Meow

▼ To-do List

- [ ] Finish Q&A
- [ ] Write page on telnet → Network+
- [ ] Write page on VPNs → Network+

▼ Table Of Contents

▼ Collected Q&A

▼ What is a Security Gateway (context of VPN)

Dedicated check-point server that runs check-point software to inspect traffic and enforce security policies for connected network resources

▼ What is IPSec

▼ What are IPSec profiles?

▼ What is a security association (SA)?

The establishment of shared security attributes between network entities is called security association and is used for secure communication.

An SA may include:

- cryptographic algorithm and mode
- traffic encryption key
- parameters for network data to be passed over connection

The necessary framework for establishing a SA is provided by the Internet Security Association and Key Management Protocol (ISAKMP)

▼ What is an ICMP Packet?

▼ Module Questions

▼ **What does the acronym VM stand for?**

→ Acronym VM stands for [virtual machine]

What is a VM?

A virtual machine is a compute resource that uses software instead of physical hardware to run an OS, programs, … . Multiple guest machines can run in one single host machine. Each VM runs its own operating system and functions separately from other VMs and host.

What are VMs used for?

Allows to run an OS that behaves completely sseparate computer. Possible use-cases for VMs:

- accommodating different levels of processing power needs
- run software that requires a different OS

- test applications in safe, sandbox environment

in ethical Hacking:

- ability to bring it back to a known state
- isolation of services
    - you can try things out without fear of destroying something valuable
- isolate infected apps / files
- preventing spread of malicious software

> Since the VM is separated from the rest of the system, the sotware inside the VM cannot tamper with the host computer.

How do VMs work?

The VM runs as a process in an application window on the OS of the physical machine. Key files that make up a VM are:

- log files
- NVRAM setting file
- virtual disk file
- configuration file

Advantages and disadvantages of VMs

Advantages:

1. easy to manage and maintain
2. can run multiple OS environments on a single host cmputer
    a. saves physical space, time and management costs

Disadvantages:

1. running multiple VMs on one physical machine can result in unstable performance if infrastructure requirements aren't met
2. less efficient and slower than physical computers

3. support legacy applications
    a. reducing cost of OS migration
4. can also provide integrated disaster recovery and application provisioning options

Two types of VM

Process VM

- allows single process to run as an application on a host machine
    - platform-independent programming environment by masking the info of the underlying hardware/OS
- example: Java virtual machine, which enables any OS to run Java applications as if they were native

System VM

- fully virtualized to substitute physical machine
- supports sharing physical resources of the host to multiple VMs - ofc each running its own OS
- relies on a hypervisor, which can run on bare hardware or on top of an OS

Hypervisor

Types of virtualization

Hardware virtualization

- aka server virtualization
- virtual versions of computers and OS - VMs - are created in a single physical server
- hypervisor communicates directly with the physical server’s disk space and CPU to manage VMs

- allows hardware resources to be utilized more efficiently and for one machine to simultaneously run different OSs

Software virtualization

- Physical host run its own OS
- on top of that runs a guest operating system in a VM
    - utilizes the same hardware as the host machine
- Applications can be virtualized and delivered from a server to an end user's device - i.e. workstation or pohone.
    - allows employees to access centrally hosted applications

Storage virtualization

- storage can be virtualized to appear as one single storage device, although it is made of multiple devices

Benefits:

- increased performance and speed
- load balancing
- reduced costs
- helps with disaster recovery planning
    - virtual storage data can be duplicated and quickly transferred
    - reduces downtime!

Network virtualization

- multiple sub-networks on the same physical networks
    - achieved by combining equipment into a single, sonftware-based virtual network resource
- divides available bandwidth into multiple, independent channels
    - can be assigned to servers and devices in real time

Benefits:

- increased reliability

- network speed, security
- monitoring of data usage

Desktop virtualization

- separates the desktop env from the physical device and stores a desktop on a remote server
    - allows user to access their desktops from anywhere on any device

Benefits:

- easy accessibility
- better data security
- cost savings on software licenses and updates
- ease of management

▼ **What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.**

→ Terminal; more Info

▼ **What service do we use to form our VPN connection into HTB labs?**

→ OpenVPN

What is OpenVPN

OpenVPN is a VPN system that implements techniques to create secure point-to-point or site-to-site systems in routed or bridged configurations and remote access facilities. It implements both client and server applications.

Wikipedia Entry

▼ **What is the abbreviated name for a 'tunnel interface' in the output of your VPN boot-up sequence output?**

→ tun

```
$ ifconfig # used to show network interfaces
```

```
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::2b8a:97f9:ed36:a721%utun0 prefixlen 64 scopeid 0x13
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::9265:ad11:12c8:a751%utun1 prefixlen 64 scopeid 0x14
        nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
        inet6 fe80::ce81:b1c:bd2c:69e%utun2 prefixlen 64 scopeid 0x15
        nd6 options=201<PERFORMNUD,DAD>
utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::7f35:8caf:71d3:90b2%utun3 prefixlen 64 scopeid 0x16
        nd6 options=201<PERFORMNUD,DAD>
utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::aff3:b096:9832:80bf%utun4 prefixlen 64 scopeid 0x17
        nd6 options=201<PERFORMNUD,DAD>
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1420
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVE
RT_CSUM>
        inet 10.2.0.2 --> 10.2.0.2 netmask 0xffffffff
utun6: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::985a:83c9:afe7:799f%utun6 prefixlen 64 scopeid 0x19
        nd6 options=201<PERFORMNUD,DAD>
utun7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet 10.10.16.202 --> 10.10.16.202 netmask 0xfffffe00
        inet6 fe80::bed0:74ff:fe50:69c3%utun7 prefixlen 64 scopeid 0x1a
        inet6 dead:beef:4::10c8 prefixlen 64
        nd6 options=201<PERFORMNUD,DAD>
```

VPN Tunnel Interfaces

Configuring a virtual tunnel interface (VTI) enables the creation of a VPN tunnel between peers. This supports route-based VPN with IPSec profiles attached to the end of each tunnel - allows static & dynamic routes to be used. VTI traffic traveling between the peers are encrypted and gets decrypted by the associated security association.

With VTIs, the tracking of all remote subnets and inclusion in crypto map access lists is no longer needed. Deployments becomes easier and having a static VTI which supports route based VPN with dynamic routing protocols also satisfies many requirements of a VPC → virtual private cloud.

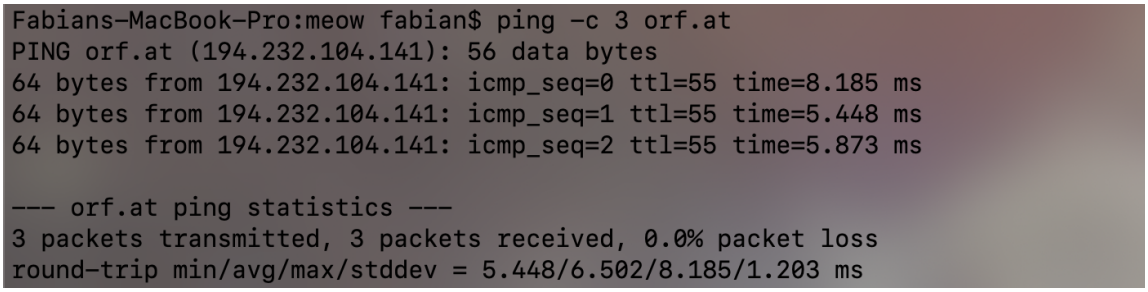
▼ **What tool do we use to test our connection to the target with an ICMP echo request?**

→ ping

Ping

The general utility tool in Linux called Ping is short for **Packet Internet Groper** and is mainly used for checking network connectivity. The command takes the URL or IP address as input and transfers the data packet to a specified address along with a “PING” message. The time between sending the request and receiving a response is known as latency.

```
$ ping [options] <hostname>/<ip>
```



from	target ip
ttl	time to live from 1-255
icmp_seq	ICMP sequence number
time	time to reach the target and comming back to origin

Important flags

- ping -4 OR -6 <ip>; for restricting to IPv4 or IPv6
- sudo ping -f <ip>; ping flood - simulates high network usage and can be used for performance testing
- ping -s <size> <ip>; change size of ICMP packet
- ping -w <time> <ip>; fixed time limit
- ping -c <value> <ip>; fixed request limit

▼ **What is the name of the most common tool for finding open ports on a target?**

→ nmap

TODO link to nmap

▼ **What service do we identify on port 23/tcp during our scans?**

→ telnet

TODO: write page on Telnet

▼ **What username is able to log into the target over telnet with a blank password?**

→ root

TODO: find out how to see this information with nmap. I think there was a way to do that

---

▼ Pawn walkthrough

```
$ telnet <ip>
```

```
Moew login: root
```

```
cat flag.txt
# b40abdfe23665f766f9c61ecba8a4c19
```

```
parallels@ubuntu-linux-22-04-desktop:~$ telnet 10.129.148.150
Trying 10.129.148.150...
Connected to 10.129.148.150.
Escape character is '^]'.
```


```
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 06 Mar 2023 11:05:08 PM UTC

  System load:           0.0
  Usage of /:            41.7% of 7.75GB
  Memory usage:          5%
  Swap usage:            0%
  Processes:             145
  Users logged in:       1
  IPv4 address for eth0: 10.129.148.150
  IPv6 address for eth0: dead:beef::250:56ff:fe96:13f3

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet co
nnection or proxy settings


Last login: Mon Mar  6 23:04:30 UTC 2023 on pts/0
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```