

DATA LEAKAGE PROTECTION WORKAROUND



DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.



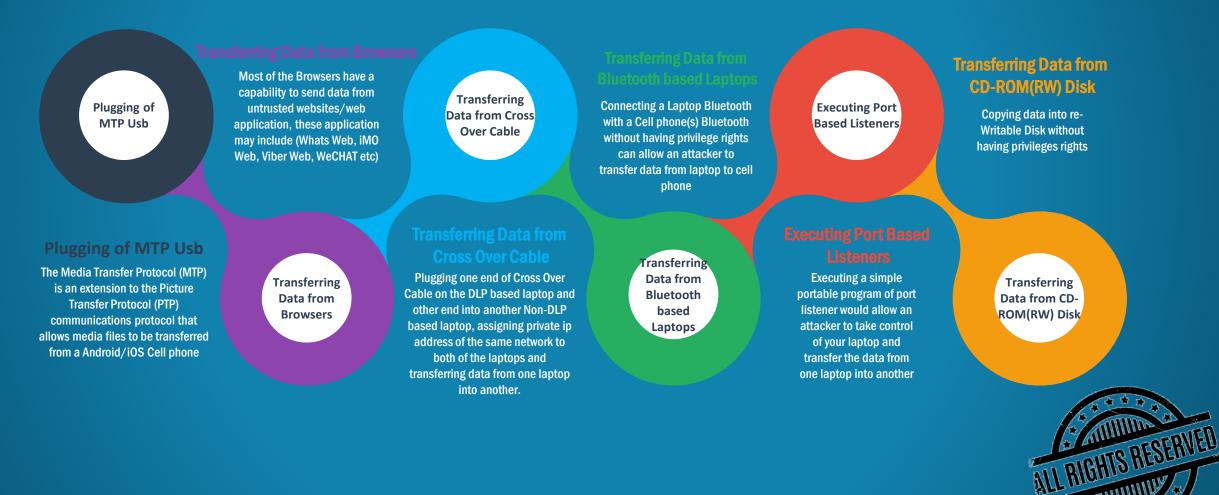


DATA LEAKAGE PREVENTION SECURITY ASSESSMENT CHECKLIST





DATA LEAKAGE PROTECTION WORKAROUND





DATA LEAKAGE PROTECTION WORKAROUND (CONT'D)

Absence of Bios Password

Absence of Bios Password

The Bios access feature allow

an attacker to change the Boot

options, Assign the System

password, in order to gain

unauthorized access by using

bootable USB disk

in Client Premises

Plugging the Personal laptop defines how a client monitored personal laptops of their employees, moreover what security controls are implemented on client premises

Web Based and Portable Client Agent Data Transfer Software

Web Based and Portable Client Agent Data Transfer

Software

Portable Software such as (Share iT, Mega, Drop Box, FilesFm, Tinyupload) etc. and web based portals(Files.fm uploadfiles.io, Zshare) etc. allow an intruder to upload the data form a DLP based system to the cloud network

Free Email Serv

Free email server (Zoho, light, freewebhost000, etc.) accessible to DLP based which allows an attacker to send files/Folder to the free email server

Transferring

File to Free

Email Servers

Ensuring Services are running on ETHERNET & WIRELESS Network

Enabling Port based Client/Server

Running portable Application of Server/Client on two machines and allowing an application to send data on different ports using Windows based environment

insuring Services are running on ETHERNET & WIRELESS

Network

Ensuring the services which are blocked on Ethernet network must also be block on Wireless Network. Since a malicious user can connect the wireless network and bypass the policies which are applied on the Ethernet Network. Enabling Port based Client/Server



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Plugging Unregistered Laptop in Client Premises



DATA LEAKAGE PROTECTION WORKAROUND (CONT'D)

Ensure the File Extension (.exe, .bat, .msi, .msc, .iso) should not Copy

Ensure the File Extension (.exe, .bat, .msi, .msc, .iso) should not Copy

Copying of files from USB, Mobile Phone, SD Card into system can be easily done by only renaming the file extensions and drag drop it to the system ccessing Blocked Application(s)

Ensuring that the applications that are blocked on the network could be accessible by simply renaming the application name For Example Firefox.exe to Fox.exe , Chrome.exe to google.exe

> Accessing Blocked Application(s)

Device Broadcast

Device Broadcast

Plugging and broadcasting a network node using portable routers, switches. Connecting and hiding the identify of the devices by using different IP Addresses on the devices

d-Hoc Web Based Serve

On a DLP Enabled machine, a cross over connection having the same subnet address could allow an unauthorized/illegitimate user to published files/Folders by creating their own web server and accessing through the URL of DLP enabled machine

Ad-Hoc Web

Based Server

Standalone Web Based Server

Bypassing User Account Control (UAC) on Windows Based Environment

By Enabling Invoker methods in windows based operating system an attacker or malicious user can install unnecessary application/software on a DLP Enabled machine

Standalone Web Based Serve

using the IP address and MAC Address of a known DLP Enabled machine. An attack or malicious user could build their own web server and could also published files and can also publish pages that could upload files from other DLP enabled machines

Bypassing User Account Control (UAC) on Windows Based Environment



DATA LEAKAGE PROTECTION WORKAROUND (CONT'D)

Remotely accessing Ethernet switch through mobile device booted on UNIX/LINUX connected to Ethernet port on the switch

Organizations put restriction on bringing in unauthorized laptops and/or tablets to their premises. Improperly configured physical ports allows the unauthorized android based mobile phones to be attached with Ethernet port using a portable USB to LAN card converter. This allows the mobile phone to get connected to physical Local Area Network and ping the available resources on network if it is not been disabled. If intelligent intruder have allowed the remote connection to this device and have 3g or 4g network enabled then significant issues can be encountered by the targeted organization and its information resources. Remotely accessing Ethernet switch through mobile device booted on UNIX/LINUX connected to Ethernet port on the switch



Ubaid



THANK YOU