FIT5037 Network Security Assignment
Total Marks 100

Due on Sunday, 4 August 2024, 11:55 PM.

1 Overview

The learning objective of this assignment is for you to gain a first-hand experience on network attacks (i.e., TCP and DNS attacks) and get a deeper understanding on how to launch these attacks in practice. All tasks in this assignment can be done on the virtual machine used in the labs.

2 Submission Policy

You need to submit a lab report (one single PDF file) to describe what you have done and what you have observed with screen shots whenever necessary; you also need to provide explanation or codes to the observations that are related to the tasks. In your report, you are expected to answer all the questions listed in this manual. Typeset your report into .pdf format (make sure it can be opened with Adobe Reader) and name it as the format:
[Your Name]- 37-Assignment.pdf.

All source code tion video is required,
you should reco video to
your Monash G **inutes in total**
duration; you a **wing face is**
mandatory. The uired. You can
use any tool you
`panopto.aarne`

Late submissi tion, the application
should be subm
plagiarism: If yo it. The demonstration
video is also use
`https://www.m`

3 Environ

In this section, will be using the
Topic 6 - Week

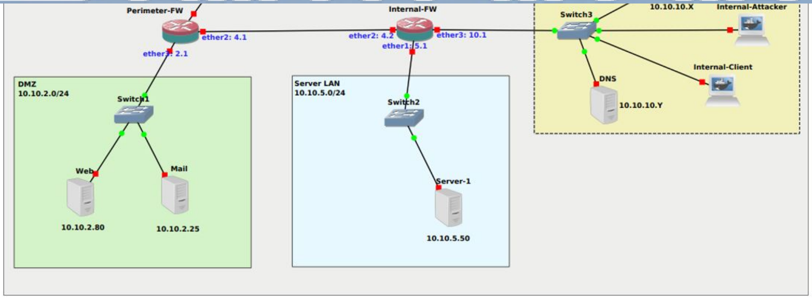


Figure 1: GNS3 Config

Otherwise, if you don't have the VM ready, we refer you to Environment Setup in Week 01. It is recommended to perform lab tasks of Topic 6 - Week 5A before proceeding.

4 TCP Attacks – Using Scapy [40 Marks]

The Transmission Control Protocol (TCP) is a core protocol of the Internet protocol suite. It sits on top of the IP layer, and provides a reliable and ordered communication channel between applications running on networked computers. TCP is in a layer called Transport layer, which provides host-to-host communication services for applications. To achieve such reliable and order communication, TCP requires both ends of a communication to maintain a connection. Unfortunately, when TCP was developed, no security mechanism was built into this protocol, making it possible for attackers to eavesdrop on connections, break connections or hijack connections. In this section, you are required to perform these attacks using Scapy—a packet manipulation tool for computer networks written in Python.

4.1 Task 1: TCP Reset Attacks [15 Marks]

In the stream of packets of a TCP connection, each packet contains a TCP header. In the header, there is a bit known as the "reset" (RST) flag. In most packets, this bit is set to 0 and has no effect; however, if this bit is set to 1, it indicates that the receiver should immediately stop using the TCP connection. That means it should not send back any more packets using the connection's identifying numbers, called ports,
and discard any
cally kills a
TCP connectio

It is possible fo
ection and then
send a "forged"
he forged packet
must indicate, f
udes the
endpoint IP add
set to a
convincing forg
ction.

The idea is quit
st spoofs a TCP
RST packet fro

Q1: Connect
all ssh if SSH
is not install
P RST attack,
from Interna
acket generator.
Internal-Cli
our python code
and the steps,
ython code: 5
marks, expla

Q2: Briefly e
easures. You do
not have to d
arks, counter-
measures: 2.

4.2 Task 2: T

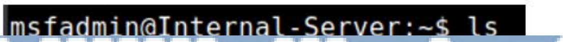
Once a TCP cli
ablished, and we
call it a TCP se
uter can have
multiple concurrent TCP sessions with other computers, when it receives a packet, it needs to know which TCP session the packet belongs to. TCP uses four elements to make that decision, i.e., to uniquely identify a session: (1) source IP address, (2) destination IP address, (3) source port number, and (4) destination port number.

We call these four fields as the signature of a TCP session. As we have already learned, spoofing packets is not difficult. What if we spoof a TCP packet, whose signature matches that of an existing TCP session on the target machine? Will this packet be accepted by the target? Clearly, if the above four elements match with the signature of the session, the receiver cannot tell whether the packet comes from the real sender or an attacker, so it considers the packet as belonging to the session.

However, for the packet to be accepted, one more critical condition needs to be satisfied. It is the TCP sequence number. TCP is a connection-oriented protocol and treats data as a stream, so each octet in the TCP session has a unique sequence number, identifying its position in the stream. The TCP header contains a 32-bit sequence number field, which contains the sequence number of the first octet in the payload. When the receiver gets a TCP packet, it places the TCP data (payload) in a buffer; where exactly the payload is placed inside the buffer depends on the sequence number. This way, even if TCP packets arrive out of order, TCP can always place their data in the buffer using the correct order.

The objective of this task is to hijack an existing TCP connection (session) between client and server by injecting malicious contents into their session.

Q3: Connect TELNET from `Internal-Client` to `Internal-Server`, the username and password are same: `msfadmin`. Write a python code, using Scapy, which can inject packets in the TELNET communication, the goal is to make a directory called "attacker" at the `Internal-Server` (as seen in the screenshot below). You can use `Internal-Attacker` workstation to run the python code. Submit python code and steps, along with video link that demonstrates you have performed the attack. **(Python code: 5 marks, explanation during recording demonstration: 5 marks)**



```
msfadmin@Internal-Server:~$ ls
```

Q4: Connect
shell from `Int`
back to the at
research abou
Write a pytho
reverse shell fr
the `Internal-`
showing that y
demonstrati

to get a reverse
hine, connecting
rage students to
`-cf154dfee6bd`.
on and create a
low, in this case
with video link
ring recording

Q5: Connect
`msfadmin`. Pe
`Internal-Ser`
SSH connectic
link showing t
detail. **(Python Code and Explanation during recording demonstration: 5 marks)**

sword are same:
cker directory in
`ker` by hijacking
along with video
ain the reason in

5 DNS Attacks – Using Scapy [60 Marks]

Domain Name System (DNS) is an essential component of the Internet infrastructure. It serves as the phone book for the Internet, so computers can look up for "telephone number" (i.e. IP addresses) from domain names. Without knowing the IP address, computers will not be able to communicate with one another. Due to its importance, the DNS infrastructure faces frequent attacks. In this section, you will explore the most primary attack on DNS. That is DNS cache poisoning by investigating both Local and Remote DNS cache poisoning attacks.

Due to the large number of computers and networks on the Internet, the domain namespace is organised in a hierarchical tree-like structure. Each node on the tree is called a domain or sub-domain when referencing to its parent node. The following figure depicts a part of the domain hierarchy.

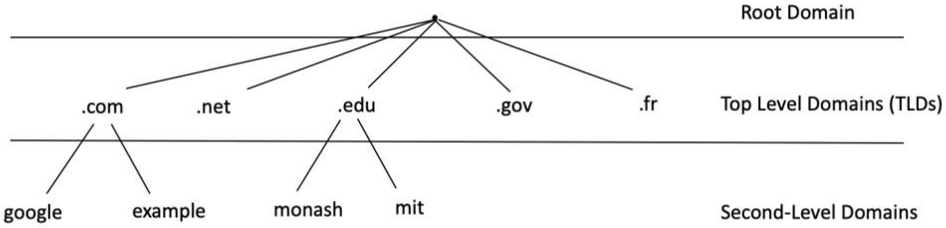


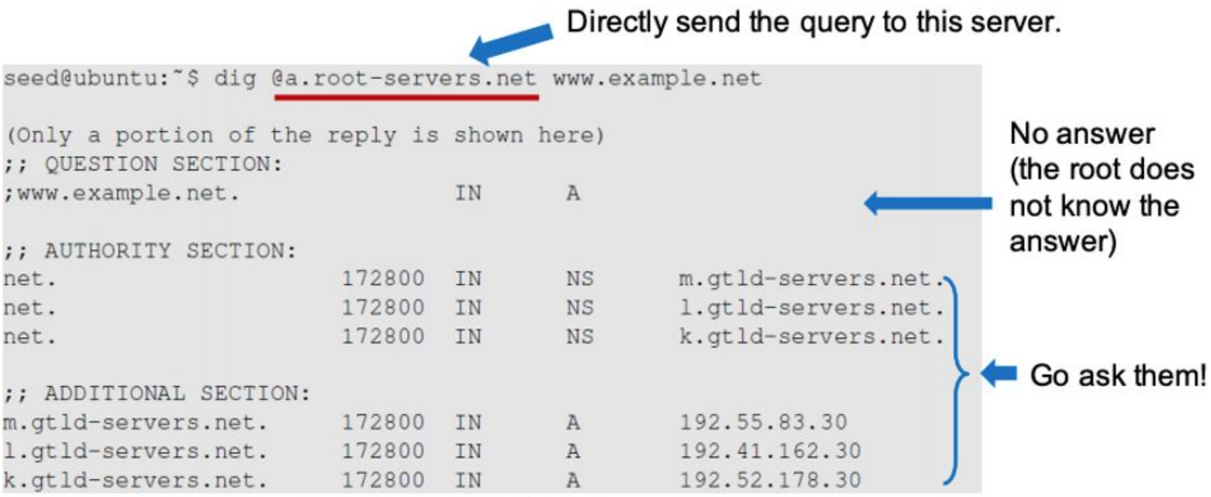
Figure 4: Domain hierarchy

The domain hierarchy tree structure describes how the domain namespace is organised, but that is not exactly how the domain name systems are organised. Domain name systems are organised according to zones. A DNS zone basically groups contiguous domains and sub-domains on the domain tree, and assign the management authority to an entity. Each zone is managed by an authority, while a domain does not indicate any authority information. The following figure depicts an example of the `example.com` domain.

Assume that `ex`
all over the
world, so the co
`a.example.com`,
`uk.example.co`
ided into
`chicago`, `bosto`

Each DNS zone
t that zone. The
goal of a DNS c
s why they are
called authorita
es, as opposed to
obtaining the a

With such arrar
the authority is
for each of its s
hes in different
countries and e
ountry manages
its own DNS in
swer, it will ask
other DNS servers on the Internet for answer via hierarchical authority servers. The following example demonstrates a dig (DNS query) for the domain www.example.net when sending the query directly to one of the root server (i.e. `a.root-servers.net`).



Directly send the query to this server.

```
seed@ubuntu:~$ dig @a.root-servers.net www.example.net

(Only a portion of the reply is shown here)
;; QUESTION SECTION:
;www.example.net.              IN      A

;; AUTHORITY SECTION:
net.                   172800  IN      NS      m.gtld-servers.net.
net.                   172800  IN      NS      l.gtld-servers.net.
net.                   172800  IN      NS      k.gtld-servers.net.

;; ADDITIONAL SECTION:
m.gtld-servers.net.    172800  IN      A       192.55.83.30
l.gtld-servers.net.    172800  IN      A       192.41.162.30
k.gtld-servers.net.    172800  IN      A       192.52.178.30
```

No answer (the root does not know the answer)

Go ask them!

Figure 6: DIG to the root server

There are four t
additional secti
(because the rep
net zone (the N
section). If you
you will finally
for `www.exampl`

rity section, and
he answer
neservers for the
n the *additional*
nameservers,
ing the website

When your loca
same informatio

nation, so if the

5.1 Task 3: I

s]

We recalled tha
additional secti
our Topic 6 - W
section by provi
is cached, when
a request to the
hostnames in th
`example.net` ar

on, and
me (as we did in
authority
e fake NS record
ain, it will send
affect all the
server of

Q6: Submit y
attack that mo
Use `Internal`
marks). If th
authoritative s

he DNS spoofing
`.attacker.com`.
thon code: 10
ch the malicious