

## Unit 3: Compromising the System



# Analysing the current trends

Over time, hackers have proven to cyber security experts that they can be persistent, more creative, and increasingly sophisticated with their attacks. They have learned how to adapt to changes in the IT landscape so that they can always be effective when they launch attacks.

1. Extortion Attacks
2. Data Manipulation Attacks
3. IOT Device Attacks
4. Backdoors
5. Mobile Devices
6. Hacking everyday devices
7. Hacking the cloud

# Extortion Attacks

- Hackers have been getting revenues for selling stolen data from companies.
- Hackers also extracting the money directly from their victims. And they hold computer files to ransom or threaten to release damaging information about a victim to the public.
- Use Cases:
  - a. WannaCry Ransomware Variant
  - b. Ransomware variant hit Ukarine
  - c. Ashley Madison
  - d. UAE bank called Sharjah

# Data Manipulation Attacks

- Data Manipulation attack is **compromise the integrity of data**.
- There is no agony that hackers can cause to a target that is greater than making it distrust the integrity of its own data.
- Data manipulation can be trivial, at times changing just a single value, but the consequences can be far-reaching.
- Data manipulation is often difficult to detect and hackers might even manipulate data in backup storage to ensure that there is no recovery.

## Use Cases:-

- Chinese Spies attacked US defense contractor to steal blueprints.
- **Officer Twitter account is hacked**

# IOT Device Attacks

- This is an emerging and rapidly growing technology, where hackers are targeting **Internet of Things (IoT)** devices available, from smart home appliances to baby monitors.
- Networks of CCTV cameras and IoT lights have been used to cause **distributed denial of service (DDoS)** attacks against banks and even schools.
- Hackers are exploiting the huge numbers of these devices to concentrate efforts at generating voluminous illegitimate traffic capable of taking down the servers of organizations that offer online services.
- Experts have warned that most IoT devices are not secure and most of the blame has fallen on the manufacturers.

# Backdoors

- In 2016, one of the leading network device manufacturers, Juniper Networks, found that some of its firewalls had firmware that contained backdoors installed by hackers.
- The backdoors enabled hackers to decrypt traffic flowing through the firewalls. It clearly meant that the hackers wanted to infiltrate organizations that had bought firewalls from the company.
- Juniper Networks said that such a hack could only have been actualized by a government agency with enough resources to handle traffic flowing in and out of many networks.
- The National Security Agency (NSA) was put in the spotlight since the backdoor had similarities to another one that was also attributed to the agency.
- The backdoor was planted at the manufacturer's premises, and therefore any organization that bought a firewall from them was infiltrated by the hacker.
- Companies selling legitimate software on their websites have also become targets for hackers.
- Hackers have been inserting codes to create backdoors into legit software in a manner that the backdoor will be harder to find.

# Mobile Device Attacks

- According to a leading cybersecurity company called Symantec, there has been a gradual increase in malicious activity targeting mobile devices.
- The most targeted **operating system (OS)** is Android, since it has the highest number of users so far. However, the OS has been making several security improvements in its architecture, making it more difficult for hackers to infect devices running on it.
- The cybersecurity company says that out of the total number of Android-based devices that have been installed, it has blocked about 18 million attacks in 2016 alone.
- This was double the number of attacks blocked in 2015, where it reported only 9 million attack attempts.
- The security company also reported that there was a rise in the growth of mobile malware.
- Symantec may report over 30 million attack attempts in its 2017 report. The increase in mobile phone attacks is attributed to the low level of protection that users afford their smartphones.
- Smartphones have browsers and web-supported apps that are vulnerable to scripting attacks, and they are also exploitable through the man-in-the-middle attack.

# Hacking everyday devices

- The peripherals such as printers and scanners, preferably those that have been assigned an IP address for the purposes of sharing.
- Hackers have been hacking into these devices, and in particular printers, since modern printers come with an inbuilt memory function and only basic security features.
- The most common security features include password authentication mechanisms. However, these basic security measures are not enough to deter motivated hackers.
- Hackers have been using printers for corporate espionage by gathering the sensitive data that users send to be printed.
- Printers have also been used as entry points into otherwise secure networks. Hackers can easily hack into a network using an unsecured printer instead of using the more difficult way of having to compromise a computer or server within a network.

## Use Cases:

- NSA has been hacking Samsung smart TVs.
- An exploit codenamed "Weeping Angel" was leaked and found to exploit the always-on voice command system of Samsung smart TVs to spy on people in a room by recording their conversations and transmitting them to a **Central Intelligence Agency (CIA)** server.



# Hacking the cloud

- There is one great vulnerability in the cloud: everything is shared. People and organizations have to share storage space, CPU cores, and network interfaces.
- Therefore, it only requires hackers to go past the boundaries that cloud vendors have established to prevent people from accessing each other's data.
- This is what hackers are always counting on in order to make their way into the backend of the cloud where all the data resides.
- There is a limit to the extent to which individual organizations can ensure the security of the data that they store in the cloud.
- The security environment of the cloud is largely determined by the vendor. The vendor may not be so thorough with the security afforded to clients' data.
- The cloud also involves the use of shared platforms with other people, yet a cloud user is only given limited access controls. Security is majorly left to the vendor.

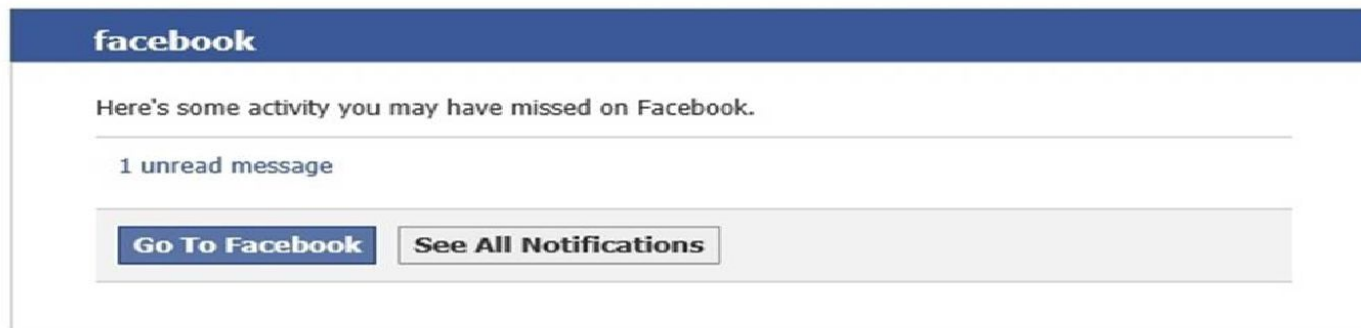
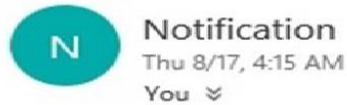
## UseCase:

US Internal Revenue Service (IRS)

# Phishing


- phishing as an external reconnaissance technique used to obtain data from users in an organization.
- Phishing can be the precursor to an attack or as an attack itself. As a reconnaissance attack, the hackers are mostly interested in getting information from users.

You have unread message that will be deleted in 5 days holding




This message was sent to [REDACTED] If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).  
Facebook, Inc. Attention: [Department 415 P.O Box 10005 Palo Alto CA 94303](#)

# Phishing



1 / 63

## One engine detected this URL


URL	<a href="http://meipt.eng.ku.ac.th/upload/culvers.php">http://meipt.eng.ku.ac.th/upload/culvers.php</a>
Host	<a href="http://meipt.eng.ku.ac.th">meipt.eng.ku.ac.th</a> 
Downloaded file	44ebc972b4bdaeb5850f9fd8f0b1059371b5d3a96cb6efef18cf01
Last analysis	2017-08-20 15:00:04 UTC

Detection

Details

Community

Trustwave

 Malicious

ADMINUSLabs

# Exploiting a Vulnerability

- The exploitation of vulnerabilities is done when hackers take advantage of bugs in a software system; this could be within an operating system, the kernel, or a web-based system.
- The vulnerabilities provide loopholes through which hackers can perform malicious actions. These could be errors in the authentication code, bugs within the account management system, or just any other unforeseen error by the developers.
- Software system developers constantly give users updates and upgrades as a response to the observed or reported bugs in their systems. This is known as patch management, which is a standard procedure at many companies that specialize in the making of systems.

# Zero Day

- Many software-developing companies have rigorous patch management, and therefore they always update their software whenever a vulnerability is discovered.
- This frustrates hacking efforts targeted at exploiting vulnerabilities that software developers have already patched.
- Zero-day attacks use advanced vulnerability discovery tools and techniques to identify vulnerabilities that are not yet known by software developers.

# Fuzzing

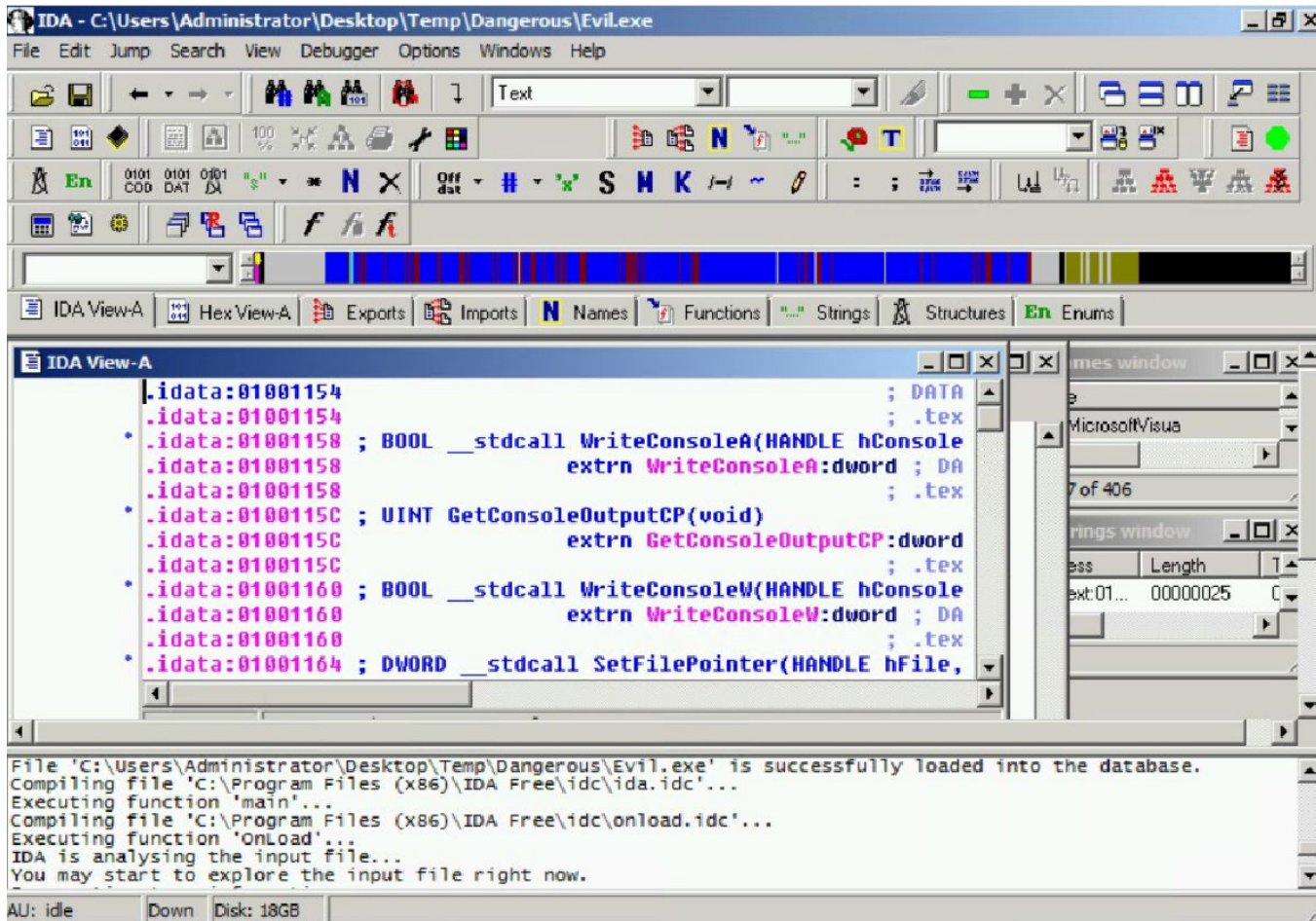
- Fuzzing involves the recreation of a system by the hacker in an attempt to find a vulnerability.
- Through fuzzing, hackers can determine all the safety precautions that system developers have to put into consideration and the types of bugs that they had to fix while making the system.
- An attacker also has a higher chance of creating a vulnerability that can be successfully used against modules of the target system.
- This process is effective since a hacker gains a full understanding of the working of a system, as well as where and how it can be compromised.
- However, it is often too cumbersome to use, especially when dealing with large programs.

# Source Code Analysis



- This is done for systems that release their source code to the public or through open source under a BSD/GNU license.
- A knowledgeable hacker in the languages used to code a system might be able to identify bugs in the source code.
- This method is simpler and quicker than fuzzing.
- However, its success rate is lower, since it is not very easy to pinpoint errors from merely looking at code.

# Source Code Analysis



- Another approach is to use specific tools to identify vulnerabilities in the code.
- Checkmarx ([www.checkmarx.com](http://www.checkmarx.com)) is an example of that. Checkmarx can scan the code and quickly identify, categorize, and suggest countermeasures for vulnerabilities in the code.



# Types of ZERO Day Exploits

## 1. Buffer Overflow:

- Buffer overflows are caused by the use of incorrect logic in the codes of a system.
- Hackers will identify areas where these overflows can be exploited in a system.
- They execute the exploit by instructing a system to write data to a buffer memory but not to observe the memory restrictions of the buffer.
- The system will end up writing data past the acceptable limit, which will therefore overflow to parts of the memory.

Ex:- CVE -2010-3939 addresses a buffer overflow vulnerability in the win32k.sys module in the kernel-mode drivers of Windows Server 2008 R2.

# Types of ZERO Day Exploits

## 2. Structured Exception Handler overwrites:

- **Structured exception handling (SEH)** is an exception handling mechanism included in most programs to make them robust and reliable.
- It is used to handle many types of errors and any exceptions that arise during the normal execution of an application.
- SEH exploits happen when the exception handler of an application is manipulated, causing it to force an application to close.
- Hackers normally attack the logic of the SEH, causing it to correct nonexistent errors and lead a system to a graceful shutdown.