Hardware Kit for Infrastructure Assessments

pentestlab.blog/category/general-lab-notes/page/3

November 2, 2016

Except of the dedicated testing laptop and a variety of tools and scripts, penetration testers should have some additional hardware kit to support the engagement with common issues that might happen during onsite visits. It is always a good practise to plan ahead before the problem knocks on the door. The following kit is recommended for every penetration tester.

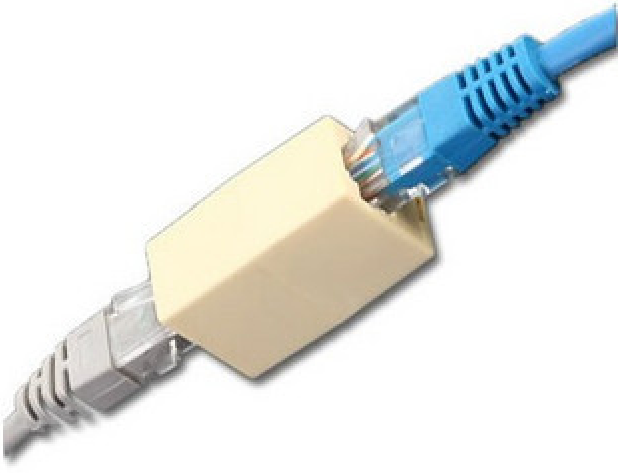
USB Ethernet Switch

There are situations where there are limited network ports and many penetration testers. Usually this problem is solved before penetration testers arrive onsite since scoping documents include this as a client requirement. However penetration testers they might seat in a conference room where there are not enough ports for all them or they can share the same desk in order to collaborate better during the engagement. A 4 port USB Ethernet switch can solve this problem.

USB Ethernet Switch

Ethernet Cable Connector

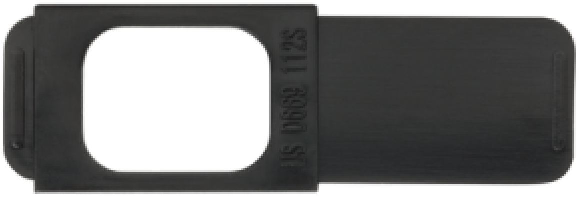
Due to the location of the Ethernet cable at client site sometimes the laptop Ethernet port is not reachable. Therefore the Ethernet cable connector can extend the length of the cable and resolve this minor issue.



Ethernet Cable Connector

Camera Protector

Some restricted locations especially Data-Centres have a policy which forbids cameras so before going onsite the laptop camera should be disabled and covered with a camera protector.



Web Cam Protector

USB Drives

It is often needed to transfer evidence files from the client systems to your laptop for reporting purposes or to share something to other consultants that are on site. Additionally as a safety net binaries of some tools like Nessus, Burp can be stored if the tools fail to run.

USB Flash Drives

Live CD's

It can be handy to have some live operating systems to perform various tasks. For example it is always nice to have a Kali Linux Live cd in case the main operating system fails or KonBoot to bypass the windows authentication mechanism.

It is recommended to carry the following live operating systems:

Backup Hard Disk

Hard disks can fail anytime and usually at the most inconvenient times. To avoid disruption of the penetration testing engagement it is wise to carry a clone disk of the existing operating system to be up and running again.

Wireless Adapter

For wireless assessments that require to crack the wireless key a card that support packet injection is necessary. Alfa USB adapters are recommended.

Alfa USB Wifi Card

USB Ethernet Card

This is handy for situations that VLAN hopping is part of the test and the existing Ethernet card doesn't support VLAN tagging.

USB Ethernet Card

Computer IEC Universal Travel Adapter AC Power Plug

This adapter could be used in Data-Centres which doesn't support thirteen amp sockets. Also when there are not enough power sockets the IEC lead at the back of the desktop monitor could be used as an alternative power resource.

IEC Adapter

Screwdrivers

In the scenario that the hard disk needs to be removed from the laptop due to a client requirement or because the hard disk has failed and it needs to be replaced while on site.

Screwdrivers

Ethernet Cable

Sometimes the RJ45 jack can be broken so stable connectivity can be an issue. Additionally in Data-Centres that it is necessary to connect with a switch but no cables are provided.

Ethernet Cable