

به نام خداوند یکتا

آموزش قدم به قدم مدیریت سرور

Step By Step Tutorial Server Management

تهیه کننده و نویسنده مطالب : [Arashdn](#) (آرش درگاهی)
گردآوری مطالب بصورت PDF : [ToooPDL](#) (عقیل حسین زاده)

فهرست

جلسه اول.....	۳
جلسه یک و نیم.....	۶
جلسه دو.....	۹
جلسه دو و نیم.....	۱۲
جلسه سه.....	۱۵
جلسه سه و نیم.....	۱۸
جلسه چهار.....	۲۲
جلسه چهار و نیم.....	۲۴
جلسه پنج.....	۲۷
جلسه پنج و نیم.....	۲۹
جلسه شش.....	۳۳
جلسه هفت.....	۳۵
جلسه هفت و نیم.....	۳۹
جلسه هشت.....	۴۳
جلسه هشت و نیم.....	۴۶
جلسه پایانی.....	۵۱

جلسه اول

سلام

بیاید کار رو شروع کنیم

من اطلاعات خواننده گان این مطلب رو در این حد در نظر گرفتم

۱- با یه ریسرلر کار کردن

۲- نصب سی ام اس های معمولی رو بلدن

۳- و کارای در همین حد دیگه

حالا میخواهید سرور بگیرید و وضعیتی مثل شکل زیر دارید



نگران نباشید نمی خواهید اپلود هوا کنید که

برای شروع کار یه سرور مجازی با رم ۲۵۶ تا ۵۱۲ و هارد ۱۰-۱۵ گیگ کافیه

حالا همش تو سایت های مختلف میرید میبینید نوشته سرور ویندوز ، سرور لینوکس

خب اجازه بدید ببینیم فرقشون چیه

نکته : آموزش ما برای هاستینگ لینوکس هست

ولی خب من فرقشون رو میگم تا بدونید

۱- لینوکس سیستم عاملی اوپن سورس و رایگان بوده ولی ویندوز سیستم عاملی غیر رایگان است

۲- هزینه سرور های مجازی لینوکس از ویندوز پایین تر است .

۳- چنانچه وی پی اس را برای هاستینگ و یا یک سایت نیاز دارید اگر سایت شما به زبان asp نیست بدون شک لینوکس مناسب تر می باشد

۴- چنانچه از سرور خود برای $v p * N$ استفاده میکنید و یا برای دانلود / اپلود از وی پی اس استفاده میکنید سرور های ویندوز برای شما مناسبتر است

۵- کار با سرور ویندوز دقیقا مانند کار کردن با یک کامپیوتر ویندوزیست و کاربر بوسیله remote desktop صفحه سرور را در کامپیوتر خود اجرا کرده و به راحتی و دقیقا مانند کامپیوتر خود با سرور کار می کند

۶- لینوکس در زمینه امنیت و هاستینگ پیشرفت فوق العاده ای نسبت به ویندوز داشته و کنترل پنل های بسیار حرفه ای تر و کاربرپسند تری برای ان طراحی شده

۷- کار با لینوکس بصورت تایپ دستور است (البته امکان نصب محیط گرافیکی نیز می باشد)

۸- سرور های لینوکسی ویروس نمیگیرند ولی ویندوز براحتی ویروس می گیرد

۹- لینوکس مصرف رم کمتری داشته و پایدار تر است

۱۰- در سرور های اختصاصی ویندوز هزینه ای در بین ۱۵ الی ۵۰ دلار دارد. ولی لینوکس رایگان می باشد

من برای تفهیم بهتر یه عکس از سرور ویندوز و یه عکس هم از سرور لینوکس میزارم

root@c7:~

```
top - 15:41:26 up 55 days, 2:39, 1 user, load average: 1.04, 1.09, 1.08
Tasks: 121 total, 1 running, 119 sleeping, 0 stopped, 1 zombie
Cpu(s): 0.2%us, 25.9%sy, 0.0%ni, 73.6%id, 0.2%wa, 0.0%hi, 0.0%st
Mem: 4138204k total, 3988676k used, 149528k free, 108396k buffers
Swap: 5406712k total, 96k used, 5406616k free, 3584368k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
27689	root	5	-10	515m	407m	396m	S	99.8	10.1	29319:07	vmware-vmx
3964	root	5	-10	382m	283m	266m	S	3.3	7.0	1713:35	vmware-vmx
3815	root	15	0	20056	16m	4188	S	0.7	0.4	217:40.45	vmware-serverd
14654	root	5	-10	520m	430m	413m	S	0.3	10.7	1153:57	vmware-vmx
1	root	15	0	2072	628	540	S	0.0	0.0	0:08.69	init
2	root	RT	-5	0	0	0	S	0.0	0.0	0:00.15	migration/0
3	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
4	root	RT	-5	0	0	0	S	0.0	0.0	0:00.00	watchdog/0
5	root	RT	-5	0	0	0	S	0.0	0.0	0:00.14	migration/1
6	root	39	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/1
7	root	RT	-5	0	0	0	S	0.0	0.0	0:00.00	watchdog/1
8	root	RT	-5	0	0	0	S	0.0	0.0	0:00.28	migration/2
9	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/2
10	root	RT	-5	0	0	0	S	0.0	0.0	0:00.00	watchdog/2
11	root	RT	-5	0	0	0	S	0.0	0.0	0:00.43	migration/3
12	root	37	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/3
13	root	RT	-5	0	0	0	S	0.0	0.0	0:00.00	watchdog/3
14	root	10	-5	0	0	0	S	0.0	0.0	0:00.18	events/0
15	root	10	-5	0	0	0	S	0.0	0.0	0:00.11	events/1
16	root	10	-5	0	0	0	S	0.0	0.0	0:00.25	events/2
17	root	10	-5	0	0	0	S	0.0	0.0	0:00.36	events/3
18	root	12	-5	0	0	0	S	0.0	0.0	0:00.00	khelper
19	root	14	-5	0	0	0	S	0.0	0.0	0:00.02	kthread
25	root	12	-5	0	0	0	S	0.0	0.0	0:00.02	kblockd/0
26	root	10	-5	0	0	0	S	0.0	0.0	0:00.02	kblockd/1
27	root	10	-5	0	0	0	S	0.0	0.0	0:02.11	kblockd/2
28	root	20	-5	0	0	0	S	0.0	0.0	0:00.65	kblockd/3
29	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
118	root	16	-5	0	0	0	S	0.0	0.0	0:00.00	cqueue/0
119	root	17	-5	0	0	0	S	0.0	0.0	0:00.00	cqueue/1
120	root	17	-5	0	0	0	S	0.0	0.0	0:00.00	cqueue/2
121	root	17	-5	0	0	0	S	0.0	0.0	0:00.00	cqueue/3

محیط کار یه سرور لینوکس
هول نکنید بابا این نوشته
ها خیلی سادست

win.gif

Recycle Bin

EN 07:16 پ.ظ ۲۰۱۰/۳/۰۳

default - 173.45.90.67 - Remote Desktop Connection

Security Configuration...

Mozilla Firefox

Administrator

- Manage Your Server
- Windows Explorer
- Command Prompt
- Internet Explorer
- WinRAR
- Shortcut to KMPlayer.exe

- My Computer
- Control Panel
- Administrative Tools
- Printers and Faxes
- Help and Support
- Search
- Run...
- Windows Security

All Programs

Log Off Shut Down

100% Downloaded - Moz...

Recycle Bin

پ.ظ 07:14 ۲۰۱۰/۳/۰۳

خب فعلا ویندوز رو فراموش کنید

بریم سراغ لینوکس

قبل هر کار وی پی اس تون رو بگیرید.

وی پی اس رو گرفتید؟؟

مبارکه

لابد به شما چیزی دادن به نام SSH

که یه آییی دادن و یه دونه پسورد و شاید یوزر نیمی به نام root

(با چیزایی مثل hypervm و هر کنترپنلی که برای ریپوت و اینجور کارها بدن فعلا کاری نداریم)

خب اول بزارید یه کم در مورد سرور بحث کنیم

سرور چیه؟

سرور نه خوردنی و نه پوشیدنی

بلکه یه کامپیوتره (البته با بهترن سیستم های تهویه و موارد مشابه که کاری نداریم) و این سرور همیشه خدا روشنه

(حیونکی) و با اینترنت با سرعت خیلی بالا وصله

دیتاسنتر چیه؟

یه ساختمان هست (معمولا در کشور های پیشرفته) که سرور ها رو تو اون نگه داری میکنن و افرادی اونجا هستن که

هوای این سرور ها رو دارن

دیتاسنتر های خوب همیشه برق اضطراری و سیستم های تهویه دارن و همچنین افرادی بطور ۲۴ ساعته اونجا هستن

سرور مجازی (VPS) چیه؟

VPS مخفف Virtual Private Server هست یعنی یه بنده خدایی (مثلا خودم) میریم از به دیتاسنتر یه سروری

میگیریم بعد میایم با نصب یه سری برنامه ها Ram - Hard - Cpu سرورمون رو بین یه عده تقسیم میکنیم

کارکردن با سرور مجازی و سرور اختصاصی ۹۹٪ عین هم دیگه است

SSH چیه ؟

SSH که فقط در سرور های لینوکس اسمشو میشنویم

در واقع یه راه ارتباطی (غیر گرافیکی و فقط با تایپ دستور) بین سرور سرور و کامپیوتر شماست

دقت کنید که لینوکس هم محیط گرافیکی داره خیلی قشنگتر از ویندوز ولی خب برای اینکه رم مصرفش کمتر شه و

همه آموزش های موجود در نت هم بر اساس تایپ دستوره پس سعی کنید با دستور ها بسازید ...

فعلا همین ها رو تمرین کنید و قشنگ یاد بگیرید.

جلسه یک و نیم

خب یه سری موارد که موقع خرید وی پی اس باهاش درگیر میشدید هست که لازم دیدم توضیح بدم
Host name چیه؟

این واژه که موقع خرید وی پی اس و سرور لینوکس باهاش سر و کار دارید در واقع اسم سرور شماست (چطور که مثلاً ما اسم داریم : آرش - تقی - علی - قلی و ...) سرور هامون هم اسم دارن به این اسم میگن host name
هاست نیم بصورت xxxxx.domain.com میشه که میتونید به جای xxxx هر چی بزارید که معمولاً مینویسن
server.domain.com این دومین لزومی نداره رو سرورتون باشه و صرفاً کار یه اسم برای وی پی اس شما رو میکنه

کرنل چیه؟

کرنل در واقع هسته سیستم عامل شماست (توضیح بهتر نمی تونم بدم)

مجازی ساز چیه؟

یادتونه پست بالا گفتم برای سرور مجازی یه کارایی رو سرو اختصاصی میکنیم
این کار ها اینه که یه سیستم مجازی سازی رو سرور نصب میکنیم
این مجازی ساز میاد سرور هایی مجازی از رو سرور من درست میکنه
اینا رو ول کنید بریم سر معرفی سیستم های مجازی ساز اینکه کدوم بره شما بهتره

۱- VmWare

این برنامه نسخه سرورش رایگانه و هم بر روی لینوکس نصب میشه هم ویندوز ما در مورد نسخه لینوکسش بحث میکنیم

نسخه های لینوکس دو دسته اند :

- نسخه کنسول دار
- نسخه تحت وب

در هر دو نسخه کرنل کاملاً اختصاصی به کاربر داده میشه و وی پی اس های ساخته شده هیچ فرقی با سرور اختصاصی ندارند همچنین نمیشه پهنای باند رو محدود کرد. همچنین تعداد هسته های سی پی یو وی پی اس نمیتونه بالای ۲ باشه.

هر وقت یه وی پی اس رو روشن کنید کل رمش مصرف میشه .

در نسخه کنسول دار شما یه برنامه رو دانلود میکنید و اکثر کار ها با اون انجام میشه

در نسخه تحت وب شما از طریق مرورگرتون به وی ام ور دسترسی دارید در این نسخه شما میتونید کارت صوت بسازید و یا به کاربر پنل بدید .

در وی ای ام ور هیچ محدودیتی برای نصب سیستم عامل وجود ندارد و برای نصب سیستم عامل باید فایل ISO رو در سرور اصلی دانلود و در وی پی اس نصب کنید (بعدا توضیح بیشتر داده میشه)

HyperVM

هایپر وی ام یه مجازی ساز نیست بلکه یه کنترل پنل رایگان برای مجازی ساز های Xen و OpenVZ هست

این پنل محصول شرکت LXLabs هست که امکانات خوبی داره و مجازی سازی رو واقعا راحت کرده

در ادامه به معرفی ۲ مجازی سازی که با این پنل کار میکنن میپردازیم.

۲- OpenVZ

این برنامه برای لینوکس و ارائه وی پی اس های لینوکسی نوشته شده و معمولا همراه با هایپر وی ام نصب میشه.

این برنامه کرنل اختصاصی به وی پی اس ها نمیده و شما موقع ساخت وی پی اس از یه منو انتخاب میکنید که کدوم ورژن لینوکس نصب بشه

در این برنامه هنگامی که یه وی پی اس رو استارت میکنید فقط رمی که وی پی اس استفاده میکنه از سرور اصلی کم میشه و بقیه رم آزاد میمونه.

وی پی اس های اوپن وی زد سی پی یو share دارن و حتی هنگام نصب فایر وال مشکلاتی وجود دارد اوپن وی زد از منابع سرور اصلی زیاد استفاده نمی کنه و با توجه به راحتی کار و امکانات بالا طرفدارن زیادی داره

در کل اوپن وی زد برنامه مناسبی برای وی پی اس های لینوکس می باشد.

۳- Xen

این برنامه برای لینوکس نوشته شده که همراه با پنل هایپر وی ام نصب میشه.

زن به سرور های مجازی کرنل اختصاصی میده و میتونید روش ویندوز یا لینوکس بزنید

یادم نره بگم که زن نمیتونه کارت صوت بده ولی کارت شبکه اش هم اختصاصی (eth) هست

در این برنامه هنگام ساخت وی پی اس های لینوکس از یه منو ورژن لینوکس رو انتخاب میکنید و برای وی پی اس های ویندوز باید فایل ISO واردش کنید

۴- مجازی ساز های دیگه ای مثل Virtuzu - HyperV و ... هست که من زیاد اطلاعاتی در موردشون ندارم اگر کسی از دوستان اطلاعاتی داره برای منپیام خصوصی کنه تا با اسم خودش در این قسمت قرار بدم
خب فعلا همینا خوبه

جلسه دوم

سلام

بالاخره وی پی اس تون رو گرفتید؟؟

بسیار عالی

فقط چیزی که جلسه قبل یادم رفت بگم حتما بگید لینوکس CenOS رو سرورتون نصب بشه

اولین قدم SSH هست که بهتون میدن

و معمولا شامل یه IP و یه پسورد هست و بعضا یه دونه یوزر نیم root هم بهتون میدن

ولی چطوری از اس اس اچ استفاده کنیم

برای کانکت شدن به اس اس اچ

اگر روی کامپیوتر خودتون ویندوز دارید باید برنامه پوتی رو دانلود کنید

لینک : <http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

بعد برنامه پوتی رو اجرا کنید و در صفحه ای که میاد در قسمت

(Host name (or IP adress

وارد کنید root@ip server

به جای ip server آییی سرورتون رو وارد کنید و فعلا به قسمت های دیگه دست نزنید و اینتر بزنید

بعد یه صفحه سیاه میاد و ازتون پسورد میخواد ، دقت کنید موقع نوشتن پسورد چیزی نشون نمی ده ولی پسورد رو

مینویسه بعد نوشتن پسورد اینتر کنید

اگر روی کامپیوترتون لینوکس دارید ترمینال رو باز کنید و بزنید

ssh ipserver

به جای ip server آییی سرورتون رو وارد کنید و اینتر بزنید

بعد ازتون یوزر نیم و پسورد میخواد ، دقت کنید موقع نوشتن پسورد چیزی نشون نمی ده ولی پسورد رو مینویسه بعد

نوشتن پسورد اینتر کنید

خب حالا در اس اس اچ هستید و میتونید هر دستوری که خواستید تایپ کنید دقت خیلی از دستور ها دستور

های سیستمیه و ممکنه باعث ایجاد اشکال و حتی حذف اطلاعات شما بشه

پس در کار با اس اس اچ دقت کنید

خب یکی از مواردی که شاید الان زیاد به دردتون نخوره ولی دوستنش خالی از لطف نیست

اونم پارتیشن بندی در لینوکسه

موقع ورود شما در دایرکتوری **home** هستید در لینوکس پارتیشن مثل **c,d,e** نیست بلکه (اینی که میگم یه حالت پیشفرضه که دیتاسنتر یا مدیر سرور مجازی بهتون میده و گرنه میتونید برای هر پوینت یه پارتیشن جدا بسازید) در لینوکس ما یه پارتیشن داریم به نام روت که به صورت / هست بعد زیر مجموعه اون موارد زیر رو داریم

۱- **bin** فرامین عمومی سیستم عامل لینوکس در این دایرکتوری قرار دارد مانند **sort ls** و

۲- **dev** حاوی نقاط دسترسی به ابزار های سخت افزاری کامپیوتر است مانند ترمینال ها دیسک های فلاپی دیسک های سخت و کاربران به طور معمول برای دستیابی به این دستگاه ها از نام های آنها استفاده می کنند. (این تو سرور زیاد کاربرد نداره)

۳- **etc** حاوی برخی فایل های پیکر بندی سیستم است

۴- **home** دایرکتوری کاربران یک سیستم لینوکسی می باشد و اطلاعات کاربران در این دایرکتوری قرار می گیرد. (فایل های هاست های کاربران هم در این قسمته)

۵- **mnt** محلی برای متصل کردن ابزار ها دیسک های سخت دیسک های **USB** و داریو های شبکه می باشد. (اینم در مورد سرور زیاد مطرح نیست)

۶- **root** دایرکتوری خانگی کاربر ریشه می باشد

۷- **sbin** دستورات مدیریت سیستم در این دایرکتوری قرار می گیرد

۸- **tmp** محل قرار گیری فایل های موقت می باشد

۹- **usr** محل قرار گیری مستندات سیستم بازی ها فایل های گرافیکی کتابخانه ها و چیزهای دیگر است (زیاد تو سرور کاربرد نداره)

خب این بالایی بیشتر بره اطلاعاتتون و در در سطوح مبتدی اصلا مورد بحث نیست

حالا بریم سر اصل بحث -- دستورات اس اس اچ

دستورات اس اس اچ خیلی زیاده من فقط چند تا رو میگم (دقت کنید کجا ها بین بخش های مختلف دستور فاصله هست) و قرار نیست همه رو هم همین الان رو سرور بدبخت امتحان کنید فقط یاد بگیریدشون

cd .. این دستور شما رو به یه پوشه بالاتر می بره مثلا در هنگام ورود در **home** هستید اگر این دستور رو بزنید میرید به روت

cd folder name : برای وارد شدن به یک فولدر که به جای **folder name** اسم پوشه رو بزنید مثلا در روت بزنید **cd home**

ls لیست فایل ها و پوشه های موجود در دایرکتوری که توش هستید رو میده (معادل دستور **dir** در داس)

ls-a تمامی فایل ها (از جمله فایل های هیدن و سیستمی) و پوشه های دایرکتوری که توش هستید رو نشون میده

wget http://fileaddress : این دستور واسه دانلود فایل روی سرور فایل رو در پوشه ای که توش هستید دانلود میکنه

yum install pack : برای نصب برنامه هاست به جای pack باید اسم برنامه رو بنویسید مثلا:
yum install php – yum install apache – yum install perl

این دستور برای آپدیت و یا حذف برنامه ها هم هست مثلا:
yum update php – yum remove php

service name action : این دستور برای کار با سرویس ها (یه جورایی میشه گفت برنامه ها البته یه جورایی) که به جای name باید اسم سرویس و به جای action عملی رو می خواهید انجام بشه بنویسید من چند تا از مهم ترین هاش رو میگم

stop : برای از کار انداختن سرویس (اگر سرویس اتواستارت باشه بعد یه بار که سرور رو ری استارت کنید دوباره میاد بالا)

start : برای شروع کار یک سرویس (اگر سرویس اتواستارت نباشه بعد هر ری بوت باید استارتش کنید)

restart : دو عمل stop و start رو با هم انجام میده

remove : برای حذف سرویس

حالا چند تا مثال :

service apache stop

service php start

service mysql restart

خب فعلا همینجا باشه

جلسه دو و نیم

شاید برای خیلی ها سوال پیش آمده باشه که این قضیه نیم تو جلسات چیه؟؟
من خودم دوست ندارم حجم مطالبی که تو یه دوره گفته میشه خیلی زیاد باشه
این جلسات نیم در اصل مکمل جلسه قبلیه
پیشنهاد میشه بین جلسات یه استراحتی بکنید

خب بریم سراغ ادامه دستورات اس اس اچی که باید بلد باشید

top : این دستور برای دیدن لیستی از پروسس های در ال اجرا و همچنین مشخصات و مقدار رم و سی پی یو سیستم هست

در اینجا هر پروسس یه شماره بره خودش داره (pid)

با زدن Shift + m پروسس ها به ترتیب مصرف رم

و با زدن Shift + p به ترتیب مصرف سی پی یو

حالا اگر بخواهیم یه پروسس رو استاپ کنیم میزنیم

kill pid به جای pid باید pid پروسستون رو بزنید

اگر بخواهید یه پروسس با تمام زیر مجموعه هاش استاپ بشه بزنید

terminate pid : بازم به جای pid باید pid پروسستون رو بزنید

معمولا هر یوزر هاست یا هر سرور مجازی یه پروسس جدا واسه خودش داره

در پایان میتونید با زدن دکمه Q از این صفحه بیاید بیرون

یه دستورم خارج از بحث بگم که واسه عوض کردن پسورد اکانتی که باهاش وارد شدید (الان فکر کنم با روت لوگین کردید) کافیه دستور passwd رو بزنید و پسورد رو تایپ و اینتر بزنید یه بار دیگه هم باید تایپ کنید اگر با روت وارد شدید میتونید پسورد بقیه اکانت ها رو هم با دستور passwd username

تو این قسمت میخوام به دستوراتی که مربوط به کار با فایل ها مربوط میشه بپردازم

اولا بگم یه فایل مینجر نیمه گرافیکی عالی در لینوکس داریم به نام mc

برای نصبش کافیه بزنید yum install mc و اگر چیزی پرسید y بزنید بعد که تموم شد برای ورود به ام سی فقط

کافیه تایپ کنید mc و بعد قشنگ با محیط گرافیکش کار کنید

اما بعضی ها دوست دارن سخت کار کنن :D

که واسه اونا یه سری دستور واسه مدیریت فایل ها میگم

اولا دقت کنید هر جا گفته شده filename یا اسم فایل حتما باید پسوند فایل رو هم تایپ کنید

برای ساخت پوشه میریم جایی که می‌خواهیم پوشه توش ساخته بشه و می‌زنیم

`mkdir folder name`

برای حذف پوشه میریم به جایی که پوشه توشه مثلا اگه می‌خواهیم فولدر با نام `arash` رو از `home` پاک کنیم میریم توی `home` و می‌زنیم

`rm -rf foldername` که به جای `folder name` باید اسم پوشه رو زد.

برای حذف فایل هم همینطور برید به جایی که فایل توشه و این دستور رو بزنید
`rm -rf filename` که به جای `file name` باید اسم فایل رو زد.

برای کپی کردن یک فایل اول میریم به جایی که فایل توشه بعد دستور زیر رو می‌زنیم

`cp oldfilename /masir jadid`

که `oldfilename` اسم فایلیه هست که قراره کپی بشه و `masirjadid` هم جایی هست که قراره فایل بره اونجا

برای انتقال یک فایل به محل جدید و حذف فایل اولیه (بعارتی `cut` کردن فایل)
اول میریم به جایی که فایل توشه بعد دستور زیر رو می‌زنیم

`mv oldfilename /masir jadid`

که `oldfilename` اسم فایلیه هست که قراره کپی بشه و `masirjadid` هم جایی هست که قراره فایل بره اونجا

اینم آموزش سورس کپی که شاید خیلی از شما استفاده نکنید

حالا فرضا من یه سرور دارم می‌خوام یه فایل رو از سرور خودم انتقال بدم به سرور دیگه (در صورتی که یوزر و پسورد سرور دیگه رو هم داشته باشم) اینکار با سورس کپی انجام میشه
برای اینکار برید جایی که فایل توشه و بزنید

`scp filename root@ipserver dige:/masir file`

حالا یه مثال : من می‌خوام فایل `file.zip` رو بفرستم رو سروری به آیپی ۱.۱.۱.۱ اول میرم جایی که فایل توشه بعد می‌زنم

`scp file.zip root@۱.۱.۱.۱:/home`

بعد یه سوال ازتون می‌پرسه که باید بنویسید `yes` و اینتر کنید بعد پسورد سرور مقصد رو باید بزنید
بعدش این `file.zip` میره تو `home` سرور مقصد

اگه به جای `home/` می‌زدیم / فایل میرفت تو روت سرور مقصد

میشه مسیر طولانی تری هم داد مثلا : `home/arash/public_html/`

برای اجرا یک فایل با فورمت `sh` کافیه برید به جایی که فایل توشه و بزنید

`sh ./filename.sh`

برای اکسترکت کردن فایل من مال zip & tar رو اینجا میزارم
بازم باید برید به جایی که فایل توشه بعد دستورات زیر

```
unzip filename.zip  
tar -xvf filename.tar
```

برای ویرایش یک فایل متنی بزنی nano /masirfile
اگه اخیانا گفت دستور پیدا نشد و اینجور چیزها بزنی

```
yum -y install nano
```

برای ریپوت سرور هم از دستور reboot استفاده کنید

خب تا اینجا اصلی ترین دستورات رو برای کار یاد گرفتید در آموزش های بعدی کم کم به نصب پنل ها و برنامه های مجازی سازی میپردازیم
یادتون باشه فقط به این مرجع وابسته نباشید هر وقت مشکلی داشتید با سرچ تو گوگل و سایر موتور های نتایج خوبی به دست میارید.

جلسه سوم

سلام

ولی شما عجله نکنید و هر روز به جلسه رو پیش برید

خب

این جلسه می‌خواهیم به معرفی کنترل پنل ها ، ویژگی ها ، قیمتشون در زمان نگارش این مقاله و شیوه نصبشون صحبت کنیم

Cpanel

محبوب ترین پنل همین سی پنل هست امنیتش در حالت عادی خیلی جالب نیست ولی با اعمال به سری تغییرات چیز جالبی میشه در حال حاضر آخرین نسخه این کنترل پنل ۱۱.۲۵ هست . سی پنل جدیداً کمتر رو تحریمات حساسیت نشون میده ولی خب هنوزم گیر میده از مزایای این پنل میشه به موارد زیر اشاره کرد

-محیط کاربری گرافیکی و دل نشین

-امکانات بالا

-طرفداران بسیار

-

و از معایبش میشه به موارد زیر اشاره کرد

-قیمت بالا (در حال حاضر نسخه وی پی اس بین ۱۰ تا ۱۶ دلار و نسخه سرور بین ۲۰ تا ۴۰ دلار قیمتشه)

-مصرف بالای رم

-مشکلات تحریم واسه ایرانی ها

در کا پنل خوبیه و نصبش توصیه میشه

DirectAdmin

این کنترل پنل کانادایی که مشکلی هم با کاربران ایرانی نداره و همین باعث شده طرفاداری زیاد در ایران داشته باشه قیمتش از سی پنل کمتر ولی خب امکانات و زیبایی محیط کارشم به سی پنل نمیرسه ، امنیتش درست بعد از نصب در مقایسه با سی پنل بهتره که خب با انجام تغییراتی بهترم میشه
من که خودم خیلی باهاش حال میکنم 🍷

از مزایای این پنل میشه به موارد زیر اشاره کرد:

-قیمت پایین (برای وی پی اس حدود ۵ تا ۷ دلار و برای سرور اختصاصی بین ۱۰ تا ۱۶ دلار)

-عدم مشکل تحریم

-مصرف رم کمتر

و از معایبش میشه به موارد زیر اشاره کرد

-امکانات متوسط

-کار کردن با این پنل برای یوزر ها مشکله (ولی کم کم عادت میکنن) 

طرفدار کمتر در بین مشتری ها

در کل برای سرور های نه چندان بزرگ خیلی چیز عالی هست (در سرور های بزرگم خیلی خوب جواب میده ها فقط کاربرها دیگه صداشون خیلی در میاد)

(Kloxo (LXadmin

این پنل که قدیم اسمش ال ایکس ادمین و در ورژن جدید اسمش رو کلوکسو گذاشتن .

در قدیم این پنل واسه ۴۰ دومین رایگان بود و بعد اون برای ارتقا تعداد دامین ها باید مبلغی رو به شرکت lxlabs میداد ولی الان این کنترل رایگان و به صورت اوپن سورس روش کار میشه لازم به ذکره که شرکت lxlabs پنل هایپر وی ام رو هم طراحی کرده و تا اونجا که من میدونم برنامه نویس هاش هندی هستن.

از مزایای این پنل میشه به موارد زیر اشاره کرد:

-رایگان هست

-کار با این کنترل پنل بسیار ساده است و فقط با دو تا دستور نصب میشه

-براحتی و با چند کلیک میتونید وب سرور و میل سرور و ... رو عوض کنید و خیلی از فانکش های پی ا پی رو فعال کنید

-این پنل همه چیزی رو که سرور لازم داره نصب میکنه مثلاً یه آنتی دی داس قوی نصب میکنه

-مصرف رم کم

و از معایبش میشه به موارد زیر اشاره کرد

-یه کم سنگینه (سرعت لودش) و امکاناتش متوسط به بالاست

-عیب اصلیش اینه که با خیلی از کنترل پنل های دیگه سازگاری نداره ، سیستم بکاپ و ترانسفرش داغونه - بعضا ناجور قاط میزنه

Plesk

این پنل محصول شرکت parallels هست که هم نسخه لینوکس و هم نسخه ویندوز داره که ما در اینجا در مورد لینوکس بحث میکنم
از مزایای این پنل میشه به موارد زیر اشاره کرد:
- محیط نسبتا خوب
- ساپرت قوی
- امکانات متوسط به بالا
و از معایبش میشه به موارد زیر اشاره کرد
- قیمت بالا
- این پنل خیلی سنگینه و با سرعت اینترنت ایران زیاد جور نیست
- امکاناتش به نظر من خیلی باحال نیست
- بعضی کار های صدا رو خیلی مشکل کرده

WebMin

یه کنترل پنل ساده و خیلی ابتدایی با امکانات پایین و البته مصرف رم و سی پی یو واقعا کم

دمو کنترل پنل ها :

[Demo - cPanel Inc](#). سی پنل

[DirectAdmin Web Control Panel Demo](#) دایرکت ادمین

[DirectAdmin Web Control Panel Demo](#) کلوکسو

<http://www.parallels.com/products/plesk/demo> پلسک

خب فعلا همینا خوبه

در مورد کنترل پنلی که میخواهید نصب کنید فکر کنید تا در پست بعد (جلسه ۳.۵) آموزش نصب و این که از کجا لایسنس بگیرید رو بزارم

موفق باشید

جلسه سه و نیم

خب این جلسه اختصاص داره به آموزش نصب و خرید لایسنس سه تا کنترل پنل سی پنل ، دایرکت ادمین ، کلوکسو

۱- Cpanel

خب اول بریم سر بحث لایسنس

لایسنس ها کلا دو دسته ان:

اینترنال : این لایسنس ها رو معمولا دیتاسنتر یا فروشنده وی پی اس ارائه میدن و قیمت پایین تری دارن
اکسترنال : این لایسنس ها توسط مایرور های سی پنل عرضه میشه ولی برای همه هست و خیلی قیمتشم یه کم بیشتره
لایسنس اینترنال که دیگه معلومه از کجا باید بگیرید
برای خرید لایسنس اکسترنال هم جاهای زیادی هست که نمیتونم اینجا بگم (تبلیغ حساب میشه)

دقت کنید هاست نیم شما نباید مشخصات ایرانی داشته باشه (بره مشکل تحریم)

و اما طریقه نصب

سعی کنید به خاطر مشکلات تحریم با یه ایپی غیر ایران وارد اس اس اچ بشید (حتما توجه داشته باشید که سرور شما نباید هیچ برنامه خاصی نصب داشته باشه و به هیچ عنوان قبلا روش کنترل پنل خاصی نصب نشده باشه) (اگر قبلا روش چیزی نصب کردید با سیستم عامل سرور عوض بشه یا به اصطلاح os reload بشه که در وی پی اس ها بهش rebuild هم میگن (علی الخصوص در اوپن وی زد و زن))

اول باید selinux رو خاموش کنید (در وی پی اس های اوپن وی زد نیازی به انجام اینکار نیست) برای اینکار در اس اس اچ بزنید: setup

در صفحه ای که میاد برید به قسمت Firewall configuration و بعد یه دور کلید tab رو بزنید تا بیاید روی run tools و بعد اینتر بزنید بعد در صفحه ای که میاد برید رو Disabled (با زدن یه بار دکمه فلش راست کیبرد) و بعد کلید space رو بزنید بعد اگه یه بار دیگه کلید tab رو بزنید میاد تو قسمت SELinux بعد بیاید رو Disabled و دوباره کلید space رو بزنید بعد یه tab بزنید تا بیاید رو OK بعد اینتر بزنید و دوباره بر میگردید به صفحه اول این بار با زدن tab بیاد رو Quit و اینتر کنید حالا دوباره بر میگردید به صفحه اس اس اچ ، این دستور رو بزنید :

wget http://layer1.cpanel.net/latest

اینو بزنید : sh latest

بعد بین ۱۵ تا ۸۰ دقیقه کلی * و # میکشه و نصب میشه

usr/local/cpanel/cpkeyclt/ حالا این دستور رو بزنید :

بعد با یه آیپی غیر ایران از لینک http://ip:۲۰۸۶ وارد بشید

حالا تنظیمات رو پیش برید تنظیمات سختی نیست فقط به موارد زیر دقت کنید
میل سرور رو بزارید exim
وب سرور apache
SMTP رو هم بزارید dovecot
یه جایی هم هست که ان اس های مد نظرتون رو ست کنید
اگر در این مورد سوالی داشتید بره من پیام خصوصی بزنید تا در همین تاپیک اضافه کنم

۲- DirectAdmin

اول که بحث شیرین لایسنس

این لایسنس ها دو دسته هستن ولی خب برای شما فرقی نمیکنه کدومش باشه و قیمت ها هم مشابه پس از هر کی تونستید بگیرید اون شخص باید به شما کلاینت آیدی و لایسنس آیدی بده

خب برای نصب :

برای نصب دایرکت ادمین وارد اس اس اچ بشید (حتما توجه داشته باشید که سرور شما نباید هیچ برنامه خاصی نصب داشته باشه و به هیچ عنوان قبلا روش کنترل پنل خاصی نصب نشده باشه) (اگر قبلا روش چیزی نصب کردید با سیستم عامل سرور عوض بشه یا به اصطلاح os reload بشه که در وی پی اس ها بهش rebuild هم میگن (علی الخصوص در اوپن وی زد و زن))

اول باید selinux رو خاموش کنید (در وی پی اس های اوپن وی زد نیازی به انجام اینکار نیست) برای اینکار در اس اس اچ بزنید: setup

در صفحه ای که میاد برید به قسمت Firewall configuration و بعد یه دور کلید tab رو بزنید تا بیاید روی run tools و بعد اینتر بزنید بعد در صفحه ای که میاد برید رو Disabled (با زدن یه بار دکمه فلش راست کیبرد) و بعد کلید space رو بزنید بعد اگه یه بار دیگه کلید tab رو بزنید میاد تو قسمت SELinux بعد بیاید رو Disabled و دوباره کلید space رو بزنید بعد یه tab بزنید تا بیاید رو OK بعد اینتر بزنید و دوباره بر میگردید به صفحه اول این بار با زدن tab بیاد رو Quit و اینتر کنید حالا دوباره برمیگردید به صفحه اس اس اچ ، دستورات زیر رو به ترتیب بزنید :

```
yum -y install gcc
```

```
yum -y install flex
```

```
yum -y install gcc-c++
```

```
yum -y install make
```

حالا بزنید

```
wget http://www.directadmin.com/setup.sh
```

بعد بزنید : `chmod ۷۵۵ setup.sh`

`setup.sh/.` بعد اون هم بزنید

خب حالا اولین چیزی که ازتون میپرسه لایسنس آیدی و کلاینت آیدی و هاست نیمتون هست همه رو بزنید و بعدش هم یه بار دیگه بهتون نشون میده و میپرسه که درسته یا نه که اونم اگه درست زده بودید `y` بزنید و اگه اشتباه بود `n` بزنید تا دوباره ازتون بخواد این موارد رو

بعدش اگه درست یادم مونده باشه میپرسه که `Is eth۰ your ethernet device` یا یه همچین چیزی که اگر سرور اختصاصی دارید و یا مجازی سازتون `Xen` , `Vmware` و... هست بزنید `y` ولی اگه سرور مجازی با `OpenVZ` و `Virtuzu` و... دارید بزنید `n` بعدش ازتون میپرسه اسم `device ethernet` رو وارد کنید شما بزنید `venet۰:۰` و اینتر بزنید

بعدش میپرسه که آیا آییبتون با آپی لایسنس یکیه که اونم `y` بزنید بعد فک کنم میگه یه ورژن انتخاب کنید بین ۱ و ۲ که شما ۲ رو بزنید و بعد هم `y` بزنید تا نصب شروع بشه

آخر سر هم روی صفحه پسوردتون رو مینویسه

اگر به هر دلیلی نتونستید پسورد رو بردارید میتونید با زدن دستور زیر اونو ببینید

```
cat /usr/local/directadmin/setup.txt
```

خب اینم از این

۳- Kloxo

پنل با نصب بسیار ساده

بره اینکه تعداد دامین هاتون از ۴۰ تا بیشتر بشه باید تو سایت `lxlabs.com` عض بشید و بعد در پنلتون آیی سرورتون رو ادد کنید

برای نصب :

اگر وی پی اس با هایپر وی ام دارید : کافیه در هایپر وی ام `install kloxo` رو بزنید و کمی صبر کنید
اگر سرور اختصاصی یا وی پی اس بدون هایپر وی ام دارید : اول باید `selinux` رو خاموش کنید (در وی پی اس های اوپن وی زد نیازی به انجام اینکار نیست) برای اینکار در اس اس اچ بزنید: `setup`
در صفحه ای که میاد برید به قسمت `Firewall configuration` و بعد یه دور کلید `tab` رو بزنید تا بیاید روی `run tools` و بعد اینتر بزنید بعد در صفحه ای که میاد برید رو `Disabled` (با زدن یه بار دکمه فلش راست کیبرد) و بعد کلید `space` رو بزنید بعد اگه یه بار دیگه کلید `tab` رو بزنید میاد تو قسمت `SELinux` بعد بیاید رو `Disabled` و دوباره کلید `space` رو بزنید بعد یه `tab` بزنید تا بیاید رو `OK` بعد اینتر بزنید و دوباره بر میگردید به صفحه اول این بار

با زدن tab بیاد رو Quit و اینتر کنید حالا دوباره برمیگردید به صفحه اس اس اچ ، دستورات زیر رو به ترتیب بزنید :

کد:

```
wget http://download.lxlabs.com/download/kloxo/production/kloxo-install-master.sh
```

بعدش : `sh ./kloxo-install-master.sh`

بعد صبر کنید تا نصب تموم بشه هر وقت تموم شد از آدرس `http://ip:۷۷۷۸` وارد بشید یوزر و پسورد اولیه هر دو

admin

هست

خب بره این جلسه فک کنم همین ها کافیه

پیروز باشید

جلسه چهارم

سلام

خب این جلسه در مورد اولین کارایی هست که بعد از نصب کنترل پنل باید بکنید که در این جلسه به تنظیمات کنترل پنل و در جلسه بعدی به نصب فایروال و ... میپردازیم
من اطلاعات خودم در مورد سیپنل و دایرکت ادمین تکمیل (البته یه نیم نگاهی هم به کلوکسو میندازیم)
اول بریم سراغ

Cpanel

خب برای اینکار اول با یوزر و پسورد روت برید به دابلو اچ ام (۲۰۸۶)
خب اصلی ترین و کلی ترین تنظیمات سی پنل تو tweak setting هست
اولا بگم که قسمت Basic cPanel/WHM Setup که همون تنظیماتیست که موقع نصب سی پنل انجام دادید

خب برید تو قسمت tweak setting

اولا این مورد رو بدونید که همه تنظیمات در کنارشون توضیح داره و خب خیلی هاشون سلیقه ایه
من اونایی رو که اهمیت بالایی داره بررسی میکنم
مواردی رو که در پایین میزارم غیر فعال کنید

Allow users to Park/Addon Domains on top of domains owned by other users. (probably a bad idea)

Enable verbose dns zone syncing (for testing purposes only, not for production use)

موارد زیر رو بد نیست فعال کنید

Allow Creation of Parked/Addon Domains that are not registered

Prevent users from parking/adding on common internet domains. (i.e. hotmail.com, aol.com و اینجور چیزها رو پاک کنن یا نه) google (این مورد میگه که آیا اجازه بدم یوزر ها دامنه هایی مثل aol.com

موارد زیر هم حتما فعال کنید

When adding a new domain, automatically create A entries for the registered nameservers if they would be contained in the zone.

مواردی که کاملا سلیقه ای ولی مهمه

Prevent the user "nobody" from sending out mail to remote addresses (PHP and CGI scripts generally run as nobody if you are not using PHP Suexec and Suexec respectively).

این میگه که بزاریم nobody ایمیل بفرسه یا نه

بره پیش گیری از ارسال اسپم جدا خوبه
ولی بعضی از اسکریپت هایی که بصورت ساده نوشته شدن نمیتونن ایمیل ارسال کنن

قسمت Notifications کاملاً سلیقه ایه مورد خاص و کلمه انگلیسی دشواری هم نداره

دیگه مورد خاصی که نیاز به تغییر داشته باشم رو یادم نیست
اگر موردی یادم رفته از دوستان خواهشمندم در پیام خصوصی مطرح کنن

خب حالا برید به قسمت

Configure PHP and SuExec

در ورژن جدید اگر نگاه کنید PHP ۵ Handler هستش suphp که خوب از نظر امنیتی خیلی خوبه ولی خیلی از اسکریپت ها از جمله نیوک و ... باهاش سازگار نیستن
اگر سرور بره سایت شخصیه که نیوک و ... نیست بزارید رو suphp
ولی در هاستینگ های عمومی dso توصیه میشه
آپدیت : جدیداً اکثر اسکریپت ها از suphp ساپرت میکنن در نتیجه استفاده از suphp پیشنهاد میشه (در جلسه ۷ به این موارد کامل اشاره شده)

بعد برید به قسمت FTP Server Configuration و این دو مورد زیر رو حتما و حتماً انجام بدید که در امنیت خیلی تاثیر دارن

Allow Anonymous Logins ---> No
Allow Anonymous Uploads ---> No

DirectAdmin

تنظیمات پیش فرض دایرکت ادمین تا حد زیادی قابل قبوله و فقط چند تا مورد جزئی نیاز به توضیح داره
در جلسه ۴.۵ به تنظیمات دایرکت ادمین و کلوکسو میپردازیم

جلسه چهار و نیم

سلام

خب همانطور که قول داده بودم این جلسه اختصاص داره به تنظیمات دایرکت ادمین و کلوکسو

DirectAdmin

پنل کم دردسر با تنظیمات اولیه مناسب

خب اول هر کار برید به قسمت Message System (در گوشه بالا سمت راست زیر لوگو دایرکت ادمین)

اونجایی که نوشته Email a copy of all messages to در اون کادر ایمیل خودتون رو وارد کنید

تیک زدن و نزدنش هم اختیاری و دست خودتونه (تیک بزنید بد نیست)

برگردید به همون صفحه اصلی

برید به قسمت List Administrators و روی admin کلیک کنید

admin's user data رو بزنید و در صفحه ای که میاد در قسمت ایمیل ، ایمیل خودتون رو وارد کنید و سیو کنید و

برگردید به صفحه اصلی

برید به قسمت

Administrator Settings

در اینجا میتونید خیلی از تنظیمات رو تغییر بدید

خیلی از موارد واضح و نیازی به توضیح نداره

فقط در قسمت Max Request/Upload Size (bytes) پیشنهاد من اینه که یه صفر هم بهش اضافه کنید تا بشه

۱۰۰ مگ

تیک Prevent ۱۲۷.۰.۰.۱ from being Blacklisted رو بزنید

مورد Blacklist IPs for excessive login attempts اگه تیک بخوره بره وقتی خوبه که مثلاً وقتی یکی اومد

بیشتر از یه تعدادی پسورد اشتباه زد آپیش بلاک میشه این کمک میکنه تا ربات ها نتونن پسورد کاربر رو پیدا کنن

به نظر من Blacklist IPs for excessive login attempts رو تیک بزنید و مقدارش رو هم بزارید ۸۰

تنظیم ان اس های اصلی سرور هم که دیگه توضیح نمیخواد

میمونه Enable Automatic Lost Password Recovery که اگه فعالش کنید یه دونه گزینه ورگت پسورد به

صفحه لوگین تون اضافه میشه و اگه یوزر اونو بزنه ازش یوزر نیم یا ایمیل میپرسه و بعد پسورد رو میفرسته به میلش

فعال کردن یا نکردنش سلیقه ایه

در مورد دمو هم مال demo_admin رو به هیچ عنوان فعال نکنید اون دوتای دیگه سلیقه ایه

دیگه تنظیم خاصی بره خود دایرکت ادمین بفکرم نمیرسه

Kloxo

یوزر و پسورد پیشفرض کلوکسو هر دوتا admin هست موقعی که بره بار اول وارد سرور میشد ازتون میخواد که عوضش کنید

عوضش کنید و update رو بزیند

اگر با مورد زیر مواجه شدید

Lxguard for this server is not configured. Please Click here to configure Lxguard since it is very important that you understand what it does. Lxguard is critical for the security of your server, at the same time, it can block your own IP address from accessing the server, which can be frustrating if you don't know what's happening.

رو همون قسمتی که گفته Click here to configure Lxguard کلیک کنید

I Have Read About Lxguard And Understands در صفحه که میاد مقدارش رو بزارید رو ۴۰ و تیک

What It Does رو بزیند و update رو بزیند

از بالا زیر لوگو کلوکسو روی home(admin) کلیک کنید

بعد احتمالا با مورد زیر مواجه میشد

Alert: The identification name for your mail server is not set. This means that many public mail

servers like hotmail will reject mails from your server. Click here to set it

رو قسمت click here to set it کلیک کنید و مقدار زیر رو درست کنید

My Name : یه اسمی بدید مثلا من میدم webhostingtalk

Max Smtip Instances : اینو بزارید رو ۸۵

Additional Smtip Port : بزارید ۲۵

به بقیه موارد دست نزنید و update رو بزیند

اگر با این مورد مواجه نشدید باید دستی برید به این قسمت

در صفحه اصلی home در قسمت Web & Mail& DB برید به Server mail setting و مقادیر زیر رو درست کنید

My Name : یه اسمی بدید مثلا من میدم webhostingtalk

Max Smtip Instances : اینو بزارید رو ۸۵

Additional Smtip Port : بزارید ۲۵

به بقیه موارد دست نزنید و update رو بزیند

از بالا زیر لوگو کلوکسو روی (admin/home) کلیک کنید

احتمالا پایین صفحه گزینه Information: Your Contact Information is not set properly. Click here to fix it بیاد

روی Click here to fix it کلیک کنید و در قسمت Email Address آدرس ایمیلتون رو وارد کنید و آپدیت رو بزنید

دوباره برگردید به صفحه اصلی

در کلوکسو برای ساخت هر اکانت یا دومینی باید DNS Template بسازید
برای اینکار برید در بخش Resources برید به قسمت DNS Templates هر جا که من گیگ نیک زدم شما دومینی که میخواهید ان اس ها روی اون باشه رو بزنید
اول از بالا add DNS Template رو بزنید بعد موارد مربوطه رو تکمیل کنید مثال زیر هم میتونه بره تفهیم بهتر کمک کنه

DNS Template Name : مثلا ns۱.gignic.com

آیپی وب و آیپی میل باید همون آیپی سرورتون باشه

Primary DNS : مثلا ns۱.gignic.com

Secondary DNS : مثلا ns۲.gignic.com

بعد هم add رو بزنید

خب برگردید به صحنه اصلی

از قسمت Web & mail & DB برید به FTP Config و بعد تیک Enable Anonymous Ftp رو بردارید و آپدیت رو بزنید و برگردید به صفحه اصلی

از قسمت Web & mail & DB برید به PHP Config و دقیقا تنظیمات زیر رو انجام بدید

جز دو مورد Enable Zend و Enable Ioncube تیک بقیه رو بردارید و آپدیت رو بزنید بعد برید به

Advanced PHP Config

و تیک موارد زیر رو بردارید

Enable Dl و Output Buffering و Allow Url Fopen و Allow Url Include و آپدیت رو بزنید

این موارد بالایی اکثرا بره امنیت بودن از اونجا که من زیاد با این پنل کار نکردم اطلاعاتم در همین بود

ولی در مورد امنیت سی پنل و دایرکت ادمین به طور کامل در جلسات بعدی صحبت میکنیم

جلسه پنجم

در این جلسه میرسیم به نصب فایروال

نصب فایروال رو سرور مزایای زیادی داره و جلوی بسیاری از جملات رو میگیره ...

فایروال های زیادی داریم من از بین شون با CSF کار کردم و ازش راضیم همین رو هم آموزش میدم
برای نصب اول دستورات های زیر رو به ترتیب بزنید
کد:

```
rm -fv csf.tgz
wget http://www.configserver.com/free/csf.tgz
tar -xzf csf.tgz
cd csf
sh install.sh
```

اگر احيانا بعد از زدن دستور اخر با ارور

You need to install the LWP perl module (libwww-perl) and then install csf

یا هر ارور ديگه ای مبنی بر نصب نبودن libwww-perl برخوردید دستور زیر رو بزنید
کد:

```
yum -y install perl-libwww-perl
```

و بعد دستور زیر رو بزنید تا فایروال نصب شه
کد:

```
sh install.sh
```

اگه سرور اختصاصی یا سرور مجازی با کرنل اختصاصی (وی ام و و زن) دارید کار تمومه

اگه وی پی اس تون با OpenVZ یا virtuzzu باشه باید مراحل زیر رو هم برید (در این مورد که مجازی ساز چیه از کسی که وی پی اس خریدید سوال کنید)

پس تاکید میکنم دارندگان سرور اختصاصی و سرور های مجازی با کرنل اختصاصی نیازی به مراحل زیر ندارن

ویژه وی پی اس های اوپن وی زد و ویرتوزو

اول دستور زیر رو بزنید (یادتون باشه نانو رو نصب کرده باشید)
کد:

```
nano /etc/sysconfig/iptables
```

بعد تمام ۴ خط زیر رو توش کپی پیست کنید
کد:

```
A FORWARD -j ACCEPT -p all -s ۰/۰ -i venet۰-
A FORWARD -j ACCEPT -p all -s ۰/۰ -o venet۰-
A INPUT -i venet۰ -j ACCEPT-
A OUTPUT -o venet۰ -j ACCEPT-
```

و بعد سیو کنید و بیاد بیرون (اول Ctrl + X بعد Y و بعد دو بار اینتر)

حالا دستور

کد:

```
nano /etc/csf/csfpre.sh
```

و بازم خطوط زیر رو توش کپی پیست کنید

کد:

```
iptables -A INPUT -i venet• -j ACCEPT
```

```
iptables -A OUTPUT -o venet• -j ACCEPT
```

```
iptables -A FORWARD -j ACCEPT -p all -s •/• -i venet•
```

```
iptables -A FORWARD -j ACCEPT -p all -s •/• -o venet•
```

بعد دستور

کد:

```
nano /etc/csf/csf.conf
```

خط زیر رو پیدا کنید

```
ETH_DEVICE="" =
```

و به صورت زیر تغییرش بدید

کد:

```
ETH_DEVICE = "venet"+
```

حالا دستور

```
nano /etc/pure-ftp.conf
```

خط زیر رو پیدا کنید

```
PassivePortRange
```

و مثل زیر تغییرش بدید

کد:

```
PassivePortRange      ۳۰۰۰۰ ۳۵۰۰۰
```

و یه بار کل سرور رو با دستور

```
reboot
```

ری استارت کنید

الان فایروال نصبه ولی فعلا بصورت تست هست و عملا کار نمیکنه در جلسه ۵.۵ توضیح میدم که چطور کانفیگ بشه و

چه تغییراتی توش بدید

با سپاس

جلسه پنج و نیم

سلام به همه دوستان

این جلسه میخوام یه مورد خیلی ساده و خیلی کارا در امنیت سرور رو توضیح بدم
اصولا باید من در مورد فعال کردن فایروال و کانفیگش بگم ولی فعلا از اون صرف نظر میکنیم و همونطور اجازه بدید
فایروال بصورت تست نصب بشه
امروز میخوام در مورد یه اسکریپت ساده و مفید و کم حجم صحبت کنم

ELS

Easy Linux Security

این برنامه همونطور که از اسمش پیداست برای تامین بسیاری از موارد امنیتی لینوکس بصورت خیلی ساده است ...
برای نصبش دستور زیر رو تو اس اس اچ بزنیند
کد:

```
wget --output-document=installer.sh http://servermonkeys.com/projects/els/installer.sh;  
chmod +x installer.sh; sh installer.sh
```

و حالا دستور

کد:

```
els --all
```

رو بزنیند

حالا مراحل رو توضیح میدم

ممکنه در سرور شما برخی از موارد پرسیده نشه زیاد بهش اهمیت ندید

Admin (your) E-Mail Address (this should NOT be on this server :(

ایمیل خودتون رو وارد کنید و اینتر رو بزنیند

و وقتی در مورد درست بودنش سوال کردن Y بزنیند و اینتر کنید

Several packages installed by yum may not be compatible or may cause problems with DirectAdmin or cPanel. To help prevent complications, ELS can add special

packages to be skipped when running yum.

These packages can still be updated manually with yum .

Y رو بزنیند و اینتر کنید

sysctl is used to harden the kernel. If you have not hardened your kernel with sysctl or do not know how to, it is recommended to have ELS do it for you. Your current /etc/sysctl.conf will be backed up to /usr/local/els/bakfiles/sysctl.conf .

n رو بزنیند و اینتر

This will only run cPanel's pre-installed scripts to update itself.

updatenow, upcp, sysup, and several other software updaters will be executed .

این سوال که فقط در سرور های سی پنل میاد جوابش y هست

ELS can tweak several cPanel/WHM settings for you to further optimize and secure your server

این سوال که فقط در سرور های سی پنل میاد جوابش y هست

ELS can have an alert email sent to you each time someone logs in as root .

اینم میگه وقتی کسی به عنوان روت وارد شد براتون میل ارسال بشه ، انتخاب با خودتونه

ELS can now install RKHunter .

y بزنید و اینتر

نصب این برنامه و اینکه تنظیمش کنید هر روز اسکن کنه به امنیت سرور کمک زیادی میکنه

Would you like for RKHunter to run and send you scan details to your admin email address nightly? (y/n :)

y

ELS can now install CHKROOTKIT .

y

نصب این برنامه و اینکه تنظیمش کنید هر روز اسکن کنه به امنیت سرور کمک زیادی میکنه

Would you like for CHKROOTKIT to run and send you scan details to your admin email address nightly? (y/n :)

y

ELS can now install APF .

n

این یه فایروال هست با توجه به اینکه این آموزش بر مبنای فایروال CSF هست به هیچ عنوان این فایروال رو نصب نکنید

نصب همزمان دو تا فایروال مشکلات جدی رو به دنبال داره

ELS can now install BFD .

اینم یه پلاگین بره فایروال بالاست که به هیچ عنوان نباید نصب شه

پس n بزنید

ELS can now install Libsafe .

y

ELS can now install MyTOP .

y

This feature can make the SSH daemon force SSH Protocol ۲

n

فعال کردنش به امنیت یه کمک جزیی میکنه ولی ممکنه با بعضی از کلاینت ها اس اس اچ قابل دسترسی نباشه

This feature can chmod dangerous files only to root

y

This feature can disable PHP register_globals .

y

This feature can disable dangerous PHP functions .

y

This feature can secure and optimize your MySQL configuration .

y

You can now renice MySQL to -10 (higher CPU priority).

In MySQL intensive environments, overall performance can increase dramatically by using highest CPU priority, however in a few cases, this may offer no performance gain or even decrease performance slightly.

If you wish to undo this, use the following command:

els --undomysqlrenice

n

انجامش در برخی سرور ها ایجاد مشکل میکند

This feature can optimize and repair all the MySQL database tables .

y

ImageMagick is not installed.

ELS can now install ImageMagick.

y

ELS can install the Exim Dictionary Attack ACL

Created by Chirpy from ConfigServer Services

n

این قابلیت به طور پیشفرض در سی پنل ۱۱ وجود دارد و این برنامه هم باگ دارد و سازنده دیگه پشتیبانیش نمیکند
پس جواب n هست

Changing SSH to use a non-default port helps prevent against Brute Force attacks and potential hackers.

If you choose to change the SSH port, ensure the port is not already in use by another program. There is a chance of locking yourself out of SSH, so it is recommended to add your Desktop's IP address to /etc/apf/allow_hosts.rules.

ELS can now change your SSH port for you .

با این کار پورت اس اس اچ رو میتونید تغییر بدید که کمک زیادی به امنیت میکنه ولی دو تا مورد مهم

۱- باید قبل این کار حتما و حتما پورت مورد نظر رو در فایروال باز کنید (آموزش در جلسات بعد)

۲- حواستون باشه که از دفعه بعد با پورت جدید به سرور کانکت شید

فعلا n بزنید تا هر موقع که آموزش باز و بسته کردن پورت در فایروال رو گفتم این رو تغییر بدید

Disabling root login to SSH adds an extra layer of security

to prevent hackers from gaining root access. It requires you to login as a special user and then use the command 'su -' to get prompted for root password and become root.

You should be careful and write the information necessary down incase you need it .

این کار هم لوگین روت رو غیر فعال میکنه که دردسرش بیشتر از امنیتی که ایجاد میکنه
پس پیشنهاد من n هست (اگر y بزنید حتما و حتما باید یه یوزر داشته باشید که بتونه به اس اس اچ لوگین
کنه)

تموم

خب تا اینجا آموزش ها بره سی پنل و دایرکت ادمین مشترک بود

از این به بعد آموزش ها متفاوت خواهد بود

با توجه به درخواست کاربرها که اکثرا طرف سی پنل اول سی پنل رو توضیح میدم بعد میرم سراغ دایرکت ادمین
با سپاس

جلسه ششم

سلام

در این جلسه شروع میکنیم به توضیحات و کانفیگ سی پنل (هر چند من خودم با دایرکت ادمین حال میکنم ولی اکثر کاربرها درخواست سی پنل رو دادن انشالله بعد سی پنل میرسیم دایرکت ادمین)
خب حتما طبق جلسه پنجم سی اس اف رو نصب کردید ..
حالا وارد WHM بشید

اگه دقت کنید در منوی سمت چپ دایبلو اچ ام در پایینترین قسمت یه گزینه ConfigServer Security&Firewall اضافه شده .

برید توش

از سومین قسمت (csf - ConfigServer Firewall) دومین دکمه یعنی firewall configuration رو بزنی

هول نکنید چیزی نیست کلا دو تا عدد رو میخوایم تغییر بدیم

در همون اولش یه جا داره که مقدار TESTING = رو تغییر میدی

این مقدار رو به ۰ تغییر بدید و بعد یه کم بیاید پایینتر تا مورد Allow incoming TCP ports رو ببینید در اینجا میتونید پورت های مورد نظرتون رو باز یا بسته کنید

اگه یادتون باشه تو جلسه ۵.۵ تاکید کردم که پورت اس اس اچ رو عوض نکنید چون حتما باید پورت در فایروال باز بشه برای بستن یه پورت که کافیه اونو از قسمت های TCP_IN = و TCP_OUT = حذف کنید (دقت کنید که کاما (,)) مربوط به اون پورت هم بردارید در کل باید بین هر پورت یه کاما باشه) که اگر اطلاعات کامل ندارید قویا پیشنهاد میکنم پورتهای از این لیست حذف نکنید

برای اینکه یه پورت رو باز کنید (مثلا پورتهای که در نظر دارید به اس اس اچ بدید باید مراحل زیر رو طی کنید)
مثلا من میخوام پورت ۱۲۳۴ رو به اس اس اچ اختصاص بدم برای اینکه باید در همین قسمت های TCP_IN = و TCP_OUT = بعد آخرین عدد یه علامت کاما بزنی (,) و عدد مورد نظر رو اضافه کنیم
حالا عبارت CT_LIMIT = رو در صفحه پیدا کنید با تغییر این مقدار میشه جلوی بعضی از حملات دی داس رو گرفت

مقدارش رو به ۲۵۰ تغییر بدید (این یعنی تعداد کانکشن های همزمانی که یه ایپی میتونه به سرور داشته باشه)

حالا صفحه رو تا آخر بیارید پایین و change رو بزنی بعد هم restart csf+lfid رو بزنی

حالا هم return رو بزنی

بر میگردید به همون صفحه اصلی فایروال

حالا بزارید یه کم گزینه های این صفحه رو توضیح بدم و ببینیم چی به چی

اولین گزینه که نوشته Check server security یه گزینه بسیار مهم و پرکاربرده این گزینه امنیت و کارایی سرور شما رو از جهت های مختلف چک میکنه و همه رو بره شما لیست میکنه و مواردی که اوکی نباشه راه حل هم میگه در مورد این قسمت دو جلسه مفصلا بحث میکنیم

دیگه تو قسمت اول چیز پر کاربردی نیست

در قسمت آپگرید هم اگه ورژن جدیدی از فایروال موجود باشه یه دکمه ظاهر میشه و با زدن اون فایروال آپدیت میشه
در سومین قسمت (ConfigServer Firewall - csf) سه تا گزینه پشت سر هم داریم Quick allow و Quick deny و Quick Ignore که کنار همه شون هم یه کادر هست

اگه در کادر سبز رنگ Quick allow یه آیپی رو بزنیند و بعد دکمه Quick allow رو بزنیند این آیپی برای همیشه در لیست سبز میمونه و هیچ وقت بلاک نمیشه و اگه بلاک شده باشه هم آزاد میشه
اگه در کادر قرمز رنگ Quick deny یه آیپی رو بزنیند و دکمه Quick deny رو بزنیند دسترسی اون آیپی برای همیشه رو سرور بسته میشه

Quick Ignore هم بره عدم بررسی یه آیپیه

قسمت Firewall allow IPs دقیقا معادل همون Quick allow هست با این تفاوت که یه لیست باز میکنه و لیست تمام آیپی هایی که رو سرور در لیست سبز هستن رو میاره و میتونید هر چند تا آیپی رو که خواستید از لیست بردارید یا به لیست اضافه کنید

قسمت Firewall Deny IPs دقیقا معادل همون Quick Deny هست با این تفاوت که یه لیست باز میکنه و لیست تمام آیپی هایی که رو سرور واسه همیشه بلاک هستن رو میاره و میتونید هر چند تا آیپی رو که خواستید از لیست بردارید یا به لیست اضافه کنید

گزینه های Enable و Disable هم که مشخصه : برای فعال و غیر فعال کردن فایروال

گزینه Remove Deny هم بره اینه که آیپی بلاک شده رو از لیست حذف کنید

Temporarily allow/deny هم بره بلاک یا allow کردن یه آیپی برای یه زمان مشخصه

بقیه گزینه ها زیاد کاربرد ندارن یا حرفه ای هستن یا شاید من حال ندارم توضیح بدم ...

بره این جلسه کافیه ، بازم تاکید میکنم هر طور سوال ممکن ، پیشنهاد و انتقاد رو در تاپیک بحث و بررسی و بیان مشکلات در مورد آموزش مدیریت سرور مطرح کنید و تشکر هم فراموش نشه
با سپاس

جلسه هفتم

سلام

در این جلسه به روش ساده و بی نهایت موثر بره افزایش امنیت و کارایی سرور می‌گم
اگره دقت کرده باشید در قسمت ConfigServer Security&Firewall اولین گزینه Check server security
هست که جلسه پیش وعده بحث در موردشو داده بودم

همونطور که گفتم : این گزینه امنیت و کارایی سرور شما رو از جهت های مختلف چک میکنه و همه رو بره شما لیست
میکنه و مواردی که اوکی نباشه راه حل هم می‌گه

وقتی سی پنل رو با کانفیگ پیشفرض و در به سرور خام نصب میکنید به سری گزینه به طور پیشفرض سبز و اوکی
هست (حدودا نصفشون) و با نصب ELS به تعداد دیگه هم سبز میشه
من اینجا در مورد موارد مهمش که باید تغییر بدید بحث میکنم

Check root forwarder

این گزینه که وسط هاست ولی بهتره از اول انجام بشه بره اینه که به ایمیل ست کنید تا سی اس اف از طریق اون با شما
در ارتباط باشه

برای این کار

بزنید

کد:

```
nano /root/.forward
```

و آدرس ایمیلتون رو داخلش بنویسید و سیوش کنید

خب حالا از اول شروع کنیم مواردی که معمولاً قرض میشه رو بررسی کنیم

Check csf LF_SCRIPT_ALERT option

قرمز بودن این مورد یعنی وقتی به حجم انبوه ایمیل ارسال میشه سی اس اف براتن به اخطار بفرسته (بره جلوگیری از
اسپم)

Check csf PT_ALL_USERS option

این گزینه می‌گه که بررسی یوزر ها فقط محدود به یوزر های هاست نباشه و کل یوزر های سرور بررسی شه
همونطور که میبینید تمام گزینه ها در کنارش به توضیح خیلی عالی داره و ممکنه خیلی موارد رو توضیح ندیم و راه
حل بگم

برای فعال کردن این دو مورد (که مورد اول رو بنا به خواسته خودتون و مورد دوم رو حتما) فعال کنید

در قسمت ConfigServer Security&Firewall اضافه شده .

برید توش

از سومین قسمت (csf - ConfigServer Firewall) دومین دکمه یعنی firewall configuration رو بزنید بعد

مقدار عبارت LF_SCRIPT_ALERT رو به ۱ تغییر بدید (برای گزینه اول)

مقدار PT_ALL_USERS رو هم به ۱ تغییر بدید (برای گزینه دوم)

و سیو کنید

حالا قبل اینکه بقیه گزینه ها رو توضیح بدم یه سری کار امنیتی توضیح میدم که انجام بدید که باعث میشه خود به خود خیلی از گزینه ها سبز شه

۱- حتما طبق آموزش جلسات قبل ELS نصب و مراحلشو انجام بدید

۲- پورت اس اس اچ رو عوض کنید (طبق آموزش جلسه ۶ حتما و حتما اول پورت مورد نظر رو در فایل وال باز کنید بعد:)

وارد اس اس اچ بشید حالا یه راه خیلی ساده داریم ویه راه طولانی
اگه ELS نصب کرده باشید کافیه دستور زیر رو بزنیند و پورت مورد نظر بدید و اینتر کنید
کد:

```
els --sshport
```

ولی اگه نصب نکرده باشید باید اول دستور زیر رو بزنیند
کد:

```
nano /etc/ssh/sshd_config
```

بعد مقدار Port رو پیدا کنید و # کنارشو بردارید و به جای ۲۲ هر عددی که میخواهید رو بزنیند و سیو کنید

حالا چه از روش ای ال اس و چه از روش دوم رفته باشید یه بار دستور زیر رو بزنیند
کد:

```
service sshd restart
```

۳- حالا کارای زیر:

(ممکنه خیلی از این کارا تو سرور شما به صوتی باشه که من میگم بهش تبدیل کنید در انجور مواقع که اکثرا به خاطر نصب ELS هست نیاز نیست اون مورد رو تغییر بدید)

در قسمت Service Configuration از منوی بقلی WHM برید به قسمت Apache Configuration و بعد
Global Configuration حالا موارد زیر رو به گزینه ای که میگم تغییر بدید

Trace Enable----> OFF

Server Signature --->off

Server Tokens ---->product only

File ETag --->none

مقادیر پایین اصولا باید با توجه به مشخصات سرور تنظیم شه ولی خب من یه سری اعداد میدم که رو همه سرور ها
اوکی باشه

(موارد رو به ترتیب ننوشتیم پس موقع وارد کردن دقت کنید)

کد:

ServerLimit ۱۸۰۰

KeepAlive On

KeepAliveTimeout ۶۰

MaxClients ۱۲۰۰

MaxSpareServers ۲۰۰

MinSpareServers ۵۰

حالا که همه رو تغییر دادید Save رو بزنید و تو صفحه جدید حتما گزینه Rebuild Configuration and Restart Apache رو بزنید

تموم که شد برگردید به همون قسمت Apache Configuration و اینبار گزینه Configure PHP and SuExec رو بزنید

مقادیر رو به شکل فوق تغییر بدید
کد:

Default PHP Version (.php files) ---> ۵

PHP ۵ Handler --->suphp

PHP ۴ Handler --->none

Apache suEXEC --->on

و بعد گزینه Save new configuration رو بزنید

حالا از منوی بقل WHM برید به FTP Server Configuration (فک کنم اینا رو در جلسات قدیم هم ی سری گفتم ولی اینجا میگم و از جلسات قدیم حذف میکنم)
حالا سه تا گزینه ای که در پایین میگم رو به No تغییر بدید (هر سه تا رو به no تغییر بدید)

Allow Anonymous Logins

Allow Anonymous Uploads

Allow Logins with Root Password

و بعد هم Save کنید

از منوی بقل WHM قسمت Security Center و از زیرمجموعه هاش PHP open_basedir Tweak رو پیدا کنید

و تیک قسمت Enable php open_basedir Protection رو بزنید و Save کنید

از منوی WHM گزینه System Health و در زیرمجموعه هاش وارد Background Process Killer بشید و همه گزینه ها رو تیک بزنید و Save کنید

و اما میرسیم به یکی از بهترین قسمت های سی پنل

EasyApache

در این قسمت شما میتونید خیلی از فانکشن های و ماژول های آپاچی رو براحتی نصب یا حذف کنید

مثلا GD که برای تصاویر امنیتی و فوق العاده پر کاربرد

خب از منوی بقلی (EasyApache (Apache Update) رو بزنید

در صفحه که میاد دکمه start customizing on based profile رو بزیند
در اولین قسمت ووزن اپاچی تون رو انتخاب کنید در زمان نگارش این مقاله بهترین ورژن ۲.۲ هست
ورژن پی ایچ پی تون هم انتخاب کنید
پیشنهاد میکنم گزینه ۴ رو تیک نزیند مگر اینکه بهش نیاز داشته باشید
برید مرحله بعد

ورژن پی ایچ پی در زمان نگارش این مقاله ۵.۲.۱۷ پیشنهاد میشه
درسته که ۵.۳ هم خیلی وقته اومده ولی هنوز تعداد زیادی از اسکریپت ها باهاش مشکل دارن
برید مرحله بعد

در این اینجا یه تعدادی از فانکشن ها و برنامه ها هست
برای اینکه لیست کل رو ببینید در پایین دکمه

Exhaustive Option List

رو بزیند

تیک گزینه Frontpage رو بردارید چون دیگه پشتیبانی نمیشه و نصبش ممکنه خطر امنیتی ایجاد کنه
نصب موارد زیر پیشنهاد میشه (اگه موقع تیک زدنشون چیزی پرسید OK کنید)

IonCube Loader for PHP

GD

Gettext

SOAP

TTF

Mod Security

MPM Prefork

Zend Optimizer/Guard Loader for PHP

و هر موردی که احساس کردید لازمه ولی حتما قبلش در مورد مسائل امنیتی اون فانکشن تحقیق کنید
حالا گزینه Save and Build رو بزیند و هر چی پرسید OK کنید یا I Understand رو بزیند
حالا صبر کنید تا کار تموم بشه (یه مقدار زمان میبره) و در این مدت نباید اینترنت شما قطع بشه
اگه قطع شد دوباره از اول کار با Easy apache رو انجام بدید
در پایان تنظیمات رو به صورت زیر انجام بدید

کد:

Default PHP Version (.php files) ---> ۵

PHP ۵ Handler --->suphp

PHP ۴ Handler --->none

Apache suEXEC --->on

و سیو کنید

هنوز کارمون ادامه داره و خیلی کارا بره تامین امنیت سرور در حد متوسط (سطح مورد نظر این آموزش) مونده
ولی خب بره این جلسه کافیه ...

بازم تاکید میکنم زدن دکمه تشکر فراموش نشه و همچنین هر طور سوال ممکن ، پیشنهاد و انتقاد رو در تایپیک بحث و بررسی و بیان مشکلات در مورد آموزش مدیریت سرور مطرح کنید.
با سپاس

جلسه هفت و نیم

درود بر همه دوستان
اصلا تعداد تشکر اتون جالب نیست یعنی من این مقاله رو دارم واسه ۱۰ نفر مینویسم؟؟
بگذریم ... ولی اینو بگم که این تعداد تشکر اصلا قابل قبول نیست ...

این جلسه کارای امنیتی و ایتیمایز کردن رو ادامه میدیم
از منوی بقل WHM گزینه PHP Configuration Editor رو بزنید و تیک رو در advance mode بزارید
disable_functions رو پیدا کنید و مقدار زیر رو توش بزارید

کد:

```
symlink,shell_exec,exec,proc_close,proc_open,popen,pclose,system,dl,passthru,escapeshellarg,escapeshellcmd,readfile
```

حالا سه تا مقدار زیر رو حتما و حتما برابر off قرار بدید (ممکنه بعضی ها در حالت پیشفرض خاموش باشه)
کد:

```
allow_url_fopen = Off  
register_globals = Off  
enable_dl=Off
```

موارد زیر رو هم قویا پیشنهاد میشه به صورتی که جلوشون نوشتیم تغییر بدید
کد:

```
display_errors = Off  
display_startup_errors = Off  
safe_mode = On  
log_errors = On  
expose_php = Off  
magic_quotes_gpc = On  
magic_quotes_sybase = Off
```

در پایان save رو بزنید

اگه در جلسه قبل همونطور که گفته بودم در Easy apache تیک Mod Security رو زده باشید در قمت آخر منوی WHM یه گزینه به همین اسم Mod Security اضافه میشه
اونو باز کنید

edit config رو بزنید و Default Configuration رو انتخاب کنید و بعد Save Configuration رو بزنید
در منوی بقل WHM گزینه Compiler Access رو باز کنید و Disable compilers رو بزنید

از منوی بقل WHM گزینه Exim Configuration Editor رو پیدا کنید و از پایین ترین قسمتش Advanced editor رو بزنید

در صفحه ای که باز میشه در هون قسمت های بالایی یه کادر بره وارد کردن تکست هست متن زیر رو در اون بزنید

log_selector = +arguments +subject +received_recipients

در اخر هم Save رو بزنید

از منوی بقل WHM گزینه Tweak Settings رو بزنید

مقدار BoxTrapper Spam Trap رو به OFF تغییر بدید

مقدار Max hourly emails رو به ۱۰۰ تغییر بدید

Email password reset رو OFF کنید

Block common domain usage رو ON کنید

Allow domain parking across accounts رو OFF کنید

Cookie IP validation رو روی strict بزارید

Use MD۵ passwords with Apache رو ON کنید

Blank referrer safety check و Referrer safety check رو ON کنید (اختیاری چون فعال شدنش خوبه

ولی یه کم ممکنه تو لوگین ها اذیت کنه و همش پسورد بخواد)

Security Tokens رو هم on کنید

Require SSL رو off کنید درسته که فعال بودنش خیلی خوبه ولی تو ایران ISP ها سر SSL ادا در میارن

آخر سر Save کنید

حالا اس اس اچ رو باز کنید و دستور زیر رو بزنید

کد:

```
nano /etc/ssh/sshd_config
```

با زدم دکمه CTRL + W از کیبرد عبارت UseDNS رو پیدا کنید اگر کنار # بود بردارید و مقدارشو به no تغییر

بدید (اگه جلوش نوشته بود no به هیچی دست نزنید و اگه نوشته yes فقط اون yes رو به no تبدیل کنید و فایل رو

سیو کنید و بیاید بیرون

دستور

کد:

```
nano /etc/my.cnf
```

رو بزنید

اگه عبارت local-infile وجود داشت مقدارشو به ۰ و اگه نبود در خط اخر اینو اضافه کنید

کد:

```
local-infile=۰
```

فایل رو سیو کنید و بیاید بیرون

حالا در منوی بقل WHM به Security&Firewall ConfigServer برید و

SECURITY رو بزنید

اولا یاد آوری کنم قرار نیست همه گزینه ها سبز بشه (شاید در آخر یه ۱۰-۱۵ تایی بمونه که هیچ مشکلی نداره)
 برید به آخرین قسمتش که نوشته **Server Services Check** و پایینش حدود ۱۰-۱۲ مورد رو چک کرده
 اگه همش سبز باشه که خدا رو شکر اگه یکی یا چند تا یا همش قرمز باشه اگه دقت کنید کنار هر کدوم دو تا دستور
 نوشته اون دو تا دستور رو در اس اس اچ بزنید و اگر هم دستور ها ارور داد ارورش رو بیخیال شید: **D:**
 اگه سرور مجازی با **OpenVZ** یا **Virtuzu** دارید کار تمومه و یه **reboot** بزنید (و قسمت بعد که سکیو کردن **tmp/**
 هست رو بیخیال شید و فقط بیاید سراغ خطوط پایانی
 اگه سرور اختصاصی دارید یا سرور مجازی با **Vmware** و **Xen** یه مرحله دیگه هم دارید ...
 ولی خب با توجه به اینکه دیگه حوصله تایپ ندارم و در سایت **Linuxtalk.ir** آقای پیمان قربانی این مطلب رو به
 خوبی آموزش داده من مال ایشون رو براتون کپی پیست میکنم
امن کردن tmp/:
 کد:

```
cd /dev
```

ساخت ۲۰۰۰ مگابایت فضا ذخیره سازی:
 کد:

```
dd if=/dev/zero of=tmpMnt bs=۱۰۲۴ count=۲۰۰۰۰۰۰
```

ساخت فایل سیستم **ext** :
 کد:

```
/sbin/mke2fs /dev/tmpMnt
```

ایجاد یک پشتیبان:
 کد:

```
cp -R /tmp/ /tmp_backup
```

mount کردن فایل سیستم جدید با **noexec**:
 کد:

```
mount -o loop,rw,nosuid,noexec /dev/tmpMnt /tmp
```

سطح مجوز را هم تغییر دهید:
 کد:

```
chmod ۰۷۷۷ /tmp
```

پشتیبانی را که تهیه کرده بودیم، کپی میکنیم:
 کد:

```
cp -R /tmp_backup/* /tmp/
```

پشتیبان را حذف میکنیم:
 کد:

```
rm -rf /tmp_backup
```

امن کردن **var/tmp/** :
 تهیه یک پشتیبان:

کد:

```
mv /var/tmp /var/tmpbck
```

آدرس دهی میکنیم:

کد:

```
ln -s /tmp /var/tmp
```

فایل های داخل پشتیبان را کپی میگیریم:

کد:

```
cp /var/tmpbck/* /tmp/
```

امن کردن /dev/shm :

فایل زیر را با ویرایشگر باز میکنیم:

اگر ویرایشگر nano را نصب ندارید، با دستور زیر نصب کنید.

کد:

```
nano /etc/fstab
```

مقدار زیر را پیدا کنید :

کد:

```
none /dev/shm tmpfs defaults,rw . .
```

مقدار زیر را جایگزین مقدار فوق میکنیم:

کد:

```
none /dev/shm tmpfs defaults,nosuid,noexec,rw . .
```

مجدداً mount میکنیم:

کد:

```
mount -o remount /dev/shm
```

و حالا به بار سرور رو با دستور reboot ریboot کنید

قابل توجه همه (هم وی پی اس دارا هم سرور دارا)

من در نظر داشتم سی پنل رو تا همین حد آموزش بدم یادتون باشه هیچ وقت به آموزش های چرت و پرت من متکی نباشید و در گوگل سرچ کنید و از فروم هم بهره ببرید و سوال بپرسید ...

همونطور که به دایرکت ادمین دارا هم قول داده بودم از جلسه بعد آموزش این کنترل پنل رو (که مورد علاقه خودمم هست) رو شروع میکنم و پس از تموم شدنش به امید خدا این آموزش رو که پرونده اش از عید ۸۹ روی میزه رو میبندم

با سپاس

کوچیک همه شما

آرش

جلسه هشتم

سلام

این جلسه میرسیم به کنترل پنل محبوب خودم : دایرکت ادمین

این کنترل پنل که طریقه نصبش رو در جلسات اول گفتم و آموزش نصب فایروال و ELS هم براش گفته شد .

دایرکت ادمین در موقع نصب با تنظیمات پیشفرض خودش امنیت و کارایی خیلی قوی تری نسبت به سی پنل داره و کارایی که باید انجام بشه خیلی کمتره

برای بهینه سازی و ایمن سازی دایرکت ادمین مراحل زیر رو طی میکنم

۱- نصب فایروال CSF

۲- نصب ELS که هر دوش در جلسات قبل گفته شده

و بعد بریم تو دایرکت ادمین

اگه دقت کنید در قسمت admin level (جایی که به طور پیشفرض هم توش هستید) در پاییناش یه گزینه ConfigServer Security&Firewall اضافه شده .

برید توش

از سومین قسمت (csf - ConfigServer Firewall) دومین دکمه یعنی firewall configuration رو بزیند

هول نکنید چیزی نیست کلا دو تا عدد رو میخوایم تغییر بدیم

در همون اولش یه جا داره که مقدار TESTING = رو تغییر میده

این مقدار رو به ۰ تغییر بدید و بعد یه کم بیاید پایینتر تا مورد Allow incoming TCP ports رو ببینید در اینجا میتونید پورت های مورد نظرتون رو باز یا بسته کنید

اگه یادتون باشه تو جلسه ۵.۵ تاکید کردم که پورت اس اس اچ رو عوض نکنید چون حتما باید پورت در فایروال باز بشه برای بستن یه پورت که کافیه اونو از قسمت های TCP_IN = و TCP_OUT = حذف کنید (دقت کنید که کاما ,) مربوط به اون پورت هم بردارید در کل باید بین هر پورت یه کاما باشه) که اگر اطلاعات کامل ندارید قویا پیشنهاد میکنم پورتهای از این لیست حذف نکنید

برای اینکه یه پورت رو باز کنید (مثلا پورتهای که در نظر دارید به اس اس اچ بدید باید مراحل زیر رو طی کنید)

مثلا من میخوام پورت ۱۲۳۴ رو به اس اس اچ اختصاص بدم برای اینکار باید در همین قسمت های TCP_IN = و

TCP_OUT = بعد آخرین عدد یه علامت کاما بزینم (,) و عدد مورد نظر رو اضافه کنیم

حالا عبارت CT_LIMIT = رو در صفحه پیدا کنید با تغییر این مقدار میشه جلوی بعضی از حملات دی داس رو گرفت

مقدارش رو به ۲۵۰ تغییر بدید (این یعنی تعداد کانکشن های همزمانی که یه ایپی میتونه به سرور داشته باشه)

حالا عبارت AUTO_UPDATES رو پیدا کنید و مقدارش رو ۱ بزارید

عبارت SAFECHAINUPDATE رو هم پیدا کنید و مقدارشو ۱ بزارید

حالا صفحه رو تا آخر بیارید پایین و change رو بزنید بعد هم restart csf+lfid رو بزنید
حالا هم return رو بزنید

بر میگردید به همون صفحه اصلی فایروال

حالا بزارید یه کم گزینه های این صفحه رو توضیح بدم و ببینیم چی به چی

اولین گزینه که نوشته Check server security یه گزینه بسیار مهم و پر کار بوده این گزینه امنیت و کارایی سرور شما رو از جهت های مختلف چک میکنه و همه رو بره شما لیست میکنه و مواردی که اوکی نباشه راه حل هم میگه بعدا از این قسمت استفاده خواهیم کرد

دیگه تو قسمت اول چیز پر کاربردی نیست

در قسمت آپگرید هم اگه ورژن جدیدی از فایروال موجود باشه یه دکمه ظاهر میشه و با زدن اون فایروال آپدیت میشه در سومین قسمت (csf - ConfigServer Firewall) سه تا گزینه پشت سر هم داریم Quick allow و Quick deny و Quick Ignore که کنار همه شون هم یه کادر هست

اگه در کادر سبز رنگ Quick allow یه آپپی رو بزنید و بعد دکمه Quick allow رو بزنید این آپپی برای همیشه در لیست سبز میمونه و هیچ وقت بلاک نمیشه و اگه بلاک شده باشه هم آزاد میشه اگه در کادر قرمز رنگ Quick deny یه آپپی رو بزنید و دکمه Quick deny رو بزنید دسترسی اون آپپی برای همیشه رو سرور بسته میشه

Quick Ignore هم بره عدم بررسی یه آپپیه

قسمت Firewall allow IPs دقیقا معادل همون Quick allow هست با این تفاوت که یه لیست باز میکنه و لیست تمام آپپی هایی که رو سرور در لیست سبز هستن رو میاره و میتونید هر چند تا آپپی رو که خواستید از لیست بردارید یا به لیست اضافه کنید

قسمت Firewall Deny IPs دقیقا معادل همون Quick Deny هست با این تفاوت که یه لیست باز میکنه و لیست تمام آپپی هایی که رو سرور واسه همیشه بلاک هستن رو میاره و میتونید هر چند تا آپپی رو که خواستید از لیست بردارید یا به لیست اضافه کنید

گزینه های Enable و Disable هم که مشخصه : برای فعال و غیر فعال کردن فایروال

گزینه Remove Deny هم بره اینه که آپپی بلاک شده رو از لیست حذف کنید

Temporarily allow/deny هم بره بلاک یا allow کردن یه آپپی برای یه زمان مشخصه

بقیه گزینه ها زیاد کاربرد ندارن یا حرفه ای هستن یا شاید من حال ندارم توضیح بدم ...

حالا که یاد گرفتید پورتی رو در فایروال باز کنید وقتشه پورت اس اس اچ رو تغییر بدیم

وارد اس اس اچ بشید حالا یه راه خیلی ساده داریم ویه راه طولانی

اگه ELS نصب کرده باشید کافیه دستور زیر رو بزنید و پورت مورد نظر بدید و اینتر کنید
کد:

```
els --sshport
```

ولی اگه نصب نکرده باشید باید اول دستور زیر رو بزنید
کد:

```
nano /etc/ssh/sshd_config
```

بعد مقدار Port رو پیدا کنید و # کنارشو بردارید و به جای ۲۲ هر عددی که میخواهید رو بزنید و سیو کنید

حالا چه از روش ای ال اس و چه از روش دوم رفته باشید یه بار دستور زیر رو بزنید
کد:

```
service sshd restart
```

حالا باید یه ایمیل به سرور بدید تا سی اس اف از طریق اون با شما در ارتباط باشه
برای این کار در اس اس اچ بزنید
کد:

```
nano /root/.forward
```

و آدرس ایمیلتون رو داخلش بنویسید و سیوش کنید

هنوز خیلی کار داریم ولی بره این جلسه کافیه
با سپاس

جلسه هشت و نیم

سلام

این جلسه هم به ادامه امنیت دایرکت ادمین می‌رسیم

دستور زیر رو بزنید

کد:

```
cd /usr/local/directadmin/custombuild
```

بزنید

کد:

```
nano options.conf
```

حالا مقادیر رو به شکل زیر تغییر بدید

```
default_php=۵
```

```
php۵_ver=۵.۲
```

```
php۴_cli=no
```

```
php۴_cgi=no
```

```
php۵_cli=yes
```

```
php۵_cgi=no
```

```
zend=yes
```

```
mysql=۵.۱
```

```
mysql_inst=no
```

```
mysql_backup=yes
```

```
apache_ver=۲.۲
```

```
phpmyadmin=yes
```

```
atmail=no
```

```
squirrelmail=yes
```

```
roundcube=yes
```

```
uebimiau=no
```

```
exim=no
spamassassin=no
mail-header-patch=yes
dovecot=yes
```

```
awstats=no
webalizer=no
```

```
proftpd=no
pureftpd=yes
```

و به بقیه موارد دست نزنید
سیو کنید و بیاید بیرون
حالا دستور زیر رو بزنید و صبر کنید تا کارش انجام بشه
کد:

```
./build all
```

حالا برید تو دایرکت ادمین برید به قسمت File Editor و از منوی کشویی که میاد usr/local/lib/php.ini/ رو انتخاب کنید و show file رو بزنید حالا disable_functions رو پیدا کنید و بکنیدش مثل شکل زیر
کد:

```
disable_functions =
symlink,shell_exec,exec,proc_close,proc_open,popen,pclose,system,dl,passthru,escapeshellarg,escapeshellcmd,readfile
```

حالا سه تا مقدار زیر رو حتما و حتما برابر Off قرار بدید (ممکنه بعضی ها در حالت پیشفرض خاموش باشه)
کد:

```
allow_url_fopen = Off
register_globals = Off
enable_dl=Off
```

موارد زیر رو هم قویا پیشنهاد میشه به صورتی که جلوشون نوشتم تغییر بدید
کد:

```
display_errors = Off
display_startup_errors = Off
safe_mode = On
log_errors = On
expose_php = Off
magic_quotes_gpc = On
magic_quotes_sybase = Off
```

در پایان save رو بزنید

برگردید به صفحه اصلی دایرکت ادمین

برید به Administrator Settings و تیک گزینه های زیر رو بردارید

Enable User Demo. Login: demo_user Password : demo

Enable Reseller Demo. Login: demo_reseller Password : demo

Enable Admin Demo. Login: demo_admin Password : demo

حالا گزینه ها رو به صورتی که میدم تغییر بدید

Max Request/Upload Size (bytes) ---->۱۰۴۸۵۷۶۰۰۰

Warn Admin's at ۹۵ % partition usage ---> ۹۵ , Day

Enable Automatic Lost Password Recovery --->NO

Blacklist IPs for excessive login attempts <--- عدد رو بزارید ۳۰ و تیک رو هم بزنید

Prevent ۱۲۷.۰.۰.۱ from being Blacklisted --- < تیک بزنید

Time before failed login count resets --->۱۰

Check domain owner for Subdomain creation ---->yes

Daily Email Limit per DirectAdmin User ---->۱۰۰

و بعد سیو کنید

برگردید صفحه اصلی دایرکت ادمین و Php Safe Mode Settings رو بزنید

Default Safe Mode for new domains: رو ON کنید و Default Open BaseDir for new domains

رو OFF و سیو کنید

حالا اس اس اچ رو باز کنید و دستور زیر رو بزنید

کد:

nano /etc/ssh/sshd_config

با زدم دکمه CTRL + W از کیبرد عبارت UseDNS رو پیدا کنید اگر کنار # بود بردارید و مقدارشو به no تغییر

بدید (اگه جلوش نوشته بود no به هیچی دست نزنید و اگه نوشته yes فقط اون yes رو به no تبدیل کنید و فایل رو

سیو کنید و بیاید بیرون

دستور

کد:

nano /etc/my.cnf

رو بزنید

اگه عبارت local-infile وجود داشت مقدارشو به ۰ و اگه نبود در خط آخر که خالیه اینو اضافه کنید

کد:

local-infile=۰

فایل رو سیو کنید و بیاید بیرون

حالا در صفحه اصلی دایرکت ادمین به ConfigServer Security&Firewall برید و CHECK SERVER SECURITY رو بزیند

اولا یاد آوری کنم قرار نیست همه گزینه ها سبز بشه (شاید در آخر یه تعداد قرمز بمونه که هیچ مشکلی نداره) برید به آخرین قسمتش که نوشته Server Services Check و پایینش حدود ۱۰-۱۲ مورد رو چک کرده اگه همش سبز باشه که خدا رو شکر اگه یکی یا چند تا یا همش قرمز باشه اگه دقت کنید کنار هر کدوم دو تا دستور نوشته اون دو تا دستور رو در اس اس اچ بزیند و اگر هم دستور ها اروری داد ارورش رو بیخیال شید: D: اگه سرور مجازی با OpenVZ یا Virtuzu دارید کار تمومه و یه reboot بزیند (و قسمت بعد که سکیو کردن tmp/ هست رو بیخیال شید و فقط بیاید سراغ خطوط پایانی اگه سرور اختصاصی دارید یا سرور مجازی با Vmware و Xen یه مرحله دیگه هم دارید ... ولی خب با توجه به اینکه دیگه حوصله تایپ ندارم و در سایت Linuxtalk.ir آقای پیمان قربانی این مطلب رو به خوبی آموزش داده من مال ایشون رو براتون کپی پیست میکنم امن کردن tmp/:

کد:

```
cd /dev
```

ساخت ۲۰۰۰ مگابایت فضا ذخیره سازی:

کد:

```
dd if=/dev/zero of=tmpMnt bs=۱۰۲۴ count=۲۰۰۰۰۰۰
```

ساخت فایل سیستم ext :

کد:

```
/sbin/mke2fs /dev/tmpMnt
```

ایجاد یک پشتیبان:

کد:

```
cp -R /tmp/ /tmp_backup
```

mount کردن فایل سیستم جدید با noexec:

کد:

```
mount -o loop,rw,nosuid,noexec /dev/tmpMnt /tmp
```

سطح مجوز را هم تغییر دهید:

کد:

```
chmod ۰۷۷۷ /tmp
```

پشتیبانی را که تهیه کرده بودیم، کپی میکنیم:

کد:

```
cp -R /tmp_backup/* /tmp/
```

پشتیبان را حذف میکنیم:

کد:

```
rm -rf /tmp_backup
```

امن کردن /var/tmp/ :

تهیه یک پشتیبان:

کد:

```
mv /var/tmp /var/tmpbck
```

آدرس دهی میکنیم:

کد:

```
ln -s /tmp /var/tmp
```

فایل های داخل پشتیبان را کپی میگیریم:

کد:

```
cp /var/tmpbck/* /tmp/
```

امن کردن /dev/shm/ :

فایل زیر را با ویرایشگر باز میکنیم:

اگر ویرایشگر nano را نصب ندارید، با دستور زیر نصب کنید.

کد:

```
nano /etc/fstab
```

مقدار زیر را پیدا کنید :

کد:

```
none /dev/shm tmpfs defaults,rw . .
```

مقدار زیر را جایگزین مقدار فوق میکنیم:

کد:

```
none /dev/shm tmpfs defaults,nosuid,noexec,rw . .
```

مجدداً mount میکنیم:

کد:

```
mount -o remount /dev/shm
```

و حالا به بار سرور رو با دستور reboot ریست کنید

قابل توجه همه (هم وی پی اس دارا هم سرور دارا)

من در نظر داشتم دایرکت ادمین رو تا همین حد آموزش بدم ، یادتون باشه هیچ وقت به آموزش های چرت و پرت من

متکی نباشید و در گوگل سرچ کنید و از فروم هم بهره ببرید و سوال بپرسید ...

از کل آموزش ها و حرف هام به جلسه بیشتر نمونده و بعد اون این آموزش بالاخره تموم میشه

با سپاس

آرش

جلسه پایانی

خدایا چنان کن سرانجام کار تو خشنود باشی و ما رستگار

سلامی دوباره به تمام دوستان

بالاخره این ۱۵ جلسه رو تموم کردم و آموزش های مدیریت سرور رو تا اون حدی که در نظرم بود اینجا نوشتم خوشحالم که تونستم این مقاله رو تا اینجا بنویسم و برای یه تعداد مفید باشم

ولی یه درد دل کوچیک با کاربران عزیز

من یه سال دیگه همین موقع ها باید کنکور بدم ولی با این حال این آموزش های رو تکمیل کردم و اینجا گذاشتم ...

از تمام کاربران این انجمن میخوام که برای موفقیتم تو کنکور دعا کنن

و اما یه بحث دیگه من این آموزش رو رایگان منتشر کردم ، از ابتدا هدف این آموزش این بود که رایگان در دست تمام کاربرها باشه

بیاید منصف باشیم من ساعت ها وقت گذاشتم تا این آموزش رو بنویسم آموزشی که شاید خیلی از مینجرها هزینه های زیادی رو برای انجامش میگیرن ، شاید به کمک این آموزش ها بتونید خیلی از سرورها رو خودتون مدیریت کنید ... شاید بارها عبارت Donation رو در سایت های خارجی دیدم ولی متاسفانه در سایت های فارسی این مورد به چشم نمیخوره

من از تمام کاربرانی که این آموزش رو خوندن و براشون مفید بوده درخواست دارم یه مبلغی رو ، هر چقدر که میتونید ۱۰۰۰ تومان ، ۵۰۰۰ تومان ، ۱۰۰۰۰ تومان ، یا هر رقمی که دلتون خواست از طریق لینک زیر بصورت آنلاین به بنده اهدا کنید ...

سامانه پرداخت زرین پال

لطفا در قسمت توضیحات نام کاربریتون در WHT و اینکه مایل هستید اسمتون در لیست اهدا کننده گان قرار بگیره یا خیر رو قید بفرمایید

پیشاپیش از همه دوستان تشکر میکنم که یه مبلغی رو به بنده اهدا میکنن

من هیچ کاربری رو به پرداخت الزام نمیکنم ولی از همه کاربران خواهش میکنم بنا به توانایشون یه مبلغی رو اهدا کنن این مورد هم اضافه کنم که ۱۰ درصد کل این مبالغ اهدایی متعلق به موسسه خیریه و نیازمندان هست

برای همه دوستان آرزوی موفقیت دارم

softsara.ir

امیدوارم این آموزش براتون مفید باشه
کوچیک همه شما
آرش درگاهی