آموزش هک کنسول های بازی PS4 یا همون پلستیشن4

موزشی که بعنوان یک هک یا جیلبریک در اختیار عموم قرار خواهد گرفت، درواقع یک جیلبریک یا هک نمی باشد؛ بلکه به اصطلاح یک دور زدن در محیط اینترنتی کنسول می باشد. با استفاده از این آموزش میتوان یک بازی را بر روی تمامی کنسول ها نصب نمود اما معایبی نیز در این آموزش وجود دارد؛ بطور مثال با بازیهای فعال شده با این روش پس از اولین اتصال به اینترنت غیرفعال می شوند.

بخش اول؛ باز کردن کنسول پلی استیشن 4

قبل از انجام هرگونه عملیات، از مدل کنسول خود مطمئن شوید؛ ابتدا مدل کنسول خود را شناسایی کرده و سپس اطلاعات آن را در محیط اینترنت جستجو کنید. اگر مادربرد کنسول شما از نوع SAA باشد، با خیال راحت آموزش را تا انتها ادامه دهید. اگر مادربرد کنسول شما از نوع SAB باشد بهتر است آن را به مراکز ارائه دهنده خدمات برسانید تا آن ها عملیات را برای شما انجام دهند.

خش دوم؛ جداسازی فلش مموری Macronix MX25L25635FMI 256Mb Serial

طعه ای که نام آن را در بالا مشاهده میکنید، یک فلش مموری با حافظه 256 مگابایت می باشد که اطلاعات مهم کنسول را در خود نگهداری میکند.

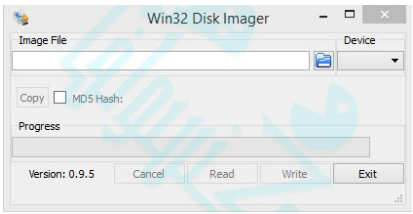
اطلاعات مهم از طریق این فلش مموری با سرور های پلی استیشن ارتباط برقرار میکنند و بدین صورت است که عملیات هایی مانند Trophy Synchronization و Restore License و Activate Primary انجام میشوند. در این بخش از آموزش شما باید این فلش مموری را از کنسول خود جدا کنید. راه های مختلفی مانند استفاده از سشوار های صنعتی و ... می باشد که انجام این عملیات را آسان تر می سازد. اگر ذره ای در انجام این عملیات شک دارید بهتر است آن را به یک تعمیر کار معتبر برسانید زیرا این بخش حساس ترین بخش این آموزش می باشد. در تصویر اخر از بخش قبل، یک قطعه مشاهده میکنید که با حاشیه آبی رنگ مشخص شده است. آن قطعه همان فلش مموری Macronix MX25L25635FMI 256Mb Serial می باشد.

بخش سوم؛ آماده سازی Raspberry Pi 2

وسیله Raspberry Pi 2 ما باید اطلاعات فلش مموری ذکر شده که از روی مادربرد کنسول جدا کرده ایم را از آن دریافت کنیم که به این عملیات Dump گفته میشود. قطعه Raspberry Pi 2 در توضیحات کامل آن که در وبسایت های معتبر خارجی نیز ذکر شده است، یک رایانه کدباز می باشد که برای عملیات های آموزشی از آن استفاده میشود و به همین دلیل نیز تهیه آن در بازار ساده تر از سایر قطعه ها می باشد.

بخش سوم مرحله اول؛ پیاده سازی Raspbian

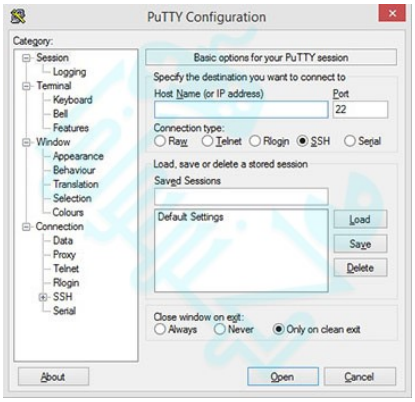
در این مرحله به برنامه ای بنام Win32DiskImager و یک عدد رم SD یا حجم بالاتر از 4 گیگابایت و فایل Raspbian نیاز دارید. حجم فایل Raspbian کمی بالاتر از سایر نیاز های این آموزش می باشد و همچنین نسخه فشرده فایل نیز حجم کمتری دارد. دقت داشته باشید که در هنگام دانلود، فایل Raspbian Wheezy را دانلود کنید. پس از دانلود و آماده سازی موارد ذکر شده در بند قبل، حالا برنامه Win32DiskImager را بر روی رایانه خود نصب کرده و آن را اجرا کنید.



ایل Raspbian Wheezy را که دانلود کردید از حالت فشرده خارج کنید و سپس فایل img موجود در آن را به بخش "..." بدهید. سپس رم ذکر شده با حجم بالاتر از 4 گیگابایت را به رایانه وصل کرده و در بخش انتخاب درایو به رایانه بدهید. حالا گزینه Write را انتخاب کنید و صبر کنید تا برنامه پردازش های لازم را بر روی رم SD وصل شده به رایانه انجام دهد. دقت داشته باشید که تا پایان عملیات هرگز رایانه را در حالت Sleep و یا حالات دیگر قرار نداده و همچنین رم SD را از آن جدا نکنید.

بخش سوم مرحله دوم؛ ورود به قطعه Raspberry Pi 2

پس از این که عملیات Write توسط این برنامه به اتمام رسید، رم SD را از رایانه جدا کرده و به قطعه Raspberry Pi 2 وصل کنید و سپس قطعه را با کابل لن به رایانه وصل کرده و روشن کنید. حالا برنامه Puttyرا دانلود و از حالت فشرده خارج کنید. پس از چند دقیقه که قطعه 2 Raspberry Pi روشن می باشد، برنامه Putty را اجرا کنید.



در بخش Host Name عبارت raspberrypi را وارد کنید (اگر این آدرس در برنامه مورد قبول واقع نشد، به بخش Network Settings در رایانه خود رفته و آی پی قطعه Raspberry Pi 2 را یادداشت کرده و در این بخش قرار دهید. حالا در بخش Connection Type گزینه SSH را انتخاب کنید و در نهایت گزینه Open را از پائین برنامه انتخاب کنید. حالا برنامه از شما یک نام کاربری و یک کلمه عبور درخواست میکند. در بخش نام کاربری عبارت pi و در بخش کلمه عبور نیز عبارت raspberry را وارد کنید. پس از ورود به قطعه، کد زیر را جهت تنظیمات خواسته شده ثبت کنید.

```
sudo -s
cd /bin
wget http://jaicrab.org/Ps4/Tools/JAISPI/jaispi
chmod +x jaispi
echo “#blacklist spi-bcm2708” > /etc/modprobe.d/raspi-blacklist.conf
echo “blacklist i2c-bcm2708” >> /etc/modprobe.d/raspi-blacklist.conf
reboot
```

پس از دستور بالا، قطعه بطور کامل آماده سازی شده است. حالا می توانید دستورات مورد نظر خود را بر روی قطعه پیاده سازی کنید تا عملیات لازم صورت گیرد. دستور زیر جهت تهیه Dump از فلش مموری برداشته شده از مادربرد کنسول می باشد.

```
sudo -s
cd /bin
wget http://jaicrab.org/Ps4/Tools/JAISPI/jaispi
chmod +x jaispi
echo “#blacklist spi-bcm2708” > /etc/modprobe.d/raspi-blacklist.conf
echo “blacklist i2c-bcm2708” >> /etc/modprobe.d/raspi-blacklist.conf
reboot
```

تنظیمات قطعه نیز با قطعه کد زیر قابل رویت می باشد.

```
i /dev/spidevX.X Get ID from flash-
r file.bin /dev/spidevX.X Read entire flash to file-
e /dev/spidevX.X Erase entire flash-
p file.bin /dev/spidevX.X Only write blocks differences from file-
v file.bin /dev/spidevX.X Verify blocks with file-
```

نحوه تهیه Dump از فلش مموری جدا شده از کنسول:
این بخش مخصوص کنسول پلی استیشن 4 تهیه شده است که کاربران بتوانند از کنسول خود دامپ تهیه کرده و دوباره آن را به کنسول بازگردانند. ابتدا بازیهای مورد نظر را بر روی کنسول خود نصب کرده و سپس وارد بخش Settings/PlayStation Network شوید. حالا گزینه Activate as Your Primary را انتخاب و سپس گزینه Activate را انتخاب کنید. حالا بازیهای مورد نظر بر روی کنسول فعال شدند. در این مرحله کنسول را بطور کامل خاموش کرده و از برق بکشید. سپس طبق توضیحاتی که در بخش اول داده شد کنسول را باز کرده و فلش مموری را از روی مادربرد کنسول جدا کنید. حالا فلش مموری را به قطعه Raspberry Pi وصل کنید. سپس فایل jaispi را دانلود و در مکان برنامه Putty که دانلود کرده بودید قرار دهید. حالا دستور زیر را وارد کنید تا یک دامپ از فلش مموری تهیه شود.

jaispi -r DUMP.bin /dev/spidev0.0

پس از انجام مراحل بالا، حالا دامپ شما از بازیهای فعال شده در اختیارتان می باشد. کنسول را دوباره بسته بندی کرده و وارد بخش Settings/PlayStation Network شوید. حالا گزینه Activate as Your Primary را انتخاب و سپس گزینه Deactivate را انتخاب کنید. حالا دوباره کنسول را باز کرده و فلش مموری موجود بر روی مادربرد را در قطعه Raspberry Pi قرار دهید و سپس دامپ را با استفاده از دستور زیر در فلش مموری قرار دهید.

jaispi -p Base.bin /dev/spidev0.0

اگر مراحل را درست پیش رفته باشید، هم اکنون بازیهای غیرفعال شده بر روی کنسول دوباره بر روی فلش مموری شما فعال شدند. فلش مموری را بر روی مادربرد بازگردانید و دوباره کنسول را بسته بندی کنید. دسترسی اینترنت را بطور کامل از روی کنسول خود قطع کنید و سپس کنسول را روشن کنید. حالا از بازیهای خود بصورت آفلاین لذت ببرید.

نکاتی درباره کنسول مادر:
فروشگاه ها و مغازه هایی که خدمات مرتبط با این آموزش را انجام می دهند، از یک کنسول مادر استفاده میکنند که دیگر نیازی به باز کردن چندین باره ی کنسول شما نخواهد بود. به همین دلیل اگر قصد دارید بصورت تنها و یا با دوست خود این عملیات را انجام دهید، استفاده از بازیهای ظرفیتی بهتر از باز کردن کنسول می باشد.
مزایای این روش :دسترسی به بازیها با هزینه ناچیز-قرار گرفتن بازیها بر روی حافظه کنسول و فعال ماندن بازیها برای همیشه (درصورت وصل نشدن به اینترنت)
معایب این روش: عدم امکان انجام بازیها بصورت آنلاین -باز شدن کنسول.

درباره آنلاین شدن بازیها به این روش: با استفاده از این روش بازیها را می توان تا مدتی بصورت آنلاین بازی کرد و حتی برخی بازیها نیز بصورت دائمی قابل بازی هستند. بهترین روش این است که با استفاده از یک User دیگر بازیها را بر روی کنسول قرار دهید و سپس با User خود آن ها را استفاده کنید و هرگز وارد User اصلی بازیها نشوید.
تهیه شده توسط کانال : @HACKGM