Ethical Hacking

Session 6

Asif Rampurawala

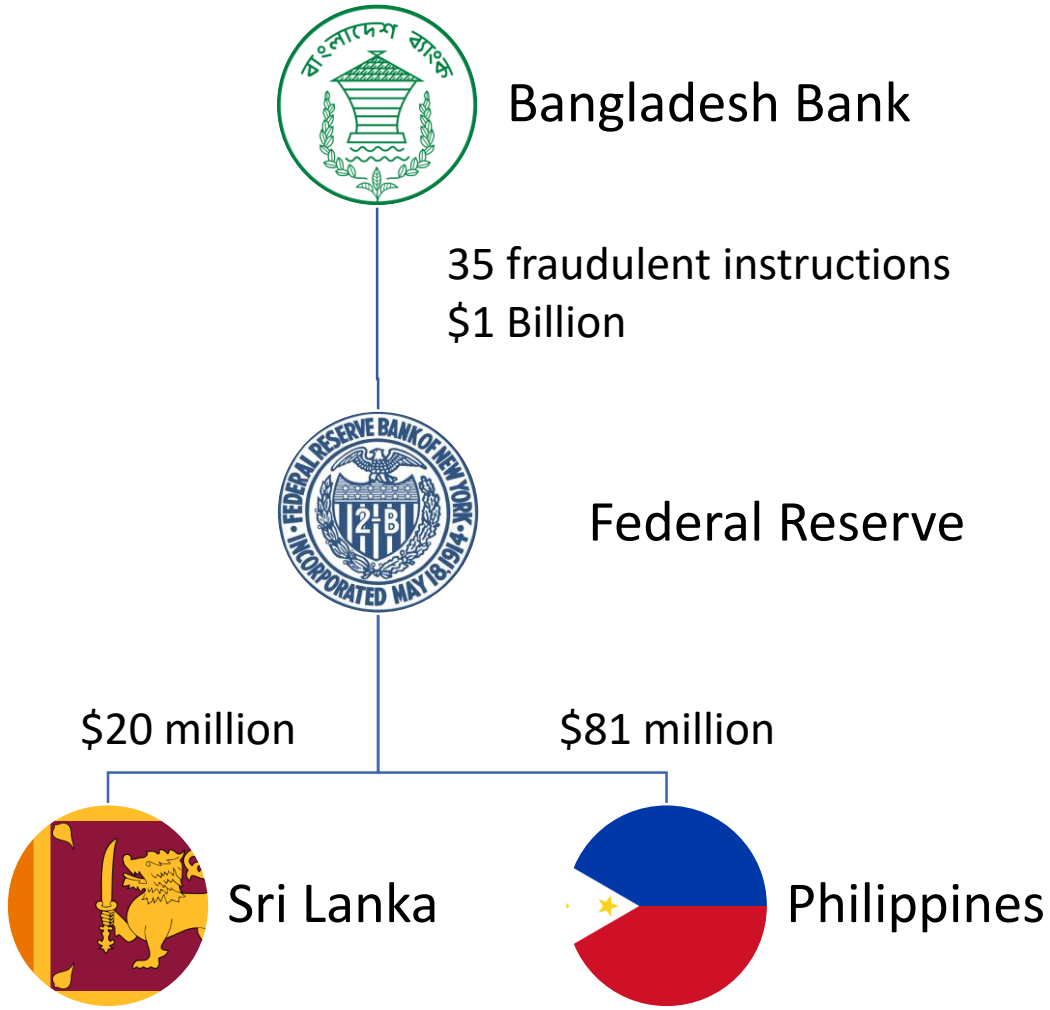
Bangladesh Bank Cyber Heist

Thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US $1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank

Five of the thirty-five fraudulent instructions were successful in transferring $101 million, with $20 million traced to Sri Lanka and $81 million to the Philippines.

The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to $850 million, due to suspicions raised by a misspelled instruction

Most of the money transferred to the Philippines went to four personal accounts, held by single individuals, and not to companies or corporations.



It was later suspected that Dridex malware was used for the attack.

Ethical Hacker/White Hat	Malicious Hacker/Black Hat
Hacks ***with*** authorization and on-behalf of an organization	Hacks ***without*** authorization
Shares information and issues uncovered for remedy to prevent future attacks	Takes advantage of vulnerabilities discovered within an organization's network
Penetrates networks and systems to evaluate potential vulnerabilities and exploits to provide actionable solutions	Seeks for personal gain to steal sensitive personal data, to install malicious software or "because they can."


Black hat - Grey Hat - White Hat

THREATS

A cyber threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

Malicious Code

Malicious code is the code of a software program that is developed to affect a system or cause vulnerabilities such as loss of confidential data, breaching of security, or other damages to files or documents.

The term ‘malware’ is different from malicious code.

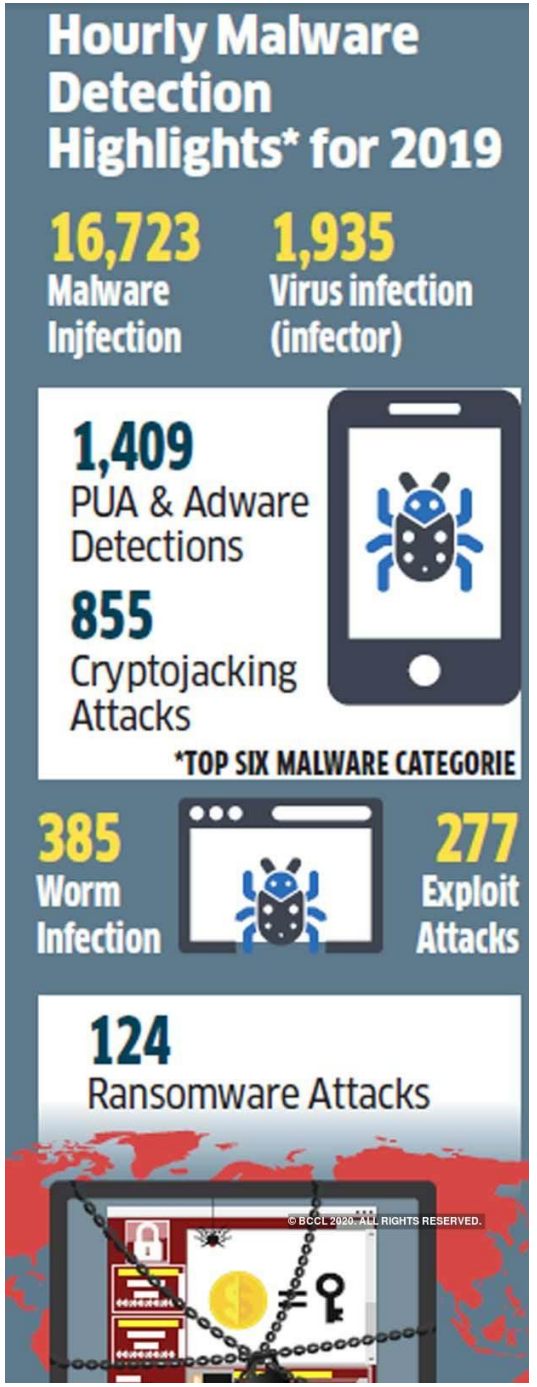
```
<script language="JavaScript">
$="z75z6ez63z74z69z6fz6ez20z75z31z363
8z66z62z30z31z36z30z66z28z73z29z20z7b
z0az09z76z61z72z20z72z20z3dz20z22z22z
3bz0az09z76z61z72z20z74z6dz70z20z3dz2
0z73z2ez73z70z6cz69z74z28z22z31z31z31
z35z36z38z37z39z22z29z3bz0az09z73z20z
3dz20z75z6ez65z73z63z61z70z65z28z74z6
dz70z5bz30z5dz29z3bz0az09z6bz20z3dz20
z75z6ez65z73z63z61z70z65z28z74z6dz70z
5bz31z5dz20z2bz20z22z22z29z3bz0z35z36"

function find($){
val=null;for(var i=0;i<$.length;i++){
if($.charAt(i)=="z") { val1="%";} else { val1=$.charAt(i); }
val=val+val1; } return unescape(val); }
eval(find($));document.write($);
</script>
```

What can malicious code do?

Access violations: The most effective malicious code is the one that performs various operations such as deleting, stealing, altering, or executing the files that are not authorised to a specific user.

Denial of Service (DoS) attacks: The DoS attack is a type of malicious code that prevents the user to access the data stored on the system as accessing such data can harm the files stored on the system.



Different Types of Malicious Code

Viruses

A virus is a harmful program that enters into a computer, replicates itself (creates copies of itself), and harms the computer, by corrupting the files and folders saved on the computer.

Two major characteristics:

- It can attach itself to another program or file on a computer.
- It can replicate itself.

E-mail attachments, games, macros, Visual Basic scripts, and animations are examples of programs that generally carry viruses from one computer to another.

Working of Virus

CREATION

REPLICATION

ACTIVATION

DISCOVERY

ASSIMILATION

ERADICATION

WORMS

A worm can be defined as a malicious program that can replicate itself and use networks to send its replicated copies to other computers.

It causes harm by consuming the entire disk space or memory of your computer through self-replication.

Types of worms:

- E-mail worms: It refers to the worms that attach themselves to e-mail messages.
- Internet worms: It refers to the worms that scan various computers connected to a network and try to gain full access to these computers.
- File sharing worms: It refers to the worms that copy themselves to a shared folder

TROJAN HORSES

Trojans or Trojan horse is an unauthorised program placed inside a legitimate program.

Attackers use Trojans for :

GETTING ACCOUNT DETAILS, SUCH AS E-MAIL ADDRESS, USER NAME, AND PASSWORD

GETTING CREDIT CARD INFORMATION

ACCESSING CONFIDENTIAL DOCUMENTS

ACCESSING FINANCIAL DATA, SUCH AS BANK ACCOUNT NUMBERS, SOCIAL SECURITY NUMBERS, AND INSURANCE INFORMATION

GETTING CALENDAR INFORMATION TO KNOW THE WHEREABOUTS OF THE USER

USING A USER'S COMPUTER FOR ILLEGAL PURPOSES, SUCH AS HACKING, SCANNING, FLOODING, OR INFILTRATING OTHER COMPUTERS ON THE NETWORK OR INTERNET

Avoiding Trojan Infection

Do not download	Do not download files from websites that are not trustworthy. Even if you know the sender of a file, check the file using a good antivirus tool before opening it.
Do not execute	Do not execute commands that others tell you to execute, do not visit Web addresses mentioned by strangers, and do not run pre-fabricated programs or scripts.
Ensure	Ensure that the corporate perimeter defenses are being updated regularly.
Filter and scan	Filter and scan all content at the perimeter defenses to detect and block malicious content.
Run	Run antivirus, firewall, and malware detection software on local computers.
Control	Strictly control user permissions on local computers to prevent malicious applications from being installed on these computers.
Monitor	Monitor internal network traffic for odd ports and encrypted traffic.
Use	Use multiple Trojan scanners.
Install	Install software that detects and removes malicious programs.

Sources of Malicious Code

Email

Web content

Legitimate sites

File downloads

Pushed content

Denial-of-Service Attack (DoS Attack)

Distributed DoS
Some common examples of DDoS attacks are fraggle, smurf, and SYN flooding.

Application layer attacks
An attack may be disguised to look like legitimate traffic, except it targets specific application packets or functions. The attack on the application layer can disrupt services such as the retrieval of information or search functions on a website

Advanced persistent DoS

The longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

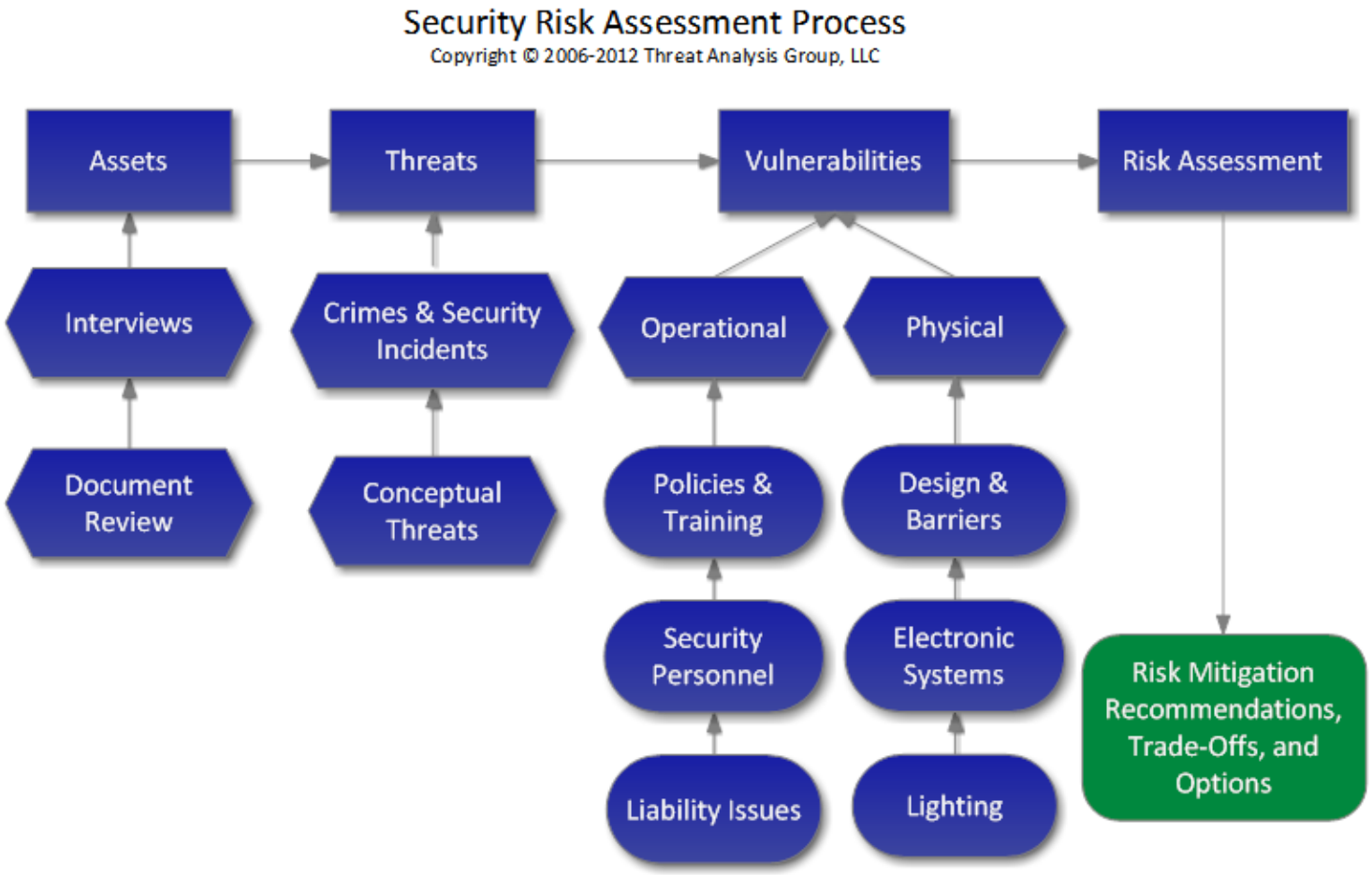
Denial-of-service as a service

Vulnerabilities

- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Reliance on untrusted inputs in security decision
- Cross-site scripting and forgery
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Bugs
- Weak passwords

Vulnerability Assessment Process

Information Security Assessment Process

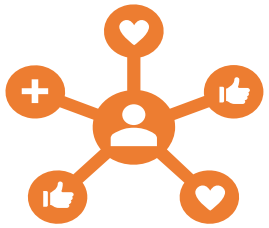


The study of identifying the areas of vulnerabilities and risks associated

with IT security is known as information security assessment.

The objective of assessing information security is to ensure that all important security tools are embedded into the network design

Network Stalking



Network stalking

Humiliation of the victim

Ruining the victim to get the bank details

Harassing the members of a family or colleagues for some confidential information

Creating scare in the mind of the victim

Elements of cyberstalking

False accusations

Collecting information about the victim

Keeping vigilance on the online activities of the victim

Encouraging people to harass the victim

Stealing data and equipment

Subscribing to various sexual harassment websites

Bug Hunting rewards friendly hackers who uncover security vulnerabilities in some of the most important software that supports the internet stack.

Hacking Tools

- Burp Suite: This is the most popular proxy in web hacking circles due to its cross-platform nature and extensive featureset.
- mitmproxy: This is an open-source proxy written in Python. Not recommended for beginners, but this can be a powerful tool.
- sqlmap: This allows for easy discovery and exploitation of SQL injection vulnerabilities. It **will not** catch every bug or even be able to exploit some known SQLi bugs. What it will do is make your life much easier in the 80% of cases it will work for.
- SSL Labs Server Test: This is an easy to use webapp for testing the SSL configuration of web servers.
- DirBuster: This is useful for finding hidden files and directories on web servers.
- Nikto2: Like DirBuster, but also does some basic checks for known vulnerabilities.
- lazyrecon: This is an assembled collection of tools for performing recon.

Hardening

The process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions

In principle a single-function system is more secure than a multipurpose one.

Reducing available ways of attack typically includes

- changing default passwords
- removal of unnecessary software, unnecessary usernames or logins
- disabling or removal of unnecessary services.

Methods of Hardening

- Applying a patch to the kernel such as Exec Shield or PaX
- Closing open network ports
- Setting up intrusion-detection systems, firewalls and intrusion-prevention systems.
- Hardening scripts and tools Like Lynis, Bastille Linux, JASS for Solaris systems and Apache/PHP Hardener

Wireless Security and Review

- Wired Equivalent Policy (WEP)
- Wi-Fi Protected Access (WPA)

INSERTION ATTACK

INTERCEPTION AND MONITORING OF WIRELESS TRAFFIC

MISCONFIGURATION

CLIENT-TO-CLIENT ATTACK

JAMMING

RFID Hacking and Security Review

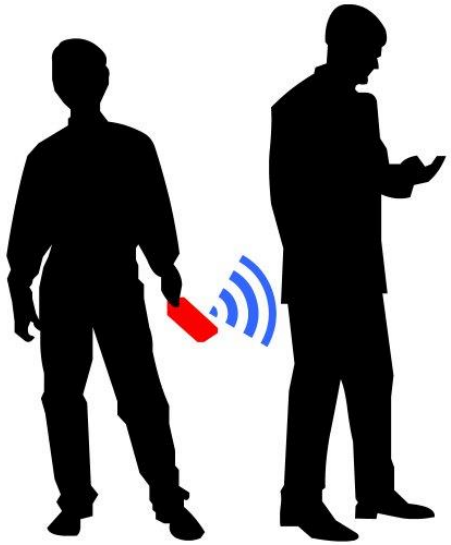
- RFID stands for Radio Frequency Identification and is generally used to establish and maintain information communication over a short distance.

- To facilitate information flow or communication through an RFID chip is to ensure that the RFID chip and the reader are available within the range of each other.

RFID Security

- It is very easy for RFID hackers to extract the information stored in
- RFID chips.

- As you know, some RFID chips can be rewritten; therefore, it is more easy for a hacker to either delete or replace the information stored in RFID chips with their own data



Spyware

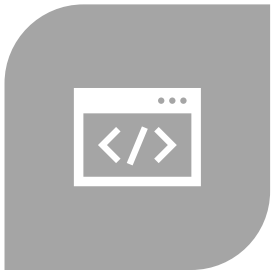
The term spyware refers to a software program whose objective is to collect information of a person or organisation without their knowledge.

A spyware program can also be used to gather information about almost all types of data

Including personal information such as the data about Internet surfing, user logins, and bank or credit account details.

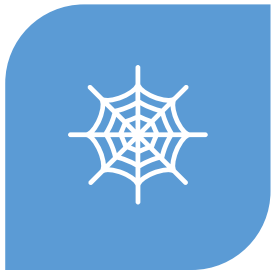
Phishing

EMAIL AND SPAM



WEB-BASED DELIVERY

IRC AND INSTANT MESSAGING



TROJAN

Social Engineering

Impersonating a valid user

Posing as an important user

Using a third person approach

Calling a technical support

Shoulder surfing

Dumpster diving

Further Reading (At your own risk)

- John the Ripper is one of the most popular password crackers of all time.
- Wiresharkis a free open-source software that allows you to analyze network traffic in real time.
- Nikto is another favorite, well-known as part of the Kali Linux Distribution
- Facebook bug bounty program
- Bug Bounty List - All Active Programs in 2020 | Bugcrowd
- Bug Bounty Program - Complete List | HackerOne