





# ATTACK METHODOLOGIES



# INTRODUCTION




AWARENESS OF THE METHODOLOGIES INTRUDERS USE TO BREAK INTO COMPUTER SYSTEMS IS AS ESSENTIAL AS KNOWING THE SECURITY MODELS PRESENTED EARLIER

To meet their targets effectively, attackers follow specific intrusion methodologies:

-  WITH TYPICAL, REMOTE ATTACKS, an intruder sets out to gather as many information as possible about the targeted system
-  NEXT, THE ATTACK WILL TRY to enumerate all the hosts connected to the Internet or a local network of the target



# INTRODUCTION

-  **THERE IS A WEALTH** of confidential data sent over the networks, and the attacker may obtain it by eavesdropping on the packets
-  **AFTER ACCESSING** and taking over the targeted system, the attacker will try to obtain admin privileges, obtain all user passwords and make another connection feasible
-  **THE LONGER AN ATTACK** remains undiscovered, the more benefits the attacker will reap from illegally accessing the information



# LOCAL ATTACKS

## MOST COMPUTERS ARE NOT PROTECTED FROM LOCAL ATTACKS

A computer's operating system cannot ensure its total security: even the best OS is not an obstacle if an attacker wants to connect a device to the computer



# LOCAL ATTACKS

Protective measures:



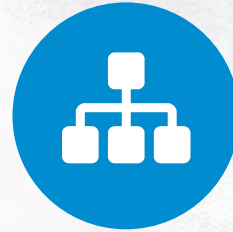
---

Outside parties should not be able to access company premises unaccompanied



---

Don't just assume the man wearing courier shirt is really who he claims to be



---

All personnel on company's premises should wear a hard-to-forge identity card conspicuously

# LOCAL ATTACKS

Protective measures:



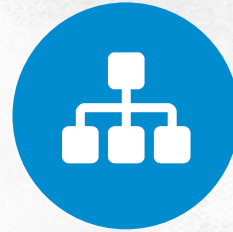
---

The primary boot volume should be the hard drive that contains your operating system



---

Every time someone takes apart a PC case, admins and users should be present

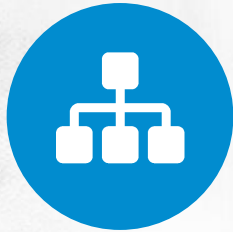


---

Make sure you are not observed when entering a password

# LOCAL ATTACKS

Protective measures:



---

When you end work, shut down your computer instead of hibernating it



---

If unattended, a computer must be automatically blocked



---

The BIOS should be password-protected

# LOCAL ATTACKS





# TARGET SCANNING AND ENUMERATION TECHNIQUES

**NETWORK  
PROTOCOLS  
DESIGNED  
DECADES AGO  
ARE STILL IN USE  
TODAY.**

They cannot provide adequate security for computers against current threats:

## LOWER-LAYER PROTOCOLS

(layers 1-4) lack even the most basic of security measures

## ALTHOUGH RFC DOCUMENTS

defining the OSI model feature a great level of detail, they don't cover some implementation issues, for example don't specify how Ethernet frames should be padded. In 2003 Ofir Arkin and Josh Anderson noticed many operating systems (Windows and Linux included) pad the too-short frames with random data culled from memory

## PROTOCOLS

of different layers trust each other

# TARGET SCANNING AND ENUMERATION TECHNIQUES

**THE OSI MODEL PROTOCOLS** have been created forty years ago and their age means they cannot be secured well without introducing new standards and redesigning every network device and program. To give you an example:



**THINKING THAT NETWORK** switches prevent people from eavesdropping on packets sent between computers is a myth



**IT'S NOT TRUE** that you can isolate computers effectively using managed switches and trunking

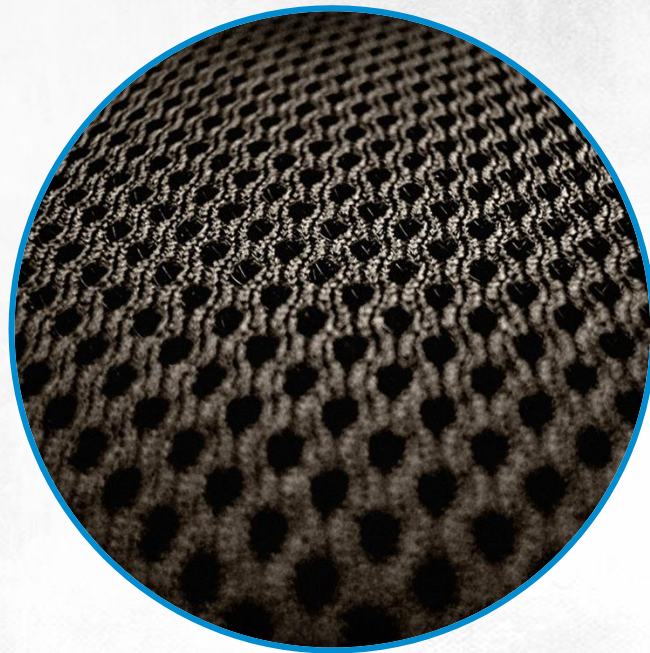
# TARGET SCANNING AND ENUMERATION TECHNIQUES

## THE WAY NETWORK PROTOCOLS

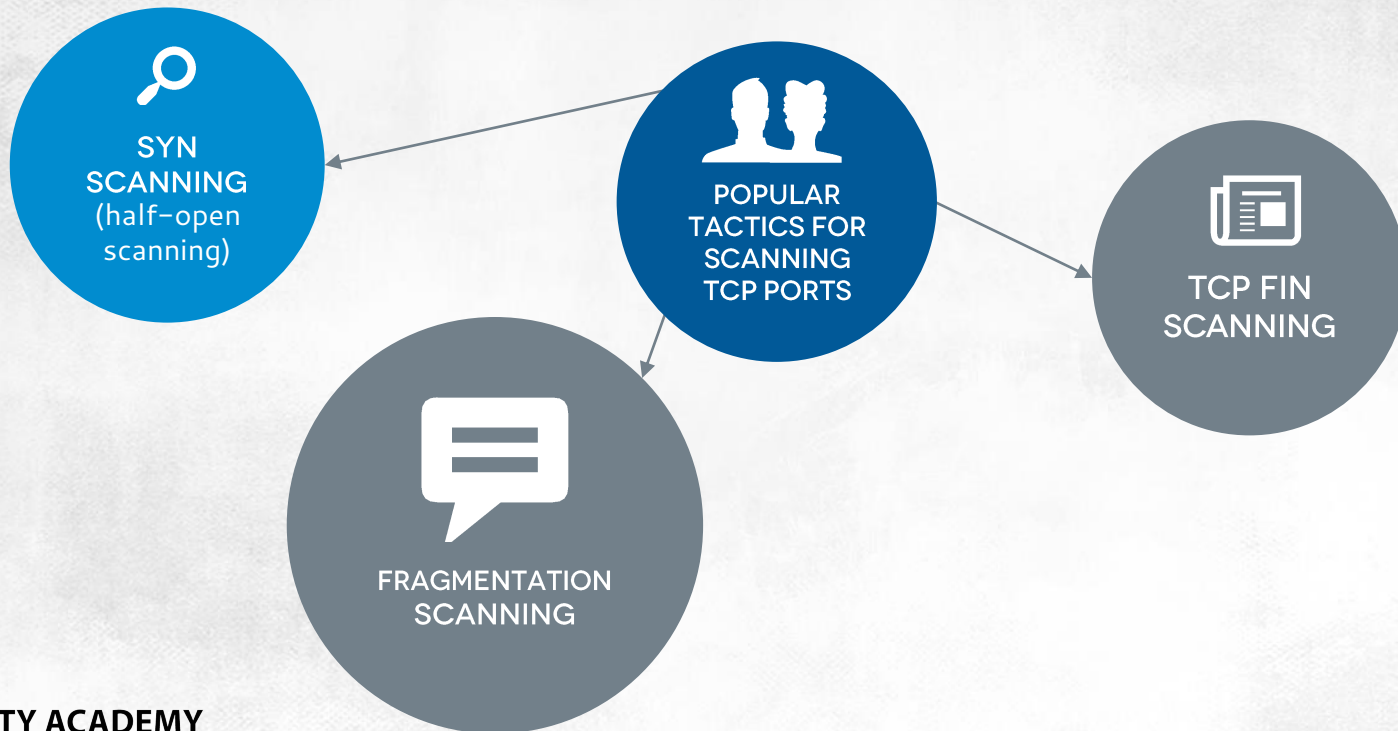
are built and implemented means the most popular and easiest manner of retrieving information about a remote system is scanning.

## SCANNING INVOLVES TESTING

if the transport layer protocols (TCP or UDP) can be used to establish a connection with remote hosts. Because the majority of standard network services makes operate on well-known ports, knowing which ports are open lets you enumerate which network services are running in a remote system and what operating system is used

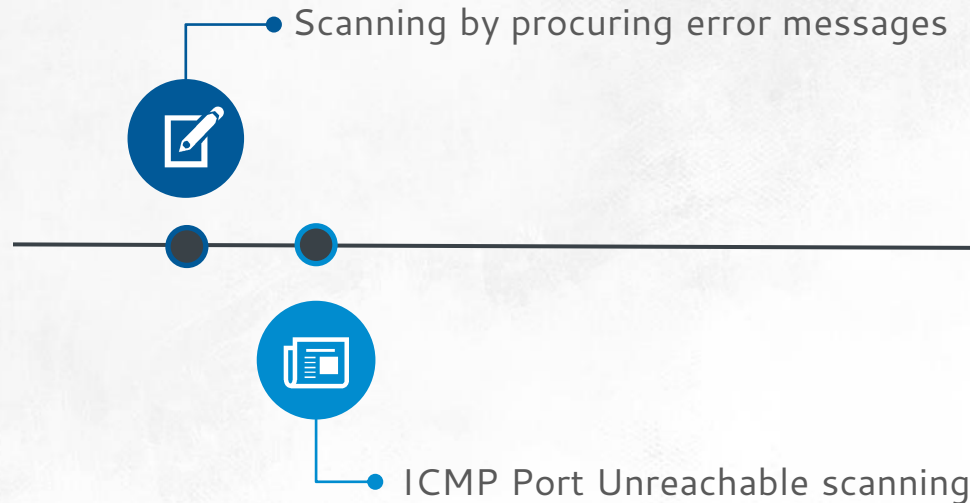


# TARGET SCANNING AND ENUMERATION TECHNIQUES



# TARGET SCANNING AND ENUMERATION TECHNIQUES

**BECAUSE UDP**  
is a connectionless  
protocol, the tactics for  
identifying open UDP  
ports are more  
complex:



# TARGET SCANNING AND ENUMERATION TECHNIQUES

## SCANNING CAN KEEP ATTACKER'S IDENTITY HIDDEN:

- ✓ Scanners are running on computers that have been broken into
- ✓ Packets are sent using the attacker's IP and a certain number of fake IP addresses (diversion scanning)



# TARGET SCANNING AND ENUMERATION TECHNIQUES

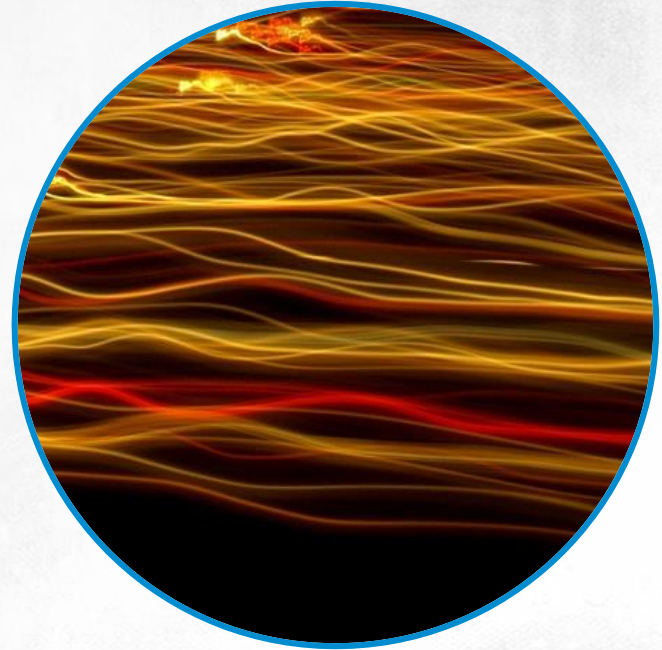


In 1998 Salvatore Sanfilippo came up with the notion of an idle scan. This scan exploits a computer procedure described in RFC 791. When a host receives an unexpected packet, it should send back the RST message to the sender. An exception is when it receives an unexpected RST packet, which should be ignored



# TARGET SCANNING AND ENUMERATION TECHNIQUES

**ALSO PASSIVE SCANNING**  
techniques can make an attack undiscoverable. The basis of this scanning, which consists of the analysis of scan packets sent over the web, is the fact there are no two identical implementations of the OSI model protocols





# TARGET SCANNING AND ENUMERATION TECHNIQUES

## THE TTL ATTRIBUTE (TIME TO LIVE) OF IP PACKETS.

Since RFC doesn't specify what the initial value of TTL should be, OS developers pick one that suits them best. Windows systems, for instance, set it at 128, Linux – at 64, and earlier versions of Unix the value equals 225

## TCP WINDOW SIZE.

This attribute specifies the maximum potential amount of data that can be received within a TCP session without sending an acknowledgement.

The default window size depends on OS version run by a computer. In earlier Linux systems it's 16,384, while in

Windows it's 64,512

## IP SERVICE TYPE

In theory, it should specify packet priority, but since it doesn't have any effect on sending the packet over the web, it is practically set to a fixed value standard for a given system

## TCP MESSAGE SOURCE PORT NUMBER

every OS uses a different formula to assign TCP source ports to applications

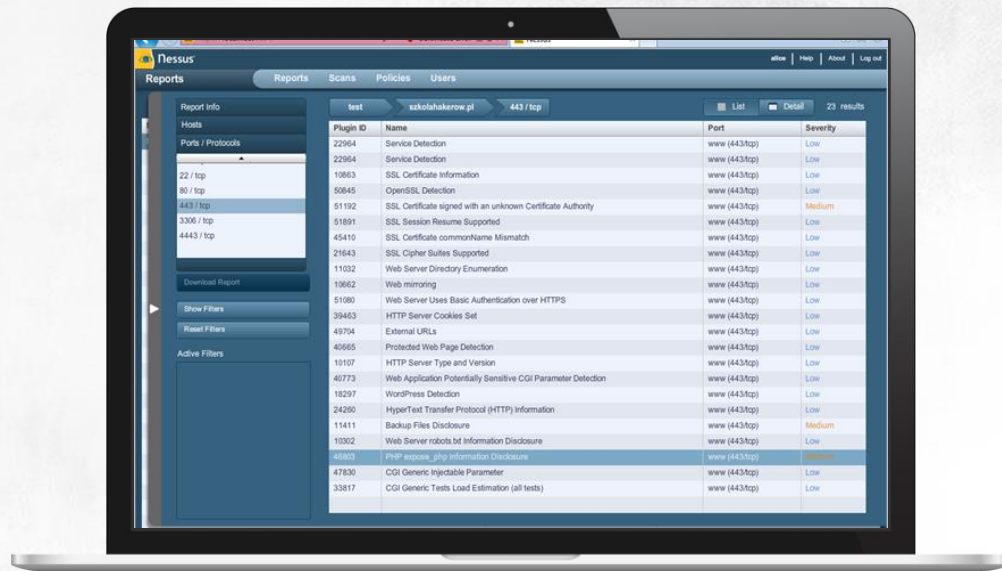
## PASSIVE SCANNING USES



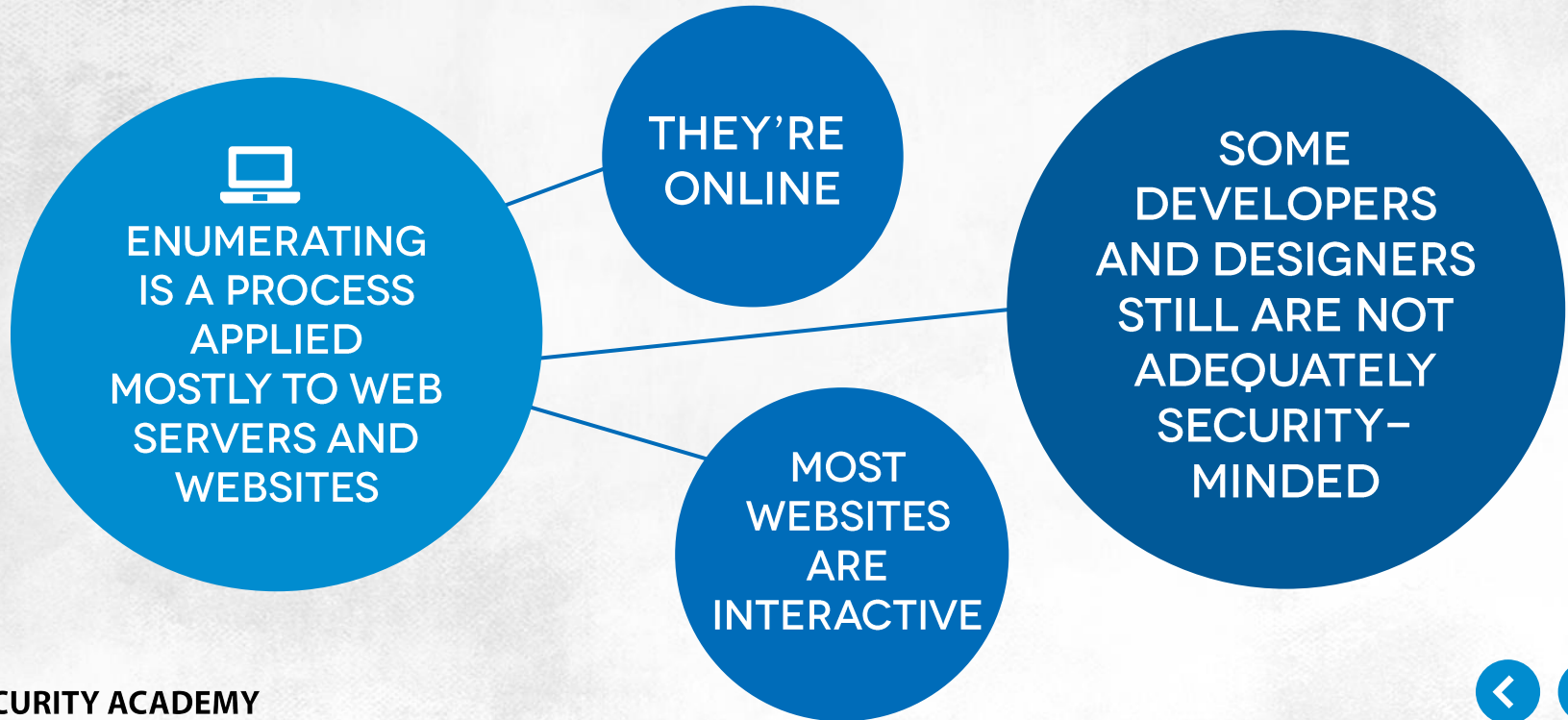
# TARGET SCANNING AND ENUMERATION TECHNIQUES

SCANNING IS USED TO FIND AND IDENTIFY REMOTE SYSTEMS, WHILE THE GOAL OF ENUMERATING IS TO IDENTIFY WEAK POINTS AND VULNERABILITIES OF A SYSTEM

Security scanners like Nessus are used for enumeration



# TARGET SCANNING AND ENUMERATION TECHNIQUES



# EXERCISE

## Scanning to identify a target



### PUBLICLY AVAILABLE REGISTRATION INFO:

www.news.netcraft.com, whois



### TRACING PACKET ROUTES:

pathping, VisualRoute



### FOUNDSTONE'S SCANLINE



### IDLE SCAN

using nmap



### PASSIVE SCANNING

using POf



### FINDING VULNERABLE SERVERS

and websites using Site Digger



### ENUMERATING USING NESSUS



# INTRUSION METHODS **AND TAKING OVER**

Three groups of attacks:



## ATTACKS

---

that stem from failing to properly validate input, including buffer overflow attacks, SQL Injection attacks, running malicious scripts and modifying files



## PASSWORD

---

and user credential theft attacks: password may either be cracked or determined otherwise



## USER-TARGETING

---

attacks: by manipulating the feelings of fear, greed or trust (three social engineering pillars), attackers are trying to obtain confidential data from users or encourage them to run malicious software







# INTRUSION METHODS **AND TAKING OVER**

ONCE ATTACKERS HAVE BROKEN INTO COMPUTER, THEY WILL ENSURE THEY CAN RETURN TO IT. THIS REQUIRES HAVING THE COMPUTER RUN MALWARE

If the attacked system is running Windows, to control it remotely it's enough to use the Sysinternals Suite package available at <http://technet.microsoft.com/en-us/sysinternals>

**GAINING CONTROL OVER A TARGET COMPUTER ALLOWS AN ATTACKER TO:**

-  Run any program
-  Stop and launch any service
-  Modify system settings and program settings
-  Obtain passwords for all other users in the remote system

# WAYS TO **HIDE AND ATTACK**

## **IF IT IS EXECUTED WELL, THE ATTACK CAN REMAIN UNDETECTED**

Once attackers have full control over a system, preventing them from removing traces of the intrusion is very difficult.

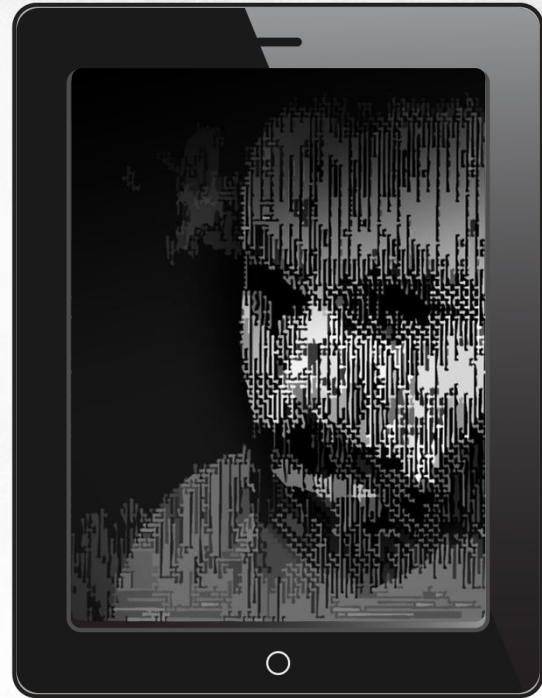
**WHILE WINDOWS USERS ACTIVITY MAY BE AUDITED AND RECORDED** in a security log, an attacker is able to turn off event auditing and wipe out security logs. To stop monitoring, it's enough to use AuditPol, a program included in the Resource Kit package, while to delete a security log, you may use for example ClearLogs (available at <http://ntsecurity.nu/toolbox>)



# WAYS TO **HIDE AND ATTACK**

**HOWEVER, AN EMPTY LOG IS A CLEAR SIGN OF AN INTRUSION**, and the attacker would probably prefer to remove only some specific entries. This can be done for example by running WinZipper on the attacked machine

**THE BEST TECHNIQUE ATTACKERS MAY USE TO ENSURE** they will be able to re-connect with the targeted computer is installing an additional service in the computer. Malicious services may be easily hidden behind either system services like svchosts or obfuscated by using a rootkit





**THANKS**

