|  |  |
| --- | --- |
|  | LunaUSB Security Tester  GNU General Public licensed security utility  Demonstrate the speed and ease that a password may be exfiltrated when a secure logon policy is not in place. Easy setup and run, established framework, and extendible.  saintcrossbow@gmail.com |

What is it?

Luna is a security utility to demonstrate a significant weak link: the unlocked workstation. An unsecured workstation does not just leave your data vulnerable, but allows other attack vectors such as installing malware or using false logins to acquire a password. The Sony attack was likely just that: an effort to steal credentials using unlocked PCs via physical access. Stealing a password effectively and undetectably is much more damaging: its theft may not be discovered, and a single password often provides access to many other assets within a network other than just the PC.

Existing pen-test software will provide a payload to manipulate the workstation, but Luna focuses on one primary thing – exfiltrate the password quickly and disappear quickly. Once complete, the attack is not discovered: there are no tracks left on the PC, and no evidence of anything unusual. .With LunaUSB you can make a convincing and memorable demonstration of how a password can be obtained and the potential damage an unlocked PC would do.

Why would I use it?

To demonstrate a security issue that is really easy to solve. Workstations have been left unlocked for ages, and people really don’t know the damage that could be wrought. This allows you to demonstrate that either as a security manager or tester.

How do I counter it?

Very easily and cheaply:

1. Set a policy to enable Ctrl-Alt-Delete logons.
2. Set screen savers to lock after *n* minutes.

So how does it work?

LunaUSB uses two basic things: *curtains*, which are mocked up screens that prompt for a logon; and *exfiltration methods*, which provide the password to the tester in all sorts of ways.

Why would you even create something like this?

I’ve wanted to find a white-hat demonstration of this attack. The Kautilya attack via the Teensy USB was promising but not quite the item I had in mind. So I created it myself, and then decided it might be useful to the rest of the world as well.

Could I be used for evil?

Sure, but shame on those that do that for two reasons: 1) obviously it’s unethical; and 2) there are more devious tools out there than LunaUSB that can actually cause significant damage. LunaUSB is nice to the workstation, I sort of doubt the others are.

How do I run it?

* Starting Luna directly will place it in a setup mode and will guide you through creating an attack vector: creating the curtain you want, the method of exfiltration, and copy it to a USB as a randomized file name.
* Luna can also be started with all curtains and methods through the command line.
* Luna also offers additional utility functions through the command line such as decrypting an exfiltrated password or running a PowerShell script in the background.

How do I customize it for my testing?

LunaUSB was written in C# and was designed to be extended. The curtains and exfiltration methods use a common interface. If you need a new screen or exfiltration, just add a new class that matches that interface. As of this writing, the main form is still tightly coupled to the classes to write graphics, but that shouldn’t too big of a deal for creating new screens. The methods that are taken upon LunaUSB launch are also customizable using delegates.

The code has been documented clearly to show what it is doing and why it is doing it. If you are new to C#, links are included where appropriate, and there are good examples on how to use some C# concepts that some might consider difficult.

Can you add *x* feature or answer *y* question?

The answer is probably yes, but I have done this in my spare time when I am not working, not being a parent, and not having fun in other areas. Email [saintcrossbow@gmail.com](mailto:saintcrossbow@gmail.com) or follow the project on <https://github.com/saintcrossbow/LunaUSB/>.

What’s up with the name SaintCrossbow?

Most of it is because it wasn’t taken. Other than that, I’m a big fan of the literary Saint by Leslie Charteris: a vigilante type who very kindly takes on problem people, serves his own justice, and has a great deal of fun doing it. Also, I just can’t help but think that crossbows are cool.