ΣΚΛΗΡΥΝΣΗ ΔΙΚΤΥΑΚΩΝ ΣΥΣΚΕΥΩΝ

Π.Μ.Σ. στις Τηλεπικοινωνίες και Δίκτυα Η/Υ

Αριστοτέλης Διαμαντής

Σέρρες 2024

Σκοπός της εργασίας

Ο σκοπός της διπλωματικής μου εργασίας, είναι η μελέτη και η πρόταση ενεργειών σχετικά με τη σκλήρυνση των δικτυακών συσκευών. Επίσης, αναλύονται κάποιες εντολές στο περιβάλλον CLI των συσκευών Cisco, οι οποίες σχετίζονται με την ασφάλεια των συσκευών.

ΔΟΜΗ ΤΗΣ ΕΡΓΑΣΙΑΣ

- Ανάλυση κινδύνων και τρόποι αντιμετώπισης

  Η πρώτη ενότητα αφορά τη θεωρητική ανάλυση των ενδεχόμενων κινδύνων ασφάλειας που μπορεί να διατρέχει μια συσκευή δικτύου, καθώς και κάποιους τρόπους μετριασμού αυτών των κινδύνων.

- Προσομοίωση

  Στη δεύτερη ενότητα αναφέρονται κάποιες εντολές που παραμετροποιούν τις συσκευές Cisco ώστε να ενισχυθεί η ασφάλεια τους.

- Ανάπτυξη λογισμικού

  Στη τρίτη ενότητα αναπτύσσεται λογισμικό σε γλώσσα python με το οποίο αυτοματοποιούνται κάποιες ρυθμίσεις σε μια συσκευή router της Cisco.

1η Ενότητα

Στην πρώτη ενότητα αναλύονται τα παρακάτω:

- Αρχιτεκτονική Δικτύου

  Το δίκτυο θα πρέπει να είναι δομημένο έτσι ώστε να δημιουργείται μια αποστρατικοποιημένη ζώνη προκειμένου η επικοινωνία μεταξύ των εσωτερικών και των εξωτερικών συσκευών δικτύου να ελέγχεται καλύτερα.

- Υιοθέτηση Τοπικής Διαχείρισης Λογαριασμών και Κωδικών Πρόσβασης

  Σημαντικό επίσης είναι να εφαρμόζονται και τοπικοί λογαριασμοί στη συσκευή για περιπτώσεις στις οποίες οι servers έχουν βγει εκτός λειτουργίας.

- Αυθεντικοποίηση , Εξουσιοδότηση και Καταγραφή

  Η αυθεντικοποίηση, η εξουσιοδότηση και η καταγραφή είναι σημαντικές διαδικασίες, διότι δυσχεραίνουν σημαντικά την απόκτηση πρόσβασης των επιτιθέμενων σε ένα σύστημα. Είναι σημαντικό αυτές οι ενέργειες να εκτελούνται σε απομακρυσμένους servers, ώστε να διασφαλίζεται η αξιοπιστία τους.

- Απομακρυσμένη Καταγραφή και Παρακολούθηση Δικτυακών Συσκευών

  Τα γεγονότα που συμβαίνουν σε ένα δίκτυο επιτρέπουν στους διαχειριστές να ελέγχουν για τυχόν ύποπτες δραστηριότητες εντός του δικτύου. Για μεγαλύτερη αξιοπιστία και αποφυγή τυχόν αλλοιώσεων στις καταγραφές θα πρέπει αυτές να αποστέλλονται σε απομακρυσμένους serves αφού έχουν κρυπτογραφηθεί.

- Υπηρεσίες Δικτύου

  Οι υπηρεσίες δικτύου οι οποίες δε χρησιμοποιούνται σε ένα δίκτυο θα πρέπει να απενεργοποιούνται, επίσης θα πρέπει να γίνεται χρήση υπηρεσιών που μεταφέρουν την κίνηση να υποστηρίζουν κρυπτογράφηση δεδομένων.

- Δρομολόγηση

  Οι δρομολογητές θα πρέπει να ρυθμίζονται κατάλληλα διότι σε μια ενδεχόμενη “κακή” ρύθμισή τους, ένας κακόβουλος χρήστης μπορεί να αποκτήσει τη δυνατότητα να ορίσει την πορεία των δεδομένων, καθώς και ποια διαδρομή θα ακολουθήσουν. Για να αποφευχθούν τέτοια φαινόμενα θα πρέπει για παράδειγμα να απενεργοποιηθεί το IP source routing.

- Θύρες Διεπαφών

  Στις συσκευές δικτύου θα πρέπει να απενεργοποιούνται οι φυσικές διεπαφές οι οποίες δε χρησιμοποιούνται. Εάν δεν απενεργοποιηθούν μπορεί κάποιος να συνδέσει συσκευές οι οποίες δεν είναι εξουσιοδοτημένες και να αποκτήσει πρόσβαση στο δίκτυο. Επίσης θα πρέπει αυτές οι διεπαφές να ομαδοποιούνται σε ένα VLAN το οποίο θα είναι απομονωμένο από το υπόλοιπο δίκτυο.

- Χρήση Banners

  Αποτελούν μηνύματα που εμφανίζονται κατά τη σύνδεση του χρήστη και αποσκοπούν στην ενημέρωση του για τις πολιτικές ασφαλείας, τους όρους χρήσης κ.α. Επιπλέον, παρέχουν προειδοποιήσεις σε κακόβουλους χρήστες σχετικά με τις συνέπειες παραβίασης του συστήματος.

2η Ενότητα

Σ΄ αυτή την ενότητα παρουσιάζονται κάποιες εντολές παραμετροποίησης συσκευών για την ενίσχυση της ασφάλειας.

- Τμηματοποίηση Δικτύων και VLANs
  Η τμηματοποίηση των δικτύων είναι σημαντική, καθώς επιτρέπει τη διαχείριση και την ασφάλεια των δικτύων. Μπορεί να γίνει είτε με φυσική τμηματοποίηση κάνοντας χρήση των δικτυακών συσκευών , routers, switches , firewalls, είτε εικονικά μέσω των VLAN.

- Αναβάθμιση Λογισμικού
  Είναι σημαντικό η δικτυακή συσκευή να είναι ενημερωμένη πάντα με τη τελευταία έκδοση. Οι πιο πρόσφατες εκδόσεις αντιμετωπίζουν γνωστές ευπάθειες που θέτουν σε κίνδυνο την ασφάλεια της συσκευής.

- Αυθεντικοποίηση , Εξουσιοδότηση και Καταγραφή δικτυακών συσκευών
  Η απομακρυσμένη αυθεντικοποίηση μπορεί να υλοποιηθεί με δύο τύπους servers. Είτε με τον TACACS+ ή με τον RADIUS. Επιπλέον, θα πρέπει να ορίζεται και η αυθεντικοποίηση τοπικά στη συσκευή.

- Ενεργοποίηση συγχρονισμού ρολογιού
  Τα ρολόγια των δικτυακών συσκευών πρέπει να συγχρονίζονται σε μια ώρα, ώστε η καταγραφή των γεγονότων να είναι ακριβής και η διαχείριση πιο αποτελεσματική. Ο συγχρονισμός πρέπει να γίνεται μέσω ενός απομακρυσμένου server.

- Καθορισμός των Access Lists (ACL)
  Οι Access Control Lists ελέγχουν και περιορίζουν την κίνηση που περνάει από έναν δρομολογητή. Μέσω του ορισμού κατάλληλων κανόνων ACL επιτυγχάνεται η αποτελεσματική διαχείριση και η προστασία από ανεπιθύμητες εισβολές.

- Εισαγωγή μηνυμάτων banner
  Τα Message of the Day banner παρέχουν προσωρινές ενημερώσεις, όπως αναγγελίες προγραμματισμένων συντηρήσεων του συστήματος. Τα Login banners επισημαίνουν κυρίως ότι η μη εξουσιοδοτημένη πρόσβαση απαγορεύεται και ποιες κυρώσεις υπάρχουν.

3η Ενότητα

Στη τελευταία ενότητα γίνεται ανάπτυξη ενός λογισμικού σε γλώσσα προγραμματισμού Python, το οποίο αυτοματοποιεί κάποιες παραμετροποιήσεις ενός δρομολογητή της Cisco. Οι αυτόματες ρυθμίσεις που πραγματοποιούνται είναι οι παρακάτω.

- Διαμόρφωση AAA

  Ρύθμιση της αυθεντικοποίησης ενός χρήστη μέσω AAA server.

```
Choose an option:
1. Configure AAA
2. Configure NTP
3. Configure Enable Secret
4. Configure Timestamps
5. Configure Logging to Syslog Server
6. Configure MOTD Banner
7. Configure Login Banner
8. Check for Updates
9. Configure an Access List
10. Show information
11. Save changes
99. Exit
Enter your choice: 1
Enter TACACS+ server IP: 192.168.122.4
Enter TACACS+ server username: gns3
Enter TACACS+ server password: gns3
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#tacacs server MyTacServ
R1(config-server-tacacs)#address ipv4 192.168.122.4
R1(config-server-tacacs)#key  gns3
 WARNING: Command has been added to the configuration using a type 0 password. Ho
recated. Migrate to a supported password type
 WARNING: Command has been added to the configuration using a type 0 password. Ho
recated. Migrate to a supported password type
R1(config-server-tacacs)#exit
R1(config)#aaa group server tacacs+ gns3group1
R1(config-sg-tacacs+)#server name MyTacServ
R1(config-sg-tacacs+)#exit
R1(config)#aaa authentication login default group gns3group1 local
R1(config)#end
R1#
Successful Configuration
```

- Διαμόρφωση NTP

  Συγχρονισμός του ρολογιού του router με έναν απομακρυσμένο server.

```
Enter your choice: 2
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 64.209.210.20
R1(config)#clock timezone ATHENS 2
R1(config)#end
R1#
Successful Configuration
```

- Ενεργοποίηση secret password

  Ενεργοποίηση του κωδικού πρόσβασης που απαιτείται για την είσοδο στη λειτουργία enable του router.

```
Enter your choice: 3
Enter enable secret password: newcisco
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret newcisco
R1(config)#end
R1#
Successful Configuration
```

- Ενεργοποίηση των Timestamps

  Με την επιλογή αυτή ενεργοποιείται η λειτουργία των χρονικών σφραγίδων στα μηνύματα που τυπώνει ο δρομολογητής.

```
Enter your choice: 4
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service timestamps debug datetime localtime show-timezone msec year
R1(config)#service timestamps log datetime localtime show-timezone msec year
R1(config)#end
R1#
Successful Configuration
```

- Ενεργοποίηση καταγραφής

  Το logging αναφέρεται στη διαδικασία καταγραφής των διαφόρων γεγονότων, ενεργειών και εκδηλώσεων που συμβαίνουν σε ένα δίκτυο ή σε μια δικτυακή συσκευή.

```
Enter your choice: 5
Enter syslog server IP address: 192.168.122.192
Enter interface for syslog: g0/0
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#logging host 192.168.122.192
R1(config)#logging trap notifications
R1(config)#logging source-interface g0/0
R1(config)#end
R1#
Successful Configuration
```

- Ενεργοποίηση του MOTD Banner

  Ο χρήστης μπορεί να καθορίσει ένα μήνυμα που θα εμφανίζεται κατά την είσοδό του στον δρομολογητή, γνωστό ως Message of the Day (motd).

```
Enter your choice: 6
Enter delimiter character: #
Enter Message of the Day (MOTD):
 ********** \n Welcome \n **********
```

- Ενεργοποίηση του Login Banner

  Ο χρήστης μπορεί να ορίσει ένα μήνυμα που θα εμφανίζεται κατά την είσοδο του στον δρομολογητή, γνωστό ως Login Banner.

```
Enter your choice: 7
Enter login banner: **********Autorized use only**********
```

- Διαμόρφωση Λιστών Ελέγχου Πρόσβασης

  Με την επιλογή 9, ο χρήστης έχει τη δυνατότητα να δημιουργήσει μια access-list και να την εφαρμόσει σε μια συγκεκριμένη διεπαφή του δρομολογητή.

```
Enter your choice: 9
Enter the number of the access list to configure (e.g., 10): 10
Configure Access List:
1. Permit
2. Deny
Enter your choice (1/2): 1
Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet): any
Do you want to add another rule? (yes/no): yes
Configure Access List:
1. Permit
2. Deny
Enter your choice (1/2): 2
Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet): host
Enter source IP address: 192.168.1.1
Do you want to add another rule? (yes/no): yes
Configure Access List:
1. Permit
2. Deny
Enter your choice (1/2): 2
Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet): net
Enter source IP address: 192.168.2.0
Enter mask type ('subnet' for subnet mask or 'wildcard' for wildcard mask): wildcard
Enter wildcard mask (in the format 0.0.0.255): 0.0.0.255
Do you want to add another rule? (yes/no): no
Enter interface (e.g., GigabitEthernet0/0): g0/0
Enter traffic direction (in or out): in
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit any
R1(config)#access-list 10 deny 192.168.1.1
% Access rule can't be configured at higher sequence num as it is part of the existing rule at sequence num 10
R1(config)#access-list 10 deny 192.168.2.0 0.0.0.255
R1(config)#interface g0/0
R1(config-if)#ip access-group 10 in
R1(config-if)#end
R1#
```

- Εμφάνιση ρυθμίσεων

  Προβάλλονται λεπτομερείς πληροφορίες σχετικά με τις τρέχουσες ρυθμίσεις που έχουν εφαρμοστεί στον δρομολογητή (router).

```
AAA Configuration:
aaa new-model
aaa group server tacacs+ gns3group1
aaa authentication login default group gns3group1 local
aaa session-id common

NTP Configuration:

ntp server 64.209.210.20

Enable Secret Configuration:

enable secret 9 $9$9uGXhVRmUXi2rM$A8CD1nggUK97p9RNYbpmvI5mNAH5IsFcCi90M11rZ.2

Timestamps Configuration:

service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year

Logging Configuration:
logging host 192.168.122.111
logging host 192.168.122.192

MOTD Configuration:

banner motd ^C

Login Banner Configuration:

banner login ^C**********Autorized use only**************^C

IP Access-Group Configuration:
 ip access-group 10 in
 ip access-group 15 out

Interface Configuration:
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
logging source-interface GigabitEthernet0/0
Software Version:

Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.9(3)M6, RELEASE SOFTWARE (fc1)
ROM: Bootstrap program is IOSv
Cisco IOSv (revision 1.0) with  with 460089K/62464K bytes of memory.
```

- Αποθήκευση αλλαγών

  Με την τελευταία επιλογη, οι αλλαγές που έχουν γίνει στις ρυθμίσεις του δρομολογητή αποθηκεύονται μόνιμα. Αυτή η ενέργεια εξασφαλίζει ότι οι τροποποιήσεις που έχουν γίνει θα διατηρηθούν ακόμα και μετά από επανεκκίνηση της συσκευής ή απώλεια ενέργειας.

```
Enter your choice: 11
Changes saved to startup configuration.
```

Ευχαριστώ πολύ για το χρόνο σας.