Kautilya: Teensy beyond shells

Kautilya Toolkit for Teensy device

Nikhil Mittal

Contents

Abstract

As hackers, we have been exploiting the inherent trust by Operating System on Human Interface Devices for some time now. Teensy is a USB Micro-controller; a device which can act as a Human Interface Device when connected to a computer and is able to do the job pre-programmed in it.

Many interesting things have been done using Teensy as a keyboard. We have mostly seen shells, many types of them. It is time we start looking at Teensy as a pentesting device capable of doing much more than popping shells. Introducing Kautilya, a toolkit which can be used to perform various pre-exploitation and post-exploitation activities. Kautilya aims on easing the use of attack vectors which traditionally require human intervention but can be automated using Teensy. Kautilya contains some nice customizable payloads which may be used for enumeration, info gathering, disabling countermeasures, keylogging and using Operating System against itself for much more.

Attack Surface and Scenarios

Talking about the attack surface, during the usage of Teensy during live penetration tests and also during the development of Kautilya the author never came across any countermeasure software which blocks it or a user environment where USB port is disabled. Note that it works even if USB Mass Storage is disabled. So the attack surface turns out to be quite large and that too unprotected.

Usage of teensy device can broadly in many scenarios; two most likely (obviously) are Internal Penetration Tests and External Penetration Tests. In the first scenario, you can wait for someone to leave a system unlocked for few seconds or leave it on someone's desk disguised in a thumb drive or USB toy etc. In the second scenario, the usage is quite similar and you need some simple Social Engineering skills to get someone to plug this in his computer. Teensy can again be disguised as a thumb drive, USB toy or mouse etc and can be left in parking lot, reception area etc.

Current Usage

Currently, nice attack vectors using Teensy are implemented in the Social Engineering Toolkit (SET)[1]. The attack vectors in SET as of this writing are almost all for "popping" shells. You cannot do a variety of pre and post exploitation things with that. The author believes that Teensy should be used for much more, some nice suggestions and implementations can be found in the Hak5 Rubber Ducky Forums[2].

Kautilya

Usage of Teensy can be expanded beyond shells and this is the point of the paper and to some extent Kautilya. Kautilya is a toolkit which aims to make Teensy a complete penetration test tool. It is written in ruby and is a menu driven program. A user can choose options from menu and is asked some questions to create a customizable payload.

In Kautilya, you have pre and post exploitation payloads which come in handy during a penetration test. The payloads are combination of OS commands, built-in tools and powershell/bash script or mixture of commands and scripts. Let's have a look at some of them.

Keylogger

The keylogger is written entirely in powershell. Teensy is used to type the powershell script on the victim machine. All keys and mouse-clicks are logged and uploaded every twenty seconds by default to pastebin as a private paste. There is a separate powershell script to parse the uploaded keys.

Uninstall MSIExec compatible application

This payload allows you to silently remove any MSIExec compatible application (many AVs are MSIExec compatible)[3]. You have to give name of the application and it will remove the application. This too is written in powershell. There is another payload under development for using WMI for un-installation.

Information Gather

This payload uses a powershell script to extract useful registry keys and other information from a victim machine and paste it to pastebin as a private paste. The registry keys are mostly taken from Metasploit's[4] meterpreter scripts. Of course, the registry keys accessible depend upon the privileges of current user.

Download and Execute

This payload is written in powershell. It can either download and execute an executable from google docs or byte converted exe can be downloaded in form of text from pastebin or google docs, the text will then be converted back into exe and is executed. File format exploits have also been tested with this module, as long as file format can be converted to text or can be downloaded directly from google docs, this works. Although, file format exploits are not currently implemented in Kautilya.

MSF Modules

Currently, two modules from metasploit have been used, namely, enable telnet and enable rdp. Both modules (as in msf too) add a user, enable the requested service and add an exception too windows firewall. More useful modules will be added in future.

Network Sniffer

A network sniffer in powershell, based upon get-packet script by Robbie Foust[5]. The sniffed data is uploaded to a ftp server. This payload leaves a lot to be improved as

Breaking Browser Security

This is a class of payloads actually. One payload runs Chrome's Remoting Plugin ((plugin should be installed already) and copies the access code to pastebin as a private paste. Other one disables NoScript in firefox. Both they payloads are in "visible" category, that is, they do NOT operate from command line and works on the browser windows. This makes them noisy and easy interruptible, but is useful if used correctly.

Sethc and Utilman “backdoor”

This payload uses registry tweaks to launch user defined executable in place of sethc.exe (called when SHIFT keys is pressed five times) and utilman.exe. This payload if executed successfully provides a execution with system privileges on a locked machine, when the correct key combination is pressed.

Hashdump

This payload uses powerdump script from metasploit to dump password hashes from the victim. The script is executed as a task to run it under system privileges. The hashes are then uploaded to pastebin as a private paste.

Wireless Rogue AP

This payload utilizes Windows wireless hosted network functionality popularized by this video at Securitytube[6] . This payload creates a wireless hosted network on a target machine with user defined SSID and network key.

Other Windows Payload

Some other payloads are, forceful browsing, change default dns, edit hosts file, add a user and Tweet some text.

Linux built-in Reverse Shells

Implementation of few reverse shells as defined here[7].

Other Linux Payloads

Some other payloads for Linux are edit host file, change nameserver, add user, turn off ASLR and turning off iptables. Many payloads for Linux are tested but are not included in Teensy as, most of them need root permissions and generally desktops are based on windows.

Other than payloads, Kautilya implements some stealth measures which include obscured command prompt while typing, clearing some registry keys and cleaning up dropped files after usage.

Limitations

Teensy cannot read back from a system as of now. This is one major limitation while writing payloads for Teensy as it makes payloads less responsive to the state of a system. You have to pre-define possible situations for a payload as it is not possible to read response from the system at runtime. This is however somewhat curbed when you use powerful scripting languages like powershell and bash. Another limitation is the small default storage available with teensy, however some recent works [8] have successfully attached and utilized a SD card with teensy.

Kautilya has its own limitations. For example, right now if you want to use payloads generated by metasploit, say for download and exec you have to generate them separately and post them at google docs or pastebin. The URL can then be provided at Kautilya command menu. Some payloads are not stealthy and may alert a watchful user. There may also be limitations in the efficiency and effectiveness of coding limited by author’s knowledge of different Operating Systems.

Also, all the payloads have been designed for a teensy without additional storage. This is done so that a user completely unaware of how to attach a SD card to teensy can start using Kautilya straightaway.

Future and TODO

You may see more payloads for Linux in Kautilya as in Linux you can do everything from command line and that makes it more prone to attack vectors such as teensy. Also, Kautilya which right now is a toolkit will be developed in a framework aiding in code reuse and will provide modules as libraries[9] to make payload development easier. Also, better and uniform coding standards, support for non-english keyboards, payloads for Mac OS X may be implemented. Current payloads will be definitely improved after feedback from community.

Conclusion

Kautilya tries to bring teensy to more hackers, penetration testers and security administrators. It provides some easy to use customizable payloads useful in security testing and penetration tests. We had a look at the payloads and their functionality. We also had a look at the limitations of Kautilya nd the future work. In coming time, much more can be done using Kautilya and the author expects to take feature requests and feedbacks from the community. Kautilya is at nascent stage right now but it aims to become an indispensible part of a Penetration Tester’s toolchest.

“Once you start working on something, don't be afraid of failure and don't abandon it. People who work sincerely are the happiest.” – Kautilya a.k.a Chanakya (370BC – 283BC)

References

[1] http://www.secmaniac.com/
[2] http://forums.hak5.org/index.php?showforum=56
[3] http://www.room362.com/blog/2010/11/16/silently-uninstall-sep.html
[4] http://www.metasploit.com
[5] http://blog.robbiefoust.com/?p=9
[6] http://www.securitytube.net/video/2272
[7] http://lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/
[8] Using the Teensy for so much more... David Kennedy & Josh Kelley, BSides LasVegas
[9] PHUKD. http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle