



VIT[®]

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Analysis and Audit

Course Code: CSE3501

Slot: L47-48

Faculty: Dr. Anil Kumar K

Assessment: 4

18BCI0247

Rohan Allen

Exercise 1:

Experiments in E-Matrix Power Spy software.

The Best PC Spy Software Downl... x +

ematrixsoft.com/index.php

eMatrixSoft 24x7 Ordering & Technical Support

HOME PRODUCTS PURCHASE SUPPORT KNOWLEDGE

Power Spy - The best internet & PC activity surveillance software!

Perfect for monitoring employees, protecting kids and catching a cheating spouse!

Monitor employees in the office

Windows 10
XP/Vista/7/8/Server

Power Spy software is a Windows PC user activity monitoring software. It lets you know EXACTLY what others do on your desktop, laptop and tablet PC while you are away. It secretly monitors and records all activities on your computer. Such monitoring acts so stealthily that the user won't know its existence.

Power Spy software records all Facebook use, keystrokes, emails, web sites visited, online searches, chats

Power Spy 2014

Fichier Accueil Partage Affichage Outils d'application Gestion

Épingler dans Accès rapide Copier Coller Couper Copier le chemin d'accès Coller le raccourci Presse-papiers Déplacer vers Copier vers Supprimer Renommer Nouveau dossier Accès rapide Nouveau Ouvrir Modifier Historique Sélectionner tout Sélectionner

Logi > CEHv9 Module 05 System Hacking > Spyware > General Spyware > Power Spy 2014 Rechercher dans : Power Spy ...

Nom	Modifié le	Type	Taille
pcspy14	18/09/2014 08:39	Application	3 688 Ko

Accès rapide

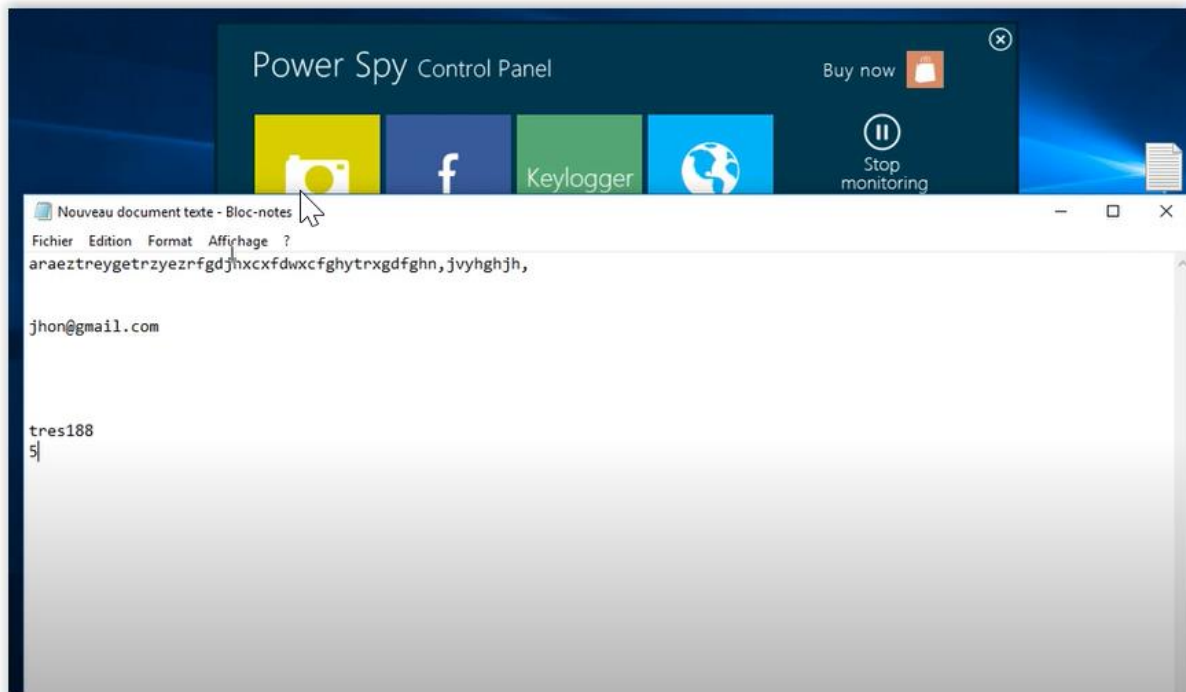
- Module 5 System
- Bureau
- Téléchargement
- Documents
- Images
- CEH v9 Labs
- Logi
- Musique
- Song
- OneDrive
- Ce PC
- Réseau



Start monitoring



Make text document:



Open keylogger:



The screenshot shows a web application window titled "Log View - Websites Visited (3 records)". On the left side, there are two panels. The top panel, "Logged Users:", lists "Mathy". The bottom panel, "Log Types:", lists various categories like Screenshots, Keystrokes, Applications, Websites Visited (which is highlighted), Yahoo Messenger, Skype, Documents, Clipboard, Administrator, and Microphone. The main area of the window contains a table with three columns: Timestamp, User Name, and Website URL. It displays three records of website visits by the user "Mathy".

Timestamp	User Name	Website URL
15/05/2017 10:39:45	Mathy	https://www.offensive-security.com/blog/
15/05/2017 10:39:44	Mathy	https://www.google.fr/?gws_rd=ssl#q=offensive+security
15/05/2017 10:39:28	Mathy	https://www.google.fr/?gws_rd=ssl

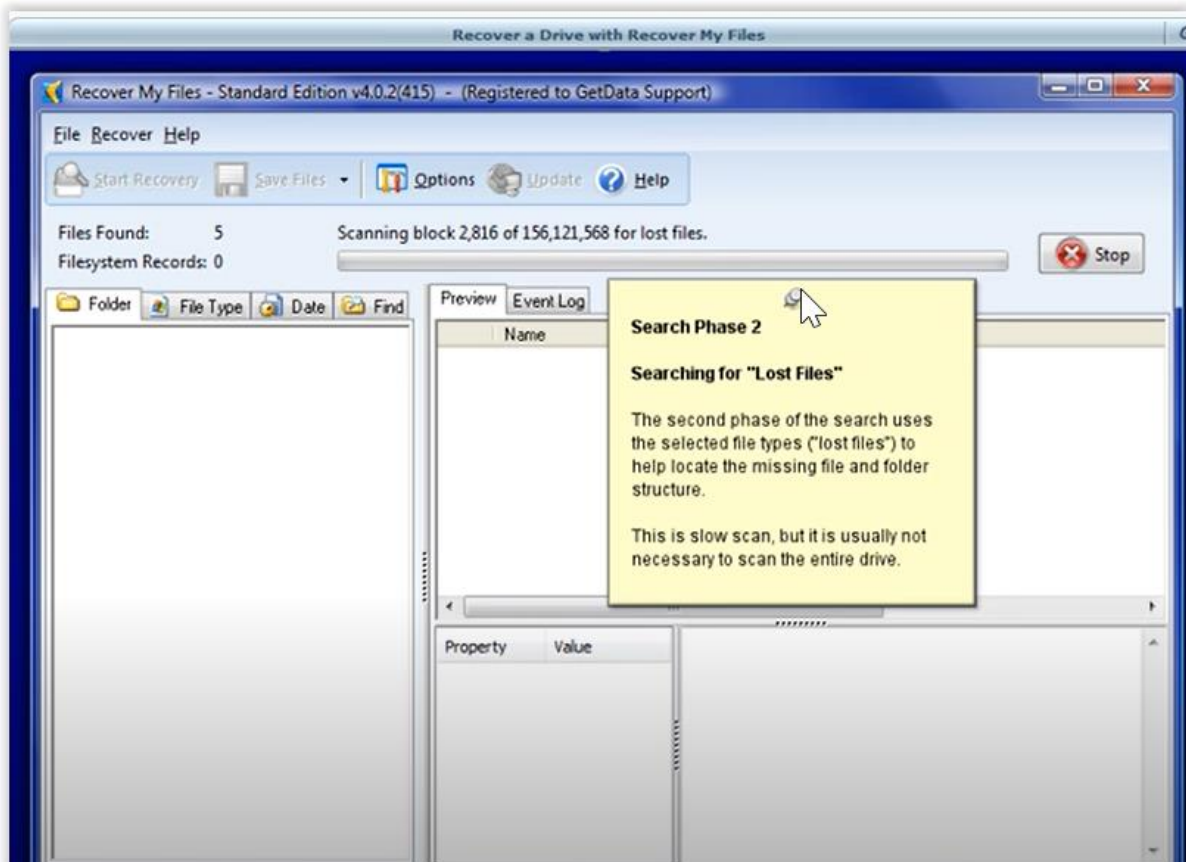
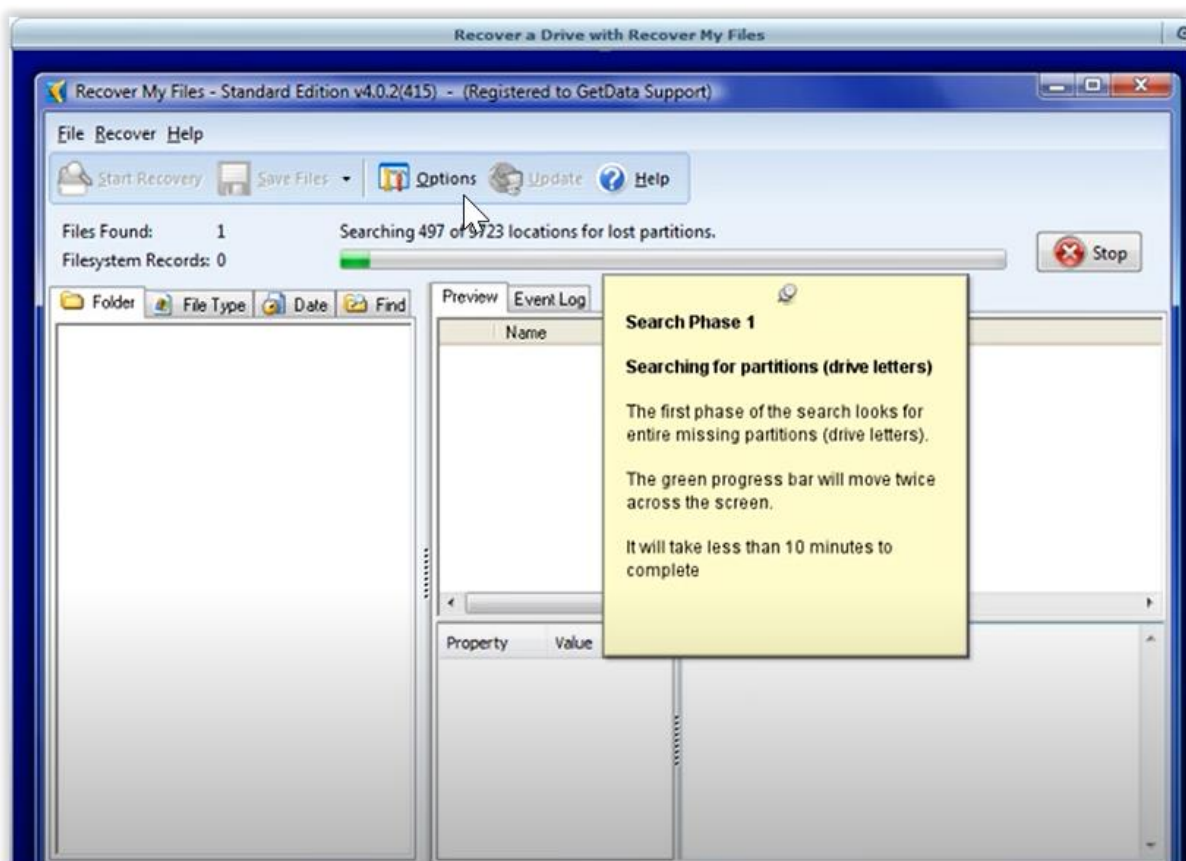
Exercise 2:

Experiments in Recover my File software.

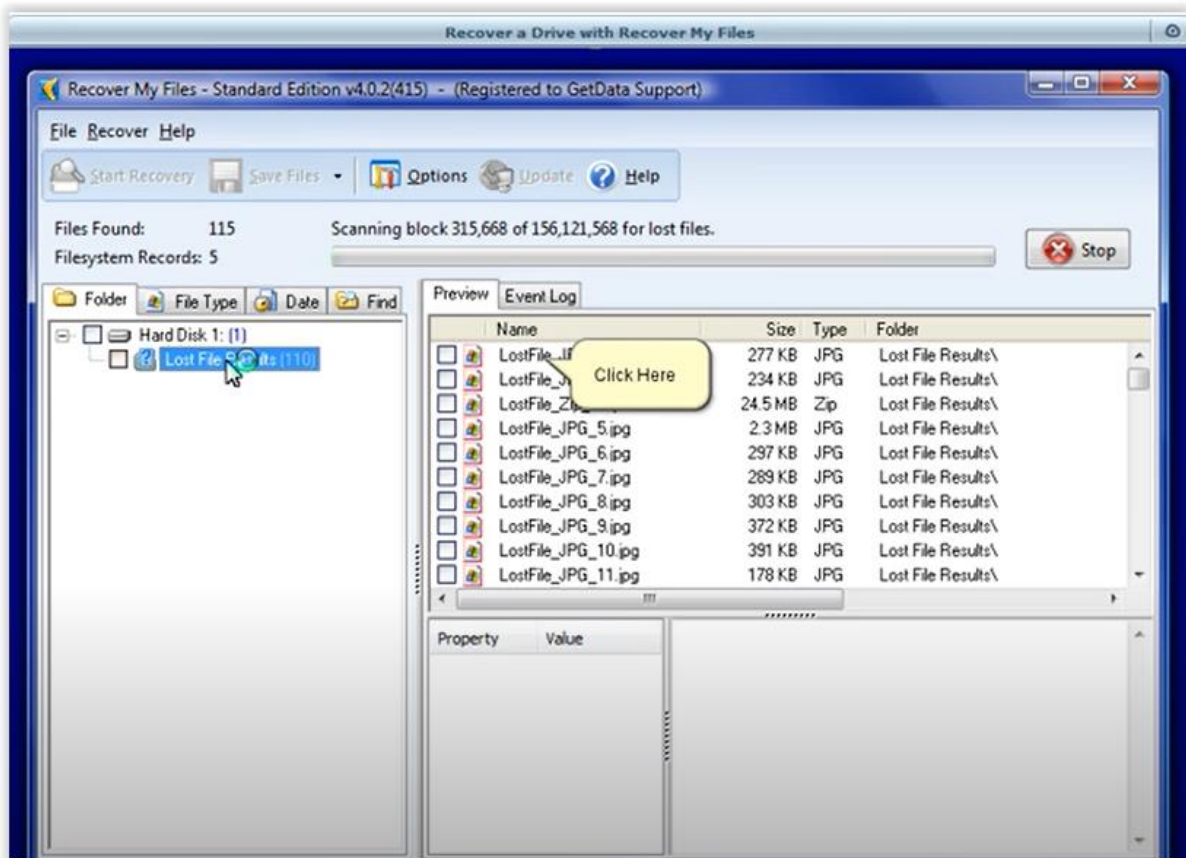


Select hard-disk

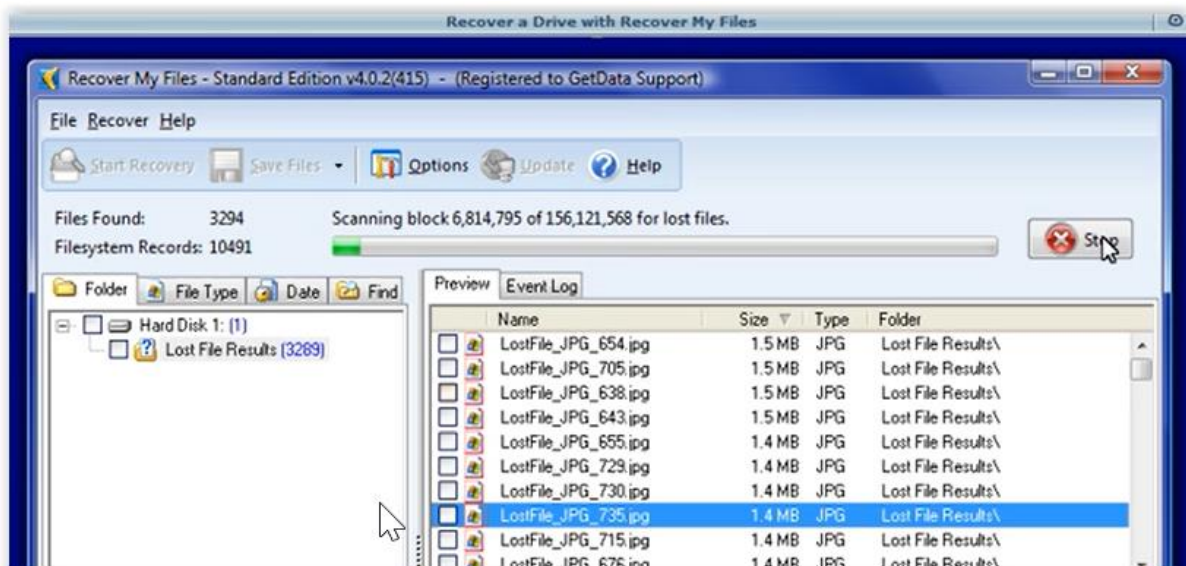




Displaying Lost files:



Stopping search for lost files:



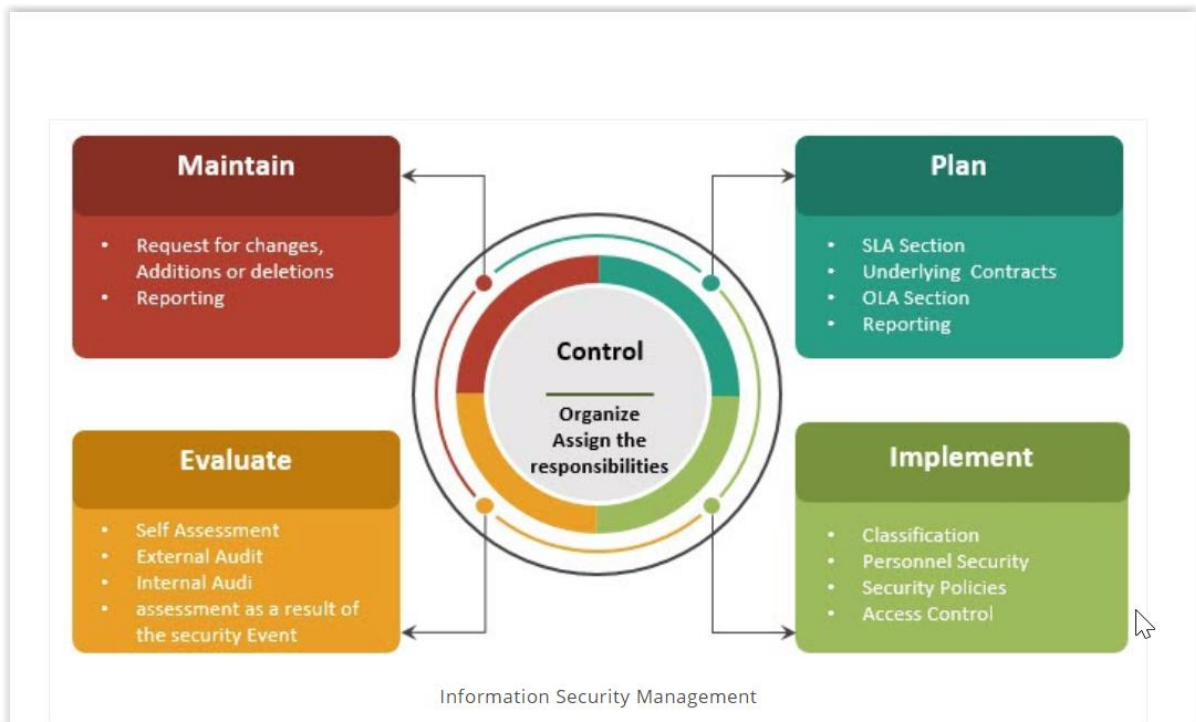
Exercise 3:

Find the few Security templates from ITIL & ISO.

ITIL:

Download ITIL All Templates

Types of Risks	Internal Risks	External Risks
Strategic	Research & Development	Competition and Customer Needs and Demands
Operational	Systems & Processes (HR & Payroll)	Suppliers, Regulations & Contracts
Financial	Cash flows & Liquidity	Credit
Hazard	Equipment, Process, People, Safety & Security	Natural disasters, cybercrimes, and criminal acts
Compliance	The organizational system, legal and regulatory policies. Confidential information technical and physical controls.	New policies and regulations are introduced, existing policies are changed, and the organization may be at risk due to non-compliance if monitoring is not done regularly.



IT Security Management:

As companies have entered the digital era and are digitalizing, more and more companies are vulnerable to cyber-attacks. Cybercrime supervision is not an easy approach. It should be monitored 24 hours a day. Businesses are of different sizes with varied needs, risks, and threats. Government agencies and companies have been practicing and managing security risks to reduce their likelihood of falling victim to cyber-attacks. IT Security Management which adheres to follow some recommendations and regulations to protect against cybercrimes they are:

1.Enforce digital and physical security methodologies:

The use of anti-malware solutions like firewalls, antivirus, network and server control, and other forms of physical and digital security measures should be enforced against cybercrimes.

2.Secure and update asset and patches :

Supervising involves maintaining the company's assets like hardware, software, and digital assets to keep up to date through proper IT Security Management. Hackers hack through security gaps that prevail due to outdated or unpatched IT infrastructure and software. It is the responsibility of the company to secure and maintain up-to-date inventory, hardware, software, data, and security certificates so that you are aware of the networks, servers, and other IT systems components. Maintaining up-to-date information helps you informed about the assets and also helps you with the vital information on your fingertips so that you're not searching for the information whenever

of cybersecurity events that takes place

ISO:

ISO 27001 CONTROLS CHECKLIST TEMPLATE				
SECTION/ CATEGORY	REQUIREMENT/TASK	ASSIGNED TO	IN COMPLIANCE?	DATE LAST UPDATED
5. Information Security Policies				
5.1	Security policies exist.		<input type="checkbox"/>	
5.2	All policies approved by management.		<input type="checkbox"/>	
5.3	Evidence of compliance.		<input type="checkbox"/>	
6. Organization of Information security				
6.1	Roles and responsibilities defined.		<input type="checkbox"/>	
6.2	Segregation of duties defined.		<input type="checkbox"/>	
6.3	Verification body / authority contacted for compliance verification.		<input type="checkbox"/>	
6.4	Establish contact with special interest groups regarding compliance.		<input type="checkbox"/>	
6.5	Evidence of information security in project management.		<input type="checkbox"/>	
6.6	Defined policy for mobile devices.		<input type="checkbox"/>	
6.7	Defined policy for working remotely.		<input type="checkbox"/>	

ISO 27001 Risk Assessment Template

ISO 27001 RISK ASSESSMENT TEMPLATE

COMPANY NAME

CONTROL	ISO 27001 CONTROL REFERENCE	ASSET	ASSET REFERENCE NUMBER	CONFIDENTIAL?	RISK DETAILS	RISK RATING (1 - LOWEST, 10 - HIGHEST)	COMPLETE?
Information Security Policies	5			<input type="checkbox"/>			<input type="checkbox"/>
Management direction for information security	5.1			<input type="checkbox"/>			<input type="checkbox"/>
Organization of information security	6			<input type="checkbox"/>			<input type="checkbox"/>
Information security roles and responsibilities	6.1.1			<input type="checkbox"/>			<input type="checkbox"/>
Human resources security	7			<input type="checkbox"/>			<input type="checkbox"/>
Terms and conditions of employment	7.1.2			<input type="checkbox"/>			<input type="checkbox"/>
Asset management	8			<input type="checkbox"/>			<input type="checkbox"/>
Responsibilities for assets	8.1.2			<input type="checkbox"/>			<input type="checkbox"/>
Access control	9			<input type="checkbox"/>			<input type="checkbox"/>
Responsibilities for assets	9.2.6			<input type="checkbox"/>			<input type="checkbox"/>