی روی معماری تعریف شده

۳- تعریف بسته ها و هدرهای بسته ها جهت کنترل آنها در فایروال

۴- به کار گیری شبکه ای از IDS ها یا NIDS برای تشخیص نفوذ روی سیستم عامل

۵- بستن پورت های ناهنجار و غیر متعارف

۶- پیاده سازی سیستم های ISMS برای مدیریت امنیت کارکنان

دستور Nmap و سوییچ های آن:

Nmap یکی از نرم افزارهای قوی در یونیکس است که الگوریتم های زیر را در اسکن، شبکه، پورت و سیستم عامل به صورت زیر دارد:

۱- اسکن TCP Connection: این اسکن ارتباط TCP و اتصال گرا را اسکن میکند

۲- Xmass یا اسکن درخت کریسمس: این سرویس بسته هایی را به صورت درختی، مالتی لول به سمت هدف ارسال میکند که در آن ها Flag های عملیاتی بسته با یک مقدار خاص پر شده اند

۳- Syn Scan : این نوع اسکن، یک بسته Syn را ارسال میکند و معمولا روی نشست های TCP به صورت نیمه باز عمل میکند و پاسخ Ack را از TCP میگیرد.

۴- Null Scan: اسکن چراغ خاموش: این یک اسکن پیشرفته است که Flag های آن هیچ تغییری نمیکنند و روی فایروال به صورت چراغ خاموش عمل میکند

۵- Windows Scan: این روش روی ویندوز عمل میکند و موقع پاسخ گرفتن پورت های باز را نشان میدهد

۶- ACK Scan: این سیستم روی یونیکس کار میکند و اطلاعات فایروال را بیرون میکشد.

پارامترهای Nmap، پارامترهایی که با s شروع میشود:

-sS	TCP SYN scan
-sT	TCP connect() scan
-sF **-sX** **-sN**	Stealth FIN Xmas Tree Null scan modes
-sP	Ping scanning
-sV	Version detection
-sU	UDP scans
-sO	IP protocol scans
-sI	Idlescan
-sA	ACK scan
-sW	Window scan
-sR	RPC scan
-sL	List scan
-b	FTP bounce attack

More parameters and info: www.linuxcommand.org/man_pages/nmap1.html

جلسه ششم

عملیات اسکنرها و بررسی الگوریتم های آنها:

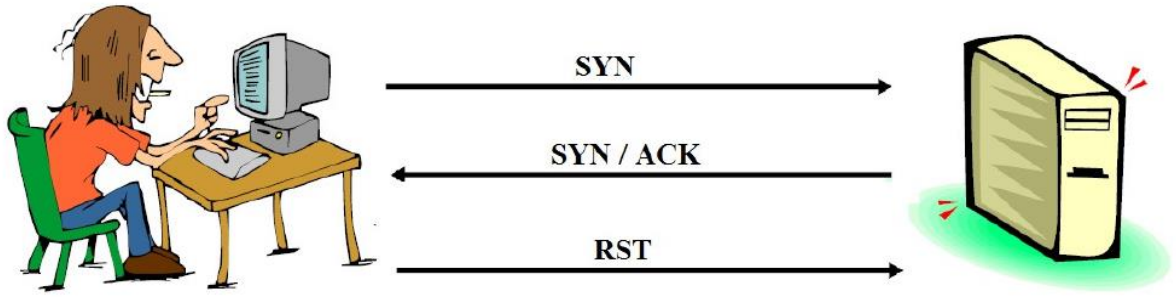
اسکنرها میتوانند، با ترکیبی از خدمات مختلف اسکن، عمل اسکن را روی پورت ها، مثلا نرم افزار HPING 2، این نرم افزار هم Trace را انجام میدهد، هم میتواند یک بسته NULL روی نشست TCP ارسال کند و هم اینکه روی پورت های مختلف و با ارسال پیام های از نوع SYN از شناسایی IDS ها و فایروال ها عبور کند. مثلا دستور زیر عمل ارسال SYN را با کمک یک IP جعلی به پورت ۸۱ انجام میدهد:

Hping 2-a 10.0.0.5 –s –p 81 10.0.0.25

HPing یکی از نرم افزارهایی است که معمولا از فایروال عبور میکند

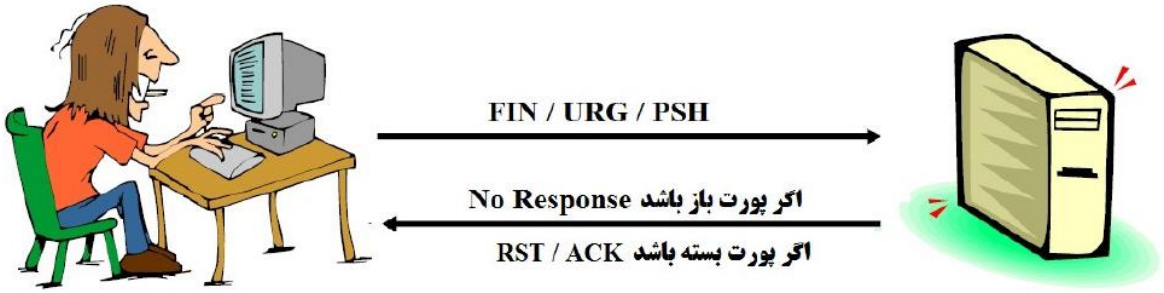
الگوریتم های مختلف اسکن:

الگوریتم اسکن SYN: در این الگوریتم که به عنوان اسکن نیمه باز نیز معروف است، از دست تکانی سه مرحله ای استفاده میکنیم، در این روش کامپیوتر حمله کننده به مقصد یک SYN میفرستد، سپس هدف پاسخ ACK به آن میدهد و بعد حمله کننده پاسخ RST به آن میدهد. این روش یک شبیه سازی کلی از ارتباط های معمولی شبکه است و IDS آنرا شناسایی نمیکند. در این روش وقتی ACK برمیگردد ارتباط کامل میشود و مشخص است که پورت آماده دریافت یک سوکت میشود.



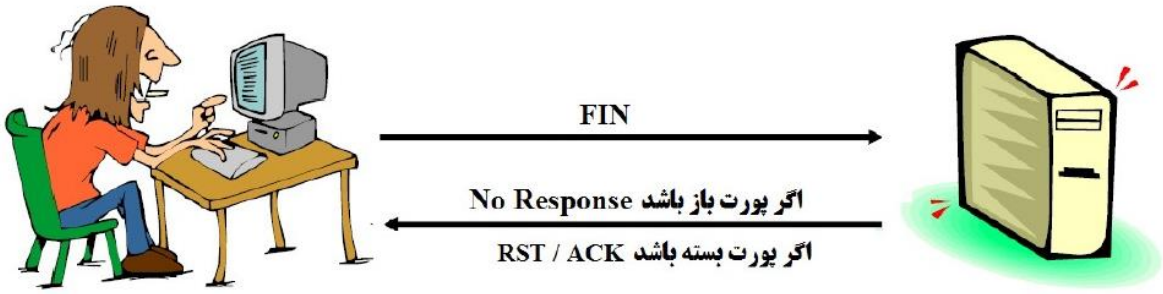
اسکنXMAS

این روش در سیستم عامل یونیکس کار میکند و بسته ای را روی نشست TCP با فلگ های FIN/URG/PSH ارسال میکند. اگر پورت باز باشد، پاسخی نیست، اگر پورت بسته باشد، ACK یا RST برمیگردد.



الگوریتم Fin :

این الگوریتم شبیه xmas است و فقط flag بسته ای که روی آن set شده است ارسال می شود.



الگوریتم Null Scan نیز مانند XMAS است، ولی در بسته ارسالی، هیچ فلگی ست نمیشود، یا فلگ ها با Null، ست میشود.

الگوریتم IDLE Scan: این الگوریتم از آدرس جعلی استفاده میکند و بسته هایش را با Flag SYN بار میکند. در این روش IP Header مونیتور میشود و شماره سریال آن کنترل میگردد.

به کارگیری فلگ ها در ارتباط دست تکانی سه مرحله ای

از آنجائیکه در شبکه طرف اول پیام را میفرستد و طرف دوم پاسخ دریافت صحیح پیام را میدهد، طرف اول نیز به آن یک پاسخ صحیح را میدهد. در این صورت اگر در ارتباطات شبکه ای بیت SYN یا بیت ACK دچار مشکل شوند در آن صورت ارتباط کامل نخواهد شد. کل ارتباطات شبکه ای از FLAG های زیر استفاده میکنند.

SYN (Synchronize): ارتباط را بین سیستم‌ها شروع می‌کند.

ACK (Acknowledge): ارتباط را بین سیستم‌ها برقرار می‌سازد.

PSH (Push): سیستم، داده بافر شده را فروارد می‌کند.

URG (Urgent): داده‌های داخل بسته، باید سریعتر پردازش شوند.

FIN (Finish): دیگر انتقال انجام نگیرد.

RST (Reset): ارتباط را دوباره راه‌اندازی می‌کند.

تمرین: با توجه به الگوریتم های اسکن بیان شده بگویید در هر الگوریتم به ترتیب چه فلگ هایی تغییر پیدا میکند.

ابزار مهم IPEye : این ابزار از تمام، الگوریتم های اسکن بیان شده استفاده میکند، در خط فرمان لینوکس کار میکند و کمترین مقدار بافر را استفاده میکند.

ابزار IPSec Scan: این ابزار به صورت نیمه باز یا نیمه دوطرفه یا HalfConnection آدرس های IP را جستجو میکند و IPSec را روی سیستم ها شناسایی میکند.

ابزار War-Dialing: این ابزارها برای حمله به سرورهایی است که به مودم متصلند. این سیستم از رمزگذاری ساده ای برخوردار است چون پردازش رمز سنگین میشود و مودم نمیتواند آنرا مبادله کند، از رمز سبک و کلمه کلید کوتاه استفاده می کنند به همین منظور ابزار War-Dialing میتواند به صورت Remote Access به سرور مورد نظر حمله کند.

این ابزار ها، دسترسی مستقیم به سرور پیدا میکنند و حمله از طریق آنها بسیار ثمر بخش است.

Dialer ها، شامل ابزارهای زیر میباشند:

Telesweep , THC-Scan, ModemScan, ToneLoc, Phonesweep, War dialer

تکنیک های Banner Grabbing و شناسایی سیستم عامل:
در سیستم عامل ها، مهمترین بخش، Cache یا بافر سیستم عامل است، فرایند banner Grabbing باعث میشود به دو صورت اکتیو و یا پسیو، Cache دچار حمله شود. در حالت اکتیو ارسال داده ها به سوی سیستم به طوری است که پاسخ داده های دریافت شده نشان میدهد سیستم عامل از Cache یا Buffer استفاده کرده است یا خیر. اگر پاسخ با ابزار مربوطه در بانک اطلاعاتی آنها یکی باشد، یعنی سیستم عامل Active Cache / Active Buffer داشته است.

در حالت Passive ترافیک شبکه و همچنین عملیات Sniffing باعث میشود تا Cache سیستم عامل درگیر شود. حالت Passive توسط فایروال یا IDS شناسایی نمیشود. در سیستم عامل یونیکس از دستور pof استفاده میشود.

ابزار زیر Cache سیستم عامل را قلقلک میدهند.

Bidiblah
Qualys web-based Scanner (www.qualys.com/eccouncil)
SAINT
ISS Security Scanner
Nessus (for Softwares)

برای اسکن آسیب پذیری سیستم عامل ها، از نرم افزارهای خاصی مانند Nessus استفاده میکنیم. این نرم افزار در دو مود کلاینت و سرور کار میکند. در مود کلاینت روی کامپیوتر کاربر یا به صورت مهندسی اجتماعی و یا به صورت نفوذ از طریق ایمیل نصب میشود و از اطلاعات کاربر روی کامپیوترش و صفحه تصویر کامپیوترش Image میگیرد و به سرور آن میفرستد، در حالت سرور، در کامپیوتر حمله کننده این برنامه نصب است و فایل های کم حجمی که روی نشست TCP برای حمله کننده فرستاده میشود را ذخیره میکند. این فایل معمولا بین ۲۰ تا ۵۰ کیلو بایت است. Nessus از ضعف بافر و از حالت Passive Stack استفاده میکند.

در Nessus عمدتا ضعف های عملیاتی سیستم عامل، خط شبکه، مدیریت DNS و همچنین کارکرد Buffer و Cache در سیستم عامل تعریف میشود.

تذکر: بعضی از ورژن های نرم افزارهای نقاط آسیب پذیر از مسائل آسیب پذیری سیستم عامل ها و شبکه ها دیاگرام نیز طراحی میکنند. علاوه بر اینکه از شبکه نیز دیاگرام تعریف میکنند. این نرم افزارها شامل موارد زیر است:

FriendlyPinger
LANsurveyor
Ipsonar
LANState
Insightix Visibility (www.insightix.com)
IPCheck Server Monitor (www.paessler.com)
PRTG Traffic Grapher

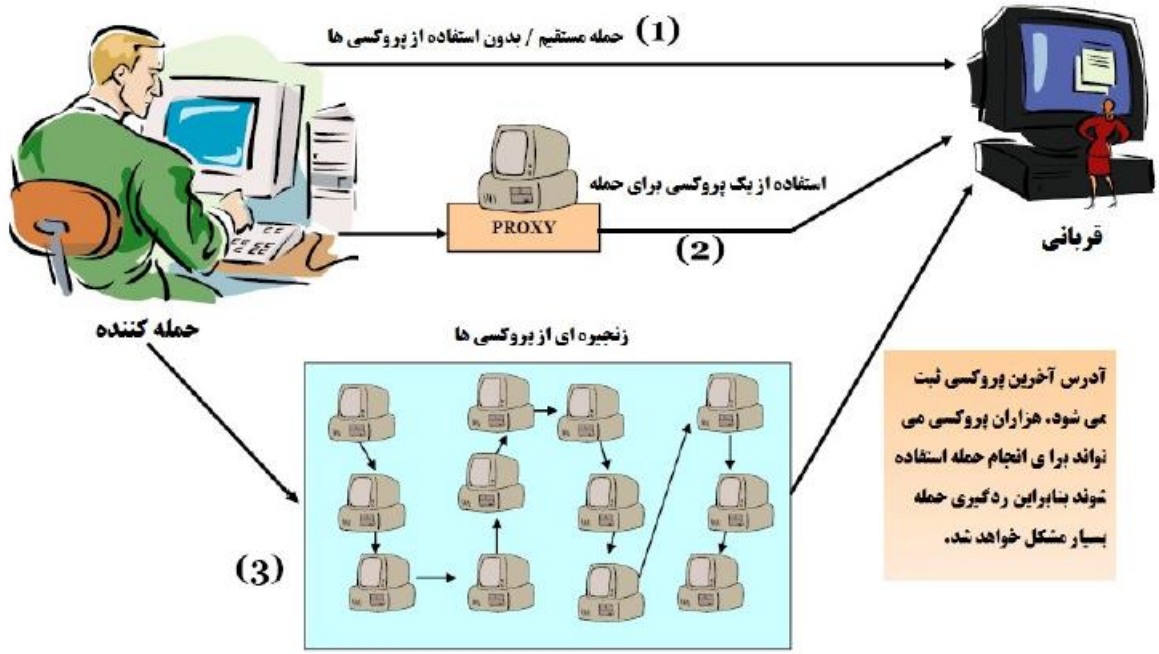
عملکرد پراکسی ها و حمله از طریق آنها
پراکسی یک سرور یا یک سرویس دهنده است که سه نوع عمل در آن تعریف شده است.

۱- پراکسی به عنوان Cache Server، به طوری که اولویت بندی درخواست ها را انجام میدهد.

۲- پراکسی به عنوان DNS Forwarder که میتواند هم به عنوان فیلتر استفاده شود، هم DNS های موجود را سریع تر برای کاربر ارسال نماید.

۳- پراکسی میتواند یک عامل بازدارنده در شبکه باشد و درخواست های کاربر را از طریق یک کانال ارتباطی خاص به اینترنت وصل کند.

هکرها میتوانند از این خاصیت پراکسی ها، استفاده کنند و در شبکه چندین پراکسی را در آن واحد به هم متصل کنند و از طریق آن یک حمله مبتنی بر پراکسی را سازمان دهی کنند. شکل زیر نشان دهند این حمله می باشد.



در این جور حمله ها شخص حمله کننده زمان های اتصال پراکسی ها و همچنین زمان های که آن ها در شبکه سپری میکنند و کاربرانش را نشان میدهند.

نرم افزارهای زیر از دسته نرم افزارهای حمله پراکسی میباشد.

Socks Chain
Proxy Workbench
Proxy Manager
Super Proxy Helper
Multi Proxy
TOR Proxy Chaining Software
Proxy Finder
Proxy Bag
Automated Proxy Leecher

چگونه در اینترنت خود را ناشناس کنیم:

در اینترنت میتوانیم از ابزارهای تغییر IP، تغییر آدرس MAC و Tunneling استفاده کنیم.
نکته: اگر تغییر IP روی نشست TCP داشته باشیم، دچار مشکل خواهیم شد، چون نشست TCP ارتباط اتصال گرا است و تغییر IP باعث میشود که این اتصال قطع شود و با IP جدید مجددا برقرار شود. معمولا تغییر IP باعث میشود تا به کمک Tunnel ارتباط را حفظ کنیم و بعد IP را عوض کنیم، نرم افزارهای زیر برای تغییر IP استفاده میشود.

StealthSurfer / Browzar / Torpak Browser / GetAnonymous / IP Privacy / Anonymity 4 Proxy / Psiphon / AnalogX Proxy / NetProxy / Proxy + / ProxySwitcher Lite / JAP / Proxomitron

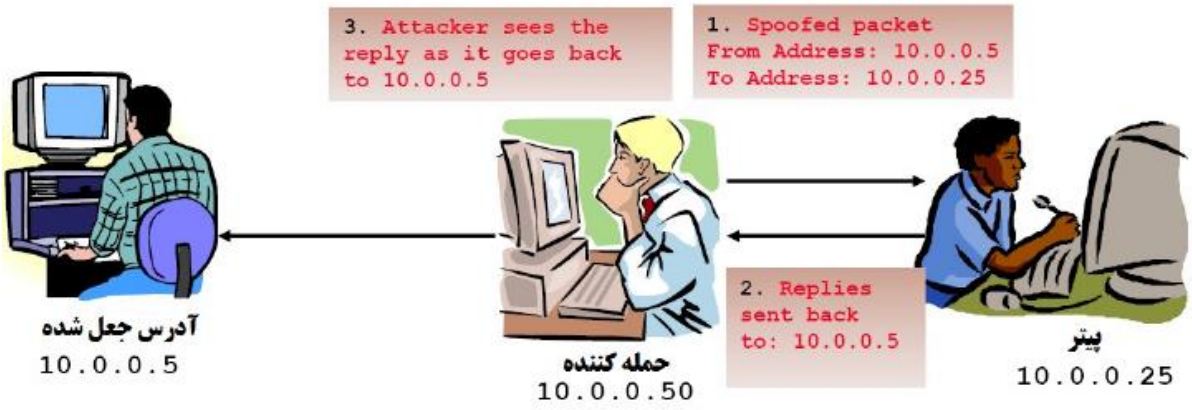
برای Tunneling میتوانید از ابزار مدل Server / Client استفاده کنید. این روش باعث میشود تا یک ارتباط مجازی دو طرفه مانند VPN شکل بگیرد. مثلا میتوانیم در روی ویندوز سرور از دستور hts یا مشابه آن روی یک سرور خاص، ترافیک را عوض کنیم و در ویندوز کلاینت به کمک htc یا مشابه آن یک پراکسی روی پورت جدید تعریف شده قرار دهید. در این صورت تونل ایجاد میشود، بعد با telnet به آن وصل شوید.

hts –F server.text.com: 23 80
htc –P proxy.corp.com:80 –F 23 server.test.com:80

در سمت سرور این دستور، پورت ۸۰، ترافیک هایش روی پورت ۲۳ ریدایرکت میشود.
این عمل از IDS ها و فایروال ها عبور میکند.

عملیات Spoofing و جعل IP

در این عملیات، اگر نشست UDP باشد، موفقیت آمیز خواهد بود و میتوان IP هکر را جای IP دیگری گذاشت، یا IP شخص دیگر را روی IP هکر قرار داد که به این امر مسیریابی از مبدا یا Source Routing گویند. شکل زیر نشان می دهد که حمله کننده، در بین راه آدرس جعل شده ای را از شخص دیگری در کامپیوتر خود قرار میدهد.



در شکل فوق حمله کننده با کمک IP 10.0.0.5 مسیر یابی از مبدا را شروع میکند، این عمل با کمک دستور Tracertیا Traceroute انجام میشود، بدین وسیله، IP مورد نظر جایگزین میشود، بعد با کمک ابزارهای دیگر، عمل Time یا زمان گیری Packet ها صورت میگیرد و مشخص میشود که یک IP مورد حمایت یا مورد نظر برای شبکه مورد نظر است

Tracert –j 10.0.0.50 10.0.0.5
hping2 –G 10.0.0.50 10.0.0.5

Enumeration

وقتی عملیات اسکن و جمع آوری انجام میشود، میتوانیم از حساب ها و IP های به دست آمده استفاده کنیم و همین طور MAC آدرس کامپیوتر خود را تغییر دهیم. (جعل MAC Address)، مثلا در ویندوز میتوان بر روی NetBios با حساب کاربری جدید و IP جدید، یک اکانت در دامین ایجاد کرد و عضو دامنه سرور شد. دستور زیر کمک میکند تا در NetBios هکر خود را به عنوان یکی از اکانت های موجود ثبت کند.

New View / domain
NBtstat – A IP Address

Null Session جا زدن فضای خالی در نشست

در نشست های شبکه میتوانیم از Null Session استفاده کنیم، به طوری که یک فضای خالی یا یک تله برای کاربران شبکه قرار دهیم. این فضای خالی کمک میکند تا همه گروه ها و کاربران مجوز اتصال داشته باشند. این فضا میتواند روی NetBios تعریف شود و با استفاده از دستور NetUse در ویندوز آنرا اجرایی میکنیم.

Windows:	C:\> net use \\192.21.7.1\IPC$ “” /u: “”
Linux:	$ smbclient \\\\target\\ipc\$ “” –U “”

در دستور ویندوز با دادن IP مورد نظر و علامت های خالی میتوانیم روی پروتکل NetBios کاربری تعریف کنیم که حساب کاری ناشناس داشته باشد و همین طور، بدون پسورد باشد. پس از اجرای دستور شماره یک کانال ارتباطی بین هکر و سیستم عامل سرور برقرار میشود. این کانال ارتباطی قابل شناسایی نیست مگر اینکه پورت مورد نظر آن شناسایی شود.
در دستور لینوکس به جای NetBios از پروتکل Samba استفاده میشود، این پروتکل به صورت کلاینت / سرور تعریف میشود و میتوان در جای کلمه Target، IP Address مورد نظر را قرار داد.

برای مقابله با Null Session پورت های مورد نظر را اسکن میکنیم و میتوانیم آنها را ببندیم یا سرویس SMB Client را در لینوکس و سرویس Wins Client را در ویندوز ببندیم.

۱. بر روی کارت شبکه راست کلیک کنید و گزینه Properties را انتخاب کنید.
۲. بر روی TCP/IP کلیک کنید و سپس دکمه Properties را کلیک کنید.
۳. بر روی دکمه Advanced کلیک کنید.
۴. در زبانه WINS، گزینه disable NetBIOS Over TCP/IP را انتخاب کنید.

برای جلوگیری از ورود کاربران ناشناس و مدیریت رجیستری تنظیمات امنیتی زیر روی رجیستری انجام دهید.

۱. Regedit32 را باز کنید و وارد مسیر HKLM\SYSTEM\CurrentControlSet\LSA شوید.
۲. از منوی Edit، گزینه Add Value را انتخاب کنید و مقادیر زیر را وارد کنید:
Value name: Restrict Anonymous
Data Type: REG_WORD
Value: 2

در نرم افزارهایی مثل PSTools میتوانیم ابزارهای حمله به پردازش، حمله به فایل ها و همچنین تغییر پسورد ها را ببینیم.

PsExec: اجرای از راه دور پردازش ها
PsFile: نمایش از راه دور فایل های باز شده
PsGetSid: نمایش SID یک کامپیوتر یا یک کاربر
PsKill: متوقف کردن پردازش ها با استفاده از نام یا شماره پردازش
PsInfo: نمایش اطلاعات سیستم
PsList: نمایش اطلاعات جزئی درباره پردازش ها
PsLoggedOn: کسی را که به صورت local و از طریق منابع Share وارد شده اند را نشان میدهد
PsLogList: از کار انداختن رکورد های log
PsPasswd: تغییر پسورد اکانت ها

PsService: کنترل سرویس ها
PsShutdown: خاموش یا راه اندازی مجدد کامپیوتر
PsSuspend: معلق کردن پردازش ها
PsUptime: تعیین مدت زمان روشن بودن سیستم

جلسه هشتم موجود نیست (Null Session و SNMP Enumeration و انتقال ناحیه کاربری)

می توانید صفحات ۵۸ تا ۶۲ کتاب هکر قانونمند که در سایت موجود است را بخوانید

ostad-CEH-Farsi-PDF.zip

جلسه نهم

روش های شکستن پسورد:

برای شکستن پسورد به دو روش دستی و نرم افزاری پناه میبریم، معمولا در حالت دستی هکر حساب های کاربری کاربران را حدس میزند و یا با مهندسی اجتماعی پیدا میکند و یا از طریق پرسش آنها را به دست میآورد، سپس بر اساس احتمال پسورد ها را با آزمون و خطا تست میکند، معمولا در روش نرم افزاری، هکر از نرم افزار های حدس زننده پسورد، استفاده میکنند، معمولا در این حالت میتوان از اسکریپت هایی که دارای یک حلقه میباشد استفاده کرد، این اسکریپت ها با کمک آن حلقه و فایل متصل به آنها، میتوانند پسورد مورد نظر را پیدا کنند. روش دیگری از این عمل نیز وجود دارد، این روش به کارگیری دیکشنری، که این دیکشنری در خود هش یا پسورد های پر استفاده را دارد. اغلب پسورد ها در ویندوز درون فولدر Config در داخل System32 فایلی به نام SAM وجود دارد، که پسورد ها را ذخیره میکند، در لینوکس فولدری به نام Shadow وجود دارد که پسورد ها در آن تصویر گرفته میشوند. در سیستم عامل اپل امکانی برای بازیافت پسورد به صورت نرم افزاری وجود دارد که با CD سیستم عامل اپل نرم افزار مربوطه اجرا میشود و گزینه change Password دارد که در هنگام بوت شدن سیستم، قبل از نصب ظاهر میشود.

در روش نرم افزاری، میتوان در سیستم عامل های ویندوز، فایل اجرایی Command ویندوز را به جای فایل اجرایی کلید Shift جایگزین کرد. به صورتی که با یک CD Boot سیستم را بوت کرده و بعد از آن این فایل ها را جایگزین میکنیم، در هنگام ریستارت شدن کامپیوتر با نگه داشتن کلید شیفت فرمان CMD ظاهر میشود. در آن صورت با دستور NetUser میتوانیم پسورد را تغییر دهیم یا یوزر جدیدی ایجاد کنیم که Admin نیز باشد.

نرم افزار های مهمی، در این راستا وجود دارد

۱- نرم افزار Smbbf: این نرم افزار نشست SMB را در ویندوز بررسی میکند و پسورد های مربوط به ویندوز و دامین را بیرون میکشد.

۲- نرم افزار l0phtcrack: این نرم افزار روی نشست TCP عمل میکند، همچنین در هنگام بوت ویندوز، با ارسال یک بسته، پسورد را در جوابیه بسته میگیرد.

۳- نرم افزار John the Ripper: این ابزار پسورد یونیکس و اپل را باز میکند. این ابزار میتواند پسورد های متشابه به پسورد اصلی را به دست آورد.

۴- KerbCrack: این نرم افزار در دو قسمت شنیدن لاگین ها و یافتن پسورد های آنها کار میکند که اولی را Kerbsniff و دومی را Kerbcrack گویند. نوع حمله این ابزار از نوع Dictionary و Brute Force حمله است.

نکته: در ویندوز، پسورد ها به کمک LM HASH و NLMT Hash رمزگذاری میشود، این رمزگذاری دارای هش های یکسان با طول ۱۴ کاراکتر برای ویندوز میباشد. اشکال ویندوز در این است که رمز LM با کمک قاعده رمزگذاری دو تکه دو Hash را به هم پیوند میدهد و در فایل SAM در آدرس زیر ذخیره میکند

C:\windows\system32\config

نحوه کار LM: مبنای LM بر این است که پسورد باید ۱۴ حرف باشد، اگر کمتر از ۱۴ حرف کاربر وارد کند تا ۱۴ حرف برای او با Null پر میشود. سپس به دو قسمت تقسیم میشود، هر قسمت به صورت مجزا که دو کلمه هفت حرفی میباشد با الگوریتم DES رمز میشود. دو قطعه Hash شده و در آخر به هم پیوند میخورد.

در ویندوز ۷ به بعد همین ۱۴ کاراکتر محدودیت را داریم، اما دو قسمت جدا شده به صورت یکپارچه Hash MD5 میشوند. به همین دلیل تکرار آن کمتر میشود و امنیت بالاتری دارد. لازم به ذکر است این نوع روش در ویندوز ۷ و ۸ از لینوکس Debian گرفته شده است.

نکته قابل توجه این است که در LM هش تکراری وجود داشت، مثلا اگر ویندوز خود را با عدد ۱۲۳ رمز میکردید، ممکن بود با عدد ۶۷۸ نیز تولید شود.

جلسه دهم

در سیستم های ویندوز، رمزی به عنوان NTLM از ویندوز هفت به بعد از رمز LM قوی تر بود و بر اساس هش MD5 کار میکرد، در این سیستم، جدولی به نام Rainbow Table وجود دارد، که به کمک آن میتوانیم پسورد های موجود را بانک کنیم و در عملیات مربوط به Brute Force Attack در امان میباشد. در این حملات نکته قابل توجه این است که اگر اسم رمز بیشتر از شانزده کاراکتر و همچنین به صورت فینگلیش نوشته شود در آن صورت، Brute Force Attack دچار ضعف خواهد شد.

در حملات مربوط به پسورد میتوانیم فرایند رجیستری و همچنین فرایند های مربوط به کنترل group Policy و طول کلمه پسورد بالا را اجرا کنیم، به صورتی که از روش های زیر استفاده کنیم:

روش ۱: از Group Policy، وارد قسمت Security Options و Local Security Policy شوید و گزینه زیر را غیر فعال کنید: Network security: Do not store LAN Manager hash value on next password change

روش ۲: از طریق رجیستری وارد مسیر زیر شوید:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa و سپس کلیدی به نام NoLMHash ایجاد کنید.

روش ۳: از پسوردی که طول آن بیشتر از ۱۵ کاراکتر است استفاده کنید.

همچنین برای مقابله با شکستن پسورد، موارد زیر را در نظر بگیرید:

۱. پسوردهای پیش فرض را تغییر دهید.
۲. پسوردهایی که در دیکشنری وجود دارند را استفاده نکنید.
۳. از پسوردی استفاده نکنید که مربوط به اسم دستگاه، اسم دامین، یا هر چیز دیگری که می‌توان در whois پیدا کرد باشد.
۴. پسوردی که مربوط به علایق شما یا تاریخ تولد شما است استفاده نکنید.
۵. اگر از کلمات دیکشنری می‌خواهید استفاده کنید، از کلمه‌ای که بیشتر از ۲۱ کاراکتر دارد استفاده کنید.

در رمزگذاری پسوردها، زمان رمزگذاری نیز مهم است، این مدت زمان، برای تعویض پسورد ها و همچنین مدیریت آنها میباشد. بهترین بازه تعویض معمولا بین ۱۰ تا ۳۰ روز است.

بررسی event viewer log:

در سیستم های شبکه ای مدیران شبکه می توانند لایه های شبکه را View کنند. این مدیران از ابزاری مانند VisualLast استفاده میکنند. در این ابزار زمان های ورود و خروج، اجراهای کاربر، مدیریت IP ها و رد پاها وجود دارد. فایل های log معمولا در آدرس زیر پیدا میشوند.

C:\\windows\system32\config\sec.event.evt

برای جلوگیری از Brute Force or Dictionary Attack میتوانیم از طبقه بندی پسوردها استفاده کنیم. این طبقه بندی شامل موارد زیر می باشد.

- تنها حروف
- تنها اعداد
- تنها کاراکترهای خاص
- حروف و اعداد
- تنها حروف و کاراکترهای خاص
- تنها اعداد و کاراکترهای خاص
- حروف، اعداد و کارکترهای خاص

در این طبقه بندی معمولا طول بیش از هشت کاراکتر و شامل علامت های غیر الفبایی، اعداد، حروف بزرگ حروف کوچک میباشد.
میتوانید کلمات انگلیسی را با حروف فارسی یا کلمات فارسی را با حروف انگلیسی بنویسید.

حملات شناسایی برای پسوردها میتواند به سه صورت باشد:

۱- Passive Online: این حمله از طریق استراق سمع مثل Sniffer ها و حملات واسط انجام میشود.

۲- Active Online: این حملات از طریق حدس زدن انجام میشود، به همین منظور برای جلوگیری از آنها از شکل ها یا علامت های گرافیکی خاص استفاده میشود.

۳- Offline: در این روش، حملاتی مانند دیکشنری، هیبرید و BruteForce انجام میشود.

تذکر: حملات از نوع reply حمله passive online است که پسورد را به سرور ارسال میکند و با احراز هویت از جانب سرور نتیجه بازخورد سرور را میگیرد.
معمولا این حملات روی شبکه های بزرگ و سرورها انجام میپذیرد و کمتر روی دیتابیس ها صورت میپذیرد.

تذکر۲: در حملات Active Online معمولا فاکتور انسانی برای ایجاد پسورد های ضعیف مطرح میشود و شکستن آنها نیز بر این منوال نیز راحت تر خواهد بود. معمولا پسورد ها در درایو های مشترک یا در پروتکل IPC قرار میگیرد و هکر میتواند با نام کاربری sysadmin یا admin یا administrator حمله کند.
معمولا هکر، IP آدرس را وارد کرده، بعد در پشت آن با علامت اسلش نام درایو share را وارد میکند C$

تذکر مهم: ویندوز از این ناحیه درایوهای مشترک بسیار ضربه پذیر است.

برای حمله اتوماتیک به پسورد، میتوانیم در خط فرمان، یک فایل اجرایی تولید کنیم و بانک اطلاعاتی پسوردهای خود را در یک فایل قرار دهید، سپس با وارد کردن آن فایل، در یک حلقه شرطی تکرار رابطه حمله را بنویسید

۱. با استفاده از برنامه Windows Notepad، یک فایل username و password ساده بسازید. ابزارهای خودکاری از قبیل Dictionary Generator، برای ساخت لیست این کلمات وجود دارند. فایل را در مسیر C: drive as credentials.txt ذخیره کنید.

۲. این فایل را با استفاده از دستور FOR، pipe کنید:

C:\> FOR /F “token=1, 2*” %i in (credentials.txt)

۳. دستور net use \\targetIP\IPC$ %i /u: %j را تایپ کنید تا از فایل credentials.txt استفاده کند و به پوشه share شده مخفی آن وارد شود.

جلسه یازدهم

تروجان چیست و چگونه با آن مقابله میشود:

از عمده حملات به شکل آسیب پذیری است به طوری که به کمک آن میتوانیم ابزاری را وارد سیستم مقابل نماییم و حملات درونی سازمان یافته به سیستم مقابل انجام دهیم. تروجان ها به کمک یکسری ابزار پیش ساخته ایجاد می شود و به کامپیوتر مقصد ارسال میگردد. معمولا راه های مقابله با آنها استفاده از AntiTrojan, Spyware detection و استفاده از مقابله کننده با Backdoor هاست. تروجان ها از backdoor ها و spyware ها در ضمائم ایمیل ها در فایل های word, powerpoint, PDF استفاده میکنند و وارد کامپیوتر مقابل میشوند.

برای شناسایی تروجان عملیات زیر را انجام دهید.

- پورت را با استفاده از ابزارهایی همچون TCPView, Fport, netstat اسکن کنید تا پورت های باز مشکوک را پیدا کنید.
- پردازش های در حال اجرا با استفاده Insider, What's on my computer, Process Viewer اسکن کنید تا پردازش های مشکوک را ببینید.
- با استفاده از ابزارهای همچون MSConfig, what's on my computer رجیستری را اسکن کنید تا ورودی های مشکوک را پیدا کنید.
- فعالیت های مشکوک شبکه را با استفاده از Ethereal اسکن کنید.
- از Trojan Scanner ها برای یافتن تروجان ها استفاده کنید.

برای شناسایی پورت ها از نرم افزار Fport, Advanced Port Scanner , Port Scan استفاده میکنیم. برای جلوگیری از حملات مخفیانه میتوانیم از DSNIFF کمک بگیریم. این نرم افزار برای مانیتور کردن نیز استفاده میشود. نرم افزار PRCView پردازش های سیستم را نشان میدهد. برای اینکه سیستم از لحاظ یکپارچگی زمان تراکنش ها و یکپارچگی زمان ارسال و دریافت پکت ها بررسی شود، از نرم افزار TripWire استفاده میکنیم.

سیستم فایل نیز از تروجان ضربه میخورد، به همین دلیل از Patcher های آپدیت ویندوز استفاده میشود تا مقابل تروجان ها بایستد، در ویندوز ۸,۱ ساختار فایل ویندوز کاملا عوض شده و تروجان ها روی آن اثر ندارد. برای این منظور میتوانیم از نرم افزار sigverif برای کنترل امضای برنامه های کاربردی و سالم بودن آنها استفاده کنیم.

این نرم افزار اگر ابزاری تحت ویندوز باشد، تاییدیه آن را از مایکروسافت میگیرد. در ویندوز این ابزار را میتوانیم از run اجرا کنیم.

ابزار دیگری به نام system file checker وجود دارد که تشخیص میدهد درون فایل تغییر کرده است یا خیر.

برای کنترل کردن محتوای فایل نیز از فولدر زیر عملیات restore انجام میشود.

Windows\system32\dllcache

پـــــایـــــان