Testing and Research with BlackArch Linux

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

COMMENT?

It's the 24th of May as I write this, just two days prior to Memorial Day in the US. I am reminded, as Wallace Bruce states in his poem of the same name, "who kept the faith and fought the fight; the glory theirs, the duty ours." I also write this on the heels of the Department of Justice's indictment of five members of the Chinese People's Liberation Army, charging them with hacking and cyber theft. While I will not for a moment draw any discussion of cyber conflict together with Memorial Day, I will say that it is our obligation and duty as network defenders to understand offensive tactics to better prepare ourselves for continued digital conflicts. To that end we'll focus on BlackArch Linux,[1] "a lightweight expansion to Arch Linux[2] for penetration testers and security researchers." I was not familiar with Arch Linux prior to discovering BlackArch but found myself immediately intrigued by the declarations of its being lightweight, flexible, simple, and minimalist—worthy goals all. Add a powerful set of information security-related tools as seen in BlackArch Linux and you've got a top-notch distribution for your tool kit.

Likely, any *toolsmith* reader has heard of BackTrack, now Kali, and for good reason as it set the standard for pentesting distributions, but it's also refreshing to see other strong contenders emerge. BlackArch is distributed as an Arch Linux unofficial user repository, so you can install[3] it on top of an existing Arch Linux installation, where packages may be installed individually or by specific categories. There is also a live ISO, which I utilized to create a BlackArch virtual machine. Arch Linux, while independently developed, is very UNIX-like and draws inspiration from the likes of Slackware and BSD.

According to Evan Teitelman, the founder and one of the primary developers, BlackArch started out as ArchTrack, a small collection of PKGBUILD files mostly collected from the Arch User Repository (AUR) for his own personal use. PKGBUILDs are Arch Linux package build description files (a shell script) used when creating packages. At some point, Evan created a few metapackages and uploaded them to the AUR; these metapackages allowed people to install packages by category with AUR helpers. He also created an unofficial user repository but only a few people used it. About six months after ArchTrack began, Evan merged with a smaller project called BlackArch, which consisted of about 40 PKGBUILD files at the time, while ArchTrack had about 160. The team ultimately decided to use the BlackArch name as it was more favorable and also came with a website and a twitter handle.[4] The team abandoned the AUR metapackages and put their focus on the unofficial user repository. Over time, they picked up a few more contributors and the original BlackArch contributor left the project to focus elsewhere. Around the same time, noptrix[5] joined the group who redesigned the website, created the live ISO, and brought in many new packages. Elken[6] and nrz[7] also joined the team and are currently two of the most active members. There are currently about 1200 packages in the BlackArch repository. The team's goal is to provide as many packages as possible and see no reason to limit the size of the repository but are considering trimming down the ISO.

If you would like to contribute or report a bug, contact the BlackArch team[8] or send a pull request via Github.[9] Evan describes the team as one with little structure and no formal leader or rank; it's just a group of friends working together who welcome you to join them.

Quick configuration pointers

When booting the ISO in VMWare, I found making a few tweaks essential. The default display size is 800x600 and can be changed to 1440x900, or your preferred resolution, with the following:

```
xrandr --output Virtual1 --mode 1440x900
```

BlackArch configures the network interface via DHCP; if you wish to assign a static address, right-click on the desktop, choose *network*, then *wicd-gtk*.

System updates and package installations are handled via pacman.[10] To sync repositories and upgrade out-of-date packages, use `pacman -Syyu`. To install individual packages, use `pacman –S <package>`.

1 http://blackarch.org/about.html.
2 https://wiki.archlinux.org/.
3 http://blackarch.org/download.html.
4 https://twitter.com/blackarchlinux.
5 https://twitter.com/noptrix.
6 https://twitter.com/elken__.
7 https://twitter.com/nrzizrn.
8 http://blackarch.org/contact.html.
9 https://github.com/blackarch/blackarch.
10 http://michael.otacoo.com/manuals/arch-linux/packaging/pacman/.

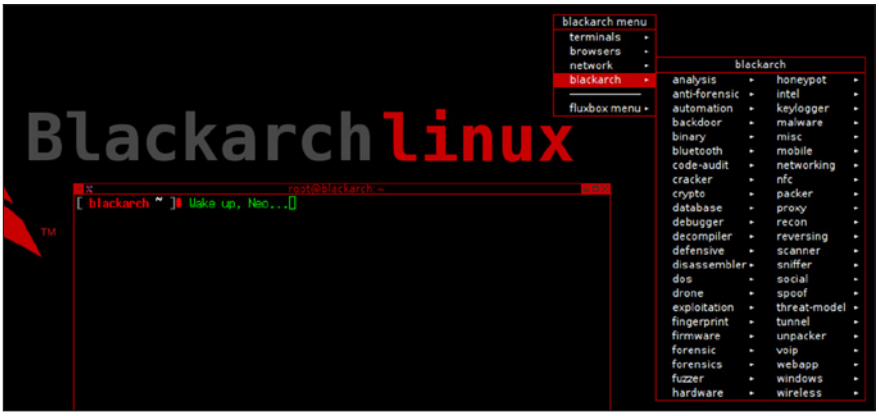

Figure 1 – Down the rabbit hole with BlackArch

Using BlackArch Linux

BlackArch exemplifies ease of use, as intended. Right-click anywhere on the desktop and the menu is immediately presented. Under *terminals* I prefer the green xterm as I am in fact writing this from the Nebuchadnezzar while flying through the tunnels under the megacities that existed before the Man–Machine war. ☺ "You take the blue pill – the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill – you stay in Wonderland, and I show you how deep the rabbit hole goes." Sorry, unavoidable *Matrix* digression. Anyway, you've got Firefox and Opera under *browsers*, and we've already discussed using *network* to define settings. It's under the *blackarch* menu that the magic begins on your journey down the rabbit hole as seen in figure 1.

Pick your poison; what are you in the mood for? The options are clearly many. I was surprised to see Gremwell's MagicTree[11] under the threat modeling menu, having just discussed threat modeling last month. While not quite classic threat modeling, MagicTree allows penetration testers to organize and query nmap and Nessus data, list all findings by severity (prioritize for ordered mitigation), and generate reports. This activity most assuredly supports both good threat models and penetration testing reporting, the bane of the pentester's existence. I was even more amused, given our emerging theme for this month, to note that MagicTree includes a Matrix view.

Malware analysts will enjoy an entire section dedicated to their cause under the *malware* menu, including cuckoo and malwaredetect (checks Virustotal results from the command line) as seen in figure 2. I downloaded a Blackhole payload (Zbot password stealer) from my malware repository and ran `malwaredetect updateflashplayer.exe`.

The forensic options are vast and include your regular odds-on favorites such as Maltego and Volatility as well as hash computation tools such as hashdeep, md5deep, tigerdeep, whirlpooldeep, etc. Tools for the EnCase EWF format are included such as ewfacquire, ewfdebug, ewfexport, ewfinfo, and others. Snort fans will enjoy the inclusion of u2spewfoo, which I mention purely for the pleasure of the rolling assonance of the tool name. For forensicators investigating Windows systems with Access databases, you can utilize the MDB Tools[12] kit included in BlackArch. To acquire schema, execute `mdb-schema access.mdb`; to determine the Access version, run `mdb-ver access.mdb`; to dump tables, try `mdb-tables access.mdb`; and if you wish to export that table to CSV, use `mdb-export access.mdb table > table.txt, all` as seen in figure 3.

While threat modeling, malware analysis, and Access forensics may be interesting to some or many of you, most anyone interested in BlackArch Linux is probably interested in the

11 http://www.gremwell.com/using_magictree_quick_intro.

12 http://mdbtools.sourceforge.net/.

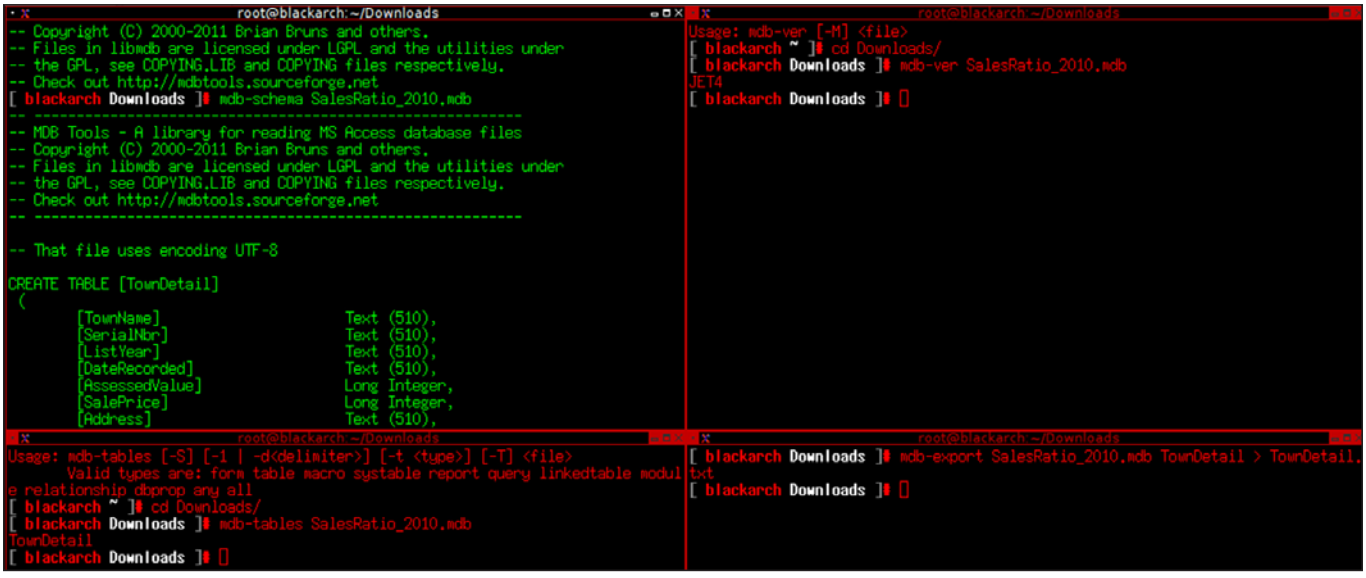

Figure 2 – malwaredetect identifies malware

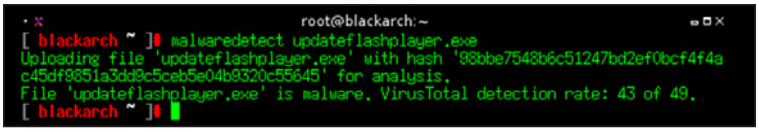

Figure 3 – Carving up access DBs with MDB Tools

pwn. "Show us some exploit tools already!" Gotcha, will do. In addition to the Metasploit framework you'll find Inguma, the killerbee ZigBee tools, shellnoob—a shellcode writing toolkit, as well as a plethora of other options.

Under the *cracker* menu you'll find the likes of mysql_login, useful in bruteforcing MySQL connections. As seen in figure 4 the syntax is simple enough. I tested against one of my servers with `mysql_login host=192.168.43.147 user=root password=password`, which of course failed. You can utilize dictionary lists for usernames and passwords and define parameters to ignore messages as well.

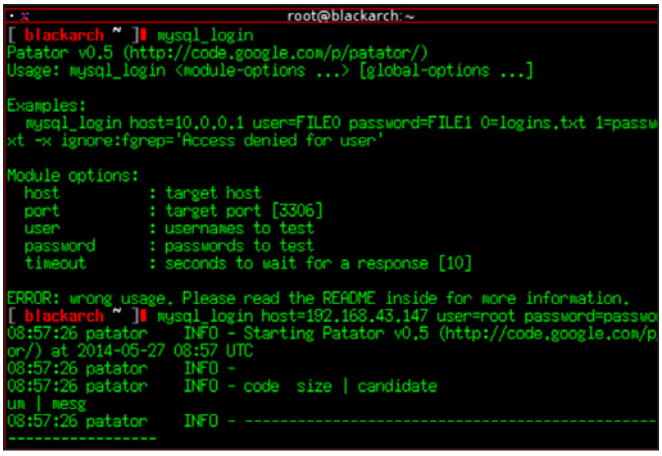

Figure 4 – Bruteforcing MySQL connections

In fact, BlackArch includes the whole patator[13] toolkit—the multi-purpose brute-forcer—with a modular design and a flexible usage, and login brute-forcers for MS-SQL, Oracle, Postgres, as well as other non-database options too as seen in figure 5.

Figure 5 – Patator

13 https://code.google.com/p/patator/.

For your next penetration testing engagement, you definitely want BlackArch Linux in your toolbag. For that matter, incident response and forensics personnel should carry it as well as it is useful across the whole spectrum.

In conclusion

This is one of those "too many tools, not enough time" scenarios. You can and should spend hours leveraging BlackArch across any one of your preferred information security disciplines. Jump in and help the project out if so inclined, and keep an eye on the website and Twitter feed for updates and information.

Ping me via email if you have questions or suggestions for topic via russ at holisticinfosec dot org or hit me on Twitter @holisticinfosec.

Cheers…until next month.

About the Author

Russ McRee manages the Threat Intelligence & Engineering team for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.