

FORMAN CHRISTIAN COLLEGE (A CHARTERED UNIVERSITY)



COMP 421 (Information Security)

SECTION - B

2023 FALL

QUIZ # 5

NMAP: Live Host Discovery

Gulraiz Noor Bari (231-525536)

TASK # 1 – INTRODUCTION

100%

Task 1 Introduction

When we want to target a network, we want to find an efficient tool to help us handle repetitive tasks and answer the following questions:

1. Which systems are up?
2. What services are running on these systems?

The tool that we will rely on is `Nmap`. The first question about finding live computers is answered in this room. This room is the first in a series of four rooms dedicated to Nmap. The second question about discovering running services is answered in the next Nmap rooms that focus on port-scanning.

This room is the first of four in this `Nmap` series. These four rooms are also part of the Network Security module.

1. [Nmap Live Host Discovery](#)
2. [Nmap Basic Port Scans](#)
3. [Nmap Advanced Port Scans](#)
4. [Nmap Post Port Scans](#)

This room explains the steps that `Nmap` carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that `Nmap` uses to discover live hosts. In particular, we cover:

1. `ARP` scan: This scan uses ARP requests to discover live hosts
2. `ICMP` scan: This scan uses ICMP requests to identify live hosts
3. `TCP/UDP` ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

We also introduce two scanners, `arp-scan` and `masscan`, and explain how they overlap with part of Nmap's host discovery.

As already mentioned, starting with this room, we will use `Nmap` to discover systems and services actively. Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under GPL license. Nmap is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services. Nmap's scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities. A Nmap scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.

1

Enumerate targets

2

Discover live hosts

3

Reverse-DNS lookup

4

Scan ports

5

Detect versions

6

Detect OS

7

Traceroute

8

Scripts

9

Write output

Answer the questions below

Some of these questions will require the use of a static site to answer the task questions, while others require the use of the AttackBox and the target VM.

No answer needed

Question Done

TASK # 2 – SUBNETWORKS



The figure above shows two types of subnets:

- Subnets with `/16`, which means that the subnet mask can be written as `255.255.0.0`. This subnet can have around 65 thousand hosts.
- Subnets with `/24`, which indicates that the subnet mask can be expressed as `255.255.255.0`. This subnet can have around 250 hosts.

You might want to refer to Task 2 in the [Intro to LAN](#) room if you need to learn more about subnetting.

As part of active reconnaissance, we want to discover more information about a group of hosts or about a subnet. If you are connected to the same subnet, you would expect your scanner to rely on ARP (Address Resolution Protocol) queries to discover live hosts. An ARP query aims to get the hardware address (MAC address) so that communication over the link-layer becomes possible; however, we can use this to infer that the host is online. (We revisit link-layer in Task 4.)

If you are in Network A, you can use ARP only to discover the devices within that subnet (10.1.100.0/24). Suppose you are connected to a subnet different from the subnet of the target system(s). In that case, all packets generated by your scanner will be routed via the default gateway (router) to reach the systems on another subnet; however, the ARP queries won't be routed and hence cannot cross the subnet router. ARP is a link-layer protocol, and ARP packets are bound to their subnet.

Click on the "View Site" button to start the network simulator. We will use this simulator to answer the questions in tasks 2, 4, and 5.

Answer the questions below

Send a packet with the following:

Send Packet

From:
computer1

To:
computer1

Packet Type:
arp_request

Data:
computer6

Send Packet

- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

Correct Answer

Hint

Did computer6 receive the ARP Request? (Y/N)

N

Correct Answer

Send a packet with the following:

Send Packet

From:
computer4

To:
computer4

Packet Type:
arp_request

Data:
computer6

Send Packet

- From computer4
- To computer4 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

Correct Answer

Hint

Did computer6 reply to the ARP Request? (Y/N)

Y

Correct Answer

TASK # 3 – ENUMERATING TARGETS

Try Hack Me

Dashboard

Learn

Compete

Other

Access Machines

Go Premium

1

2856

SCANNING FOR TARGET...

Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

Start AttackBox

Help

100%

Task 1 Introduction

Task 2 Subnetworks

Task 3 Enumerating Targets

We mentioned the different *techniques* we can use for scanning in Task 1. Before we explain each in detail and put it into use against a live target, we need to specify the targets we want to scan. Generally speaking, you can provide a list, a range, or a subnet. Examples of target specification are:

- list: `MACHINE_IP scanme.nmap.org example.com` will scan 3 IP addresses.
- range: `10.11.12.15-20` will scan 6 IP addresses: `10.11.12.15`, `10.11.12.16`, ..., and `10.11.12.20`.
- subnet: `MACHINE_IP/30` will scan 4 IP addresses.

You can also provide a file as input for your list of targets, `nmap -iL list_of_hosts.txt`.

If you want to check the list of hosts that Nmap will scan, you can use `nmap -sL TARGETS`. This option will give you a detailed list of the hosts that Nmap will scan without scanning them; however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain their names. Names might reveal various information to the pentester. (If you don't want Nmap to the DNS server, you can add `-n`.)

Launch the AttackBox using the Start AttackBox button, open the terminal when the AttackBox is ready, and use Nmap to answer the following.

Answer the questions below

What is the first IP address Nmap would scan if you provided `10.10.12.13/29` as your target?

Correct Answer

Hint

How many IP addresses will Nmap scan if you provide the following range `10.10.0-255.101-125` ?

Correct Answer

Hint

Task 4 Discovering Live Hosts

Task 5 Nmap Host Discovery Using ARP

Task 6 Nmap Host Discovery Using ICMP

Task 7 Nmap Host Discovery Using TCP and UDP

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

Created by tryhackme and strategos

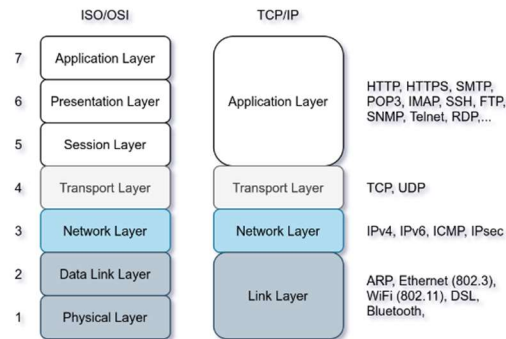
This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 128202 users are in here and this room is 822 days old.

TASK # 4 – DISCOVERING LIVE HOSTS

Task 4 🟢 Discovering Live Hosts

Let's revisit the TCP/IP layers shown in the figure next. We will leverage the protocols to discover the live hosts. Starting from bottom to top, we can use:

- ARP from Link Layer
- ICMP from Network Layer
- TCP from Transport Layer
- UDP from Transport Layer



Before we discuss how scanners can use each in detail, we will briefly review these four protocols. ARP has one purpose: sending a frame to the broadcast address on the network segment and asking the computer with a specific IP address to respond by providing its MAC (hardware) address.

ICMP has many types. ICMP ping uses Type 8 (Echo) and Type 0 (Echo Reply).

If you want to ping a system on the same subnet, an ARP query should precede the ICMP Echo.

Although TCP and UDP are transport layers, for network scanning purposes, a scanner can send a specially-crafted packet to common TCP or UDP ports to check whether the target will respond. This method is efficient, especially when ICMP Echo is blocked.

If you have closed the network simulator, click on the "View Site" button in Task 2 to display it again.

Answer the questions below

Send a packet with the following:

- From computer1
- To computer3
- Packet Type: "Ping Request"

What is the type of packet that computer1 sent before the ping?

ARP Request

Correct Answer

What is the type of packet that computer1 received before being able to send the ping?

ARP Response

Correct Answer

How many computers responded to the ping request?

1

Correct Answer

Send a packet with the following:

- From computer2
- To computer5
- Packet Type: "Ping Request"

What is the name of the first device that responded to the first ARP Request?

router

Correct Answer

What is the name of the first device that responded to the second ARP Request?

computer5

Correct Answer

Send another Ping Request. Did it require new ARP Requests? (Y/N)

N

Correct Answer

TASK # 5 – NMAP HOST DISCOVERY USING ARP

02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	ARP Announcement for 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.12? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.13? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.14? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.15? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.16? Tell 10.10.210.6

Address Resolution Protocol: Protocol Packets: 1207 · Displayed: 512 (42.4%) Profile: Default

If you have closed the network simulator, click on the "Visit Site" button in Task 2 to display it again.

Answer the questions below

We will be sending broadcast ARP Requests packets with the following options:

- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

How many devices are you able to discover using ARP requests?

Correct Answer

Task 6 Nmap Host Discovery Using ICMP

Task 7 Nmap Host Discovery Using TCP and UDP

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 128202 users are in here and this room is 822 days old.

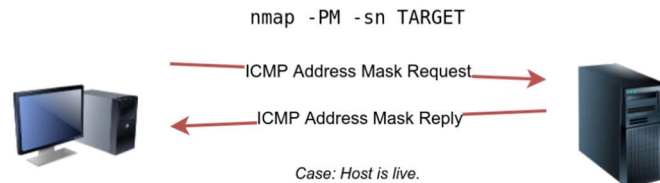


TASK # 6 – NMAP LIVE DISCOVERY USING ICMP

10.11.35.214	10.10.68.7	ICMP	Timestamp request	id=0x5de2, seq=0/0, ttl=
10.11.35.214	10.10.68.8	ICMP	Timestamp request	id=0x884d, seq=0/0, ttl=
10.11.35.214	10.10.68.9	ICMP	Timestamp request	id=0xb735, seq=0/0, ttl=
10.11.35.214	10.10.68.10	ICMP	Timestamp request	id=0x6b44, seq=0/0, ttl=
10.11.35.214	10.10.68.1	ICMP	Timestamp request	id=0x1a28, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Timestamp request	id=0x8586, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Timestamp request	id=0xacce, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Timestamp request	id=0xcfa, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Timestamp request	id=0xa39f, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Timestamp request	id=0x2279, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Timestamp request	id=0x884d, seq=0/0, ttl=

nmmap-PP-sn-openvpn.pcapng Packets: 1131 · Displayed: 512 (45.3%) Profile: Default

Similarly, Nmap uses address mask queries (ICMP Type 17) and checks whether it gets an address mask reply (ICMP Type 18). This scan can be enabled with the option `-PM`. As shown in the figure below, live hosts are expected to reply to ICMP address mask requests.



In an attempt to discover live hosts using ICMP address mask queries, we run the command `nmmap -PM -sn MACHINE_IP/24`. Although, based on earlier scans, we know that at least eight hosts are up, this scan returned none. The reason is that the target system or a firewall on the route is blocking this type of ICMP packet. Therefore, it is essential to learn multiple approaches to achieve the same result. If one type of packet is being blocked, we can always choose another to discover the target network and services.

```
Pentester Terminal

pentester@TryHackMe$ sudo nmmap -PM -sn 10.10.68.220/24

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 12:13 EEST
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.17 seconds
```

Although we didn't get any reply and could not figure out which hosts are online, it is essential to note that this scan sent ICMP address mask requests to every valid IP address and waited for a reply. Each ICMP request was sent twice, as we can see in the screenshot below.

Source	Destination	Protocol	Info
10.11.35.214	10.10.68.1	ICMP	Address mask request id=0xa3c4, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request id=0xb793, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request id=0x2d87, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request id=0x091c, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request id=0x692c, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request id=0x4bec, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request id=0x4d61, seq=0/0, ttl=
10.11.35.214	10.10.68.8	ICMP	Address mask request id=0xb84f, seq=0/0, ttl=
10.11.35.214	10.10.68.9	ICMP	Address mask request id=0x7d19, seq=0/0, ttl=
10.11.35.214	10.10.68.10	ICMP	Address mask request id=0x92be, seq=0/0, ttl=
10.11.35.214	10.10.68.1	ICMP	Address mask request id=0xd204, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request id=0x683d, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request id=0x2711, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request id=0xfde3, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request id=0x2eb1, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request id=0x8300, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request id=0x7100, seq=0/0, ttl=

nmmap-PM-sn-openvpn.pcapng Packets: 1178 · Displayed: 512 (43.5%) Profile: Default

Answer the questions below

What is the option required to tell Nmap to use ICMP Timestamp to discover live hosts?

-PP

Correct Answer

What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

-PM

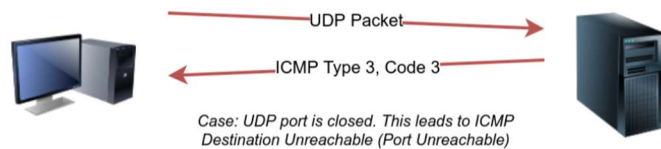
Correct Answer

What is the option required to tell Nmap to use ICMP Echo to discover live hosts?

-PE

Correct Answer

TASK # 7 – NMAP LIVE DISCOVERY USING TCP AND UDP

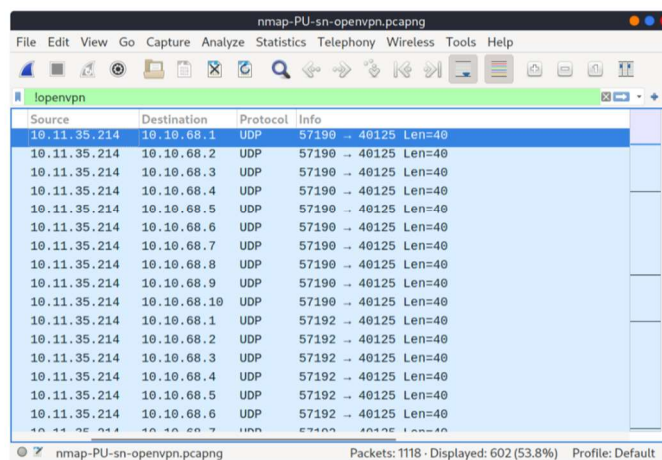


The syntax to specify the ports is similar to that of TCP SYN ping and TCP ACK ping; Nmap uses `-PU` for UDP ping. In the following example, we use a UDP scan, and we discover five live hosts.

```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -PU -sn 10.10.68.220/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:45 EEST
Nmap scan report for 10.10.68.52
Host is up (0.10s latency).
Nmap scan report for 10.10.68.121
Host is up (0.10s latency).
Nmap scan report for 10.10.68.125
Host is up (0.14s latency).
Nmap scan report for 10.10.68.134
Host is up (0.096s latency).
Nmap scan report for 10.10.68.220
Host is up (0.11s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 9.20 seconds
```

Let's inspect the UDP packets generated. In the following Wireshark screenshot, we notice Nmap sending UDP packets to UDP ports that are most likely closed. The image below shows that Nmap uses an uncommon UDP port to trigger an ICMP destination unreachable (port unreachable) error.



Masscan

On a side note, Masscan uses a similar approach to discover the available systems. However, to finish its network scan quickly, Masscan is quite aggressive with the rate of packets it generates. The syntax is quite similar: `-p` can be followed by a port number, list, or range. Consider the following examples:

- `masscan MACHINE_IP/24 -p443`
- `masscan MACHINE_IP/24 -p80,443`
- `masscan MACHINE_IP/24 -p22-25`
- `masscan MACHINE_IP/24 --top-ports 100`

Masscan is not installed on the AttackBox; however, it can be installed using `apt install masscan`.

Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

Correct Answer

Which TCP ping scan requires a privileged account?

TCP ACK Ping

Correct Answer

What option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port?

-PS23

Correct Answer

Hint

TASK # 8 – USE REVERSE-DNS LOOKUP

DashboardLearnCompeteOtherAccess MachinesGo Premium1



Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

2856Start AttackBoxHelpSettingsBookmarkInformation Sector

100%

Task 1 Introduction

Task 2 Subnetworks

Task 3 Enumerating Targets

Task 4 Discovering Live Hosts

Task 5 Nmap Host Discovery Using ARP

Task 6 Nmap Host Discovery Using ICMP

Task 7 Nmap Host Discovery Using TCP and UDP

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

Nmap's default behaviour is to use reverse-DNS on live hosts. Because the hostnames can reveal a lot, this can be a helpful step. However, if you don't want to send such DNS queries, you use `-n` to skip this step.

By default, Nmap will look up online hosts; however, you can use the option `-R` to query the DNS server even for offline hosts. If you want to use a specific DNS server, you can add the `--dns-servers DNS_SERVER` option.

Answer the questions below

We want Nmap to issue a reverse DNS lookup for all the possible hosts on a subnet, hoping to get some insights from the names. What option should we add?

Correct Answer

Created by  tryhackme and  strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 128202 users are in here and this room is 822 days old.



TASK # 9 – SUMMARY

Try Hack Me

DashboardLearnCompeteOther

Access Machines

Go Premium

1

2856

Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

Start AttackBoxHelp

SCANNING FOR TARGET...

10 10 1110 101 01

100%

Task 1 Introduction

Task 2 Subnetworks

Task 3 Enumerating Targets

Task 4 Discovering Live Hosts

Task 5 Nmap Host Discovery Using ARP

Task 6 Nmap Host Discovery Using ICMP

Task 7 Nmap Host Discovery Using TCP and UDP

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

You have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room. Any response from a host is an indication that it is online. Below is a quick summary of the command-line options for Nmap that we have covered.

Scan Type	Example Command
ARP Scan	<code>sudo nmap -PR -sn MACHINE_IP/24</code>
ICMP Echo Scan	<code>sudo nmap -PE -sn MACHINE_IP/24</code>
ICMP Timestamp Scan	<code>sudo nmap -PP -sn MACHINE_IP/24</code>
ICMP Address Mask Scan	<code>sudo nmap -PM -sn MACHINE_IP/24</code>
TCP SYN Ping Scan	<code>sudo nmap -PS22,80,443 -sn MACHINE_IP/30</code>
TCP ACK Ping Scan	<code>sudo nmap -PA22,80,443 -sn MACHINE_IP/30</code>
UDP Ping Scan	<code>sudo nmap -PU53,161,162 -sn MACHINE_IP/30</code>

Remember to add `-sn` if you are only interested in host discovery without port-scanning. Omitting `-sn` will let Nmap default to port-scanning the live hosts.

Option	Purpose
<code>-n</code>	no DNS lookup
<code>-R</code>	reverse-DNS lookup for all hosts
<code>-sn</code>	host discovery only

Answer the questions below


Ensure you have taken note of all the Nmap options explained in this room. To continue learning about Nmap, please join the room [Nmap Basic Port Scans](#), which introduces the basic types of port scans.

No answer neededQuestion Done

Created by [tryhackme](#) and [strategos](#)

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 128202 users are in here and this room is 822 days old.

PROFILE SCREENSHOT




DashboardLearnCompeteOther


Search

Notifications

Go Premium

2





431897

Rank

6

Rooms Complete

3

Level

1

Badges

gulraizzz.exe [0x3]



Get Profile Badge ID

Share Room Badges

Rooms Complete

Badges

Created Rooms

Yearly Activity

Tickets



Burp Suite: The...
An introduction to using Burp Suite for web...



Red Team...
Learn the steps and procedures of a red team...



Nmap Live Host...
Learn how to use Nmap to discover live hosts using...



Metasploit:...
An introduction to the main components of the...



Pentesting...
Learn the important ethics and methodologies behind...



Principles of...
Learn the principles of information security that...

