Assessing a Company’s Cyber Risk

Data Sources/Variables used in assessing company’s cyber risk:

Assessing the cyber risk of a company is more than just counting the number of vulnerabilities and threats. The most commonly used risk algorithm is : Risk = Likelihood * Impact. Risk algorithms (Threat Modeling and OWASP risk Rating Methodologies) should also include the business context as it is critical for prioritizing the risk. Here I am listing few of the variables(Both Technical and Business) used in assessing the cyber risk and the way to collect them or data related to the variables.

1. Port Scanning :

Finding the open ports ,services of a host and details of server , encryption schemes used on the network or websites of a company can be considered as a variable because by gathering the information regarding the services and the cryptography schemes used,the attackers can try to compromise the host using any vulnerabilities in the service and moreover by discovering the open ports through which one can gain privilege access of the system can also enable the attackers to compromise the computers of an organization.

Using Nmap (Network mapper) scanning tool we can discover open ports,hosts ,and services on a computer network. More advanced service detection,vulnerability detection and other features of the tool can be availed using the scripts.

2. Vulnerability scanning:

Vulnerability Management is one of the important task for any organization for its security. The data source for the vulnerabilities (in software design implementions, Language Design Issues, Network and Protocols) of any company is the vulnerability scanning using tools like Nessus , Qualys and Valgrind for mainly memory corruption,
Kali Linux- Penetration Test using Metasploit Framework.
IBM App scan – Web Application & Web services Penetration Testing Solution.

3. Data from Intrusion Detection Systems:

The data from different types of Intrusion Detection Systems of an organization such as Host- IDS,Logs IDS and Network-IDS can also be considered as a variable in determining the cyber risk. Especially in Network IDS we can look for Network packets enquiring about the intellectual property of the company and sensitive files or the packets which are doing the social engineering.

Monitoring tools and sensors like Sguil,Squert,Snort,Snorby,OSSEC, ELSA,tcpdump and Wireshark are deployed in the network of an organization and are used to collect this data.

4. Openly available data regarding IT of the Organization:

Information related to the host machines -OS Version,Ipv4 addresses , Websites of an organization,default passwords and Certificates which are openly available is also considered as a parameter in determining the cyber risk associated. Because the attackers may find any of the host machine or website which still contains the vulnerability which is not yet fixed even though the fix is available.

This type of data can be collected by web scraping or from the search engines such as
1. Censys and Scans.io– which collects large amounts of data of the Host machines, Websites and certificates using Zmap scanning and Ztag.
2.Shodan – maintains the data of internet of things,webcams, power plant and building devices which are connected to the internet.
3.Builtwith & SimilarTech – maintains the data related to what the websites are built with.

5.Important Information leakage:

The amount of sensitive information which is openly available is also considered as the variable in determining the cyber risk of a company. The sensitive information of an organization includes details of the supply chain partners of an organization, Documents with the signatures which are unique to the organization, Code of applications/softwares and configuration files of routers or switches which are knowingly or unknowingly exposed by the employees in the process of seeking solutions from websites like stackoverflow, default passwords of the host machines,routers and other infrastructure, email ids and Personal contact information of the employees, information of holidays and events like picnics at company.

Because by knowing the details of the supply chain partners , the attackers may try to compromise the partner machines first and then try to enter the organization network using the supply chain partner’s infrastructure as a medium.

If the attackers come to know about signatures on any confidential documents which are unique to the organization then they may try to forge the fake documents with those signatures and replace the original files with the fake ones, thereby compromising the integrity of the messages or files transferred over the network.

Whenever the configuration files are out in open then the attackers may try to enter into the network of the organization using the knowledge gather from those files or they may gather atleast some information regarding the infrastructure which they may use in future to compromise the company’s network.

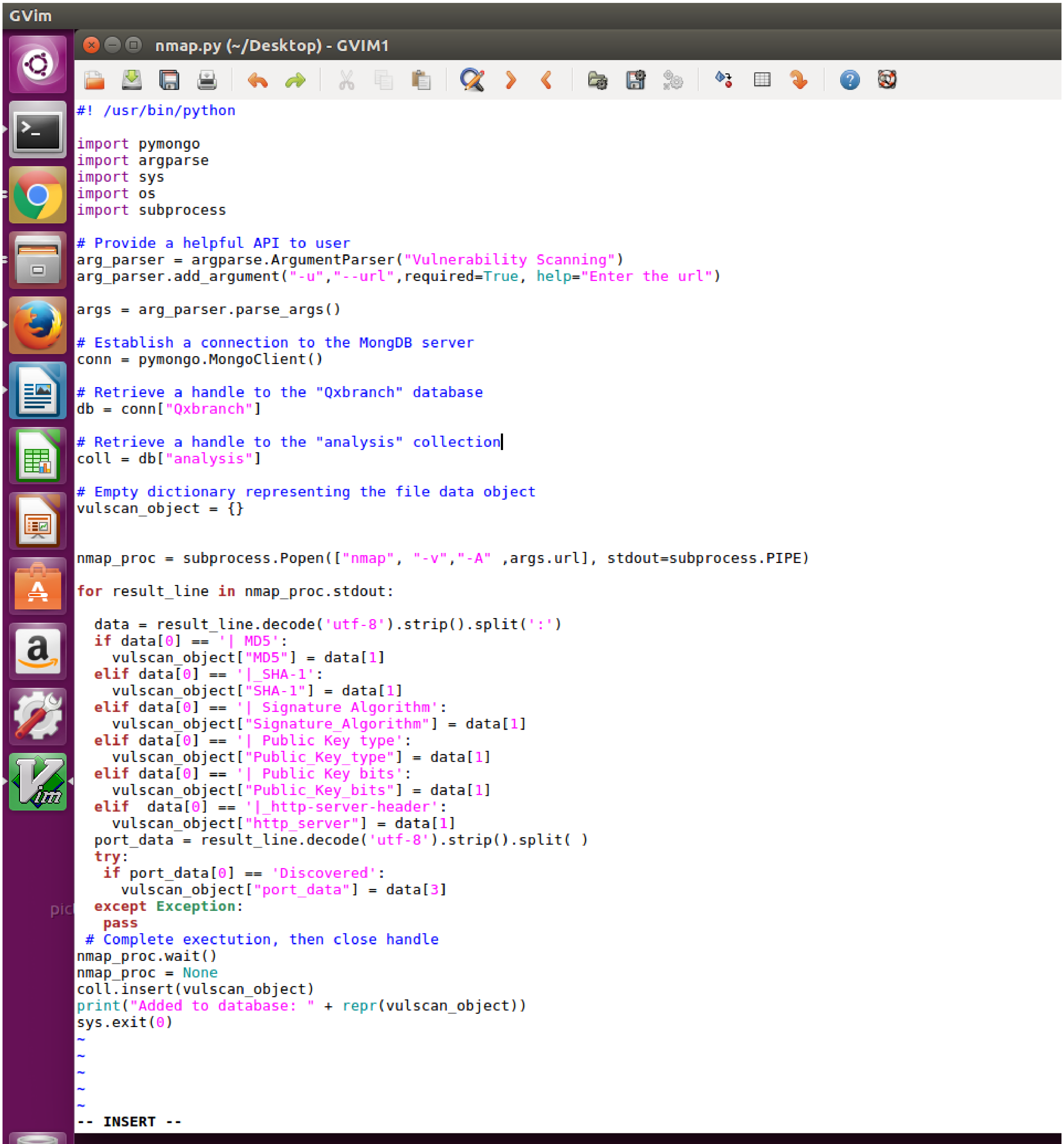
Email ids and personal contacts of the employees may be used for phishing attacks.

The information of type mentioned above can be available to the attackers from the websites like pastebin, patents database,Online Drives and cloud storage services with low level encryption schemes or vunlearbilities , stackoverflow etc.

Option A:

For any company first we have to determine what type of information the company handles and the priority list of what needs to be protected. The priority list may vary from company to company. Here I have chosen the variable PORT SCANNING for assessing the cyber risk of the company flipkart – an electronic commerce company headquartered in India.

As I mentioned in the above listing I have used nmap to perform a port scanning on the website www.flipkart.com . We can also use other tools like Kali Linux, Nessus and other Web application Scanning tools for performing a scan but I was not sure whether using powerful tools like kali linux is



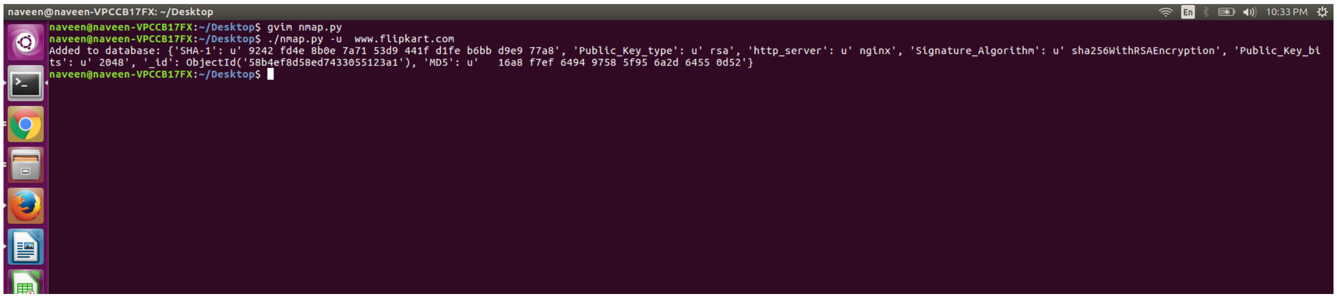
```
#! /usr/bin/python

import pymongo
import argparse
import sys
import os
import subprocess

# Provide a helpful API to user
arg_parser = argparse.ArgumentParser("Vulnerability Scanning")
arg_parser.add_argument("-u","--url",required=True, help="Enter the url")

args = arg_parser.parse_args()

# Establish a connection to the MongDB server
conn = pymongo.MongoClient()

# Retrieve a handle to the "Qxbranch" database
db = conn["Qxbranch"]

# Retrieve a handle to the "analysis" collection
coll = db["analysis"]

# Empty dictionary representing the file data object
vulscan_object = {}


nmap_proc = subprocess.Popen(["nmap", "-v","-A" ,args.url], stdout=subprocess.PIPE)

for result_line in nmap_proc.stdout:

  data = result_line.decode('utf-8').strip().split(':')
  if data[0] == '| MD5':
    vulscan_object["MD5"] = data[1]
  elif data[0] == '|_SHA-1':
    vulscan_object["SHA-1"] = data[1]
  elif data[0] == '| Signature Algorithm':
    vulscan_object["Signature_Algorithm"] = data[1]
  elif data[0] == '| Public Key type':
    vulscan_object["Public_Key_type"] = data[1]
  elif data[0] == '| Public Key bits':
    vulscan_object["Public_Key_bits"] = data[1]
  elif  data[0] == '|_http-server-header':
    vulscan_object["http_server"] = data[1]
  port_data = result_line.decode('utf-8').strip().split( )
  try:
   if port_data[0] == 'Discovered':
    vulscan_object["port_data"] = data[3]
  except Exception:
   pass
 # Complete exectution, then close handle
nmap_proc.wait()
nmap_proc = None
coll.insert(vulscan_object)
print("Added to database: " + repr(vulscan_object))
sys.exit(0)
~
~
~
~
~
-- INSERT --
```

legal/non-intrusive or not, so I restricted myself to using only nmap ,as it was mentioned in the task statement to collect the data in legal and non-intrusive manner. The python code to collect and analyze the data is in image above. I have also attached the python file along with this report. Here in this code I provided an api to the user so that one can pass the arguments from the command prompt.

After that I have established the connection to the MongoDB server (which is already installed on my laptop) and retrieved a handle to the database with the name “Qxbranch” and thereafter retrieved a handle to the collection “Analysis”. This is where I wanted to store the outcomes of my data collection tool and use it for further analysis.

Then after I have performed nmap scanning using the command “nmap -v -A <url>” in the python script and parsed the result of the scanning to gather and analyze only the information which is considered important like Signature Algorithms, public key types, open ports, hashing algorithms and server header etc. All the required information is stored in dictionary.

The screenshots of result of executing the above python code is :



```
naveen@naveen-VPCCB17FX:~/Desktop$ gvim nmap.py
naveen@naveen-VPCCB17FX:~/Desktop$ ./nmap.py -u  www.flipkart.com
Added to database: {'SHA-1': u' 9242 fd4e 8b0e 7a71 53d9 441f d1fe b6bb d9e9 77a8', 'Public_Key_type': u' rsa', 'http_server': u' nginx', 'Signature_Algorithm': u' sha256WithRSAEncryption', 'Public_Key_bi
ts': u' 2048', '_id': ObjectId('58b4ef8d58ed7433055123a1'), 'MD5': u'   16a8 f7ef 6494 9758 5f95 6a2d 6455 0d52'}
naveen@naveen-VPCCB17FX:~/Desktop$ 
```

Similarly we can collect and analyze any large data set which belongs to any of the variables used in assessing the cyber risk of a company.

Prepared by
Naveen Reddy Aleti