آموزش گام به گام هك

فهرست:

بخش اول – خطر استفاده از اينترنت
بخش دوم – آشنايي با مهندسي اجتماعي
بخش سوم – زبان هكرها L33t
بخش چهارم – فرستادن ايميل ها جعلي با telnet
بخش پنجم – آشنايي با IP و Port و نحوه بدست آوردن آن
بخش ششم – آشنايي با NetBIOS
بخش هفتم – آشنايي با اسب هاي تراوا
بخش هشتم – نحوه كار با يك اسب تراوا
بخش نهم – نفوز به ويندوز
ضميمه يك – نحوه بدست آوردن پسورد
ضميمه دوم – روش هاي اجراي همزمان برنامه ها در ويندوز
درباره نويسنده مقاله

مقدمه:

هك چيست؟ هكر كيست؟
هك به معناي نفوذ است. هكر كسي است كه اقدام به نفوذ در فضاي سايبر را مي كنيد.
يك مثال عامه از هكر: هكر به شخصي گفته مي شود كه براي باز كردن يك گاوصندوق يك شاه كليد يا كليد اصلي آن را پيدا مي كنيد. تفكر يك هكر دنياي بدون قانون كپي رايت است.
به اصطلاح: Free Information

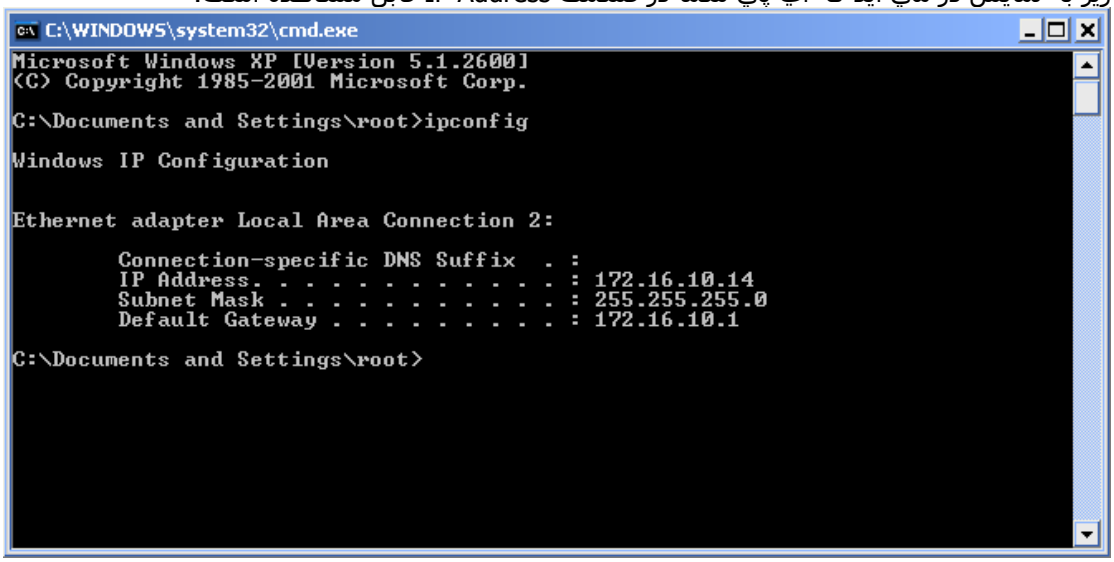
بخش اول – خطر استفاده از اينترنت:

وقتي شما به اينترنت متصل مي شويد كامپيوتر شما با چندين ميليون كامپيوتر مرتبط مي شود طبعاً حيلي از اين ارتباطات باي ميل شما نيست و دور از چشم شما صورت مي گيرد. هكر ها و روبات هاي ساخته شده توسط آن ها در فضاي اينترنت همواره اهداف خود را روي كامپيوترهاي متمركز مي سازند كه از سرعت اينترنت بالاي برخوردارند. پس استفاده از خطوطه پر سرعت اينترنتي (DSL, Cable, LAN , ...) علاوه بر داشتن محسنات بسيار زياد داراي خطر نفوذ هكر هاي بيشتري نيز هست.

وقتي شما به اينترنت متصل مي شود از طرف كامپيوتر سرويس دهنده اينترنت به شما يك آدرس آي پي (IP) داده مي شود. كه توسط اين آدرس كامپيوتر شما در بين ميليون ها كامپيوتر موجود در فضاي اينترنت شناسايي مي گردد. به هر يك از كامپيوتر هاي موجود در اينترنت يك آي پي منحصر به فرد داده مي شود. براي مثال وقتي شما آدرس سايت Microsoft.com را وارد جستجوگر اينترنت خود مي كنيد اين آدرس يه صورت خودكار به آدرس آي پي سرور Microsoft.com ترجمه مي شود. آدرس كاربر پسند Microsoft.com به آدرس كامپيوتر پسند آي پي تبديل مي شود. آدرس آي پي از 4 بخش عددي تشكيل شده است.
مثلا آدرس آي پي سايت Microsoft.com به صورت زير است:
207.046.249.252
همانطور كه مشاهده مي كنيد به خاطر سپردن اين اعداد با وجود اين همه سايت هاي اينترنتي كار ساده اي نيست به همين خاطر براي هر آدرس آي پي يك آدرس دامين مثل: Microsoft.com در نظر گرفته اند.

تمرين. نحوه پيدا كردن آي پي كامپيوتر شخصي خود در زمان اتصال به اينترنت:

بعد از اتصال به اينترنت وارد Start -> Run شويد و command را تايپ كرده روي OK كليك كنيد. در پرامپت Dos تايپ كنيد ipconfig سپس روي كليد Enter بزنيد. پنجره اي همانند شكل زير به نمايش در مي آيد كه آي پي شما در قسمت IP Address قابل مشاهده است.



ويندوز داراي 3 پروتكل اصلي مي باشد. (پروتكل = يك سري قوانين) كه توسط آ» ها با كامپيوتر هاي مختلف ارتباط برقرار ميكند:
IPX/SPX: دو پروتكلي كه سرور ها و كلاينت هاي Novell استفاده ميكنند.
NetBEUI (NetBIOS Extended User Interface): پروتكلي كه روي شبكه هاي محلي كامپيوتري مورد استفاده قرار مي گيرد.
TCP/IP: پروتكلي مشهوري كه در اينترنت و شبكه هاي كامپيوتري استفاده مي شود. TCP مخفف عبارت Transmission Control Protocol است. قانوني كه اين پروتكل از آن بهره مگيرد اين است كه پيغام ها و درخواست هاي شما را به قسمت هاي كوچك (پكت | Packet) تقسيم مي كنيد. و كامپيوتري كه اين پكت ها را مي گيرد دوباره آنها را به هم متصل ميكند. آي پي قسمتي ار پروتكل TCP/IP مي باشد كه كار آدرس دهيد اين پكت ها را به عهده مي گيرد. كه پكتها به كجا فرستاده شوند و به كجا بازگرداند.

بخش دوم – آشنايي با مهندسي اجتماعي:
مهندسي اجتماعي يكي از شگردهاي هكر ها براي گيج كردن با كلك زدن به مردم هست و يكي از موثر ترين روش ها براي نفوذ به يك سيستم مي باشد.
يكي از انواع روش هاي مهندسي اجتماعي اسپوفينگ (spoofing) است. شما (يك هكر) ايميلي را براي كسي ارسال مي كنيد و وانمود مي كنيد كه رئيس يا مسئول بخش رايانه هستيد و از آن فرد براي معتبر ساختن پسوردش سئوالاتي مي كنيد تا پسورد خود را بنويسند و براي شما ارسال كنند. بعداً متوجه مي شويد كه چگونه اين روش كار مي كنيد.
روش ديگر براي مهندسي اجتماعي: فرض مي كنيم شما در صدد به دست آوردن آدرس پسورد ايميل يكي از افراد شبكه يا دپارتمان خود هستيد. شما اين ايميل را به اين فرد مي زنيد:

"با سلام.
بخش رايانه به علت پاره اي مسائل امنيتي براي كاربران پسورد هاي جديدي را در نظر گرفته است. براي اين منظور كد زير را تايپ كنيد و روي دكمه Enter كليك كنيد:
SetPassword: U22l5
پسورد جديد شما U22l5 مي باشد لطفا آن را به خاطر بسپاريد و از نوشتن آن در جاي ديگر خودداري كنيد.

با تشكر از همكاري شما
علي كاظمي. مسئول بخش رايانه"

با اين روش بعداً شما مي توانيد با پسورد U22l5 به فضاي ايميل فرد مورد نظرتان نفوذ كنيد.
كافي است اين روش ها را يكبار امتحان كنيد!

روش ديگر براي مهندسي اجتماعي: در اين روش مخاطب شما مسئول بخش رايانه مي باشد و شما خود را جاي فردي جا مي زنيد كه قصد به دست آوردن پسورد او را داريد:

"با سلام.
من پدارم حياتي دانشجوي رشته فناوري اطلاعات هستم و به تازگي با سيستم ايميل بخش رايانه آشنا شدم. براي ورود به سيستم ايميل دچار مشكلي هستم. چندين بار نام كاربري و پسود خود را وارد كردم ولي موفق به ورود به سيستم را نشدم.
اگر مقدور هست من رو قدم به قدم راهنمايي كنيد و مشخص كنيد كه بايد چه اطلاعاتي را در چه قسمت هايي بايد وارد كنيم.

با تشكر
پدارم حياتي"

اين ترفند ممكن است رياد موفقيت آميز نباشد ولي خالي از لطف نيست!

بخش سوم – زبان هکرها L33t:

زبان l33t علاوه بر اینکه به طور مستقیم زبان بسیاری از گروههای هک بوده و هست، گاهی برخی از کاراکترهای آن در یک متن عادی هکرها به چشم می خورد و در نتیجه آموزش مقدماتی آن لازم به نظر می رسد. این زبان در حقیقت همان زبان انگلیسی است با الفبایی کمی دستکاری شده و چند قاعده ساده گرامری که توسط بسیاری از طرفداران بازیهای آنلاین و متخصصان اینترنت بخصوص آنهایی که در سنین نوجوانی هستند بسیار به کار می رود. برای هر کاراکتر در روش نگارش هکرها ممکن است 3 تا 5 شکل متفاوت موجود باشد. برخی ممکن است بیشتر حروف را بدون تغییر نگه دارند و برخی همه حروف را تغییر دهند، با این همه جدول زیر می تواند شروع خوبی باشد. کسانی که حوصله و علاقه ندارند، به خواندن جدول زیر اکتفا کنند، سایرین به جای خواندن جدول زیر، خواندن متن را ادامه دهند:

سطح مقدماتي	سطح متوسط	سطح پيشرفته
A = 4 or@	A = 4 or@	\-/ = A
B = 8	B = 8 or |3	%| = B
C = c	C = (or]	] C = (or
D = d	D(| =	(| = D
E = 3	E = 3	:| = E
F = f	F=| =	=| = F
G = 9	G = 9	_| = G
H = h	H|-| =	|-| = H
I = 1	I = 1	| = I
J = j	J|_ =	|_ = J
K = k	K>| =	>| K = |(or
L = 1	L = 1	| = L
M = m	M\/\/ =	|/| M = /\/\ or
N = n	N/\/ =	|/| N = /\/ or
O = 0	O = 0	[] O = () or
P = p	P = |> or*|	*| P = |> or
Q = q	Q = q	_[] Q = ()_ or
R = r	R\(| =	\(| = R
S = 5 or$	S = 5 or$	-_ = S
T = t or 7 or+	T = 7 or+	-|- = T
U = u	U|_| =	|_| = U
V = v	V/\ =	/\ = V
W = w	W/\/\ =	/\/\ = W
X = x	X>< =	>< = X
Y = y	Y_/\ =	>- Y = _\/ or >- or
Z = z	Z_/- =	Z_/- =

برخی از قواعد گرامری این زبان:

- در جمع بستن کلمات به جای s از z استفاده کنید.
- به جای f بهتر است از ph استفاده کنید.
- قبل از افعال از teh استفاده کنید.
- برای تاکید بیشتر، اعلام یک اتفاق تازه یا تاکید بر به کار گرفتن حداکثر تلاش، از most بلافاصلاه بعد از teh استفاده می شود.
- به جای ing از or استفاده می شود که وجود آن در پایان فعل به معنای انجام کار در این لحظه می باشد.
- استفاده از zor یا zorz: در پایان فعل مشابه or (ولی بیشتر مورد استفاده) است و در آخر اسم، به آن تاکید می دهد.
- استفاده از ored، zored و zorzed در پایان فعل به عنوان پسوند: به مفهوم انجام عمل در گذشته می باشد. در اینجا هم zorzed از بقیه پرکاربردتر است و ored از همه کمتر به کار می رود.
- فقط برای فهم برخی جملات: مبتدیها ممکن است or را به جای ed در پایان فعل و er در پایان اسم به کار ببرند.
- استفاده از ! در پایان تمامی جملات، بخصوص برای بازیهای رایانه ای معمول است.

چند کلمه بسیار متداول:

0w|\| or 0wn3d: one of the most popular l33t words it is very loosely defined as beaten or can simply be an expression of awe, for example, 'I 0wn3d you' means 'I have beaten you in a very humiliating fashion', or '0wn4ge!' which means 'That was/is very nifty'.

w00t: derived from 'hoot', this is defined as 'yay', it can be used, for example, upon victory or, possibly, the release and procurement of a new video card.

13wt: treasure, good merchandise, possessions, a misspelling of loot. Most commonly referring to pirated software, items in a game or promotional giveaways.

h4x0r: hacker, can be used for a real hacker or simply a very skillful person. This is the most common occurrence of the –0r clause.

ph33r: fear, most commonly used in such phrases as, "Ph33r m3!" or "Ph33r |\/|y 1337 sk1llz!" It can also be written as, 'ph34r'.

sk1llz: obviously derived from 'skill', referring to skill in some type of online game or programming/hacking. Many times used in conjunction with 'm4d'. As a general rule, if one has sk1llz, one is to be ph33r3d.

m4d: mad, mostly used as a descriptive term meaning great, for example, "h3s g0t m4d sk1llz".

j00: you, commonly used in such phrases as, "j00 d34d f00".

f00: fool, one who isn't very bright/skillful.

j0: yo, as in the greeting.

d00d: dude; an expression of comrader, or just used to address a random person online.

sux0r: sucks, as in "this sux0r", one of the few common examples of the -0r clause.

l4m3r: lamer, someone who is lame, someone who uses an unfair tatic or generally makes the things around him/her less fun.

n00b: short for noobie, misspelling of newbie; someone who is new to something, or just not very good at it.

لينك چند منبع براي كسب اطلاعات بيشتر:

http://www.bbc.co.uk/dna/h2g2/A772346
http://hpfanfiction.net/leet/#grammar
http://www.wtfiml33t.com/viewarticle.php?artid=132
http://www.planetquake.com/turkey/l33t_a.htm

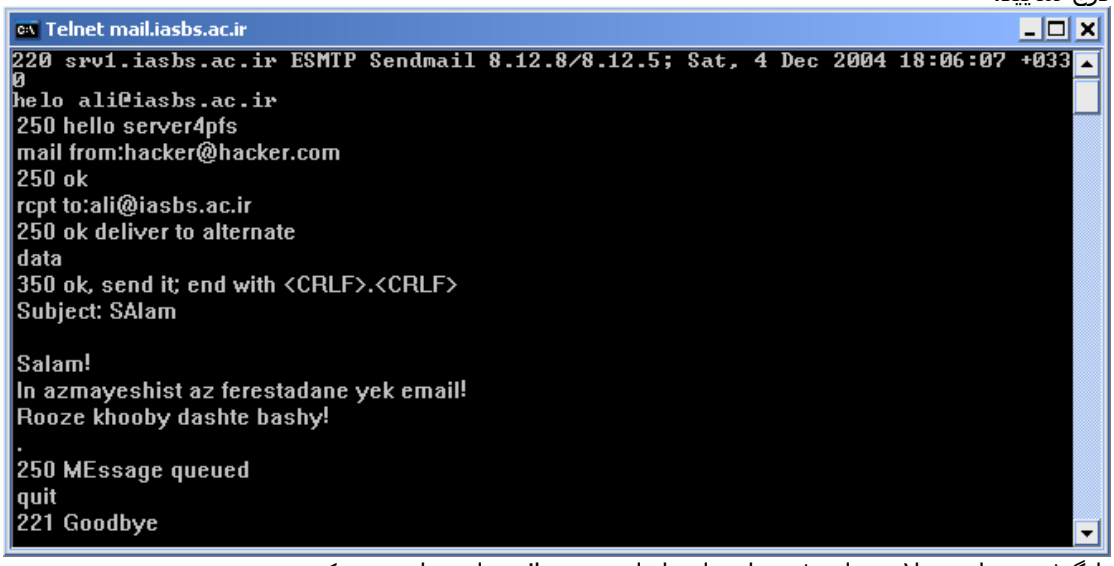
بخش چهارم – فرستادن ايميل ها جعلي با telnet:

telnet در اصل پروتكلی است كه برای login و استفاده از یک كامپیوتر دیگر به كار می رود. روش اجرای Telnet در لینوكس یا انواع دیگر Unix و نیز ویندوز 2000 تا حد خیلی زیادی شبیه چیزی است كه در این بخش مي خوانيد. برای آشنایی بیشتر با telnet و گرفتن جواب دقیقتر سوالات بالا روی مـــن كلیک كنید كه به یک میزبان واقعی Telnet شما را متصل می كند كه می توانید به رایگان عضو شوید و از خدمات آن استفاده كنید. خواهید دید كه لینک فوق در حقیقت Hyper Terminal را باز می كند. در حقیقت هم اگر به درون Hyper Terminal بروید می توانید در قسمت برقراری تماس با انتخاب TCP/IP مستقیما از آن به عنوان Telnet استفاده كنید. اما اینكه Telnet در هک چه نقشی دارد و چه فایده ای از زبان "كارولین مینل": "فقط با یک سرویسگیر Telnet شما می توانید:

- ایمیل بفرستید.
- سورس (متن برنامه) سایتها را بخوانید.
- به میزبانهای وب ورودیهای غیر منتظره بفرستید كه می تواند سبب دریافت پاسخهای شگفت انگیز و گاهی غیر قانونی شود.
- به بسیاری از دیگر سرویسهای كامپیوترهای میزبان وب ورودی دلخواه خود را بدهید.
- در سرویسهایی كه میزبانها، روترها و حتی كامپیوترهای شخصی مردم در منزلشان در اختیار شما می گذارند كاوش و جستجو كنید."

در این بخش، برای اینكه هم كمی با telnet (كه به عنوان یكی از مهمترین ابزارهای هک مطرح بوده و هست) آشنا شوید هم از موضوعی شروع كرده باشیم كه ملموس و جذاب باشد، فرستادن ایمیل از طرف هركسی به هركسی با telnet را آموزش می دهیم (راههای آسانتری برای این كار هست و راحتترین راه آن استفاده از Outlook مایكروسافت است). قبل از هر چیز telnet كردن به خودی خود جرم نیست و استفاده از telnet برای فرستادن یا گرفتن ایمیل نه ضرری برای شما دارد و نه میزبان. اما شما این حق را ندارید كه از طرف كسی به كس دیگر ایمیل بزنید مگر با اجازه آنها.اول وارد Command شوید (مراحلي كه در بخش اول آموزش داده شد.)، حالا می خواهیم از دستور telnet استفاده كنیم:
telnet target port به جای target آدرس سایت یا كامپیوتر و به جای port باید آدرس پورت را وارد كنید(port یا درگاه دروازه ورود به سیستم هاست مثلا پورت 80 پورت ورود و خروج

اطلاعات وب سایت ها به کامپیوتر شماست اطلاعات بیشتر در بخش پنجم). در مثال این شکل 4-1 با فرستادن ایمیل (smtp) سروکار داریم که پورت آن 25 است و آدرس نیز آدرس یک سرور ایمیل باید باشد. به عنوان مثال "telnet mail.iasbs.ac.ir 25" را خواهیم داشت، فقط یک مثال است و شما می توانید از هر آدرس مشابهی استفاده کنید. جوابی دریافت خواهید کرد که معمولا شامل نام میزبان ایمیل است. حالا وقت سلام کردن با دستور helo است (دستور ehlo هم داریم که می توانید امتحانش کنید). بهتر است جلوی helo آدرس ایمیل فرستنده را درج نمایید.



با گرفتن جواب سلام، برای فرستادن ایمیل از دستور mail استفاده می کنیم:

mail from hacker@hacker.com

بعد از گرفتن OK حالا گیرنده را معرفی می کنیم:

rcpt to: ali@iasbs.ac.ir

این بار بعد از گرفتن OK دستور data را تایپ و Enter کنید. توجه کنید که میزبان به شما می گوید وقتی کارتان تمام شد <CRLF>.<CRLF> بزنید که این یعنی زدن یک Enter، تایپ کردن یک نقطه و دوباره زدن Enter. حالا وقت وارد کردن Subject، to و from و سپس زدن دو Enter و وارد کردن متن ایمیل و سپس زدن Enter، تایپ کردن نقطه و زدن Enter دوم است. در عکس بالا فقط Subject وارد شده است. نمونه کاملتری که شامل To و From می باشد به صورت زیر است:

```
data
354 ok, send it; end with <CRLF>.<CRLF>
From: hacker@hacker.com
To: ali@iasbs.ac.ir
Subject: Salam!

In email faghat be ghasde azmayesh ferestade shode ast.
Rooze khooby dashte bashid
.
250 Message queued
```

به تفاوت این دو مورد در عکس زیر توجه کنید:

From: hacker@hacker.com **To:** ali@iasbs.ac.ir
Subject: Salam! **Cc:**

```
In email faghat be ghasde azmayesh ferestade shode ast.
Rooze khooby dashte bashid
```

شکل بالا نتیجه مثال ما را نشان می دهد.
شکل پایین این تفاوت را دارد که From و To در قسمت data وارد نشده اند.

From: **To:**
Subject: SAlam **Cc:**

```
Salam!
In azmayeshist az ferestadane yek email!
Rooze khooby dashte bashy!
X-UIDL: 342565731
```

دستوراتی که گفته شد روی هر میزبانی کار خواهد کرد. به احتمال زیاد جایی که از آن اینترنت گرفته اید اگر درخواست ایمیل POP3 از آنها بکنید به رایگان به شما خواهند داد و شما آدرسی که به عنوان SMTP یا Outgoing server از آنها دریافت می کنید را به جای mail.iasbs.ac.irخواهید نوشت.

بخش پنجم – آشنايي با IP و Port و نحوه بدست آوردن آن:

سوال: اسم Target که در قالب Telnet target port مطرح کردیم چیست و چرا برخی به جای آن 4 تا عدد می زنند؟

پاسخ: هر کامپیوتر روی اینترنت با 4 عدد بین 0 تا 255 که با نقطه از هم جدا می شوند مشخص می شود. در XP برای فهمیدن IP خود کافی است که روی مانیتورهای نشاندهنده اتصال شما به اینترنت دابل کلیک کنید و از بالای پنجره ظاهر شده با انتخاب قسمت جزئیات (Details)آدرس IP خود را خواهید دید.(برای کسانی که ویندوز قدیمی دارند معمولا یک راه مناسب تایپ کردن winipcfg در پنجره Run و فشردن Enter است). حال وقتی که کسی یک Domainثبت می کند، در واقع روی این عددها یک اسم می گذارد. این کار دو فایده اساسی دارد. یکی اینکه اگر عدد فرد به هر دلیل عوض شود لازم نیست دوباره به همه خبر دهد و دلیل دیگر آن این است که اسم ساده تر به خاطر سپرده می شود و احتمال اشتباه در آن کمتر است. همانطور که می بینید تشبیه IP به شماره تلفن تا حدی به فهم آن کمک خواهد کرد. در اینجا قصد نداریم وارد بحث دقیق IP بشویم اما دو عدد اول IP حتما به اینکه از کجا اینترنت دارید مربوط است و به طور تئوری با داشتن IP شما می توان مکان شما را به صورت فیزیکی هم در روی کره زمین مشخص کرد. برای دانستن IP یک سایت کافی است که از داخلCommand Prompt ، دستور Ping را اجرا کنید. به سادگی تایپ کنید Ping yahoo.com یا Ping iasbs.ac.ir تا IP را ببینید. پس حالا دیدید که در واقع منظور از Target شماره آن کامپیوتری است که قصد دارید به آن متصل شوید.

سوال: اصطلاح port که در قالب Telnet target port مطرح کردیم چیست و چرا ما آنرا برابر 25 گرفتیم؟ اگر جای آن را خالی بگذاریم چه می شود؟

پاسخ: ترجمه کلمه port به فارسی "بندر" می شود. کامپیوتر مقصد را به صورت جزیره ای تصور کنید که چندین بندر دارد و هرکدام تخصص خاص خود را دارند. یکی برای نفتکشهاست یکی برای صادرات سنگ معدن و Port . ...روی کامپیوتر هم در حقیقت همچین مفهومی داره . Portکامپیوتر جایی است که اطلاعات می توانند از آن خارج یا به آن وارد شوند. کیبورد، پرینتر، نمایشگر و مودم از پورتهایی هستند که به راحتی از آنها درک فیزیکی دارید اما پورتهای مجازی توسط نرم افزار ایجاد می شوند. وقتی پورت مودم شما به اینترنت متصل می شود، کامپیوتر شما می تواند هر کدام از پورتها را که تعدادشان بیش از 65000 عدد است ببندد یا باز بگذارد و نیز می تواند به هر کدام از این پورتهای یک کامپیوتر دیگر متصل شود (البته در صورتی که آن کامپیوتر بر روی این پورت چیزی در حال اجرا داشته باشد و نیز دیوارآتش (firewall) آن را نبسته باشد. (در ویندوز XP هنگامی که اینترنت خود را تنظیم می کنید این امکان را به شما می دهد که با استفاده از دیوار آتش جلوی نفوذ دیگران به شما را بگیرد که به طور پیش فرض خودش آنرا فعال می کند). پورتهای خاص کاربردهای خاص دارند. پورت 25 معمولا برای SMTP

)مخفف (Simple mail transfer protocol است و ما برای ارسال ایمیل از آن استفاده کردیم.
اگر قصد دریافت ایمیلهایمان را داشتیم به پورت 110 سر می زدیم، برای مشاهده صفحات وب به سراغ پورت 80 می رویم و... (درست حدس زدید Outlook !هم به طور پیش فرض برای ارسال ایمیل از پورت 25 و برای دریافت آن از پورت 110 استفاده می کند و اینترنت اکسپلورر هم به پورت 80 شماره IP آدرس سایتی که می نویسید سر می زند.) و در پایان اگر پورت را ننویسید، پورت برابر 23 فرض می شود که پورت Telnet است. به پاسخ سوال اول دوباره سر بزنید. وقتی روی لینکی که داده ام کلیک می کنید در حقیقت به پورت 23 آن میزبان متصل می شوید. امروزه بسیاری از سایتها بخصوص سایتهایی که از میزبانی ویندوزی استفاده می کنند سرویس Telnet ندارند و امکان اتصال به پورت 23 وجود ندارد اما من باز هم توصیه می کنم که برای تجربه Shell Account هم که شده Telnet واقعی را تجربه کنید. این Telnet در حقیقت معمولا یک BBS هم هست اما امکانات بسیار زیادی هم برای یک هکر دارد. برای آشنایی اولیه صرف اینکه کمی انگلیسی بفهمید و هرموقع گیر کردید تایپ کنید Help و Enter کنید باید کافی باشد.

دو روش کاربردي براي بدست آوردن IP:
از طریق ایمیل:
هنگامی که شما یک ایمیل از فردی می گیرید، معمولاً آدرس IP وی در آن نامه وجود دارد. ابتدا باید با رفتن به قسمت تنظیمات ایمیل خود آن را در حالتی قرار دهید که تمامی Header نامه را به شما نشان دهد که با کمی گردش در قسمت تنظیمات ایمیل خود آن را پیدا خواهید کرد. حال به بالای ایمیل دقت کنید و به دنبال عبارت Received: from باشید. شما معمولاً دو یا چند بار عبارت "Received: from" را در بالای ایمیل خواهید دید که ما فقط با پایینی کار داریم که معمولاً کمی با بالاییها فاصله دارد و بعد از Message ID قرار می گیرد. آدرس IP فرستنده ایمیل درست در ابتدای این عبارت قرار می گیرد. دادن روش دقیق غیر ممکن است، اما معمولاً همانطور که گفتیم در پایینترین Received باید به دنبال IP باشید. با این حال در شرایطی که فقط در بالاترین Received عددی شبیه IP مشاهده کنید، IP همان است. از سوی دیگر بسیاری از میزبانان ایمیل، راه آسانتری هم برای کمک به شما در نظر می گیرند به این صورت که قسمتی با نامی شبیه به X-Originating-Ip برای شما قرار می دهند و IP فرستنده نامه را در آن می نویسند. به مثالهای زیر توجه کنید که IP فرستنده به رنگ قرمز مشخص شده است:

Received: from yechizi@yechizi.com [62.145.61.1] by server4pfs
(SMTPD32-7.12) id A90313018E; Mon, 30 Jun 2003 00:38:43 -0700
Message-Id: <200306300104500.SM01212@yechizi@yechizi.com>
From: yechizi@yechizi.com
Date: Mon, 30 Jun 2003 01:06:38 -0700
X-RCPT-TO: yechizi@yechizi.com
Status: U
X-UIDL: 347731237

Received: from spf1.us.outblaze.com [205.158.62.158] by server4pfs
(SMTPD32-7.12) id AC9E5400EA; Sat, 07 Jun 2003 09:02:38 -0700
Received: (qmail 31068 invoked from network); 7 Jun 2003 16:03:39 -0000
Received: from unknown (205.158.62.68)
by spf1.us.outblaze.com with QMQP; 7 Jun 2003 16:03:39 -0000
Received: (qmail 61611 invoked from network); 7 Jun 2003 16:03:37 -0000
Received: from unknown (HELO ws1-7.us4.outblaze.com) (205.158.62.57)
by 205-158-62-153.outblaze.com with SMTP; 7 Jun 2003 16:03:37 -0000
Received: (qmail 54891 invoked by uid 1001); 7 Jun 2003 16:03:35 -0000
Message-ID: <20030607160335.54889.qmail@mail.com>
Content-Type: multipart/mixed; boundary="----------=_1055001809-54370-0"
Content-Transfer-Encoding: 7bit
MIME-Version: 1.0
X-Mailer: MIME-tools 5.41 (Entity 5.404)
Received: from [217.218.57.55] by ws1-7.us4.outblaze.com with http for
yechizi@yechizi.com; Sat, 07 Jun 2003 11:03:29 -0500
From: "Reza" <yechizi@yechizi.com>
To: yechizi@yechizi.com

Date: Sat, 07 Jun 2003 11:03:29 -0500
Subject: The Interactive Matrix
X-Originating-Ip: 217.218.57.55
X-Originating-Server: ws1-7.us4.outblaze.com
X-RCPT-TO: <yechizi@yechizi.com>
Status: U
X-UIDL: 344393350

اما یک استثنا: اگر فرد برای فرستادن ایمیل از فرمهای موجود در برخی سایتها مانند سایتهایی که اجازه ارسال یک خبر یا کارت را می دهند یا سایتهایی که ادعای ارسال ایمیل فارسی را دارند (هرچند واقعاً فارسی تایپ کردن در یاهو از اکثر آنها بهتر است) یا فرمهای "تماس با ما" در سایتها استفاده کنند، بعید است IP آنها در ایمیل شما باشد و معمولاً IP سرور خود سایت را در آن می بینید. در مثال زیر که ایمیلی است که با استفاده از فرم هاي "تماس با ما"وب سایت برای مدیر آن ارسال شده بوده است، فقط IP خود وب سایت را مشاهده می کنید:

Received: from server4pfs [38.118.143.98] by iasbs.ac.ir.com with ESMTP
(SMTPD32-7.12) id A5C54400DC; Sat, 07 Jun 2003 06:16:53 -0700
From: <yechizi@yechizi.com>
To: <yechizi@yechizi.com>
Subject: hadirayaneh
Date: Sat, 7 Jun 2003 06:16:53 -0700
Message-ID: <000301c32cf7$1046b740$628f7626@server4pfs>
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft CDO for Windows 2000
Thread-Index: AcMs9xBGKda5j5B/RZms1WTby6vhkQ==
Content-Class: urn:content-classes:message
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
X-RCPT-TO: <yechizi@yechizi.com>
Status: U
X-UIDL: 347730753

از طریق مسنجر ها (در زمان چت کردن):
همانطور که در مقدمه گفتیم، فقط هنگامی که شما در حال ارسال یا دریافت فایلی به طور مستقیم (یا در برخی بازیهای مسنجری) باشید می توانید از این روش استفاده کنید. این روش که به روش Netstat معروف است، از همه روشها معروفتر است ولی به نظر من به خوبی روشهای بالا نیست. با کمی Social Engineering می توان هر کسی را راضی به دریافت یک فایل یا عکس کرد. بهتر است حجم فایل کم نباشد که فرصت کافی داشته باشید. البته اگر از AOL مسنجر استفاده می کنید، در منوهای آن گزینه ای برای برقراری Direct connectionخواهید دید که مناسبتر است. هنگامی که فردی در حال دریافت یا فرستادن فایل به شما به طور مستقیم (نه روش فرستادن فایل با استفاده از Upload در یاهو مسنجر) باشد، با استفاده از Netstat می توانید IP او را ببینید. با توجه به شلوغ بودن خروجی Netstatیکبار قبل از آغاز به گرفتن/فرستادن فایل و بار دیگر بعد از آن این خروجی را بگیرید تا IPفرد را که به تازگی به لیست اضافه شده تشخیص دهید. برای ساده شدن کار بهتر است تمامی برنامه هایی که به هر طریق از اینترنت استفاده می کنند را ببندید که از شلوغی لیست کم شود. اگرچه در بیشتر راهنماها گفته می شود از پسوند -n استفاده کنید، به طور معمول در ایران استفاده نکردن از آن بهتر است. تنها تاثیر -n این است که تمام آدرسها را به طور عددی نشان می دهد و این کار یافتن آدرس IP ایرانیها را که به طور معمول به هر حال به شکل عددی است، در میان عددهای دیگر دشوارتر می کند.
برای اجرای netstat کافی است cmd.exe را از run اجرا کنید و به سادگی در آن تایپ کنید netstatو enter را فشار دهید. لیستی از تمامی اتصالهای موجود بین کامپیوتر شما و کامپیوترهای دیگر را مشاهده خواهید کرد. حال پس از برقراری ارتباط، دوباره این کار را تکرار

کنید، آدرس جدید آدرس IP فرد مورد نظر است. اگر در لیست آدرسهای عددی ندیدید، از netstat -nاستفاده کنید. با کمی تمرین این روش برایتان آسان می شود. یک روش کمکی استفاده از روش رو به رو است 'netstat > temp1.txt' :که این کار خروجی netstat را به درون فایل temp1.txt می ریزد. (که اگر وجود نداشته باشد ساخته می شود و اگر از قبل موجود باشد اطلاعات قبلی آن پاک می شود!) و سپس پس از برقراری اتصال، 'netstat > temp2.txt'را وارد می کنید و سر فرصت تفاوت فایلها را بررسی می کنید.

بخش ششم – آشنايي با NetBIOS:

مخفف عبارت Network Basic Input/Output System است NetBIOS .ابزاري است كه اجازه به اشتراک گذاشتن منابع رو به ما مي‌ده. ما برای به اشتراک گذاشتن فایل‌ها و یا پرینتر مي‌تونيم از اين پروتكل استفاده كنيم. نكته مهم اين است كه NetBIOS فقط در سيستم‌عامل ويندوز معني داره (اگرچه ابزارهايي مثل Samba در لينوكس مي‌تونن اونو شبيه سازي كنن ولي بحث ما خود پروتكل NetBIOS است). وقتي NetBIOS در ويندوز فعال باشد، بلافاصله سه تا پورت براي استفاده باز مي‌شوند. پورت مهم و اصلي پورت ۱۳۹ در tcp است كه NetBIOSرا هم با اين پورت مي‌شناسن. دو پورت ديگر، از نوع udp هستند و عبارتند از پورت ۱۳۷ براي name service و پورت ۱۳۹ براي . Datagram service وقتي قرار باشه كه يک سيستم‌عامل ويندوز هک بشه (خصوصا اگه كلاينت باشه) يكي از اولين مواردي كه به ذهن مي‌رسه، استفاده از NetBIOS ه.

حالا ببينيم منظور از به اشتراک گذاشتن (Sharing) در مورد فایل‌ها و پرینترها چیست؟ به اشتراک گذاشتن در مورد فايل‌ها يعني قرار دادن تعدادي فايل در يک كامپيوتر خاص به طوريكه توسط ساير كامپيوترها قابل دسترسي و استفاده باشه. در مورد پرينتر به اشتراک گذاشتن يعني طوري چاپگر متصل به يک كامپيوتر را تنظيم كنيم كه توسط ساير كامپيوترها هم قابل استفاده باشه. با توجه به اينكه در سيستم‌عامل‌هاي ويندوز به صورت پيش‌فرض NetBIOSفعال است، پس مي‌توان به تعدادي از فايل‌ها و فولدرهاي تعدادي از كامپيوترهاي روي شبكه دسترسي داشت و فايل‌ها را خواند و حتي كپي يا پاک كرد.

چگونه با پورت ۱۳۹ صحبت كنيم؟

اولين كاري كه مي‌كنيم اين است كه براي پورت ۱۳۹ پورت اسكن مي‌كنيم تا ip هايي را كه پورت ۱۳۹ در آنها باز است، پيدا كنيم. من اين كار را با nmap انجام مي‌دم. فرض كنيد كه يک ipبه شماره 217.218.84.29 را تست كرده و به نتيجه زير برسم:

Interesting ports on HOME-TU6U0AV86Y (217.218.84.29):
Port State Service
139/tcp open netbios-ssn

Remote operating system guess: Windows Millenn... (Me), Win 2000, or WinXP

اين خروجي اعلام مي‌كند كه پورت ۱۳۹ باز است. پس مي‌شود از اين ip استفاده كرد. حالا مي‌خوام با اين پورت ارتباط برقرار كنم. اصولا بايد مثل سابق از telnet يا nc استفاده كنم ولي در مورد پورت ۱۳۹ روش ارتباطي فرق مي‌كند. كامنت پرامت را باز كرده و دستور زير را مي‌نويسم:

nbtstat -A 217.218.84.29

دستور nbtstat يک ابزار خاص براي كار با NetBIOS است. دقت كنيد كه از پارامتر -A با ip مربوطه استفاده كردم. (دستور nbtstat داراي پارامترهاي بسياري است كه اگه مي‌خواين همه رو ببينين، بنويسين nbtstat و enter را بزنيد(.

حالا بحث اينه كه اين دستور چه كاري مي‌كنه و خروجي به چه صورتي است:

اين دستور به ip مورد نظر وصل مي‌شه و از اون مي‌خواد ليست منابعي رو كه به اشتراک گذاشته رو ليست كنه. در اين حالت ۲ حالت ممكنه اتفاق بيوفته:

الف) مواجه با پيغام Host not found بشم. اين يعني اينكه نمي‌تونه ليست منابع را از اون كامپيوتر بگيره (يعني NetBIOS غير فعاله). يعني اگرچه پورت ۱۳۹ بازه ولي قابل استفاده نيست.

ب) ارتباط برقرار بشه و ليست منابع اشتراكي ليست بشه:

NetBIOS Remote Machine Name Table

Name Type Status

HOME-TU6U0AV86Y<00> UNIQUE Registered

MSHOME <00> GROUP Registered

HOME-TU6U0AV86Y<20> UNIQUE Registered

MSHOME <1E> GROUP Registered

MAC Address = 00-53-45-00-00-00

در اين نتايج چيزي كه به درد مي‌خوره، سطري است كه <20> دارد. اگه <20> نباشد، يعني نمي‌تونين از اشتراک گذاري فايل استفاده كنيد (به عبارت ساده تر بي‌خيال شو اين كامپيوتر رو !). در اين مثال ما اين سطر را داشتيم پس ادامه مي‌دهيم. حالا مي‌نويسم:

net view \\217.218.84.29

حالا اگه گفتين چي ميشه؟ درسته! دو حالت ممكنه اتفاق بيوفته:

الف) پيغام بياد

System error 5 has occurred.

Access is denied.

اين يعني نمي‌تونين ادامه بدين. به عبارت ديگه ايست! ولي يه كاري مي‌تونيد بكنيد و اون اينه كه يه null session برقرار كنيد با اون كامپيوتر. اين حالت در مورد ويندوزهاي سري NT جواب ميده. مي‌نويسيد:

net use \\217.218.84.29\IPC$ "" /user:""

حالا چرا مي‌گن null session ؟ دليلش اينه كه يک ارتباط برقرار كردم با اون ip بدون username و بدون . password حالا اگه اين دستور جواب داد مي‌تونم دوباره دستور net view \\217.218.84.29را تكرار كنم.
ب) ممكنه دستور ذكر شده جواب بده و مثلا جواب بده:

Shared resources at \\217.218.84.29

Share name Type Used as Comment

Printer Print Acrobat PDFWriter

Printer2 Print Acrobat Distiller

SharedDocs Disk

The command completed successfully.

عاليه. دقت كنيد كه در اين كامپيوتر يک فايل (Disk) به اسم ShareDocs به اشتراک گذاشته شده (دو تاي باقي براي پرينتر است). حالا كه رسيدم به اين اسم ديگه آخرين دستور را مي‌نويسم.

حالا وقتشه که واقعا عمل به اشتراک گذاشتن رو انجام بديم. براي اينکار بايد يک درايو انتخاب کنيد. حتما مي‌دونيد که درايو چيه. وقتي شما My Computer را دابل کليک کرده و باز مي‌کنيد، يک سري آيکون مي‌بينيد که هر کدام اسمي دارند. مثلا A: براي فلاپي و و و تا مي‌رسيد به cdrom که آخرين حرف را دارد. مثلا فرض کنيد که K: باشه. حالا بايد اسم درايو رو براي اشتراک گذاشتن انتخاب کنيد. براي اين‌کار حرف بعدي در زبان انگليسي رو به کار ببريد. چون در کامپيوتر من K: آخرين بود، من حرف بعدي يعني L: را انتخاب مي‌کنم و دستور زير را مي‌نويسم:

net use L: \\217.218.84.29\SharedDocs

به اسم درايو، ipو نام مربوطه که ShareDocs دقت کنيد. چون من اصطلاحا به صورت null sessionدارم ارتباط مي‌گيرم، ممکنه کار نکنه ولي اگه درست کار کنه جواب مي‌شنوم:

The command completed successfully.

معرکه است!!! حالا My Computer رو باز کنيد و ببينيد که درايو جديد به ليست درايوها اضافه شده که مي‌تونين مثل درايوهاي معمولي با اون کار کنيد و فايل کپي کنيد و...

-۵وقتي کار تموم شد مي‌تونيد درايو رو حذف کنيد. براي اينکار مي‌تونين روي درايو رايت‌کليک کنيد و Disconnect را انتخاب کنيد. و يا اينکه از دستور

net use /delete L:

استفاده کنيد.

بخش هفتم – آشنايي با اسب هاي تراوا:

10سال بود که یونانیها شهر Troy را بدون هیچ نتیجه ای محاصره کرده بودند. سرانجام آنها وانمود کردند که عقب نشینی می کنند و فقط یک اسب بزرگ چوبی از خود به جا گذاشتند که تعدادی از دلاوران آنها از جمله ادیسه در آن پنهان شده بودند. تروجنها (اهالی شهر Troy) اسب را به عنوان یک غنیمت جنگی به داخل شهر خود بردند و سرخوش از احساس پیروزی سرگرم جشن شدند. شب هنگام دلاوران یونانی از اسب خارج شدند و با غافلگیر کردن تروجنها، شهر تروی را تسخیر کردند
داستان تاریخی بالا که احتمالاً پیش از این هم آنرا شنیده یا آن را در تلویزیون دیده بودید باید ایده ای از اسبهای تروا به شما داده باشد: اسب تروا برنامه ای است که ادعا می کند برنامه ای مفید و خواستنی است اما در حقیقت هدف دیگری دارد. اسب تروا ممکن است در قالب یک بازی، یک محافظ نمایشگر، یک آلبوم عکس و یا حتی یک ویروس کش به شما فرستاده شود، اما درست هنگامی که شما مشغول لذت بردن از تماشای آن هستید، رمزهای عبور شما و فایلهایتان را به کسی ارسال کند و یا حتی به آن فرد امکان کنترل سیستم شما و پاک کردن فایلهایتان را بدهد
اسبهای تروا را به طور کلی می توان به دو گروه اصلی زیر تقسیم کرد
1. Backdoor Trojans (تروجنهای ایجاد کننده در پشتی): یک اسب تروا از این نوع به طور کلی از یک فایل میزبان (server) و یک فایل ارباب رجوع (client) تشکیل می شود که فرد نفوذگر با چسباندن فایل میزبان (سربازها) به یک فایل مورد علاقه شما (اسب) شما را به سمت اجرای میزبان روی سیستم خود سوق می دهد. این فایل پس از اجرا با باز کردن یک پورت روی سیستم آلوده به فرد نفوذگر اجازه می دهد که با استفاده از ارباب رجوع (client) تروجن به میزبان متصل شود و از این راه کنترل سیستم شما را بر عهده بگیرد. از میان این تروجنها می توان به Sub7 ، NetBus، Giftو bf/gf اشاره کرد.
2. اسبهای تروای ارسال کننده رمز: چنین تروجنی معمولاً فقط شامل فایلی است که باید پس از چسبانیده شدن به یک فایل دلخواه برای سیستم هدف ارسال شود. این تروجن پس از اجرا، رمزهای عبور و برخی اطلاعات دیگر مانند آدرس IP سیستم قربانی را به فرد نفوذگر از طریق ایمیل (یا از طریق مسنجرها) ارسال می کند. از معروفترین تروجنهای این دسته می توان به Ajan و Barok اشاره کرد.

اگرچه معمولاً گفته می شود تفاوت اساسی تروجنها با ویروسها در این است که یک اسب تروا بر خلاف ویروسها و کرمها توانایی تولد مثل ندارد یعنی سایر فایلهای شما را آلوده نمی کند و خود را به رایانه های دیگر ارسال نمی کند؛ تروجنهایی که خصوصیات ویروسی داشته باشند هم ساخته شده اند. مثلاً Kuang2v تروجنی است که با آلوده کردن فایلهای اجرایی خود را پخش می کند و تمام خصوصیات دیگر تروجنها مانند امکان اتصال از ارباب رجوع Client)) به میزبان (Server) را هم دارا می باشد.
در یک نگاه دقیقتر به مراحل آلوده سازی یک اسب تروا، مراحل زیر را داریم :
اسب تروا (همراه با برنامه مفیدی که به آن متصل شده است) روی رایانه هدف، اجرا می شود.
اسب تروا یک نسخه از خود را جایی روی هارددیسک کپی می کند (معمولاً در یکی از شاخه هایwindows ، systemیا .(system32 برخی از تروجنها در این مرحله نسخه اصلی خود را از روی هارددیسک پاک می کنند و فقط نسخه کپی را باقی می گذارند.
اسب تروا با دستکاری) Registry یا سایر روشهای مناسب) ترتیبی می دهد که با هر بار اجرای ویندوز، نسخه کپی تروجن نیز اجرا شود.
اسب تروا منتظر برقراری ارتباط با اینترنت می ماند و پس از برقراری ارتباط وظیفه خود را انجام می دهد. مثلاً رمزهای عبور فرد قربانی را به فرد نفوذگر ارسال می کند یا با باز کردن پورتی روی سیستم آلوده امکان کنترل آن از راه دور توسط فرد نفوذگر را فراهم می کند.
ذکر این نکته هم لازم است که برخلاف آنچه ممکن است در ابتدا به نظر برسد، نوشتن یک تروجن معمولی کاری بسیار ساده است و هر فردی که کمی با زبانهای برنامه نویسی ویندوز آشنا باشد می تواند با استفاده از کنترل Winsockبه راحتی یک تروجن ساده بنویسد.

بخش هشتم – نحوه کار با یك اسب تراوا:

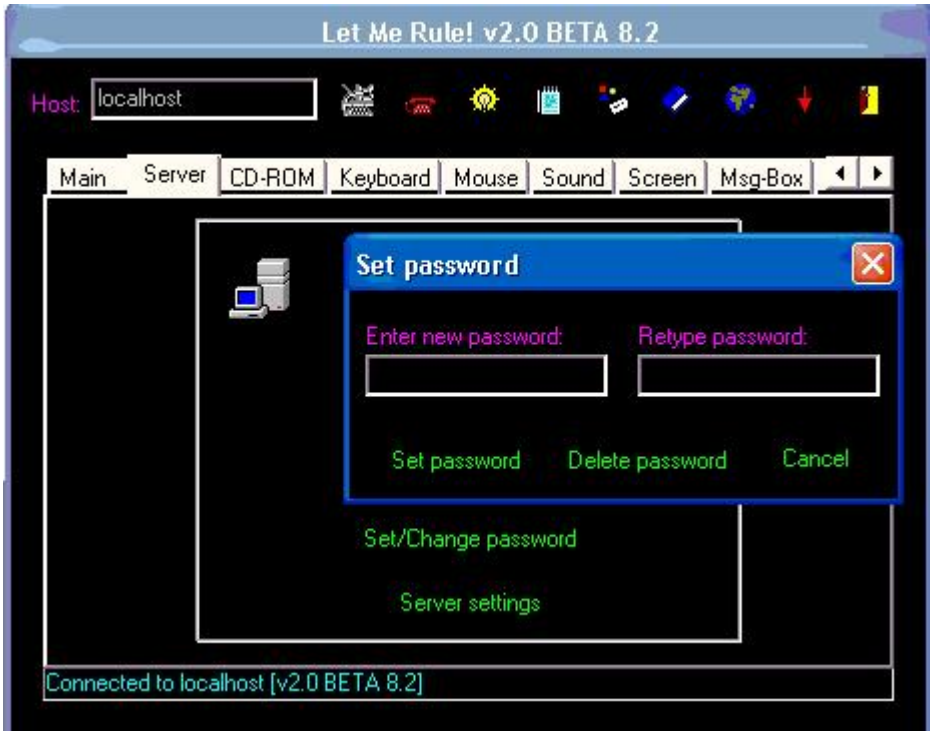
پس از بررسی مقدمات در بخش قبلي اینک آمادگی داریم که به بررسی عملی اسبهای تروا بپردازیم. از بین دهها اسب تروا، اسب تروای !Let Me Rule را انتخاب کردم که هم از نظر امکانات بسیار کامل است و هم از نظر زمانی بسیار جدید است و روی تمامی نسخه های جدید ویندوز هم به خوبی کار می کند. با این برنامه، رایانه آلوده شده به طور کامل در اختیار شما خواهد بود به گونه ای که از راه دور می توانید کیبورد آنرا کنترل کنید و کلیدهای فشرده شده روی کیبورد را ببینید، mouse را کنترل کنید یا حتی با mouse شوخی کنید یا آنرا قفل کنید، مانیتور فرد را خاموش یا محافظ صفحه نمایش او را فعال کنید، پیام دلخواه خود را روی صفحه نمایش او ظاهر و یا با او گپ بزنید، مرورگر اینترنت وی را به سایت دلخواهی بفرستید، فایلی از رایانه او بگیرید یا به آن بفرستید، صفحه نمایش وی را مشاهده کنید و قابلیتهای بسیار دیگر که در اینجا فرصت ذکر همه آنها نیست. جدیدترین نسخه این تروا در حال حاضر Let Me Rule v2.0 BETA 8.2 می باشد که کار طراحی و بهتر کردن آن کماکان از سوی سازندگانش ادامه دارد. از آنجایی که اکثر ترواها کاملاً به هم شبیه هستند، با کمی دقت در این نوشته می توانید از اکثر ترواهای معروف و قدرتمند به راحتی استفاده کنید. توجه داشته باشید که این ترواها را فقط روی دستگاههایی می توانید اجرا و یا حتی آزمایش کنید که از صاحبان آنها اجازه داشته باشید. همچنین به خاطر داشته باشید که ترواها می توانند ابزارهای مناسبی برای کنترل رایانه خودتان از راه دور باشند.

نخستین گام برای استفاده از تروا، اجرای فایل server.exe روی رایانه ای است که می خواهیم کنترل آنرا به دست آوریم. اگر قصد دارید این تروا را با کمک دوستتان آزمایش کنید یا به دو دستگاه رایانه متصل به اینترنت دسترسی دارید این فایل را روی یکی از آنها اجرا کنید، در غیر این صورت می توانید برای آزمایش، آنرا روی رایانه خود اجرا کنید. توجه داشته باشید که نام فایل server.exe اهمیتی ندارد و فقط کافیست پسوند فایل یک پسوند اجرایی باشد. به عنوان نمونه می توانید نام آنرا به Game.exe، Cool.scr، Update.com یا Elite.pif تغییر دهید. به رایانه ای که این فایل روی آن اجرا شده باشد victim یا رایانه آلوده شده می گوییم. این فایل پس از اجرا پیزی روی صفحه ظاهر نمی کند و صرفاً در پشت صحنه وظیفه خود را انجام می دهد. اگر روی اینترنت به دنبال برنامه های Binder جستجو کنید، برنامه هایی خواهید یافت که می توانند server.exe را به یک برنامه بی آزار یا حتی یک عکس بچسبانند طوری که در هنگام اجرا به نظر برسد که تنها آن عکس یا برنامه بی آزار اجرا شده است.

گام دوم به دست آوردن آدرس IP رایانه ای است که server.exe روی آن اجرا شده است. اگر به آن رایانه دسترسی دارید وارد command prompt آن شوید و دستور IPconfig را Enter کنید. برای مشاهده آدرس IP علاوه بر روش فوق می توانید در نسخه های قدیمی ویندوز در قسمت Run منوی Start برنامه WinIPcfg را اجرا کنید و در ویندوزهای جدید با دوبار کلیک روی مانیتورهای نشان دهنده اتصال به اینترنت کنار ساعت و انتخاب details آنرا بیابید.

اگر روی رایانه خود آزمایش می کنید، می توانید به جای آدرس IP واقعی خود آدرس 127.0.0.1 یا اصطلاح localhost را در نظر بگیرید. اگر به رایانه ای که قصد کنترل آنرا دارید دسترسی ندارید و نمی توانید آدرس IP آنها را از ایشان سوال کنید، یکی از روشهای نوشته شده در قسمتهای اخیر این سلسله مقالات را به کار ببرید.

حال که server.exe روی سیستمی اجرا شده و شما IP آن سیستم را به دست آورده اید، نوبت به قدم سوم یعنی اجرای فایل اصلی تروا می رسد که در همه تروجاها از روی بیشتر بودن اندازه اش نسبت به فایل server قابل تشخیص است و نامش همنام نام تروا است یا نامی مانند client.exe دارد. این فایل را که در اینجا نامی شبیه به Let Me Rule! v2.0.exe دارد و در حقیقت مرکز کنترل تروا است، روی رایانه خود اجرا می کنیم. پس از اجرا شدن برنامه، آدرس IP را که در گام دوم به دست آورده بودیم در قسمت Host می نویسیم و روی آیکون تلفن که نشانه Connect است کلیک می کنیم. اگر همه چیز به درستی پیش رفته باشد، صفحه ای برای شما باز می شود که روی آن اطلاعاتی از قبیل نسخه نرم افزار server.exe که برای آلوده سازی به کار برده شده بوده، آدرسی که برای نخستین بار فایل server.exe از آنجا اجرا شده بوده است، تعداد افرادی که برای کنترل کامپیوتر مورد نظر شما (که یک نفر آنها خود شما هستید) به آن متصل شده اند و اطلاعات دیگری مانند زبان ویندوز فرد را به شما می دهد.



اگر همه چیز تا اینجا به درستی پیش رفته باشد، از این لحظه شما کنترل رایانه آلوده شده را به دست گرفته اید. بهتر است با کلیک کردن روی منوی Server و انتخاب گزینه Set/change password روی سرور رمز بگذارید تا فقط خود شما بتوانید آنرا از این روش کنترل کنید. در این صورت هر بار قبل از اتصال به رایانه آلوده شده لازم است این رمز عبور را وارد کنید. در منوی Server گزینه جالب و کاربردی وجود دارد به نام IP notification که داخل قسمت Server settings قرار دارد و به شما این امکان را می دهد که همواره از آدرس IP رایانه آلوده شده مطلع باشید. در زیر به برخی گزینه های سایر منوهای این برنامه به شکلی بسیار خلاصه اشاره می کنیم که شما با آزمایش عملی این قسمتها آنها را بهتر خواهید شناخت:

منوی CD: برای باز و بسته کردن درایو CD رایانه آلوده شده به کار می رود. با دادن عدد به تایمر این قسمت می توان برنامه را تنظیم کرد تا هر چند لحظه یکبار درایو CD را بازو بسته کند.

منوی Keyboard: برای روشن و خاموش کردن Caps lock، Scroll lock و Numlock، قفل کردن صفحه کلید و یا با استفاده از گزینه keylogger برای مشاهده تمام کلیدهایی که روی رایانه آلوده تایپ می شود به کار می رود.

منوی mouse: برای کنترل mouse یا تغییر شکل آن به کار می رود. گزینه Crazy mouse با نوعی شوخی Mouse رایانه آلوده را به طور اتفاقی روی صفحه به حرکت در می آورد و به طور اتفاقی کلیک می کند.

منوی sound: برای پخش یک فایل صوتی روی رایانه آلوده شده یا کنترل شدت صدای آن به کار می رود.

منوی screen: این قسمت بسیار کاربردی است. از شوخیهایی مانند از کار انداختن منوی start و task bar و خاموش کردن مانیتور و حرکت دادن صفحه نمایش و مانند آنها گرفته تا قسمت Screen shot که برای مشاهده صفحه نمایش رایانه آلوده به کار می رود. گزینه Screen shot عکسی از صفحه نمایش رایانه آلوده شده می گیرد و آنرا به شما نشان می دهد.

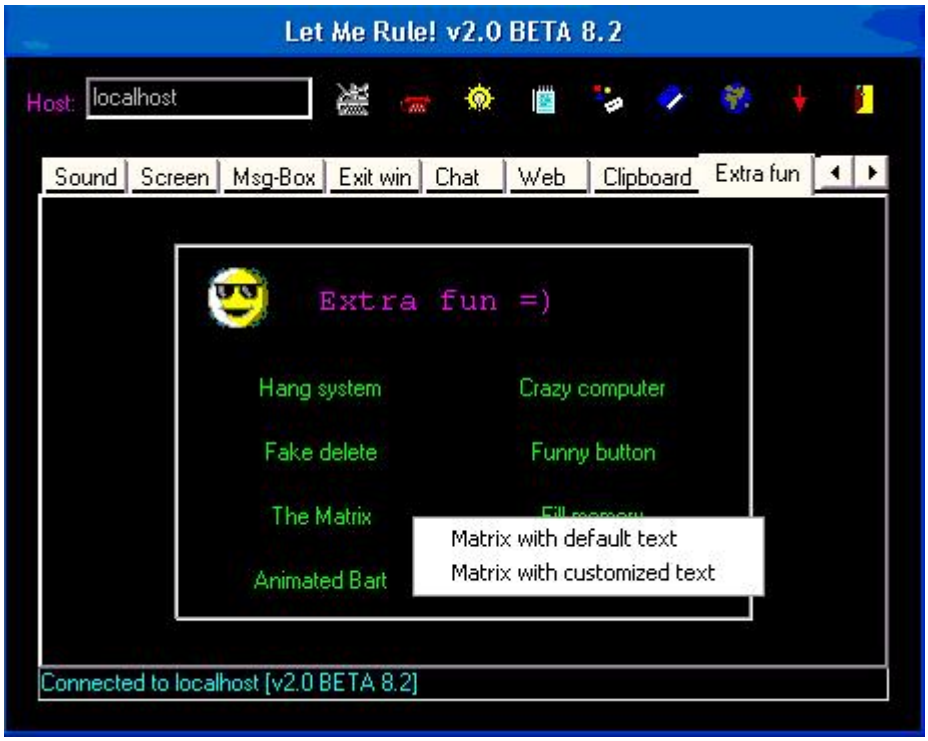
منوی Msg-Box: برای ساختن و فرستادن یک پیام خطا یا سوال به شکل ویندوزی با نوشته دلخواه شما به کار می رود.

منوی Exit win: برای خاموش یا اجرای دوباره رایانه آلوده شده و یا Log off کردن کاربر آن به کار می رود.

منوی Chat: این قسمت برای گفتگوی متنی با کاربران رایانه آلوده شده به کار می رود. صفحه ای برای آن کاربران باز خواهد شد که از طریق آن می توانند با شما گفت و گو کنند.

منوی Web: برای فرستادن کاربران رایانه آلوده به یک آدرس اینترنتی یا باز کردن برنامه ایمیل آنها به کار می رود.

منوی Clipboard: Clipboard فضایی است که هنگامی که چیزی را Copy یا Cut می کنید به داخل آن می رود. این منو برای مشاهده محتویات Clipboard رایانه آلوده شده، قفل کردن یا تغییر آن به کار می رود.



منوی Extra fun: این منو که بیشتر به منظور شوخی طراحی شده است، گزینه های بسیار جالبی دارد. مانند گزینه ای که منوی Start را به جرکت در می آورد یا گزینه ای که دگمه ای روی صفحه ظاهر می کند که از Mouse فرار می کند و یا گزینه ای که بدون ایجاد هیچ صدمه ای وانمود می کند در حال پاک کردن فایلهای رایانه آلوده شده است!

منوی File manager: برای مشاهده و مدیریت فایلهای رایانه آلوده شده و تبادل فایل با آن و نیز برای اجرای دستورات محیط Command prompt بر روی آن به کار می رود.

منوی Time: اطلاعاتی مانند ساعت و تاریخ رایانه آلوده شده را به ما می دهد و اجازه می دهد آنها را تغییر دهیم یا ساعت را از روی نوار Task bar حذف کنیم.

منوی System Info: اطلاعات مختصر و مفیدی درباره مشخصات سخت افزاری و نرم افزاری رایانه آلوده شده به دست می دهد.

منوی Printer: جهت چاپ کردن نوشته ای روی دستگاه چاپگر متصل به رایانه آلوده شده به کار می رود.

منوی Registry: با داشتن یک Registry Explorer قدرتمند به شما اجازه مشاهده، تغییر و حذف یا اضافه اطلاعات آن را می دهد.

منوی Tweaks: تنظیمات بسیار جالبی مانند تنظیمات مربوط به نام رایانه، نام My computer و Recycle bin، تنظیمات Mouse، تنظیمات اینترنت اکسپلورر و مانند آنها را در اختیار شما قرار می دهد.

منوی RAS manager: اگر رایانه آلوده شده با استفاده از مودم و خط تلفن به اینترنت متصل شده باشد با استفاده از گزینه های این قسمت می توانید لیست اکانتهای وی را به همراه نام کاربری و رمز عبور آنها (در برخی نسخه های قدیمی تر ویندوز) مشاهده کنید، آنها را تغییر دهید، تلفن را قطع کنید و یا شماره خاصی را شماره گیری نمایید!

منوی Other: در این قسمت گزینه هایی که در شاخه دیگری جای نمی گرفتند را مشاهده می کنید مانند باز کردن منوی Start، قفل کردن سیستم، خالی کردن حافظه میانی صفحه کلید و Mouse و مانند آنها.

علاوه بر منوهای مذکور، کمی بالاتر از آنها و در کنار تلفنی که در آغاز برای اتصال روی آن کلیک کردید، آیکونهای دیگری نیز وجود دارند که به عنوان نمونه Disconnect برای قطع کردن ارتباط، Ping برای اطمینان از اتصال رایانه آلوده شده به اینترنت و به دست آوردن تخمینی از سرعت تبادل اطلاعات و Options برای تنظیمات برنامه شامل تنظیمات مربوط به ظاهر و کارکرد برنامه، انتخاب Nickname که در هنگام استفاده از قسمت Chat نام شما خواهد بود، تنظیم نوع و کیفیت عکسی که در قسمت Screen shot از صفحه نمایش رایانه آلوده شده گرفته می شود و تنظیمات مشابه به کار می رود.

پس از اینکه آزمایش شما به پایان رسید برای حذف میزبان از رایانه آلوده و پاکسازی آن، کافی است به منوی Server بروید و گزینه Remove Server را انتخاب کنید. به این شکل آن رایانه آلوده نخواهد بود و دیگر نخواهید توانست به آن رایانه متصل شوید و کنترل آنرا به دست بگیرید.

بخش نهم – نفوز به ویندوز:

در این بخش با یک راهبرد عملی برای نفوذ آشنا می شویم که لازمه آن دسترسی داشتن به رایانه روشن دارای ویندوز XP می باشد و مباحث تئوریک را فقط در حد نیاز بررسی می کنیم.

در ویندوز XP علاوه بر کاربرانی که شما تعریف می کنید، کاربر دیگری به نام Administrator وجود دارد که نه تنها در لیست کاربران صفحه ورود به ویندوز نشان داده نمی شود، بلکه اگر با استفاده از گزینه User Accounts موجود در Control Panel هم لیست کاربران سیستم را مشاهده کنید، اسمی از آن برده نشده است. همین امر سبب می شود که به احتمال قوی اگر شما رمز این کاربر را به نحوی تغییر دهید و بتوانید از طریق آن وارد

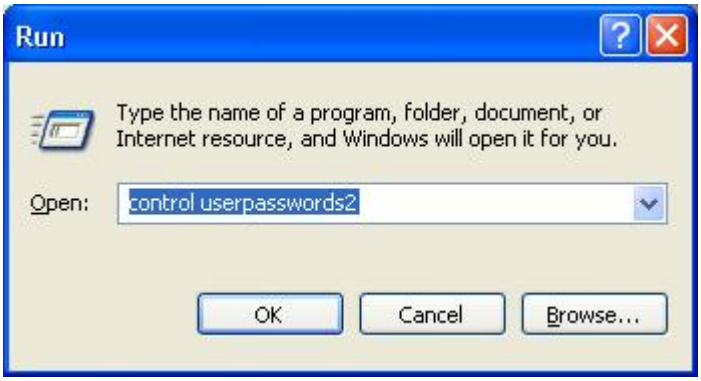
سیستم شوید تا مدتها کسی از این موضوع باخبر نشود و بتوانید با استفاده از این کاربر چه از راه دور و از طریق اینترنت (که در جای خود شرح داده خواهد شد) و چه به طور محلی وارد آن رایانه شوید و از آنجایی که این کاربر بالاترین حقهای دسترسی به تمام پوشه ها و تنظیمات را دارد، نفوذی از این کاملتر متصور نخواهد بود.

ابتدا برای آشنایی با محیط ورود به ویندوز XP، اگر روی سیستم خود تنها یک کاربر دارید با استفاده از گزینه User Accounts موجود در Control Panel و انتخاب Create a new account دو کاربر یکی از نوع Limited و دیگری از نوع Computer Administrator بسازید (بر خلاف ظاهر امر، XP از تمام انواع کاربرانی که ویندوز 2000 داشت هم پشتیبانی می کند اما در اینجا فقط همین دو حالت را نمایش می دهد) به این صورت که ابتدا نام کاربر را وارد می کنید و سپس نوع آنرا انتخاب و کلید Create account را فشار می دهید. کمی با تنظیمات این قسمت کار کنید تا بتوانید به راحتی کاربر بسازید، رمز عبور و مشخصاتش را تغییر دهید و یا آنرا حذف کنید. حال سیستم را مجدداً راه اندازی کنید.

این بار با صفحه ای مواجه می شوید که نام کاربران مختلف سیستم شما را نشان می دهد تا بتوانید با استفاده از هرکدام که تمایل داشتید وارد سیستم شوید اما بازهم اثری از Administrator نمی بینید. حال کلیدهای Ctrl+Alt+Del را دو بار پشت سر هم فشار دهید. مشاهده می کنید که ظاهر منوی ورود به سیستم تغییر می کند به صورتی که می توانید نام کاربری را هم مانند رمز عبور تایپ کنید. حال نام کاربری Administrator را با رمز عبوری که هنگام نصب ویندوز به آن داده اید وارد کنید تا به عنوان مدیر سیستم وارد ویندوز خود شوید.

تذکر: یکی از مهمترین نقایص امنیتی در ویندوزهای XP نصب شده در ایران در هنگام نصب آنها ایجاد می شود. بسیاری از افراد هنگام نصب ویندوز در مرحله ای که از آنها خواسته می شود رمز Administrator را وارد کنند آن رمز را خالی می گذارند و در برخی موارد دیگر نیز کسی این رمز را تعریف می کند که طبق قاعده نباید دسترسی به اطلاعات آن سیستم را داشته باشد. هرگز این کاربر را فراموش نکنید!

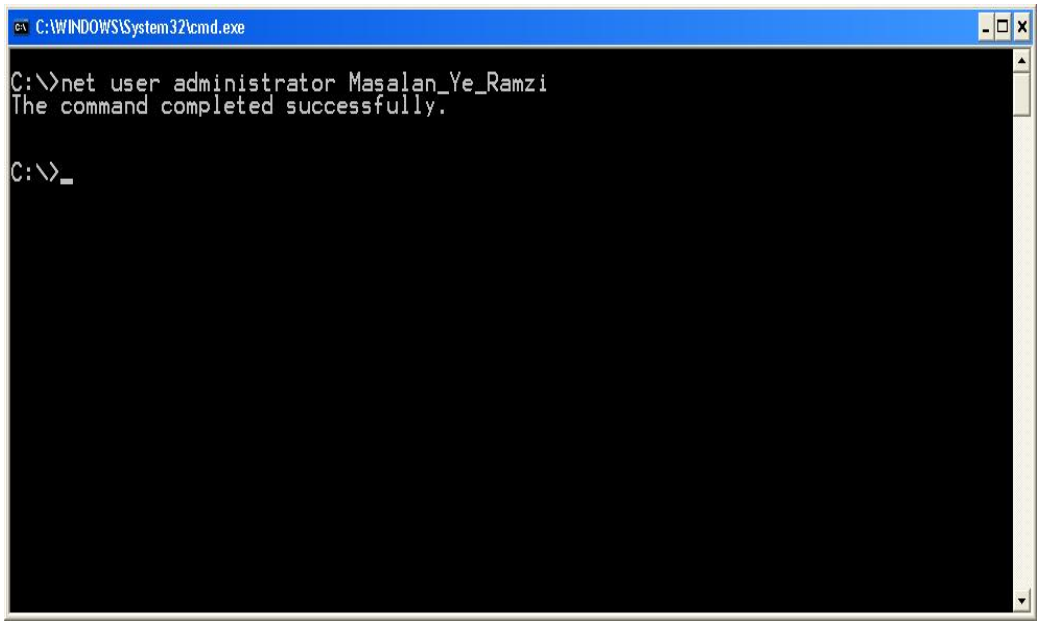
اگر رمز عبور Administrator را به یاد نیاوردید نگران نباشید، قصد داریم روشی به شما ارائه کنیم که بدون دانستن رمز این کاربر رمز عبور آن را تغییر دهید! با یک کاربر دیگر وارد سیستم شوید که از نوع Computer Administrator باشد. از منوی Start، گزینه Run را انتخاب کنید و در آن تایپ کنید: Control userpasswords2 و Ok کنید. حال از لیست کاربر Administrator را انتخاب و روی کلید Reset password کلیک کنید. کافیست رمز دلخواه خد را دو بار تایپ و Ok کنید! حال رمز Administrator در اختیار شماست و می توانید به روش گفته شده در بالا یعنی با فشردن کلیدهای Ctrl+Alt+Del دو بار پشت سر هم و تایپ نام کاربری Administrator و رمز عبوری که به آن اختصاص داده اید به عنوان مدیر سیستم وارد ویندوز خود شوید.



اگر سیستمی که شما با آن کار کردید به هر دلیل به Control userpasswords2 پاسخ نداد، نگران نشوید! راه دیگری پیش پای شما می گذاریم: از منوی Start پس از انتخاب All programs و Accessories گزینه Command Prompt را انتخاب کنید. حال دستور زیر را تایپ و Enter کنید:

net user Administrator RamzeJadid

دستور فوق رمز عبور Administrator را برابر RamzeJadid قرار می دهد.



بار دیگر مراحلی که ممکن است توسط یک نفوذگر برای ورود به سیستم شما مورد استفاده قرار گیرد را با هم مرور می کنیم: ابتدا با استفاده از فرصتی مناسب که سیستم با کاربری از نوع Computer Administrator دقایقی به حال خود رها شده باشد اقدام به تغییر رمز Administrator می کند (حدود 10 ثانیه تنها گذاشتن سیستم با چنین کاربری می تواند این نتیجه را داشته باشد پس مراقب باشید!) سپس هر زمان که بخواهد وارد سیستم شود با استفاده از رمز Administrator از طریق دو بار فشردن همزمان کلیدهای کلیدهای Ctrl+Alt+Del به راحتی به اطلاعات شما دسترسی پیدا می کند و از آنجایی که شما هرگز از این کاربر استفاده نمی کردید، احتمالاً هرگز متوجه این تغییر رمز نخواهید شد!!

تذکر: قبل از خواندن ادامه این مطلب مطمئن شوید مراحل بالا را به خوبی متوجه شده و تمرین کرده اید.

حال سوال اصلی اینجاست که فرد چگونه می تواند با استفاده از این اطلاعات از راه دور وارد سیستم شما شود. ساده ترین راه استفاده از یکی از برنامه های داخلی ویندوز به نام Remote Desktop Connection می باشد که برای اجرای آن کافیست در ویندوز XP از منوی Start گزینه Run را انتخاب (یا کلید ویندوز کیبورد خود را همزمان با حرف R فشار دهید) و تایپ کنید mstsc و Ok را کلیک کنید. همچنین می توانید این برنامه را در قسمت Communications از Accessories موجود در All Programs منوی Start خود نیز پیدا کنید.

نرم افزار Remote Desktop Connection به شما اجازه می دهد به هر رایانه ای که آدرس IP آنرا بدانید (روشهای به دست آوردن IP به طور مفصل در سلسله مقالات آشنایی با اسب تروا بیان شده است که می توانید به آنها رجوع کنید) متصل شوید. پس از نوشتن آدرس

IP و فشردن Connect وارد صفحه Login ویندوز سیستم هدف خواهید شد که می توانید با داشتن نام کاربری و رمزعبورش وارد آن شوید. پس با داشتن رمز Administrator و IP سیستم بدون اینکه کسی متوجه شود یا نرم افزار ضد ویروس کار شما را خطا بداند می توانید با کاربر دارای بالاترین حقها به رایانه های هدف دسترسی پیدا کنید. (اگر اینترنت را به دنبال رایانه هایی که پورت Remote Desktop باز دارند جستجو کنید در حوزه دومینهای ایرانی سیستمهای بسیاری را خواهید یافت که رمزهای شرم آوری مانند 123 داشته باشند یا از آن بدتر رمز آنها تنها یک Enter باشد!)

اگرچه روش فوق به نظر زیاد عملی نمی رسید زیرا به حدود 10 ثانیه دسترسی فیزیکی به سیستم در شرایط Login شده با یک کاربر از نوع Computer Administrator نیاز داشت، روش بیان شده در بالا اصول بسیاری از روشهای نفوذ به ویندوز XP از جمله روشهایی مانند استفاده از نقص امنیتی RPC بود! پس موارد بالا را به دقت بخوانید و با نرم افزارها و صفحاتی که باز کردیم کار کنید تا با آنها به خوبی آشنا شوید.

امیدواریم از این نوشته نتیجه گرفته باشید که اولاً رمز کاربر Administrator را به رمزی مناسب تغییر دهید و ثانیاً اگر امنیت سیستم شما به هر دلیل اهمیت دارد هرگز حتی برای چند ثانیه آنرا روشن و Login شده رها نکنید و ثالثاً کاربری با رمز عبور Enter یا رمزهای ضعیف دیگر نداشته باشید.

ضمیمه یك – نحوه بدست آوردن پسورد:

من می خواهم یاهو را هک کنم، چی کار کنم؟ یا یک برنامه می خواهم که ID را بگیرد و رمز را بدهد.

- یعنی واقعا انتظار دارید که چنین سایتهای عظیمی قابل هک باشند آن هم به این آسانی؟ یعنی فکر می کنید این همه مسوولان امنیتی این سایتها نفهمیده اند و کسی برنامه ای نوشته است که می تواند اسم بگیرد و رمز بدهد؟ ببینید اشتباه نشه، همشه هر سیستمی اشکالاتی داره، اما از لحظه معلوم شدن آن اشکال تا حل آن به ندرت یک روز هم طول می کشه و این مشکلات هرگز در حدی نیستند که با استفاده از آنها بتوان چنین کارهایی انجام داد. فقط کافیست کمی منطقی فکر کنید! چنین سیستمهایی بسیار خوب محافظت می شوند! حالا ممکن است بگویید: ولی من دوستی دارم که دوستش می تونه هر ID رو Hack کنه و می گه یه برنامه داره که ID می گیره و رمز می ده! اینکه دوست شما ممکنه واقعا به راحتی بتونه رمز خیلیها رو پیدا کنه ضعف یاهو نیست، ضعف اون آدماست! یعنی اون آدما هستند که رمزشون رو هدیه می کنن به دوست شما! متاسفانه اکثر کسانی که ادعای Hack دارند آنقدر روششان مسخره است که باید مواظب باشند روششان لو نرود پس ممکن است بگویند روششان چیز دیگری است یا یک موضوع خیلی محرمانه است یا... لطفا سوال زیر را بخوانید:

* من می خواهم رمز یک نفر رو در بیارم، چی کار کنم؟

- اگر فرد مورد نظر در یک سایت کوچک که تمام آن هم نوشته شده توسط برنامه نویسان است باشد، ممکن است بتوانید آن را واقعا Hack کنید، من در اینجا صرفا به ذکر روشی که از همه بیشتر لو رفته است اکتفا می کنم و آن این است که در قسمت رمز عبور (یا در صورت نیاز هم در قسمت نام کاربری و هم در قسمت رمز عبور) بنویسید:

' or 1=1 --

این یکی از ساده ترین حالتهای روش موسوم به SQL injection است که روشی بسیار قوی است اما این حالت ساده آن در حدود 90% سایتها از جمله سایتهای یاهو و هاتمیل و سایتهای معروف کار نخواهد کرد (یعنی اگر بدشانس نباشید باید حداقل این را در 10 سایت امتحان کنید تا یک جا کار کند!) اما ادامه پاسخ به سوال شما: حال فرض کنیم سایتی مثل یاهو مدنظر باشد، در اینجا اول خیال خودمون رو راحت می کنیم که نمی تونیم رمز رو از سرور یاهو دربیاریم پس یا باید رمز امتحان کنیم (Broute force) یا رمز را از صاحب رمز بگیریم (Social engineering) یا رمز را از صاحب آن بدزدیم (Trojans)! حالت اول نیاز به تخصص دارد و حتی گاهی غیر ممکن است زیرا سیستمها بعد از چند بار امتحان رمز اشتباه از سوی شما دیگر رمزی قبول نمی کنند. مثلا Yahoo شما را مجبور می کند که کلمه ای که هر بار تغییر می کند را نیز وارد کنید. می توانید در صفحه ایمیل Yahoo چندین بار رمز اشتباه بزنید تا نتیجه را ببینید و اگرچه می توان مشکل بستن IP را با استفاده از Proxy server های رایگان تا حدی برطرف

کرد، باز هم این روش بیشتر مناسب سیستمهای ساده تر است (کاربرد این روش در صفحاتی که برای کسانی که رمز خود را فراموش کرده اند طراحی شده است را فراموش نکنید! اگر تاریخ تولد وارد شده و کد پستی کسی را بدانید شاید حدس زدن بقیه اطلاعات عملی باشد!) بنابراین استفاده از نرم افزارهای امتحان کننده رمز هم برای این سرورهای معروف نتیجه ای نخواهد داشت. راه دیگر Trojan horse است که اگر تقاضا برایش زیاد باشد در مورد آن توضیح جداگانه داده خواهد شد اما از آنجایی که اولا نرم افزارهای ضد ویروس ممکن است آن را بیابند و ثانیا سیستم عامل ویندوز XP با داشتن یک Firewall به نسبت خوب می تواند جلوی اکثر اینها را بگیرد، عملا قابل استفاده نخواهد بود مگر روی کسانی که یا به کامپیوترشان دسترسی داشته باشید و یا اطمینان داشته باشید که از یک سیستم عامل قدیمی (باورتون می شه کسی از ویندوز 5 سال پیش استفاده کنه؟! از ویندوز 98؟! واقعا آدم متاسف می شه!! 5 سال!! اونم تو کامپیوتر!!) استفاده می کند و ضد ویروس ندارد یا زیاد آن را به روز نمی کند. اما راه اصلی یعنی Social Engineering(يا مهندسي اجتماعي بخش دوم):

Social Engineering تاریخی طولانی دارد و معمولا نازیهای آلمان را از جمله استفاده کنندگان موفق آن می دانند. این روش یعنی کاری کنید که خودش به ما رمز را بگوید! من فقط چند روش ممکن را برای شما می نویسم:

1- ساختن صفحه ای شبیه صفحه یاهو. به عنوان مثال یک ایمیل به شکل کارت پستال برایتان ارسال می شود که ممکن است به نظر بیاید از طرف دوست نزدیکتان آمده است و وقتی روی لینک کارت پستال کلیک می کنید پیغامی مانند Your session has been expired و Relogin می گیرید اما در صفحه ای بجز Yahoo هستید! یعنی اگر رمزتان را بنویسید عملا خودتان آن را به فرد نفوذگر هدیه کرده اید. حالت دیگر ساختن صفحاتی است که جلب توجه کند مثل صفحه ای که می گوید با یاهو قرارداد دارد و می توانید با اکانت یاهو خود وارد آن شوید!! به عنوان مثال صفحه ای با عکسهایی مستهجن از دختران ایرانی یا... خیالتان راحت باشد که رمز و اسم یاهو فقط در یاهو کار می کنند و هرجای دیگر آن را بزنید، دو دستی تقدیمش کرده اید! همیشه باید مواظب باشید که هرگز در صفحه ای بجز صفحه واقعی خود یاهو اسم و رمز خود را وارد نکنید. این روزها مد شده است که بسیاری از دوستان با ساختن صفحاتی مشابه یاهو (معمولا save کردن خود صفحه sign in یاهو و سپس تغییر مسیر فرمی که باید رمز را به میزبان یاهو انتقال دهد به صورتی که رمز شما را به سازنده صفحه ایمیل کند یا در یک فایل ذخیره کند. برای این کار کافی است یک host رایگان بگیرد و فایلهای خود را روی آن قرار دهد، فقط باید مواظب باشد که حتماً از Coffee net استفاده کند!) اقدام به دزدی رمز عبور می کنند. حالا سوال اینجاست که از کجا بفهمیم که صفحه ای که داخل آن هستیم واقعا از طرف خود یاهو است یا نه؟ به عنوان یک قاعده کلی، ابتدا F6 و سپس کلید Home را بزنید. با این کار شما ابتدای نوار آدرسی را که آدرس صفحه وب را نشان می دهد می بینید. (راه دیگر: کافی است با کلیک موش روی نوار آدرس آن را فعال کنید و با فلش سمت چپ به سراغ اول آن بروید.) اگر آغاز آن به شکل زیر نبود، صفحه را ببندید (پیشنهاد می شود قبل از بستن صفحه تعداد زیادی کلمات بی معنی به عنوان اسم و رمز جهت سرگرم کردن دزد یاد شده وارد فرمایید) و اگر مانند زیر بود و پس از آن هم فقط حروف و اعداد و علامت / و ? آمده بود، با خیال راحت اسم و رمز خود را وارد فرمایید:

http://login.yahoo.comهر چیزی/

البته اگر به جای کلمه login هر چیز دیگری باشد با دقت به اینکه به yahoo.com ختم شده باشد، باز هم از صفحات خود یاهو خواهد بود.

مهم: بهتر است علاوه بر آن، با کلیک روی "Secure" منتظر شوید تا عکس یک قفل را در Internet explorer خود ببینید. (باز هم 100% نیست!)

2- فرد نفوذگر یک ID مانند auto-password-sender@yahooc.com ثبت می کند و به شما می گوید که اگر ایمیلی به فرم خاص و عجیبی به آن آدرس بفرستید و در جاهای خاصی از آن آدرس ایمیل خود و رمز عبور خود و در جای دیگری ایمیل کسی که رمز او را می خواهید بنویسید و به آنجا ارسال کنید تا رمز برای شما ایمیل شود. زمانی که ما به نیت آزمایش همین سیستم را پیاده کردیم متاسفانه تعداد خیلی زیادی نامه گرفتیم که عملا رمز خود را به ما هدیه کرده بودند و یک پاسخ هم ارسال می کردیم که ظرف یک هفته رمز را می گیرید و ظاهر آن را با تبلیغات و طراحی زیبا واقعی کرده بودیم. برای کسانی هم که می فهمیدند و ایمیل مسخره می فرستادند ایمیل با پیغامهای خطا می فرستادیم طوری که آنها هم وسوسه می شدند!! پس مواظب باشید رمز عبور خود را به هیچ شکلی به کسی هدیه

ندهید!! خیالتان راحت باشد که هرگز هیچ سیستمی از طریق ایمیل یا تلفن رمز عبور شما را نخواهد پرشید و هرگز یاهو به شما ایمیل نمی زند که در آن رمز خود را بنویسید! اگر روزی آنها نیاز داشته باشند، رمز عبور شما را عوض می کنند و آن را به شما اطلاع می دهند نه اینکه رمز شما را بپرسند!

Social engineering به اینجا ختم نمی شود و داستانهای زیادی از آن باقی است. در پایان اشاره ای به یک داستان واقعی می کنیم: فردی که قصد نفوذ به یک ساختمان دارای اتاقهای سرور کاملا حفاظت شده با انواع دوربینها و دزدگیرها را داشت، به راحتی خود را مسوول بازبینی سرورها برای سازگاری با سال 2000 معرفی می کند و از تک تک افراد رمزشان را می پرسد و یادداشت می کند! حتی با گفتن اینکه بگویید فایلهای مهمتان کجاست تا از انها پشتیبانی تهیه کنم که مبادا در حین آزمایش سیستمها به آنها صدمه ای برسد، زحمتی برای جستجو به دنبال فایلهای مهم هم متحمل نشد! شما هرگز و تحت هیچ شرایطی نه حضوری، نه پای تلفن و نه در ایمیل نباید رمز خود را به کسی بگویید! حتی رمز اینترنت خود را به مدیر شرکتی که از آن اینترنت گرفته اید هم ندهید! چون اگر او واقعا نیاز داشته باشد به راحتی آن را تغییر می دهد.

ضمیمه دوم – روش هاي اجراي همزمان برنامه ها در ویندوز:

روشهای مختلفی که یک برنامه می تواند از طریق آنها خود را با هر بار اجرای ویندوز اجرا کند عبارتند از:

1. استفاده از :winstart.bat در این روش که مناسب ویندوزهای قدیمی است، فایلی به نام winstart.batدر شاحه ویندوز ساخته می شود و برنامه از این فایل فراخوانی می شود؛ به این صورت که اگر این فایل موجود نباشد ساخته می شود و در غیر این صورت فقط نام برنامه به آن اضافه می شود.

2. استفاده از :win.ini در این روش که امروزه زیاد مورد استفاده قرار نمی گیرد، با نوشتن عبارت) load=filename.exe که به جای filename.exe نام برنامه قرار می گیرد) یا Run=filename.exeدر قسمت[windows] ، برنامه مورد نظر با هر بار اجرای ویندوز اجرا خواهد شد. برای باز کردن فایل Win.ini و مشاهده محتویات آن، بهترین روش استفاده از برنامه System configuration editor ویندوز است. برای اجرای این برنامه از منویStart ، Run را انتخاب کنید (یا کلید ویندوز کیبورد خود را بگیرید و سپس کلید R را فشار دهید)، تایپ کنید SysEditو OK را فشار دهید. از بین فایلهای باز شده فایل مورد نظر را پیدا کنید. اگر دقیقاً با این فایلها آشنایی ندارید، مواظب باشید که تغییری در این فایلها ندهید و اگر دادید، تغییرات خود را ضبط نکنید.

3. استفاده از :System.ini این روش بسیار مشابه روش بالاست. و مانند بالا این فایل هم درون System configuration editor قابل مشاهده است. اگر در این فایل به عبارتی مشابه shell=Explorer.exe trojan.exeبرخورد کردید، سیستم شما بلافاصله پس از اجرای explorer.exe، trojan.exeرا اجرا خواهد کرد.

4. استفاده از :Start up هر برنامه ای که در منوی Start داخل قسمت Startup قرار بگیرد، با هر بار اجرای ویندوز خود به خود اجرا خواهد شد .Startup در ویندوزهای جدیدتر در قسمت All programsمنوی Start قرار دارد.

5. استفاده از رجیستری: این روش که در حال حاضر متداولترین روش مورد استفاد تروا‌ها و کرمها می باشد به این صورت است که نام فایل اجرایی به قسمت Run در رجیستری اضافه می گردد. رجیستری ویندوز حاوی اطلاعات مختلفی از سخت افزارها و نرم افزارهای گوناگون نصب شده روی سیستم شماست. برای مشاهده رجیستری، از منویStart ، Runرا انتخاب کنید (یا کلید ویندوز کیبورد خود را بگیرید و سپس کلید R را فشار دهید) و در داخل جعبه متن آن تایپ کنید RegEdit :و OK را فشار دهید. اگر دقیقاً با رجیستری آشنایی ندارید، مواظب باشید که تغییری در آن ندهید. از میان قسمتهای مختلف رجیستری در اینجا ما با HKEY_CURRENT_USERو HKEY_LOCAL_MACHINE سروکار داریم. یکی از ایندو را انتخاب

کنید و روی آن Double Click کنید (یا روی علامت + کنار آن کلیک کنید) حال به ترتیب گزینه های زیر را انتخاب کنید تا به Run برسید:

Software -> Microsoft -> Windows -> Current Version -> Run

در شرایطی که بیش از یک نفر از یک رایانه استفاده می کنند و روی آن کاربران مختلف تعریف کرده اند، معمولاً برنامه هایی که در قسمت Run موجود در HKEY_LOCAL_MACHINE نامشان نوشته شده باشد با هر بار اجرای ویندوز برای تمام کاربران آن اجرا می شوند اما برنامه هایی که نام آنها در HKEY_CURRENT_USER آمده باشد فقط برای کاربری که در حال حاضر از سیستم استفاده می کند اجرا خواهند شد .ممکن است علاوه برRun ، گزینه هایی به نامهایRunOnce ، RunServicesیا RunServicesOnce را هم دیده باشید که آنها هم همین اثر را دارند با این تفاوت که اگر نام برنامه ای در RunOnce یا RunServicesOnce قرار بگیرد فقط یکبار یعنی فقط دفعه بعدی که ویندوز اجرا می شود به همراه ویندوز اجرا خواهد شد.

6. روش ShellOpen رجیستری: در رجیستری و در زیر کلیدهای زیر باید همیشه عبارت "%1" %* نوشته شده باشد اما اگر به عبارتی مانند *% "%1" trojan.exe برخورد کردید، بدانید که فایل Trojan.exe سعی دارد کاری کند با هر بار اجرای هر فایل اجرایی روی رایانه شما، او هم اجرا شود:

[HKEY_CLASSES_ROOT\exefile\shell\open\command]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]

7. استفاده از روشهايي مانند Binding و جایگزینی: اگرچه روشهایی که در بالا نوشته شد حاوی تمامی روشهایی است که امروزه مورد استفاده قرار می گیرند، روشهای اجرا هرگز به موارد فوق ختم نمی شوند و همیشه جای ابتکار یا استفاده از روشهایی که فقط روی سیستمها یا در شرایط خاصی عمل کنند باز است بنابراین به صرف اینکه مطمئن شوید از طریق روشهای بالا سیستم شما آلوده نشده است کفایت نمی کند. به عنوان نمونه در روشهایی مانند Binding و جایگزینی که هنوز چندان مورد استفاده قرار نگرفته و پیش بینی می شود در آینده نزدیک بیشتر مورد استفاده قرار بگیرند، فایلی که قرار است با هر بار اجرای ویندوز خود را اجرا کند، فایل دیگری را پیدا می کند که این کار را انجام دهد و سپس خود را به آن می چسباند. به عنوان نمونه با تشخیص اینکه روی سیستم، فایل مربوط به ویندوز مسنجر با هر بار اجرای ویندوز اجرا می شود، کاری می کند که در هنگام اجرای ویندوز مسنجر، آن برنامه هم اجرا شود. اگر برنامه برای این کار خود را به فایل اجرایی مسنجر ویندوز بچسباند، می گویند از Binding استفاده کرده است اما اگر خود را جایگزین آن کند، می گویند از روش جایگزینی استفاده کرده است. اگرچه این روشها از قدیم توسط ویروسهای مختلف برای آلوده کردن فایلهای اجرایی به کار گرفته می شدند اما استفاده از این روش برای اجرای همزمان با ویندوز احتمالاً به زودی بیشتر مورد استفاده قرار خواهد گرفت.پس از مطالعه روشهای بالا، احتمالاً شما هم با من هم عقیده هستید که پیدا کردن یک تروا به روش دستی کار چندان ساده ای نیست؛ اما اکثریت قریب به اتفاق تروا‌ها از روشهای رجیستری استفاده می کنند و شما از تغییرات ایجاد شده در قسمتهای Run می توانید به آلوده شدن سیستم پی ببرید. یک ابزار بسیار عالی که در اکثر ویندوزها وجود دارد (در ویندوز 2000 وجود ندارد) ابزاری به نام System Configuration Utilityاست. برای اجرای این ابزار، از منویStart ، Runرا انتخاب کنید (یا کلید ویندوز کیبورد خود را بگیرید و سپس کلید R را فشار دهید) و در داخل جعبه متن آن تایپ کنید MSConfig :و OK را فشار دهید. اگرچه این ابزار کاربردهای مختلفی دارد، ما در اینجا فقط به ذکر کاربردهایی از آن می پردازیم که به موضوع بحث ما بیشتر مربوط هستند. پس از باز شدن صفحهSystem Configuration Utility ، از بالای صفحه Startup را انتخاب کنید. خواهید دید که اکثر فایلهایی که خود به خود همراه ویندوز شما اجرا می شوند در اینجا لیست شده اند و شما با حذف تیک کنار اسم آنها می توانید آنها را از کار بیندازید. در قسمت Startup itemنامی که برنامه برای خود برگزیده است، در قسمتcommand ، آدرس فایل اجرایی برنامه و در قسمت Location تکنیک مورد استفاده توسط برنامه برای اجرا را خواهید دید. توجه به نکات زیر هم در استفاده از MSConfig به شما کمک خواهد کرد:

1. چون معمولاً قسمتهای command و location فضای کافی برای نمایش کامل محتویات خود را ندارند، موش رایانه را روی خط جداکننده command از location یا خط انتهای location ببرید تا بتوانید اندازه این قسمتها را تغییر دهید.

2. عبارتهای HKCU و HKLM به ترتیب مخفف HKEY_LOCAL_MACHINE و HKEY_CURRENT_USERمی باشند که در بالا و در تکنیک شماره 5 به آنها اشاره شد.

3. برای مشاهده فایلهای System.ini وwin.ini ، علاوه بر روش گفته شده در بالا (در مورد شماره 2) کافی است که از قسمت بالای MSConfig گزینه های SYSTEM.INI و WIN.INI را انتخاب کنید.

پایان

درباره نویسنده مقاله:

نویسنده: **پدارم حیاتي** (**Pi3cH**)
تحصیلات: دانشجوي رشته فناوري اطلاعات (IT)
[redacted]
وب سایت: http://www.persianhacker.net
تاریخ: آذر ماه 1383
منابع:
وب سایت: www.persianhacker.net
کتاب: Hacker Attack!
مقالات شخصي نویسنده