

Name: Hemant Jain

Lab Progress Report Due Date: 1/25/2021

Current Week Since Start Date: Week 1 (1/26/2021– 2/01/2021)

Reporting Week: From Jan 19, 2021 to Jan 25, 2021

Summary about the TestOut Module-1 Learning:

From the TestOut LabSim Security Introduction Section, I got to learn what Security is and how it is the degree of protection against danger, loss, and criminal activity. The CIA of Security which refers out to Confidentiality, Integrity and Availability and how each Synopsys points to the key contribution they play in makes the services and infrastructure robust and more secured.

Learnt how confidentiality ensures the data is not disclosed out to the unauthorized and unintended people. Integrity ensures that there is no alteration or tampering with data. This is supplied by hashing. Availability guarantees the system's uptime so that data is accessible when required. Non-repudiation offers validation of the origin of a message. If a user sends a digitally signed email, for example, they will not say later that the email has not been sent. Non-repudiation by digital signatures is implemented.

Read about the key security components of the Security namely Physical Security, Users and Administrators and Policies. Enlightened with the Risk Management concept and what it exactly means: Risk management is the method of finding safety concerns and determining which countermeasures to take. Reducing risk to an acceptable amount. The primary aim is to minimize the risk to an entity to the degree that senior management finds appropriate. In general, risk management takes the following steps into consideration: Asset, Threat, Threat Agent, Vulnerability and Exploit. Digging out more and knowing about each item which contributes to the risk management with an example was quite easy to learn about the tool and concept idea. Reading about which all are the Threat Agents and how an Employee working in your own organization can become threat to your organization.

How Employee working at some big firm can be outlooked as a most outlooked dangerous threat agent as they have access to all the important information assets which drives the organization.

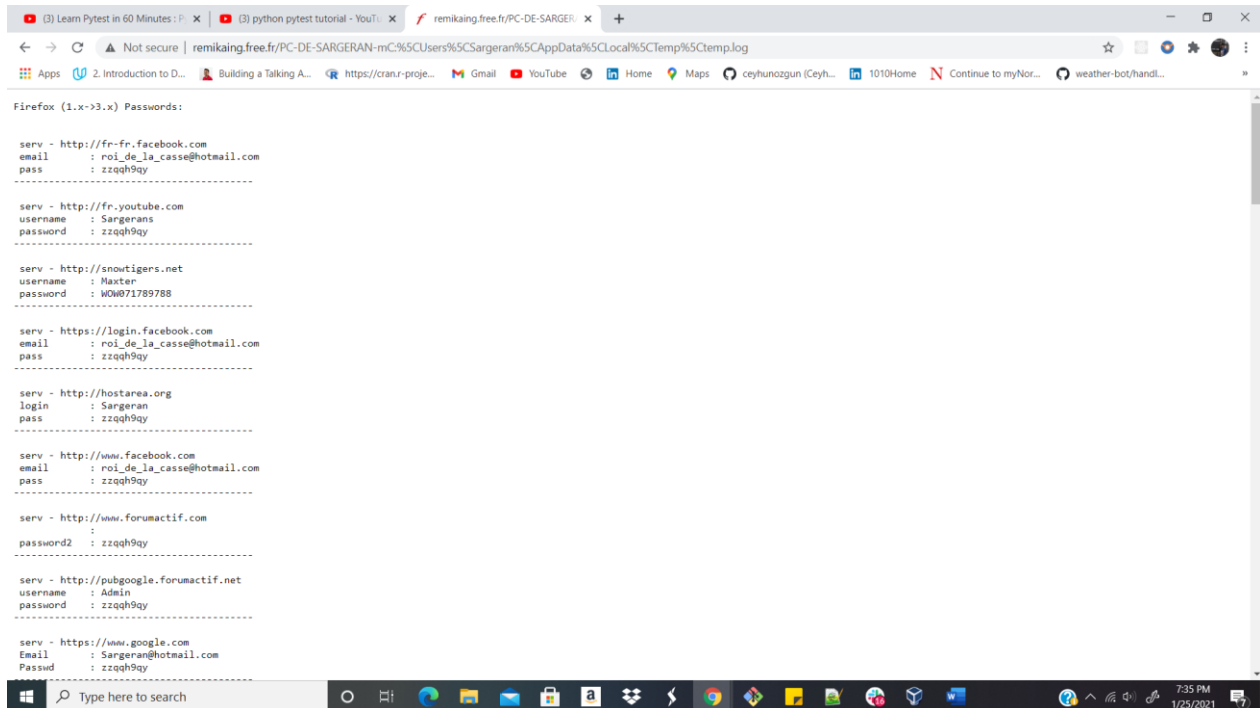
Employees are also known as internal threats. How employees can be made the biggest threat to an organization using disgruntled, bribing and some un-accidental deletion of the files causing the program corruption in the system. Spy is the other threat agent who is hired from the commercial competitors and to exploit the internal vulnerabilities and return the information from the client's product portfolios and features updates. And the third threat agent is Hacker who uses their technical expertise to bypass the security and exploit the vulnerability to access some top-secret information of an organization or competitors.

In the Defense Planning Fact, we learnt about the 7 Layers of Security namely Policies, Procedures, and Awareness, Physical, Perimeter, Network, Host, Application and Data.

Physical Security in basic terms is to protect the perimeter of the asset like organization buildings, network closets, computers etc. from various physical threat actors. Some of the perimeter barriers can be Fences, door locks, mantraps, device locks, server cages, cameras, motion detectors etc. Host could be something from the workstation, laptop and mobile device for log management, OS hardening, patch implementation, patch management, auditing.

Application layer majorly is for Authentication and authorization, user management, group policies and web application security. User Education which makes employees aware about the primary targets in most of the attacks. It makes sure workers realize that one of the most common threats aimed at employees is phishing attacks. Train staff to recognize attacks on emails, text messages, downloads, and websites. Enforcing appropriate password policies, including a policy that prevents passwords from being written down. Train staff to consider both internal and external dangers. Ensure that staff are respectful of the company.

And the last point I read was about Countermeasures which is a way to mitigate the potential risk and reduce the risk of a threat agent exploiting the vulnerability. A pre-prepared step from the listed countermeasure can prevent the hackers to exploit the system's vulnerability.

In-class Lab Homework:**1. allintext:username filetype:log -- Search for files of the .log type**

The screenshot shows a Firefox browser window with the address bar displaying "remikaing.free.fr/PC-DE-SARGERAN-mC%5CSargeran%5CAppData%5CLocal%5CTemp%5CTemp.log". The page content lists several search results, each with a URL, email, and password. The results are as follows:

```
serv - http://fr-fr.facebook.com
email : roi_de_la_casse@hotmail.com
pass  : zzqgh9qy

serv - http://fr.youtube.com
username : Sargeran
password : zzqgh9qy

serv - http://snoutigers.net
username : Master
password : W0M071789788

serv - https://login.facebook.com
email : roi_de_la_casse@hotmail.com
pass  : zzqgh9qy

serv - http://hostarea.org
login : Sargeran
pass  : zzqgh9qy

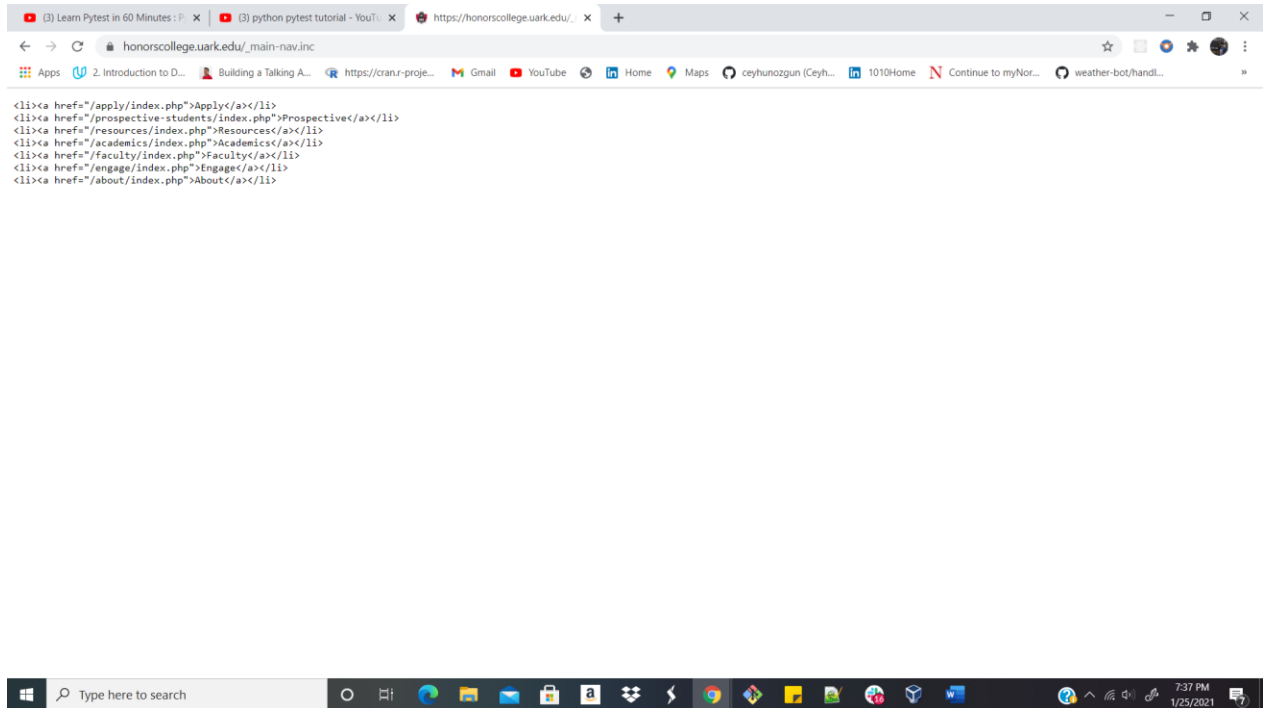
serv - http://www.facebook.com
email : roi_de_la_casse@hotmail.com
pass  : zzqgh9qy

serv - http://www.forumactif.com
password2 : zzqgh9qy

serv - http://pubgoogle.forumactif.net
username : Admin
password : zzqgh9qy

serv - https://www.google.com
Email : Sargeran@hotmail.com
Passud : zzqgh9qy
```

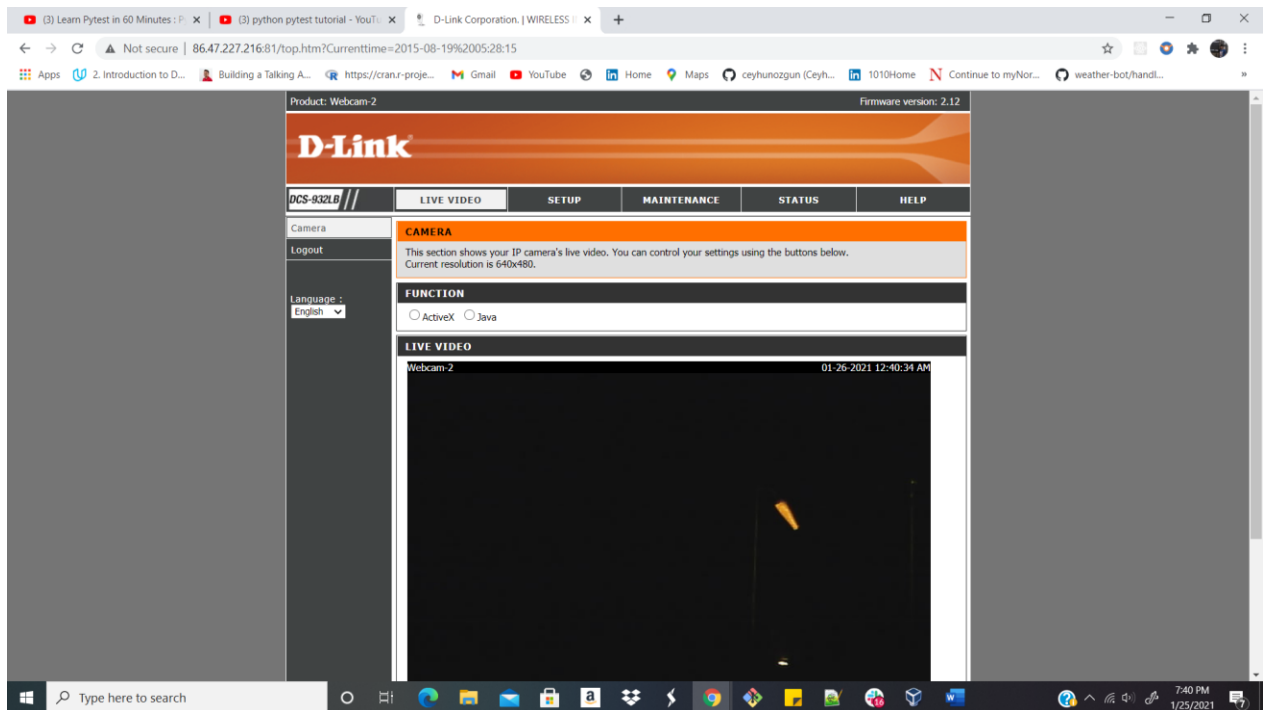
2. filetype:inc.php -site:github.com -site:sourceforge.net -- Fetching github.com and sourceforge.net records having file with php extension



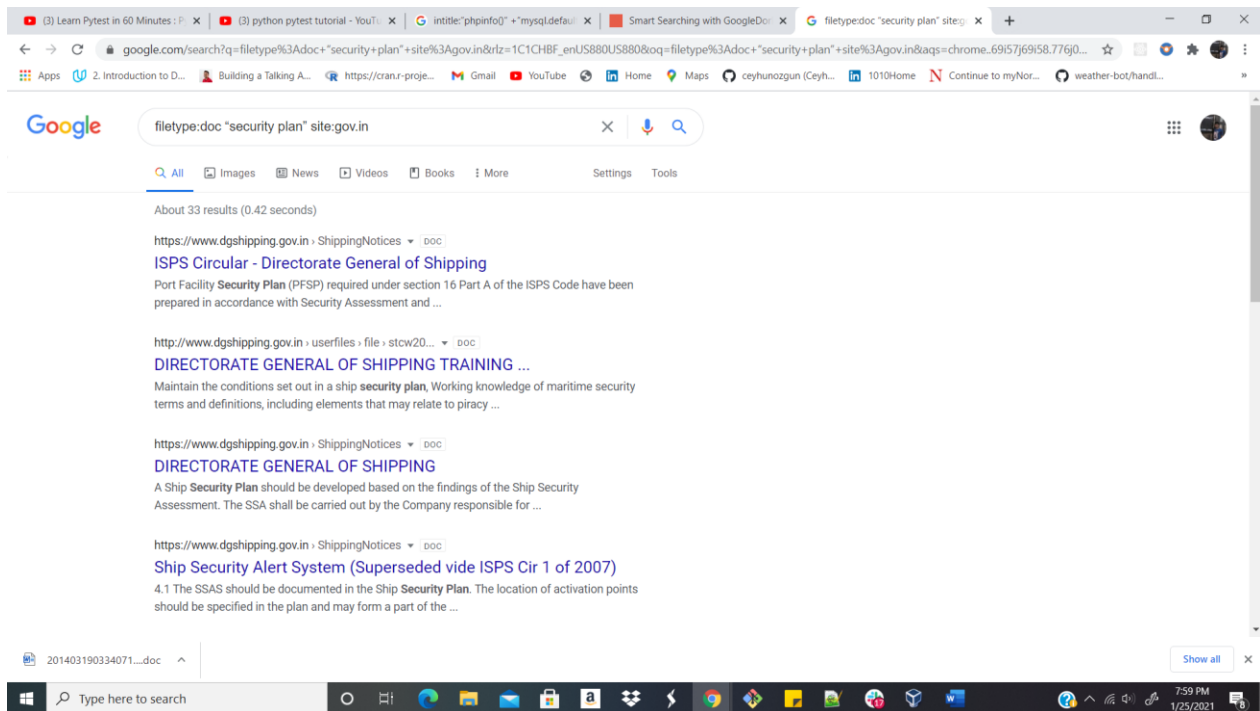
- intitle:"report" ("qualys" | "acunetix" | "nessus" | "nmap") filetype:pdf –
Fetch out the pdf format report published from qualys, acunetix, nessus, nmap.



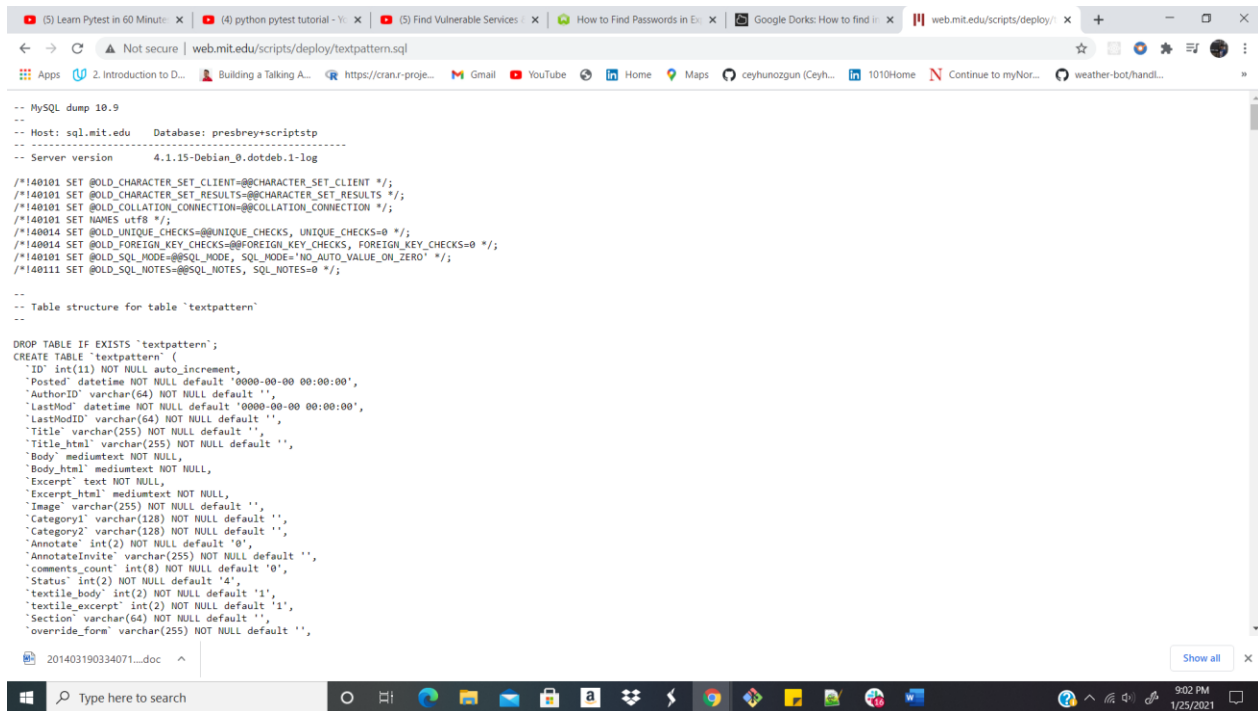
4. `inurl:top.htm inurl:currenttime` – Fetching the open camera video log in real-time



5. filetype:doc "security plan" site:gov.in -- Looking for security plans on the government of India's website



6. filetype:sql "MySQL dump" (pass|password|passwd|pwd) -- This shows spilled data from MySQL databases where you are searching for pass|password|passwd|pwd.



```
-- MySQL dump 10.9
--
-- Host: sql.mit.edu    Database: presbrey+scriptstp
--
-- Server version      4.1.15-Debian_0.dotdeb.1-log

/*!40101 SET @OLD_CHARACTER_SET_CLIENT@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40014 SET @OLD_UNIQUE_CHECKS@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `textpattern`
--

DROP TABLE IF EXISTS `textpattern`;
CREATE TABLE `textpattern` (
  `ID` int(11) NOT NULL auto_increment,
  `Posted` datetime NOT NULL default '0000-00-00 00:00:00',
  `AuthorID` varchar(64) NOT NULL default '',
  `LastMod` datetime NOT NULL default '0000-00-00 00:00:00',
  `LastModID` varchar(64) NOT NULL default '',
  `Title` varchar(255) NOT NULL default '',
  `Title_html` varchar(255) NOT NULL default '',
  `Body` mediumtext NOT NULL,
  `Body_html` mediumtext NOT NULL,
  `Excerpt` text NOT NULL,
  `Excerpt_html` mediumtext NOT NULL,
  `Image` varchar(255) NOT NULL default '',
  `Category1` varchar(128) NOT NULL default '',
  `Category2` varchar(128) NOT NULL default '',
  `Annotate` int(2) NOT NULL default '0',
  `AnnotateInvite` varchar(255) NOT NULL default '',
  `comments_count` int(8) NOT NULL default '0',
  `Status` int(2) NOT NULL default '4',
  `textile_body` int(2) NOT NULL default '1',
  `textile_excerpt` int(2) NOT NULL default '1',
  `Section` varchar(64) NOT NULL default '',
  `override_form` varchar(255) NOT NULL default ''
);
```


Progress Embedded Image of Progress Report from LabSim :

| Score Sheet: TestOut Security Pro:Jain, Hemant | | | | | | | |
|--|----------------------|---|--|-------------------------------------|---------------|--|----------|
| Product | | Resources to Show | | <input type="checkbox"/> Date Range | | <input type="checkbox"/> Show scores as points | |
| TestOut Security Pro 7.0.15 | | <input checked="" type="checkbox"/> Exams | <input checked="" type="checkbox"/> Labs | Start | | | |
| | | <input type="checkbox"/> Lessons | <input type="checkbox"/> Videos | End | | | |
| Resource | Time In Resource | Newest Score | Highest Score | Lowest Score | Average Score | Points Possible | Attempts |
| 1.1.4 Section Quiz | 7 minutes 47 seconds | 100% (1/25/2021 5:31... | 100% (1/25/2021 5:31... | 80% (1/25/2021 5:29 ... | 90% | 10 | 2 |
| 1.2.4 Section Quiz | 4 minutes 49 seconds | 100% (1/25/2021 6:01... | 100% (1/25/2021 6:01... | 100% (1/25/2021 6:01... | 100% | 10 | 1 |
| 2.1.6 Section Quiz | | | | | | 10 | 0 |
| 2.2.6 Configure Micro... | | | | | | 6 | 0 |
| 2.2.7 Section Quiz | | | | | | 10 | 0 |
| 2.3.11 Identify Social ... | | | | | | 9 | 0 |
| 2.3.12 Section Quiz | | | | | | 10 | 0 |
| 2.4.5 Section Quiz | | | | | | 10 | 0 |
| 3.1.3 Implement Phys... | | | | | | 4 | 0 |
| 3.1.4 Section Quiz | | | | | | 10 | 0 |
| 3.2.5 Section Quiz | | | | | | 10 | 0 |
| 3.3.5 Section Quiz | | | | | | 10 | 0 |
| 4.1.4 Section Quiz | | | | | | 10 | 0 |
| 4.2.5 Configure Auto... | | | | | | 3 | 0 |
| 4.2.7 Configure Micro... | | | | | | 5 | 0 |
| 4.2.9 Section Quiz | | | | | | 10 | 0 |
| 4.3.5 Configure NTFS... | | | | | | 2 | 0 |
| 4.3.6 Disable Inherita... | | | | | | 2 | 0 |
| 4.3.7 Section Quiz | | | | | | 10 | 0 |