# اموزش دیفیس سرور ها و وب سایت ها با شل گیری (نسخه PDF)

**به نام خدا**

---

# آموزش شل گیری

---

منظور از شل همان دسترسی به سرور است .

شاگرد ۱ : حال چگونه باید از سایت مورد نظر دسترسی بگیریم ؟؟

شاگرد ۲ : چرا دسترسی میگیریم ؟؟

شاگرد ۳ : چه نوع دسترسی در اختیار داریم ؟؟

استاد : شما زمانی از سرور مورد نظر شل میگیرید که تمام راهای شما بسته باشد . یعنی سایت مورد نظر باگ نداشته باشد و روش های مهندس اجتماعی که برفریب دادن انسان ها استوار است بر آن اثر نکند . در این مواقع شما باید از برنامه هایی که از سرور به شما شل می دهند کمک بگیرید .

---

برای اینکه بتوانید از سرور دسترسی بگیرید **باید این برنامه های shell script را بر روی یکی از سایت های سرور مورد نظر آپلود کنید .**

زیرا یکی از راه های هک کردن تمام شبکه ها عضو بودن در آن شبکه است و خیلی اطلاعات از شبکه را بدست می آورید و شما قادر خواهید بود بسیاری از کنترل های آن شبکه را در اختیار داشته باشید . چون یک عضو معتبر آن شبکه هستید . همین موضوع در هک کردن سرور ها هم سرایت خواهد کرد. و با داشتن یک سایت در آن سرور و آپلود کردن shell script ها بر روی آن می توانید از سرور دسترس بگیرید.( اما نه از کل سرور . ابتدا فقط از سایتی که بر روش shell script رو آپلود کردید دسترسی دارین که باید دسترسی خودتونو بالا ببرید و به مقام root برسید)

نکته : root در لینوکس همانند دسترسی administrator در ویندوز است

حال شما میتوانید یک سایت بر روی سرور را هک کنید و یک shell script بر روی آن سایت آپلود کنید . یا یک سایت از آن سرور خریداری کنید . یا از یکی از دوستانتان که بر روی آن سرور هاست دارد از آن به مدت چند ساعت قرض بگیرید. تا بتوانید بر روی سرور عملیاتی برای root شدن انجام دهید .

اینکه شما بدان چگونه shell script باید آپلود کنید مهم است . زیرا shell script ها به زبان های مختلفی نوشته می شوند . و بستگی دارد که سرور مورد نظر کدام را ساپورت کند . اگر سرور هدف لینوکس باشد بهتر است شما از php sheller ها که با زبان php نوشته شده اند استفاده کنید .

**یکی از بهترین اینگونه php sheller ها c۹۹ نام دارد .**

وقتی شما یک php sheller را بر روی یک سایت آپلود می کنید و آنرا اجرا می کنید , چند چیز برای شما باید مهم و اولویت اول را داشته باشد .

---

۱- دسترسی مجاز به پوشه ها که در لینوکس به آن perm می گویند. بالا ترین دسترسی پوشه ها که perm دارد و به آن ۷۷۷ هم می گویند دارای امکانات زیر می باشد :

Read – Write – Execute

یعنی شما میتوانید در پوشه بخوانید , بنویسید , تغییر بدهید و حتی یک فایل آپلود کنید که در php shell ها دسترسی perm به صورت

یعنی شما میتوانید در پوشه بخوانید . بنویسید . تغیر بدهید و حتی یک فایل آپلود کنید . که در php shell ها دسترسی perm به صورت زیر جلوی هر پوشه یا فایل نوشته می شود .

drwxrwxrwx اگر جلوی یک پوشه ای این علامت را در php shell ها دیدید بدانید می توانید در آن هر کاری انجام دهید . نظیر :

کپی . تغیر دادن . خواندن . نوشتن .

اگر عبارت به صورت -rwxrwxrwx بود بدانید آن فایل است .

**نکته : شما فقط تا زمانی که دسترسی کامل ندارید با اینگونه مقررات مشکل دارید اگر دسترسی کامل داشته باشید حتی در پوشه های بدونه perm که به اینگونه نوشته می شوند :dr-xr-xr-x یا r–r–r– و نوع های دیگر ..**

در c۹۹ پوشه و فایل هایی که قابل دستکاری می باشند و یا به اصطلاحی perm هستند به رنگ سبز و بدون perm به رنگ قرمز یا سفید.

---

۲- on یا off بودن قسمت safe-mode زیرا اگه on باشه به عبارتی شما نمیتوانید root باشید . زیرا برای روت شدن باید با command کار کنید که اگر safe-mod on باشه نمی شه رو command اجرا کرد .

---

**خوب حالا از بالا تمام آیتم های php shller را یک بار مرور می کنیم :**

```
Softwar
```

در این قسمت نوع سرویس دهنده سرور و ورژن اون رو نشون می ده :

```
uname -a
```

دراین قسمت اطلاعاتی در باره ی سرور میده :

اگه این قسمت off باشه شما میتونید به دایرکتوری ها برید و کامند اجرا کنید اما اگه on باشه نمی تونید همون safe-mod میشه

```
c:\drwxrwxrwx
```

در این قسمت به شما نشون میده که در کدام قسمت از سایت هستید و چه نوع دسترسی دارید

```
Total HDD Space : 1.51 TB | Free HDD Space : 518.17 GB
```

این قسمت مقدار کل فضای هارد سرور و فضای استفاده شده و باقی مانده رو نشون میده:

```
DEtected Dirves
```

این قسمت به شما درایو های سرور رو نشون می ده:

و در قسمت پاین تر یک سری ابزار است که خودتون می تونید باهاش کار کنید . ابزاری مثل brut کردن و کرک کردن سایت های دیگه و گرفتن شل بر عکس .

خوب در قسمت پاین تر هم شما میبینید اسامی پوشه ها و فایل ها هستش که رو بروش میزان دسترسی هر کدوم رو نوشته .

و در قسمت پایین تر هم ابزار هایی از جمله by-pass هستند که شما می تونید با اون پوشه هایی که دسترسی به اون ندارین رو ببینین . و در قسمت Enter هم می تونید دستوراتی مثل بالا بردن دسترسی و گرفتن revers shell رو بنویسید.

دوستان این مباحثی که تحت عنوان تست نفوذ و امنیت رو سایت قرار میگیره همش برا بالاـ بردن سطح امنیت کشور و همچنین بالا

بردن سطح دانش شماست پس استفاده غیر قانونی از اون بار منفی و تبعات جبران ناپذیر برا خودتون داره پس لطفا خوب دقت کنید

**و چیزی که هست خدا شاهده من خودم هیچوقت هیچ سایتی رو دیفیس نکردم فقط برا یادگیری بوده و بس و از شـما هم میخوام که هیچوقت دست به دیفیس یک سایت یا سروری رو نزنید.**

مطلب اصلی