Διαχείριση Δικτύων – Ευφυή Δίκτυα

ΟΝΟΜΑ: ΠΑΠΑΔΟΠΟΥΛΛΟΣ ΜΙΧΑΛΗΣ
Α.Μ: 03114702
ΟΝΟΜΑ: ΚΑΡΔΑΡΗΣ ΧΑΡΑΛΑΜΠΟΣ
Α.Μ: 03114074

ΟΜΑΔΑ: netmg034

4η Ομάδα Ασκήσεων

Άσκηση 1

Στο αρχείο trace_b.cap έχουν καταγραφεί τα πακέτα που πέρασαν από τον κόμβο **cornuto.netmode.ece.ntua.gr** σε ένα χρονικό διάστημα κάποιων δευτερολέπτων. Για την καταγραφή των πακέτων χρησιμοποιήθηκε το πρόγραμμα tcpdump. Στο διάστημα αυτό έτρεξαν τέσσερις εντολές ping, και ζητήθηκαν πληροφορίες DNS από τον Name Server **ulysses.noc.ntua.gr**. Με τη χρήση του προγράμματος wireshark αναζητήστε στο παραπάνω αρχείο τις απαντήσεις στα παρακάτω ερωτήματα:

- Ο διαχειριστής του cornuto.netmode.ntua.gr έσβησε τον πίνακα ARP του κόμβου και στην συνέχεια πραγματοποίησε δύο ping ερωτήματα. Σε ποιους κόμβους - προορισμούς (IP address & DNS name) έγιναν τα ping ερωτήματα (τα δύο πρώτα); Τι πληροφορίες - πακέτα ανταλλάχθηκαν πριν την πραγματοποίηση των ping ερωτημάτων; Εξηγήστε

  Αρχικά, βρίσκουμε τη διεύθυνση IP του μηχανήματος
  (cornuto.netmode.ece.ntua.gr => 147.102.13.30)

  Εφαρμόζουμε φίλτρο (**icmp.type==8**) ώστε να εμφανιστούν μονο τα πακετα ενδιαφέροντος:

  netmg034@maria ~> host 147.102.13.1
  1.13.102.147.in-addr.arpa domain name pointer averel.netmode.ece.ntua.gr.

  Πριν την πραγματοποίηση του παραπάνω ping request ο ο κόμβος έκανε ένα arp request για τη διεύθυνση 147.102.13.1 με σκοπό να μάθει την MAC διεύθυνση

  Wireshark →
  35 7.423929 AsustekC_ba:d1:41 Broadcast ARP 42 Who has 147.102.13.1? Tell 147.102.13.30

  netmg034@maria ~> host 192.108.114.2
  Host 2.114.108.192.in-addr.arpa. not found: 3(NXDOMAIN)
  >> IP: 192.108.114.2, Name: duth.gr

  Πριν την πραγματοποίηση του παραπάνω ping request ο ο κόμβος έκανε ένα dns request προς τον κόμβο 147.102.13.10 που είναι name server για το όνομα www.duth.gr με σκοπό να μάθει την IP διεύθυνση του.

Wireshark →
66 13.430757 147.102.13.30 147.102.13.10 DNS 71 Standard query 0xd941 A www.duth.gr

Τα παρακάτω είναι τα άλλα 2 ping requests.

netmg034@maria ~> host 195.134.71.229
Host 229.71.134.195.in-addr.arpa. not found: 3(NXDOMAIN)
>> IP: 195.134.71.229, Name: sites.uoa.gr
netmg034@maria ~> host 155.207.1.12
12.1.207.155.in-addr.arpa domain name pointer www.ccf.auth.gr.

- Τι πληροφορία ζητήθηκε από τον Name Server ulysses.noc.ntua.gr; Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε; Καταγράψτε τα identification numbers της IP επικεφαλίδας των πακέτων της απάντησης. Αποτέλεσμα ποιας εντολής είναι η ακουλουθία των πακέτων;

  Εφαρμόζουμε κατάλληλο φίλτρο (ip.dst==147.102.222.230) και παρατηρουμε ότι στάληκε αίτημα **ZONE-TRANSFER (AXFR)** για το domain: netmode.ece.ntua.gr.

  Το πακέτο όπως φαίνεται στο wireshark:
  110 0.000055 147.102.13.30 147.102.222.230 DNS 105 Standard query 0x20e4 AXFR netmode.ece.ntua.gr

  Το πρωτόκολλο που χρησιμοποιήθηκε είναι το DNS για την ερώτηση:
  dig @ulysses.noc.ntua.gr netmode.ece.ntua.gr

  DNS Query:
  Identification: 0x7ad6 (31446)
  DNS Response:
  Identification: 0xb25b (45659)

- Αναφορικά με το ping στον κόμβο www.uoa.gr: Τι πληροφορία ενθυλακώθηκε στην απάντηση του ερωτήματος; Εξηγήστε. Αποτέλεσμα ποιας εντολής είναι η ακολουθία των πακέτων;

  Στην απάντηση που λαμβάνουμε απο τον κόμβο 195.134.71.229 ενθυλακώνονται στο πακέτο IP στο πεδίο *options* πληροφορίες για τη **διαδρομή του πακέτου**.
  Συνεπώς εκτελέστηκε η εντολή: **ping -R uoa.gr**
  ntua-uoa.core.ntua.gr (147.102.224.33)
  195.134.71.1 (195.134.71.1)
  195.134.71.229 (195.134.71.229)
  195.134.71.229 (195.134.71.229)
  147.102.224.34 (147.102.224.34)
  router.netmode.ece.ntua.gr (147.102.13.200)

- Αναφορικά με το ping στον κόμβο www.auth.gr: Γιατί παρατηρούνται πολλαπλά πακέτα ερώτησης / απάντησης; Εξηγήστε. Αποτέλεσμα ποιας εντολής είναι η ακολουθία των πακέτων;

  Συγκεκριμένα παρατηρούμε οτι η απάντηση έχει κατατμηθεί σε συνολικά τρία (3) fragments των **1480, 1480, 48 bytes**.
  Παρατηρώντας το ICMP ECHO REQUEST που στάληκε στον κόμβο του auth.gr, βλέπουμε οτι το μέγεθος των δεδομένων (DATA) ειναι 2992 bytes και το οποίο στάληκε (ομοίως με την απάντηση) σε τρία (3) τμήματα (fragments). Απ' αυτό καταλαβαίνουμε ότι η MTU = 1500 bytes – αφου
  1480 (data) + 20 (header) = 1500 bytes
  Η εντολή που εκτελέστηκε: **ping -s 2992 auth.gr**

Άσκηση 2

Με τη βοήθεια του εργαλείου «openssl» ζητούνται να εκτελεστούν τα παρακάτω βήματα και να απαντηθούν οι αντίστοιχες ερωτήσεις:

a. Δημιουργία ενός πιστοποιητικού το οποίο να είναι υπογεγραμμένο από την αρχή πιστοποίησης (certificate authority) που βρίσκεται στο μηχάνημα maria.netmode.ntua.gr. Εξηγήστε τα βήματα που απαιτούνται και καταγράψτε τις αντίστοιχες εντολές.

   Δημιουργουμε τα αρχεία που χρειαζεται το /*usr/lib/ssl/openssl.cnf:*
   mkdir -p newcerts
   touch ~/index.txt{,.attr}
   echo "01" > ~/serial

   Δημιουργουμε το private key:
   netmg034@maria ~> openssl genrsa -out nm34.key

   Δημιουργουμε το certificate sign request (CSR):
   netmg034@maria ~> openssl req -new -key nm34.key -keyform PEM -out nm34.csr

   Υπογράφουμε το certificate (selfsign):
   netmg034@maria ~> openssl ca -in nm34.csr -out nm34.crt

b. Με χρήση της εντολής
   openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -tls1
   δοκιμάστε να συνδεθείτε στον secure web server που λειτουργεί στο μηχάνημα netmg.netmode.ntua.gr (port 443). Εξηγήστε τι συμβαίνει.

   netmg034@maria ~> **openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -tls1**

   openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -tls1
   CONNECTED(00000003)
   SSL_connect:before SSL initialization
   SSL_connect:SSLv3/TLS write client hello
   SSL_connect:SSLv3/TLS write client hello
   SSL_connect:SSLv3/TLS read server hello
   depth=0 C = GR, ST = ATTICA, O = NTUA, OU = NETMODE, CN = NETMAN Web Server, emailAddress = netman@netmode.ntua.gr
   verify error:num=66:EE certificate key too weak
   verify return:1
   depth=0 C = GR, ST = ATTICA, O = NTUA, OU = NETMODE, CN = NETMAN Web Server, emailAddress = netman@netmode.ntua.gr
   verify error:num=20:unable to get local issuer certificate
   verify return:1
   depth=0 C = GR, ST = ATTICA, O = NTUA, OU = NETMODE, CN = NETMAN Web Server, emailAddress = netman@netmode.ntua.gr
   verify error:num=21:unable to verify the first certificate

verify return:1
SSL_connect:SSLv3/TLS read server certificate
SSL_connect:SSLv3/TLS read server key exchange
SSL_connect:SSLv3/TLS read server certificate request
SSL_connect:SSLv3/TLS read server done
SSL_connect:SSLv3/TLS write client certificate
SSL_connect:SSLv3/TLS write client key exchange
SSL_connect:SSLv3/TLS write change cipher spec
SSL_connect:SSLv3/TLS write finished
SSL3 alert read:fatal:handshake failure
SSL_connect:error in SSLv3/TLS write finished
140180747793664:error:14094410:SSL routines:ssl3_read_bytes:sslv3 **alert handshake failure:../ssl/record/rec_layer_s3.c:1399:SSL alert number 40**

Certificate chain
 0 s:/C=GR/ST=ATTICA/O=NTUA/OU=NETMODE/CN=NETMAN Web Server/emailAddress=netman@netmode.ntua.gr
   i:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=NETMODE COURSE CA - 2008/emailAddress=root@netmode.ntua.gr
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDZjCCAs+gAwIBAgIBAzANBgkqhkiG9w0BAQQFADCBmDELMAkGA1UEBhMCR1Ix
DzANBgNVBAgTBkF0dGljYTEPMA0GA1UEBxMGQXRoZW5zMQ0wCwYDVQQKEwROVFVB
MRAwDgYDVQQLEwdORVRNT0RFMSEwHwYDVQQDExhORVRNT0RFIENPVVJTRSBDQSAt
IDIwMDgxIzAhBgkqhkiG9w0BCQEWFHJvb3RAbmV0bW9kZS5udHVhLmdyMB4XDTE0
MTExMTEyMjU0NVoXDTE1MTExMTEyMjU0NVowgYIxCzAJBgNVBAYTAkdSMQ8wDQYD
VQQIEwZBVFRJQ0ExDTALBgNVBAoTBE5UVUExEDAOBgNVBAsTB05FVE1PREUxGjAY
BgNVBAMTEU5FVE1BTiBXZWIgU2VydmVyMSUwIwYJKoZIhvcNAQkBFhZuZXRtYW5A
bmV0bW9kZS5udHVhLmdyMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJx7sRiA6WX2
+EYo2v1ruc102eCrcth5VzR5WvpBA3Nqt7u6+5f0qHSqvP3EiAn8XFwq93s06MLO
6cM2MeD68aMCAwEAAaOCARYwggESMAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8W
HU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBRLUmCxHMf0
h3RtSn6u8105gbYUtDCBtwYDVR0jBIGvMIGsoYGepIGbMIGYMQswCQYDVQQGEwJH
UjEPMA0GA1UECBMGQXR0aWNhMQ8wDQYDVQQHEwZBdGhlbnMxDTALBgNVBAoTBE5U
VUExEDAOBgNVBAsTB05FVE1PREUxITAfBgNVBAMTGE5FVE1PREUgQ09VUlNFIENB

IC0gMjAwODEjMCEGCSqGSIb3DQEJARYUcm9vdEBuZXRtb2RlLm50dWE
uZ3KCCQCS
xS+8Lo8BEzANBgkqhkiG9w0BAQQFAAOBgQB35254IiyHmJ2ZzR/
jStWiWoFcymaX
xXtWcJObGyZOxr5cZIKlkRUMarHqwADFrW6GK/Tyj96xis/
lsqAomsh1NQH0lZRH
X+YRfM+5BQYbdiTNMRA4XtKRkwg1PnfbSQAgh44qrqaAfw6MySwII/
i5m7ccJyqK
4/gXss6kWmbGZw==
-----END CERTIFICATE-----
subject=/C=GR/ST=ATTICA/O=NTUA/OU=NETMODE/CN=NETMAN Web
Server/emailAddress=netman@netmode.ntua.gr
issuer=/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/
CN=NETMODE COURSE CA - 2008/emailAddress=root@netmode.ntua.gr
---
Acceptable client certificate CA names
/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/
CN=maria.netmode.ece.ntua.gr/emailAddress=admin@netmode.ntua.gr
Client Certificate Types: RSA sign, DSA sign, ECDSA sign
Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 1284 bytes and written 248 bytes
Verification error: unable to verify the first certificate

New, TLSv1.0, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 512 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1
    Cipher   : ECDHE-RSA-AES256-SHA
    Session-ID:
    Session-ID-ctx:
    Master-Key:
A0FB75064946157C7AB522746E5B816D7459E2B1513385C7CAFC4E131D2E
907E8A7707DE682A2644E5B05FF69AACB839
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1544267023
    Timeout   : 7200 (sec)
    Verify return code: 21 (unable to verify the first certificate)
    Extended master secret: no

Alert 40: handshake_failure → Indicates that the sender was unable to negotiate an acceptable set of security parameters given the option available. This is a fatal error

c. Στη συνέχεια δοκιμάστε ξανά τη σύνδεση με χρήση της εντολής

openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -cert ca -key <private key file> -tls1

και του πιστοποιητικού που δημιουργήσατε στο πρώτο βήμα. Εξηγήστε τι συμβαίνει σε αυτήν την περίπτωση. Ποιο είναι το Common Name (CN) του web server; Ποια αρχή πιστοποίησης έχει υπογράψει το πιστοποιητικό του web server; Από ποια πιστοποιημένη αρχή πρέπει να είναι υπογεγραμμένα τα πιστοποιητικά των χρηστών ώστε να μπορούν να συνδεθούν με τον συγκεκριμένο web server

$ **openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -cert nm34.crt -key nm34.key -tls1**

CONNECTED(00000003)
SSL_connect:before SSL initialization
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS read server hello
depth=0 C = GR, ST = ATTICA, O = NTUA, OU = NETMODE, CN = NETMAN Web Server, emailAddress = netman@netmode.ntua.gr
verify error:num=66:EE certificate key too weak
verify return:1
depth=0 C = GR, ST = ATTICA, O = NTUA, OU = NETMODE, CN = NETMAN Web Server, emailAddress = netman@netmode.ntua.gr
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = GR, ST = ATTICA, O = NTUA, OU = NETMODE, CN = NETMAN Web Server, emailAddress = netman@netmode.ntua.gr
verify error:num=21:unable to verify the first certificate
verify return:1
SSL_connect:SSLv3/TLS read server certificate
SSL_connect:SSLv3/TLS read server key exchange
SSL_connect:SSLv3/TLS read server certificate request
SSL_connect:SSLv3/TLS read server done
SSL_connect:SSLv3/TLS write client certificate
SSL_connect:SSLv3/TLS write client key exchange
SSL_connect:SSLv3/TLS write certificate verify
SSL_connect:SSLv3/TLS write change cipher spec
SSL_connect:SSLv3/TLS write finished
SSL_connect:SSLv3/TLS write finished
SSL_connect:SSLv3/TLS read server session ticket
SSL_connect:SSLv3/TLS read change cipher spec
SSL_connect:SSLv3/TLS read finished

Certificate chain
 0 s:/C=GR/ST=ATTICA/O=NTUA/OU=NETMODE/CN=NETMAN Web Server/emailAddress=netman@netmode.ntua.gr
   i:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=NETMODE COURSE CA - 2008/emailAddress=root@netmode.ntua.gr

---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDZjCCAs+gAwIBAgIBAzANBgkqhkiG9w0BAQQFADCBmDELMAkGA1
UEBhMCR1Ix
DzANBgNVBAgTBkF0dGljYTEPMA0GA1UEBxMGQXRoZW5zMQ0wCwY
DVQQKEwROVFVB
MRAwDgYDVQQLEwdORVRNT0RFMSEwHwYDVQQDExhORVRNT0RFI
ENPVVJTRSBDQSAt
IDIwMDgxIzAhBgkqhkiG9w0BCQEWFHJvb3RAbmV0bW9kZS5udHVhLmdy
MB4XDTE0
MTExMTEyMjU0NVoXDTE1MTExMTEyMjU0NVowgYIxCzAJBgNVBAYT
AkdSMQ8wDQYD
VQQIEwZBVFRJQ0ExDTALBgNVBAoTBE5UVUExEDAOBgNVBAsTB05F
VE1PREUxGjAY
BgNVBAMTEU5FVE1BTiBXZWIgU2VydmVyMSUwIwYJKoZIhvcNAQkBF
hZuZXRtYW5A
bmV0bW9kZS5udHVhLmdyMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
AJx7sRiA6WX2
+EYo2v1ruc102eCrcth5VzR5WvpBA3Nqt7u6+5f0qHSqvP3EiAn8XFwq93s06
MLO
6cM2MeD68aMCAwEAAaOCARYwggESMAkGA1UdEwQCMAAwLAYJYIZ
IAYb4QgENBB8W
HU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBB
RLUmCxHMf0
h3RtSn6u8105gbYUtDCBtwYDVR0jBIGvMIGsoYGepIGbMIGYMQswCQYD
VQQGEwJH
UjEPMA0GA1UECBMGQXR0aWNhMQ8wDQYDVQQHEwZBdGhlbnMxDT
ALBgNVBAoTBE5U
VUExEDAOBgNVBAsTB05FVE1PREUxITAfBgNVBAMTGE5FVE1PREUgQ
09VUlNFIENB
IC0gMjAwODEjMCEGCSqGSIb3DQEJARYUcm9vdEBuZXRtb2RlLm50dWE
uZ3KCCQCS
xS+8Lo8BEzANBgkqhkiG9w0BAQQFAAOBgQB35254IiyHmJ2ZzR/
jStWiWoFcymaX
xXtWcJObGyZOxr5cZIKlkRUMarHqwADFrW6GK/Tyj96xis/
lsqAomsh1NQH0lZRH
X+YRfM+5BQYbdiTNMRA4XtKRkwg1PnfbSQAgh44qrqaAfw6MySwII/
i5m7ccJyqK
4/gXss6kWmbGZw==
-----END CERTIFICATE-----
subject=/C=GR/ST=ATTICA/O=NTUA/OU=NETMODE/CN=NETMAN Web
Server/emailAddress=netman@netmode.ntua.gr
issuer=/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/
CN=NETMODE COURSE CA - 2008/emailAddress=root@netmode.ntua.gr
---
Acceptable client certificate CA names
/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/
CN=maria.netmode.ece.ntua.gr/emailAddress=admin@netmode.ntua.gr
Client Certificate Types: RSA sign, DSA sign, ECDSA sign

Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 2551 bytes and written 1519 bytes
Verification error: unable to verify the first certificate

New, TLSv1.0, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 512 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1
    Cipher   : ECDHE-RSA-AES256-SHA
    Session-ID:
778DB2F81AFEDA8FE1250AF09FE063E11EE32DF28ED1711EA981E1C3F3
854C21
    Session-ID-ctx:
    Master-Key:
6DD7696367FF660B455FCEAF6DACF6B763E6FC70FFB7F2E5BB2394226A9
43CAEB4C5BF981A52EB3BB53DC10D6761F03A
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:

.
.
.
Start Time: 1544269596
Timeout   : 7200 (sec)
Verify return code: 21 (unable to verify the first certificate)
Extended master secret: no

d. Αφού γίνει η σύνδεση πληκτρολογήστε:

GET /netmg.php HTTP/1.0 <Enter> <Enter>

Τι εμφανίζεται με την εκτέλεση της παραπάνω εντολής;

GET /netmg.php HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 08 Dec 2018 11:47:23 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.5
Content-Length: 17
Connection: close
Content-Type: text/html

Welcome nm34!!!

Εμφανίζεται welcome μήνυμα με όνομα ίδιο με αυτό που ορίσαμε ως common name στο certificate sign request.

Πριν ξεκινήσετε την διαδικασία δημιουργίας του πιστοποιητικού πρέπει να δημιουργήσετε τα αρχεία index.txt και serial καθώς και τον φάκελο newcerts με τις παρακάτω εντολές:

mkdir newcerts
touch ~/index.txt
touch ~/index.txt.attr
echo "01" > ~/serial

Άσκηση 3

Δημιουργείστε στον κόμβο ***maria*** ένα ζεύγος κλειδιών RSA με χρήση των εντολών ssh-keygen ή openssl. Επίσης, δημιουργείστε το αρχείο ***~/.ssh/authorized_keys*** και εισάγετε σε αυτό το public key του ζεύγους.
Κατεβάστε το στον υπολογιστή σας με scp / sftp / sftp client.
Πλέον μπορείτε να συνδεθείτε στον κόμβο ***maria*** με χρήση του private key αντί για password.
Παράδειγμα από περιβάλλον UNIX:
ssh netmgXXX@maria.netmode.ntua.gr –i /<path>/<to>/<private_key>

Χρήσιμες εντολές: ssh-keygen, openssl, mkdir, touch, cat, chmod, scp, sftp, ssh

$ cat .ssh/authorized-keys

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDIDHIFrlCsF9o+1duljsUU5oeoKdb2igl
yyOlBQB7gDaEfShhBtcYrBfarF7xTgc/
WtzLDH88PpH5oEZr2H153VpTjxxUmUgfRExUqwhECIEypEP4Su6TsuZg+FOvA6XJ
tOhSshKlYqkJ+2QCgw5tgO+PnfXfJzHNs/Qr71n/
WpgMpnxNuDQQ3Rw5r5G+pKv6QBnQv/
WcubaLKewa6EpKvHOhD6IkjtOY9VS9p2VHMpcX9IeHvQ0JMXFpjb3Mp11fLu6TB
EIUlhsWoGeSjio+APkxqZiKYGbke1ILPV8feOR7HcCIluNGPN60IHDlab28Mgeh7TE
6TiaOoYFBhHpFn ishtar@lhc
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCtFg9QhqPcD8+mBOe6JjQcz1QliG1c
m50WJMEHB75BoQ2U8wG/
uXMVVbDecGMhH6vP+GYXsjQFwsSosd9Uj7wTCX4hz5mCcEKYig0ixGZafwaCxnd
FaxYRqk/VaUlnGL/
HFApb7R2EI2OKqm8hrzo1zs8AwwXWfsqBq1a2F5oNuQQ5tD0eh//
GFZYUgldeihG5EsS4ImPVjfWntuASAgXeR2+DiprLS6l6WF0O4ETKS/
7e5n0m4mLSG3nm9WhbP8O8ETWZkvITE0HEOZUkuXd/7fViAhUS+K9cgjWYbM/
Hb0RDLo4o8c75kW2pHgKG4MX/2C/oyVv6Vzsl5/xOxxi7 ckardaris@home