

ΕΡΓΑΣΙΑ στο μάθημα
Ανάπτυξη και Διαχείριση Δικτύων Υπολογιστών (CSE801)
Καθηγητής ΓΑΝΑΓΙΩΤΗΣ ΦΟΥΛΗΡΑΣ



Τμήμα Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας
ΑΠΡΙΛΙΟΣ 2024

ΕΦΑΡΜΟΓΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ

ΟΝΟΥΡ ΙΜΠΡΑΧΗΜ

ΠΕΡΙΛΗΨΗ

Στην παρούσα απαλλακτική εργασία αναλύονται 2 δωρεάν εφαρμογές διαχείρισης και παρακολούθησης δικτύου, με στόχο τη σύγκριση και αξιολόγησή τους.

Παρουσιάζονται και αναλύονται τα βασικά χαρακτηριστικά και οι δυνατότητες της κάθε εφαρμογής, και γίνεται επιλογή της πιο κατάλληλης εφαρμογής.

Η επιλεγμένη εφαρμογή εγκαθίσταται σε μία εικονική μηχανή και χρησιμοποιείται σε συνδυασμό με εικονικής μηχανής ubuntu server και windows υπολογιστή, για τη δοκιμή σεναρίων που στοχεύουν στην παρακολούθηση και την ανίχνευση επιθέσεων τύπου DoS.

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή
2. Εφαρμογές Διαχείρισης Δικτύου
3. Απαραίτητες προετοιμασίες
4. Cacti
5. Zabbix
6. Επιθέσεις DoS και αποτελέσματα
 - 6.1. SYN flood attack με Hping3
 - 6.2. Slowloris
 - 6.3. Slowhttptest
7. Σύγκριση
8. Βιβλιογραφία

Προειδοποίηση: Το παρόν έγγραφο περιέχει εντολές και εργαλεία που χρησιμοποιούνται για δοκιμές τύπου DoS/DDoS (π.χ. hping3, slowloris, slowhttptest). Οι εντολές αυτές παρουσιάζονται μόνο για εκπαιδευτικούς λόγους και εκτελούνται αποκλειστικά σε απομονωμένο εργαστηριακό περιβάλλον.

1. Εισαγωγή

Τι είναι η διαχείριση δικτύου (Network Management - NM) ;

Η διαχείριση δικτύου αναφέρεται στην παρακολούθηση και τη συντήρηση δικτύων υπολογιστών. Στόχος της διαχείρισης δικτύου είναι να διασφαλίσει ότι το δίκτυο λειτουργεί αποτελεσματικά, να εξασφαλίσει την προσβασιμότητα και την ασφάλεια των δεδομένων, καθώς και να βελτιώσει την απόδοση του δικτύου. Είναι απαραίτητο σήμερα για την ομαλή λειτουργία όλων των δικτύων.

Σύστημα Διαχείρισης Δικτύου (Network Management System, NMS) αποτελείται από:

- Σταθμός/Εφαρμογή Διαχείρισης Δικτύου (NMS): Το λογισμικό διαχείρισης που επικοινωνεί με τους agents για τη διαχείριση του δικτύου.
- Βάση Δεδομένων Διαχείρισης Πληροφοριών (MIB): Αποθηκεύει πληροφορίες που χρειάζονται για τη διαχείριση των συσκευών σε ένα δίκτυο.
- Πράκτορας διαχείρισης (Agent): Παρέχουν πληροφορίες ή εκτελούν εντολές για τη διαχειριζόμενη συσκευή.
- Πρωτόκολλα διαχείρισης δικτύου (NMP): Το πρωτόκολλο που χρησιμοποιείται από την εφαρμογή διαχείρισης δικτύου και τον πράκτορα διαχείρισης για την ανταλλαγή πληροφοριών. Τα δύο πιο συνηθισμένα πρωτόκολλα είναι
 - Απλό Πρωτόκολλο Διαχείρισης Δικτύου (Simple Network Management Protocol- SNMP) χρησιμοποιείται ευρύτατα για τη διαχείριση σε TCP/IP δίκτυα.
 - Κοινό Πρωτόκολλο Πληροφοριών Διαχείρισης (Common Management Information Protocol- CMIP) χρησιμοποιείται σε τηλεπικοινωνιακά περιβάλλοντα.
- Διαχειριζόμενες συσκευές (Managed device): κόμβοι στο δίκτυο όπως ένας υπολογιστής, δρομολογητής ή εκτυπωτής και άλλα, όπου περιέχουν έναν πράκτορα διαχείρισης (Agent).

Μοντέλο διαχείρισης δικτύου ISO (FCAPS)

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) έχει ομαδοποιήσει τις λειτουργίες διαχείρισης δικτύου σε πέντε τομείς, γνωστούς και ως **FCAPS**, οπου το κάθε γράμμα του, αντιπροσωπεύει μια από αυτές τις 5 τομείς με τη σειρά ως εξείς (Διαχείριση) Fault (Σφαλμάτων), Configuration (Διαμόρφωσης), Accounting (Λογιστική), Performance (Απόδοσης), Security (Ασφάλειας) management.

Αρχιτεκτονικές Διαχείρισης Δικτύου

1. Κεντρική Αρχιτεκτονική : Όλες οι λειτουργίες διαχείρισης εκτελούνται από ένα κεντρικό σύστημα.
 - a. Πλεονεκτήματα: Εύκολος έλεγχος, απλή εγκατάσταση
 - b. Μειονεκτήματα: Μονό Σημείο Αποτυχίας (SPOF) και δυσκολία κλιμάκωσης.
2. Ιεραρχική Αρχιτεκτονική: Δομείται σε επίπεδα σαν πυραμίδα, με το κεντρικό σύστημα στην κορυφή που ελέγχει υποσυστήματα.
 - a. Πλεονεκτήματα: Κλιμακωτότητα, υψηλότερη απόδοση και αυξημένη αξιοπιστία
 - b. Μειονεκτήματα: Αυξημένη πολυπλοκότητα
3. Κατανεμημένη Αρχιτεκτονική: Η διαχείριση είναι διαμοιρασμένη σε πολλαπλά σημεία, που συνεργάζονται.
 - a. Πλεονεκτήματα: Ανοχή σε αποτυχίες, μείωση επιβάρυνσης και εύκολη επεκτασιμότητα
 - b. Μειονεκτήματα: Δύσκολος συντονισμός, αυξημένη πολυπλοκότητα.

Εφαρμογές Διαχείρισης Δικτύου (Network Management Applications)

Είναι λογισμικά εργαλεία που χρησιμοποιούνται για τη διαχείριση, παρακολούθηση και ελέγχου των δικτύων υπολογιστών. Αυτές οι εφαρμογές παρέχουν διάφορες λειτουργίες, συμπεριλαμβανομένων:

- **Παρακολούθηση Δικτύου:** Συλλογοί δεδομένων σχετικά με την κίνηση, την απόδοση, τη χρήση εύρους ζώνης και άλλες μετρήσεις του δικτύου.
- **Διαχείριση Συσκευών:** Επιτρέπουν την παραμετροποίηση, την επίβλεψη και τη διαχείριση δικτυακών συσκευών, όπως δρομολογητές, διακόπτες, φίλτρα πακέτων, firewall, κλπ.
- **Ασφάλεια Δικτύου:** Παρέχουν λειτουργίες για την εντοπισμό απειλών, τον έλεγχο πρόσβασης, την ανίχνευση και αντιμετώπιση παραβιάσεων, και άλλες ασφαλειακές λειτουργίες.
- **Διαχείριση Αποδόσεων:** Αναλύουν τις αποδόσεις του δικτύου, παρέχοντας στατιστικά στοιχεία και πληροφορίες για τη βελτίωση της απόδοσης.
- **Διαχείριση Συστημάτων:** Παρέχουν εργαλεία για τη διαχείριση των λειτουργικών συστημάτων και των εφαρμογών που εκτελούνται στα δίκτυα.
- **Ανίχνευση προβλημάτων:** Παρέχουν ειδοποιήσεις και αναφορές για προβλήματα και ανωμαλίες στο δίκτυο.

Κάνουν μετρήσεις και δημιουργούν γραφήματα για τις συσκευές και το σύστημα του δικτύου, όπως :

- **Στατιστικά πόρων των συσκευών**, όπως CPU, μνήμη και αποθήκευση.
- **Κίνηση δεδομένων** στις διεπαφές δικτύου, συμπεριλαμβανομένων των πακέτων και των στατιστικών σφαλμάτων.
- **Μετρήσεις αισθητήρων** για θερμοκρασία, ταχύτητα ανεμιστήρων, τάση, ρεύμα, ισχύ και συχνότητα.
- **Στατιστικά Διαχείρισης συστήματος** σχετικά με τους χρήστες, τις διεργασίες, τη μέση φόρτωση του συστήματος και τον χρόνο λειτουργίας.

SNMP (Simple Network Management Protocol)

Πρωτόκολλο για ανταλλαγή πληροφοριών για διαχείριση συσκευών δικτύου. Πληροφορίες συλλέγονται από εφαρμογές πρακτόρων (agents) που εγκαθίστανται σε διάφορες συσκευές δικτύων (δρομολογητές, πύλες, διακόπτες κλπ). Κεντρικές εφαρμογές (οθόνες, monitors, NMS - Network Management Systems) συλλέγουν τις πληροφορίες από τους πράκτορες για περαιτέρω ανάλυση ή παρουσίαση.

Εκδόσεις SNMP:

1. **SNMPv1:** Πρώτη Έκδοση. Χρησιμοποιεί την έννοια μιας κοινότητας για αυθεντικοποίηση. Περιορίζεται σε μετρητές 32 bit.
2. **SNMPv2c:** Επέκταση της SNMPv1 για υποστήριξη μετρητών 64bit. Χρησιμοποιεί αυθεντικοποίηση με κοινότητες. Παροχή επιπλέον εντολών (getbulk)
3. **SNMPv3:** Αντιμετωπίζει θέματα ασφάλειας. Χρήση username/password

Σε αυτήν την εργασία αναφέρονται ως Σταθμοί/Εφαρμογές Διαχείρισης Δικτύου (NMS) το Cacti και το Zabbix με κεντρική αρχιτεκτονική και πρωτόκολλο επικοινωνίας SNMP.

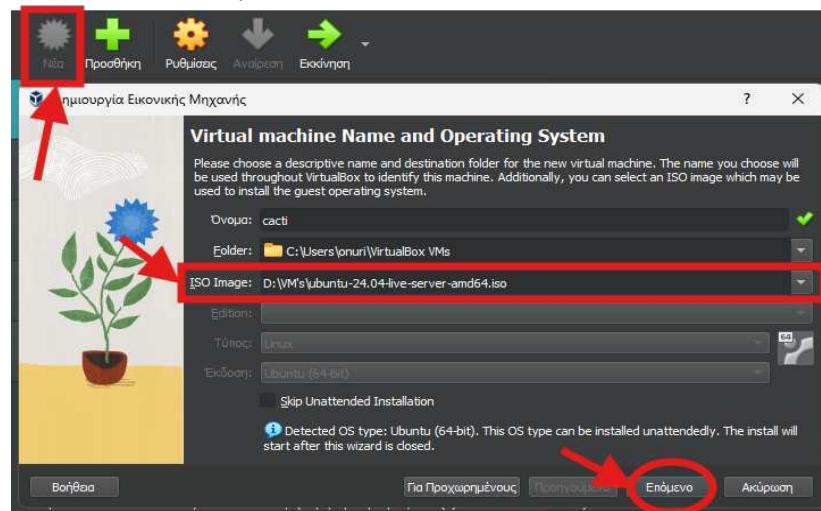
3. Απαραίτητες προετοιμασίες

Παρακάτω αναφέρονται η εφαρμογές και τα εργαλεία που χρησιμοποιούνται στα επόμενα κεφάλαια για το Cacti, Observium και Zabbix

3.1 Ubuntu Server 24.04.4 LTS

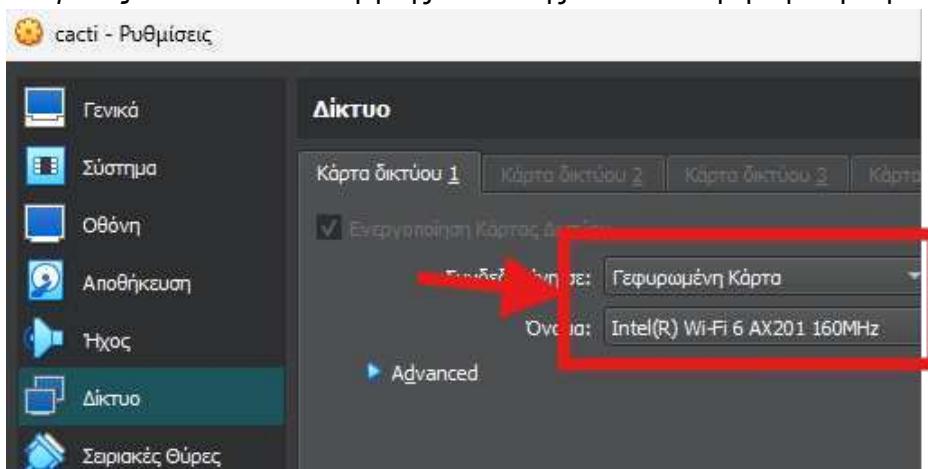
Θα υπάρχουν 3 εικονικές μηχανές Ubuntu Server ξεχωριστά για το Cacti, Observium, Zabbix και άλλη μία για τα σενάρια δοκιμής που θα λέγεται vm1. Τα παρακάτω παραδείγματα είναι από την μηχανή όπου θα εγκατασταθεί το cacti αλλά δεν αλλάζει κάτι για το zabbix και observium. Για λόγους ευκολίας η κάθε μηχανή να έχει το όνομα της εφαρμογής όπου θα εγκατασταθεί σε αυτην και όλες να έχουν ίδιο κωδικό. Ξεκινώντας:

- 1) Εγκατάσταση “Oracle VM VirtualBox” από : <https://www.virtualbox.org/wiki/Downloads>
- 2) Εγκατάσταση “Ubuntu Server 24.04 LTS” από :
<https://ubuntu.com/download/server>
- 3) Δημιουργία και προσαρμογή του εικονικής μηχανής στο VirtualBox
 - a) Νέα -> ISO image : επιλογή του ISO αρχείου από το βήμα 2 (ubuntu-22.04-live-server-amd64.iso) και Επόμενο.



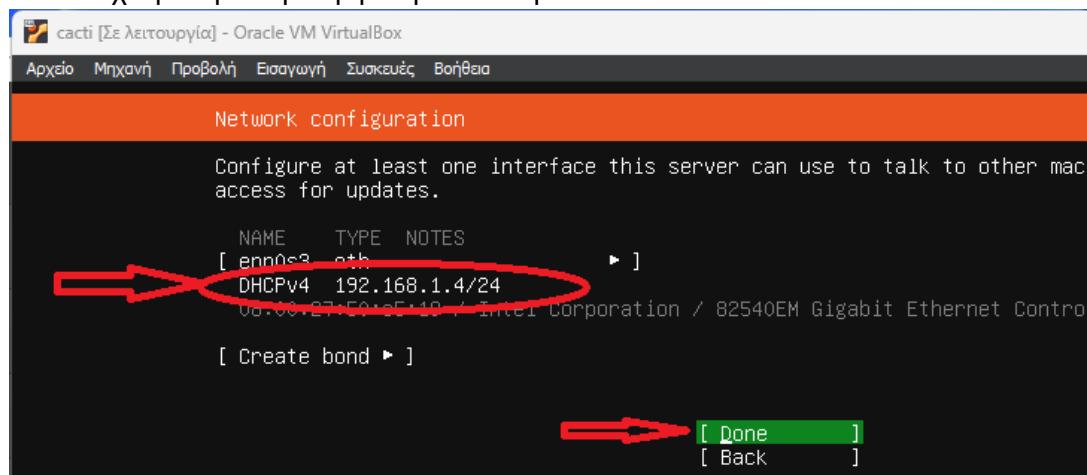
- b) Εισαγωγή *username & password* (cacti & 123) και Επόμενο
- c) Βασική μνήμη 5044MB & 4 επεξεργαστές (ή της Προκαθορισμένες τιμές) και Επόμενο
- d) Hard disk 25 GB(ή την Προκαθορισμένη τιμή) και Επόμενο
- e) Τέλος (Finish)

- 4) Ρυθμίσεις -> Δίκτυο : Αλλαγή της σύνδεσης NAT σε Γεφυρωμένη κάρτα και πατήστε *Nai*.



- 5) Εγκατάσταση και ρύθμιση του Ubuntu server 24.04 με τη σειρά

- Επιλογή γλώσσας και "Enter"
- Done*
- τύπος εγκατάστασης "(x)ubuntu server" και επιλογή *Done*
- Εδώ ορίζεται αυτόματα με DHCP το IP address της μηχανής στο router όπου είναι συνδεδεμένη η γεφυρωμένη κάρτα από το βήμα 4. Επίδει, όλες οι συσκευές που θα χρησιμοποιηθούν θα είναι συνδεδεμένα στο ίδιο router, θα έχουν IP address που θα ξεκινάει με 192.168.1.? και στο τέλος μία μοναδική τιμή που αντιστοιχεί με την συγκεκριμένη συσκευή.



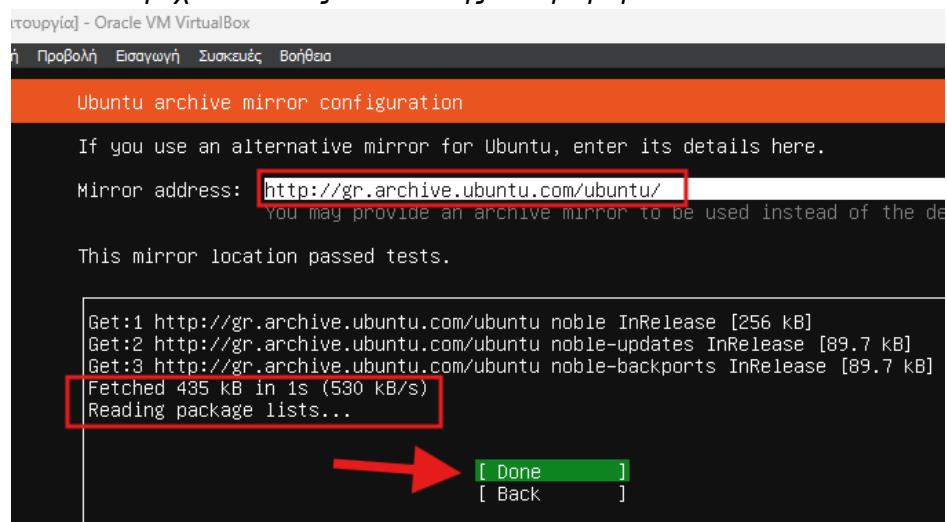
Επιλογή *Done* και "Enter"

- (Proxy configuration) και πάλι *Done*
- Μετα την επιτυχή δοκιμή Mirror address επιλογή *Done*. Αν προκύψει κάποιο σφάλμα ελέγξτε το IP address της μηχανής ειδικά αν έχει οριστεί ως Static και την σύνδεση σας στο δίκτυο. (*Mirror address: Κοντινότερο ως τοποθεσία link, για εγκατάσταση αρχείων ubuntu.*).

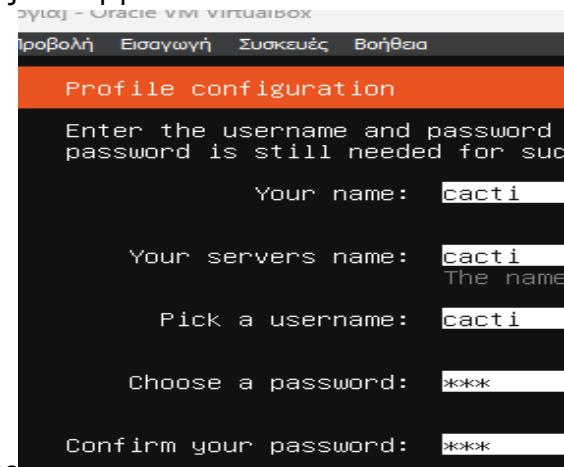
Η λίστα ανα χώρα: <https://launchpad.net/ubuntu/+archivemirrors>

Στην Ελλάδα το πανεπιστήμιο κρήτης, Εθνικό Μετσόβιο Πολυτεχνείο, ΟΤΕ και το

ubuntu παρέχουν τέτοιες διεύθυνσης “καθρέφτη”.



- g) (Guided Storage configuration) χωρίς αλλαγές επιλογή Done
- h) (Storage configuration) χωρίς αλλαγές επιλογή Done και Continue



- i) Συμπλήρωση κενών και επιλογή Done
- j) επιλογή (x)Skip for now και Continue
- k) επιλογή (x)Install OpenSSH server (για πρόσβαση μεσω cmd ή PowerShell από windows) και Done
- l) (Server snaps) Χωρίς καμία τροποποίηση επιλογή Done
- m) Επιλογή Reboot Now όταν εμφανιστεί.
- n) Συμπλήρωση ονόματος χρήστη και κωδικού.

3.2 Συνδεση με SSH

Προσφέρει ευκολία στη αντιγραφή/επικόλληση εντολών και πιο φιλικό περιβάλλον χρήστη.
Εκτέλεση της παρακάτω εντολής στο PowerShell για την διαχείριση του ubuntu server από το Windows με SHH :

ssh <ονομα του server>@<IP address> Π.Χ. ssh cacti@192.168.1.4

```
cacti@cacti: ~
PS C:\WINDOWS\system32> ssh cacti@192.168.1.4
The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established.
ED25519 key fingerprint is SHA256:iY3Ez1AXUTgJMqsQgLp6CS6EoVCzzNU13PQHcBYWFGs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.4' (ED25519) to the list of known hosts.
cacti@192.168.1.4's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-31-generic x86_64)
.....
```

3.3 SNMP(Simple Network Protocol)

Το SNMP είναι ένα τυπικό πρωτόκολλο Διαδικτύου που χρησιμοποιείται για την παρακολούθηση και τη διαχείριση συσκευών δικτύου που συνδέονται μέσω IP. Χρησιμοποιείται για επικοινωνία μεταξύ δρομολογητών, μεταγωγέων, τείχη προστασίας, εξισορροπητών φορτίου, διακομιστών, καμερών CCTV και συσκευών. Στη συνέχεια αυτό το πρωτόκολλο θα χρησιμοποιηθεί από το Cacti, Observium και Zabbix για την παρακολούθηση και τη διαχείριση συσκευών.

Αν τυχόν εμφανιστεί κάποιο σφάλμα ώς "System SNMP error - SNMP::get(): No response from <IP address>" τότε υπάρχει πρόβλημα στο SNMP της συσκευής με το IP address που αναφέρεται στο σφάλμα.

Εγκατάσταση και ρύθμιση σε Windows:

1. Εγκατάσταση Μέσω Ρυθμίσεων:
 - a. Μεταβείτε στις Ρυθμίσεις > Σύστημα > Προαιρετικά χαρακτηριστικά (Optional features)> Προβολή χαρακτηριστικών.
 - b. Επιλέξτε και εγκαταστήστε το "SNMP" και, προαιρετικά, το "WMI SNMP Provider".

ή Μέσω PowerShell: Ανοίξτε το PowerShell ως διαχειριστής και εισάγετε τις ακόλουθες εντολές με τη σειρά:

```
Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"
Add-WindowsCapability -Online Name "WMI-SNMP-Provider.Client~~~~0.0.1.0"
```

2. Ενεργοποίηση και Ρύθμιση της Υπηρεσίας SNMP
 - a) Πατήστε τα πλήκτρα Windows + R, πληκτρολογήστε services.msc
 - b) Βρείτε την "Υπηρεσία SNMP" στη λίστα, κάντε δεξί κλικ σε αυτή και επιλέξτε Ιδιότητες. Στην καρτέλα :
 - i) Γενικά: Ορίστε τον Τύπο εκκίνησης σε Αυτόματη.
 - ii) Πράκτορας: Επιλέξτε όλες τις υπηρεσίες.
 - iii) Ασφάλεια:

- (1) Προσθέστε μια κοινότητα με το όνομα "public" και ορίστε τα δικαιώματα σε MONO ΑΝΑΓΝΩΣΗ.
- (2) Στην ενότητα "Αποδοχή πακέτων SNMP από αυτούς τους υπολογιστές", προσθέστε τις διευθύνσεις IP των διακομιστών Cacti, Observium και Zabbix ή καντε το ανοιχτό σε όλους. Για τοπικές ρυθμίσεις που χρησιμοποιούν XAMPP, μπορείτε να χρησιμοποιήσετε localhost ή την τοπική διεύθυνση IP σας.
- (3) Κάντε κλικ στο Εφαρμογή-Apply για να αποθηκεύσετε τις αλλαγές.

Εγκατάσταση και διαμόρφωση σε *Ubuntu Server*:

1. Εγκατάσταση του SNMP (Όταν σας ζητηθεί, πληκτρολογήστε "Y" για να συνεχίσετε):
`sudo apt install snmpd snmp libsnmp-dev`
2. Δημιουργήστε αντίγραφο ασφαλείας του αρχικού αρχείου snmpd.conf:
`sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak`
3. Επεξεργασία του αρχείου snmpd.conf:
`sudo nano /etc/snmp/snmpd.conf`
 - a. Εντοπίστε και αλλάξτε το agentAddress σε: agentAddress udp:161
 - b. Βρείτε και προσθέστε στα rocommunity's την ακόλουθη γραμμή:
`rocommunity public`
 - c. Αποθηκεύστε και βγείτε από το αρχείο (στον επεξεργαστή nano, πατήστε Ctrl + X, έπειτα πληκτρολογήστε Y και πατήστε Enter για να επιβεβαιώσετε την αποθήκευση).
4. Επαναφορτώστε την υπηρεσία snmpd:
`sudo service snmpd restart`

3.4 Ρυθμιση της ημερομηνίας

1. `timedatectl set-timezone 'Europe/Athens'`
2. `timedatectl` (Έλεγχος)

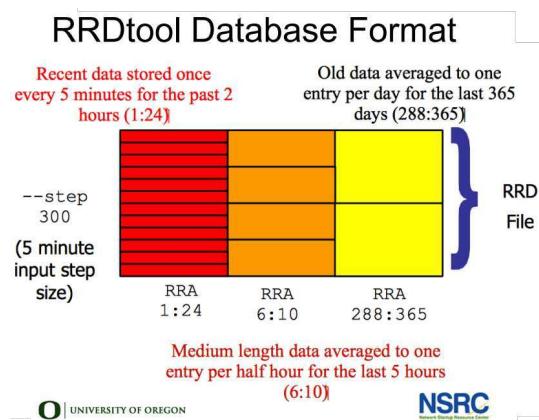
3.5 Απενεργοποίηση Firewall

- Ubuntu Server:
 - `sudo systemctl disable ufw`
 - `sudo ufw status` (έλεγχος)
- Windows
 - Στο Command Prompt (Administrator) :
`netsh advfirewall set allprofiles state off`

4. Cacti

Το Cacti ξεκίνησε από τον Ian Berry στις 2 Σεπτεμβρίου 2001, ενώ ακόμα μάθαινε PHP και MySQL στο λύκειο και διούλευε σε μία μικρή εταιρία παροχής δικτύου ISP. Ο κεντρικός του στόχος ήταν "να προσφέρει μεγαλύτερη ευκολία χρήσης από το RRDtool και μεγαλύτερη ευελιξία από το MRTG".

Είναι ανοικτού κώδικα που υλοποιήθηκε με τη γλώσσα PHP και ενημερώνεται συνεχώς μέχρι και σήμερα. Δημιουργεί γραφήματα με το RRDtool από δεδομένα απόδοσης συσκευών όπου αποθηκεύονται σε αρχεία RRD (Round Robin Database) που συλλέγονται μέσω SNMP (Simple Network Management Protocol) με προγραμματισμένες εργασίες (cron jobs). Η συχνότητα συλλογής των δεδομένων εξαρτάται από το ρυθμισμένο διάστημα συλλογής (συνήθως κάθε 5 λεπτά).



Η μακροχρόνια παρουσία του έχει καλλιεργήσει μια μεγάλη και αφοσιωμένη κοινότητα χρηστών. Διαθέτει ένα πολύ μεγάλο, κατανοητό και αναλυτικό Documentation στην επίσημη ιστοσελίδα docs.cacti.net και σε Github github.com/Cacti/documentation.

Το επίσημο φόρουμ forums.cacti.net είναι ακόμα ενεργό από το 2002 μέχρι και σήμερα με σύνολο αναρτήσεων 279.015 και 54.366 θέματα.

Μέσω της αρχιτεκτονικής του Plugins και της μεγάλης κοινότητας στο GitHub, το Cacti έχει επεκταθεί πολύ. Υπάρχουν πολλά τέτοια δημοφιλή plugins που μπορούν να προστεθούν χειροποίητα, όπως:

- Thold: επιτρέπει τη δημιουργία αυτοματοποιημένων ελέγχων σε γραφήματα ενημερώνοντας για πιθανά προβλήματα.
- Syslog: δυνατότητα ανίχνευσης σφαλμάτων και προβολής δεδομένων από εκατοντάδες χιλιάδες κόμβους.
- Monitor: παρέχει έναν πίνακα ελέγχου συσκευών και επισημαίνει τις συσκευές που αντιμετωπίζουν βλάβες.
- Weathermap: διαγράμματα και κινούμενα γραφήματα-σχέδια ενός δικτύου.
- Intro Page: εμφάνιση των κύριων γραφημάτων στην κεντρική σελίδα της κονσόλας του Cacti
- Cycle.

Επιπλέον, για όποιους επιθυμούν να χρησιμοποιήσουν API γραφήματα στα “Plugins” τους εκτός από το RRDtool, παρέχονται πακέτα γραφικής απεικόνισης βασισμένα σε JavaScript HTML5, όπως το Billboard.js, D3, Chart.js, DyGraphs και το jQuery Sparklines

Έχει εύκολη εγκατάσταση, αυτόματη ανακάλυψη συσκευών και προσθήκη επεκτάσεων plugins αλλά τα πραγματα δυσκολεύονται μετά γιατί είναι πολύ ευάλωτο στα σφαλματα. Τυχόν σφάλματα κατα τη μη αυτόματη εγκατάσταση είναι κουραστική και χρονοβόρα, αλλά με τα documentation, forums και την μεγάλη κοινότητα που έχει μπορουν να αντιμετωπιστούν .

Προσφέρει πολύ μεγάλη ευελιξία στον χρήστη, όπως:

- Δημιουργία και προσαρμογή γραφημάτων για διάφορες μετρικές και πηγές.
- Οι χρήστες μπορούν να αναπτύξουν δικά τους plugins ή Scripts.
- Διαθέτει ισχυρή διαχείριση χρηστών και δικαιωμάτων.

και άλλα.

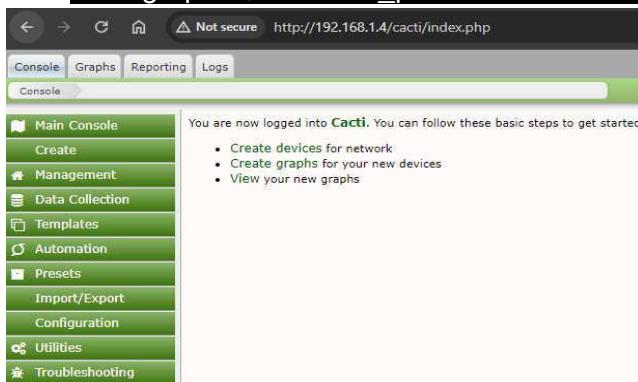
Εγκατάσταση Cacti

Στην ιστοσελίδα www.cacti.net/info/downloads υπάρχουν διάφορες επιλογές εγκατάστασης. Η πιο εύκολη είναι οι εκδόσεις σε πακέτα όπου η εγκατάσταση γίνεται με μία μόνο εντολή. Για το Ubuntu Server :

1. `sudo apt get install cacti`
2. Πληκτρολόγηση “YES” για συνέχεια.
3. Επιλογή apache2 και ENTER (Επιλογή ως HTTP server το apache2).
4. Επιλογή YES, για να εγκατασταθεί και να ρυθμιστή αυτόματα η Βάση Δεδομένων.
5. Πληκτρολόγηση κωδικού για Cacti και επιλογή YES.

Είσοδος

1. Εισαγωγή στο πρόγραμμα περιήγησης το IP address του ubuntu server και στο τέλος /cacti : Π.Χ.
<http://192.168.1.4/cacti/>
2. Συμπλήρωση Ονόματος χρήστη ως “admin” και του κωδικού που ορίστηκε στην εγκατάσταση στο βήμα 5.
Σε περίπτωση σφάλματος, για την εύρεση του κωδικού εκτέλεσε στο ubuntu server την παρακάτω εντολή:
`sudo grep "\$database_password"/etc/cacti/debian.php`

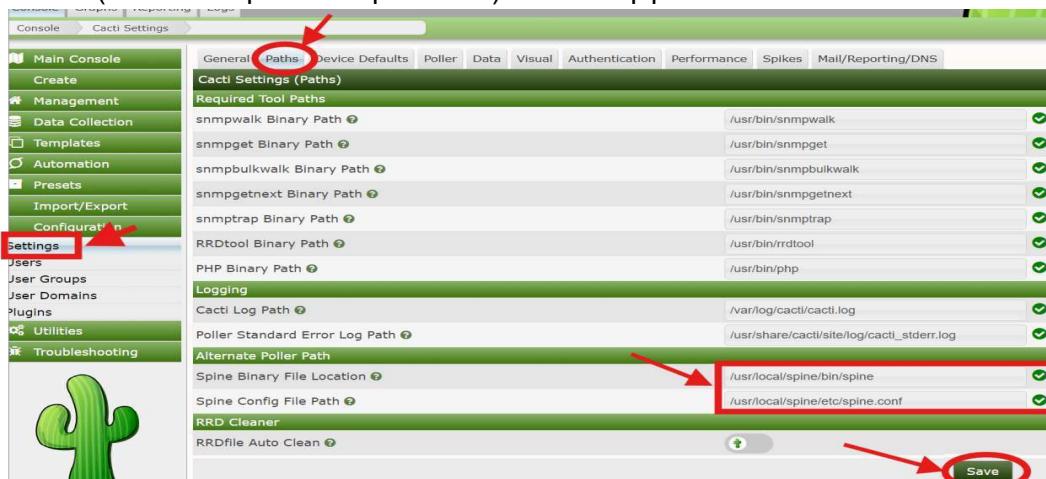


Εγκατάσταση spine

Το Spine είναι η γρήγορη αντικατάσταση για το cmd.php. Είναι γραμμένο σε C για να εξασφαλίσει την απόλυτη απόδοση για τη συλλογή δεδομένων από συσκευές και είναι

πολυνηματικό. Οι χρόνοι συλλογής δεδομένων είναι πολύ λιγότεροι από 60 δευτερόλεπτα. Η εγκατάσταση γίνεται ως εξής εκτελώντας με την σειρά της εντολές:

1. `sudo apt install build-essential dos2unix dh-autoreconf help2man libssl-dev`
2. `sudo apt install libmysql++-dev librrds-perl libsnmp-dev libmysqlclient-dev libtool`
3. `sudo apt update`
4. `sudo wget https://files.cacti.net/spine/cacti-spine-1.2.26`
Η έκδοση του spine πρέπει να είναι ίδια με του Cacti στη δεξιά γωνία στο *Main console* !!
5. `tar xfz cacti-spine-1.2.26.tar`
Αποσυμπίεση του αρχείου spine
6. `cd cacti-spine-1.2.26`
7. `./bootstrap`
8. `./configure`
9. `make`
10. `sudo make install`
11. `sudo chown root:root /usr/local/spine/bin/spine`
12. `sudo chmod +s /usr/local/spine/bin/spine`
13. `sudo cp /usr/local/spine/etc/spine.conf.dist /usr/local/spine/etc/spine`
14. `sudo nano /usr/local/spine/etc/spine.conf`
Τροποποίηση των δεδομένων ώστε να είναι ίδια με το αρχείο config.php όπου βρίσκεται συνήθως στο `/usr/share/cacti/site/include`. Για να δείτε τα δεδομένα του config.php εκτελέστε την εντολή :
`sudo nano /usr/share/cacti/site/include/config.php`
Σε εγκατάσταση χωρίς apt το αρχείο cacti μπορεί να είναι στο `"/opt/cacti/include"`.
15. Μετάβαση στο *Console* -> *Configuration* -> *Settings* -> *Path* και εισαγωγή της διαδρομής του spine(`/usr/local/spine/bin/spine`) και του αρχείου spine.conf (`/usr/local/spine/etc/spine.conf`) και επιλογή “Save”.



16. Μετάβαση στο *Console* -> *Configuration* -> *Settings* -> *Poller* και αλλαγή του “Poller type” από cmd.php σε spine.

17. Ανανέωση της σελίδας μετά από 5 λεπτά και μετάβαση στο Logs (πάνω αριστερά στη γωνία). Άν το Method = spine τότε το cacti χρησιμοποιεί το spine για polling.

Console Graphs Reporting Logs
View Log
Log Filters All 229 Entries
Log [Total Lines: 229 - Admin view - Unfiltered]
05/17/2024 23:05:02 - SYSTEM MAINT STATS: Time:0.01
05/17/2024 23:05:02 - SYSTEM STATS: Time:0.1502 Method:spine Processes:1 Threads:1 Hosts:0 HostsPerProcess:0 DataSources:0 RRDsProcessed:0
05/17/2024 23:00:02 - SYSTEM MAINT STATS: Time:0.02
05/17/2024 23:00:01 - SYSTEM STATS: Time:0.1593 Method:spine Processes:1 Threads:1 Hosts:0 HostsPerProcess:0 DataSources:0 RRDsProcessed:0

Ρυθμιση του Polling σε 30 δευτερόλεπτα

Επιθέσεις που θα δοκιμαστούν στα παρακάτω κεφάλαια θα εμποδίσουν την συλλογή δεδομένων του θύματος με SNMP από το Cacti. Η προκαθορισμένη τιμή του κύκλου της συλλογής δεδομένων (Polling) με είναι 5 λεπτά που δεν αρκεί για την προβολή των επιπτώσεων της επίθεσης. Μετά την εγκατάσταση του Spine, ακολουθούν τα βήματα για τη ρύθμιση του Polling στα 30 δευτερόλεπτα:

1. *Console -> Configuration -> Settings -> Poller :*
αποεπιλογή Data Collection Enabled, αλλαγή του Poller Interval σε 30 seconds και ,Cron/Daemon Interval σε 1 minute (Προερετικό : Αλλαγη του Data Collector Processes και Threads per Process σε 10) και Save
2. *Console -> Configuration -> Settings -> Visual :*
Αλλαγή Rows Per Page σε 750
3. *Console -> Presets -> Data Profiles -> 30 Second Collection :*
Αλλαγή του Heartbeat σε 60 seconds, ενεργοποίηση επιλογής Default και Save
4. Εκτέλεση στο VM1 ubuntu server της παρακάτω εντολές με τη σειρά:
 - a. `sudo mysql -u root -p` και εισάγεται τους κωδικούς.
 - b. `use cacti`
 - c. `UPDATE data_template_data SET rrd_step=30 WHERE rrd_step=300;`
 - d. `UPDATE data_template_rrd SET rrd_heartbeat=60;`
5. *Console -> Utilities -> System utilities* : κλίκ με τη σειρά το Rebuild Poller Cache ,Rebuild Resource Cache και τέλος Rebuild SNMP Agent Cache.
6. *Console -> Templates -> Data Source*
Select all -> Change Profile και επιλογή 30 seconds

| Name | Status |
|------------|--------|
| Collection | Active |

MikroTik - Device - Health - Core Voltage

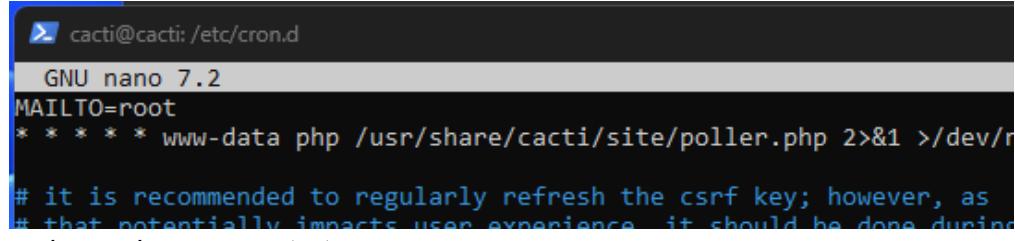
New Data Source Profile
30 Second Collection

NOTE: This change only will affect future Data Sources and does not alter existing Data Sources.

Cancel Continue

7. Αλλαγή των ρυθμίσεων cron από 5 λεπτά σε 1 , εκτελώντας :

- `sudo nano /etc/cron.d/cacti`
- Διαγραφή “/5” όπως την παρακάτω εικόνα και CTL-X, Yes και Enter.



```
cacti@cacti:/etc/cron.d
```

```
GNU nano 7.2
MAILTO=root
* * * * * www-data php /usr/share/cacti/site/poller.php 2>&1 >/dev/r
# it is recommended to regularly refresh the csrf key; however, as
# that potentially impacts user experience, it should be done during
# a low-traffic period or at night.
```

- `sudo service cron restart`

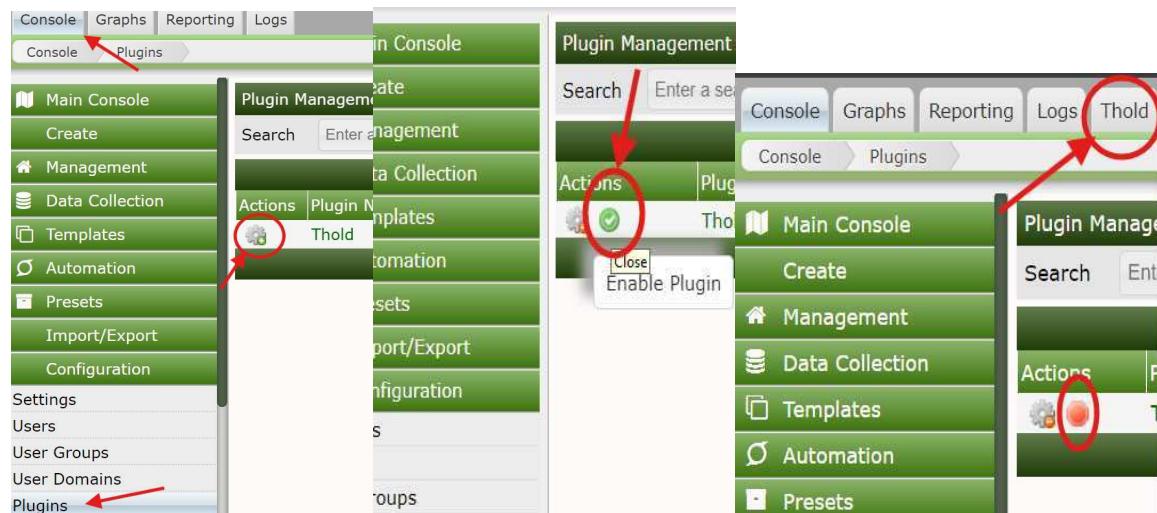
8. *Console -> Configuration -> Settings -> Poller* : Ενεργοποίηση polling επιλέγοντας Data Collection Enabled

9. Ελεγχος από το Log : Αν το SYSTEM STATS: Time:2.3053 Method:spine.... εμφανίζεται κάθε 30 δευτερόλεπτα τότε είναι επιτυχής η εγκατάσταση spine.

Εγκατάσταση Thresholds

Επιτρέπει τον καθορισμό ορίων (thresholds) για διάφορα γραφήματα που βοηθούν στον εντοπισμό ανωμαλιών και προβλημάτων, ενεργοποιώντας ειδοποιήσεις όταν υπερβαίνουν τα προκαθορισμένα όρια.

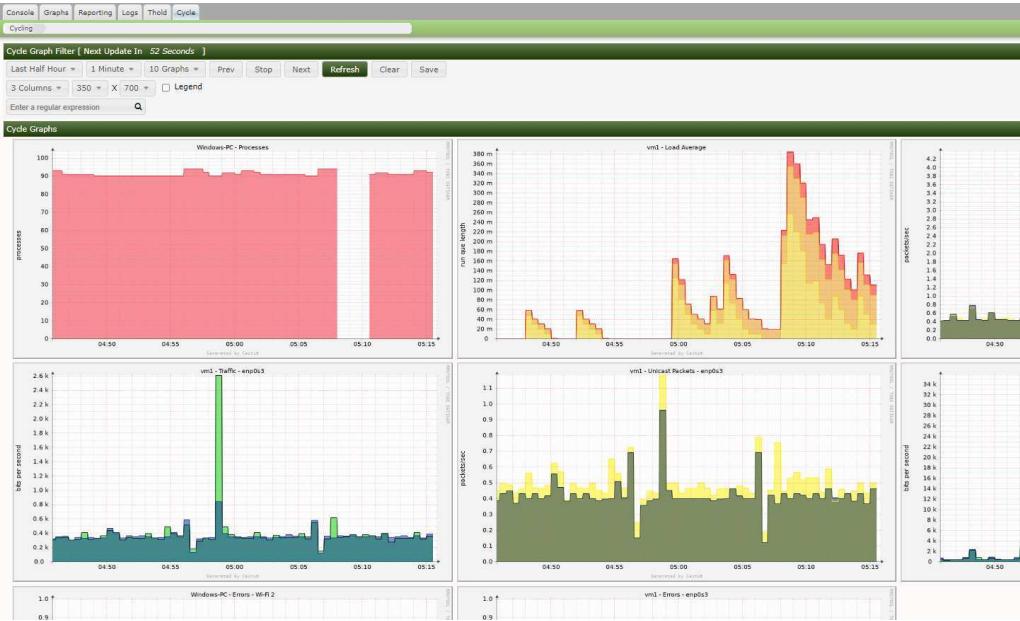
- `wget https://github.com/Cacti/plugin_thold/archive/refs/tags/v1.8.1.tar.gz`
- `tar -xf v1.8.1.tar.gz`
- Μετονομασία του αρχείου
`mv plugin_thold-1.8.1/ thold`
- Μεταφορά στο Plugins αρχείο του Cacti
`sudo mv thold /usr/share/cacti/site/plugins`
- Στο cacti *Console -> Plugins -> Install Plugin (Thold)* και ύστερα *Enable Plugin*. Και θα εμφανιστή πάνω αριστερά η επιλογή Thold.



Εγκατάσταση Cycle

Επιτρέπει τη διαχείριση των κυκλωμάτων ενημέρωσης και πιο φιλική παρουσίαση γραφημάτων.

1. `git clone https://github.com/Cacti/plugin_cycle.git`
2. Μετονομασία του αρχείου: `mv plugin_cycle/ cycle`
3. Μεταφορά στο Plugins αρχείο του Cacti
`sudo mv cycle /usr/share/cacti/site/plugins`
4. Στο cacti *Console* -> *Plugins* -> *Install Plugin (Cycle)* και ύστερα *Enable Plugin*. Και θα εμφανιστή πάνω αριστερά η καρτέλα Cycle.



- Σφαλματα

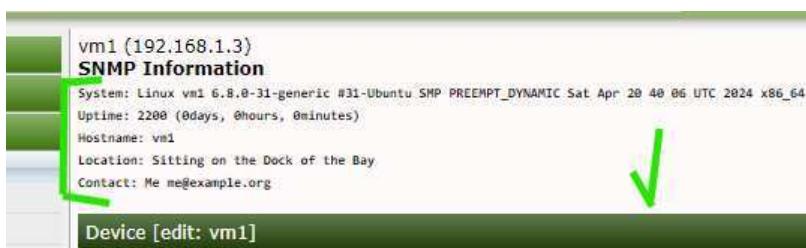
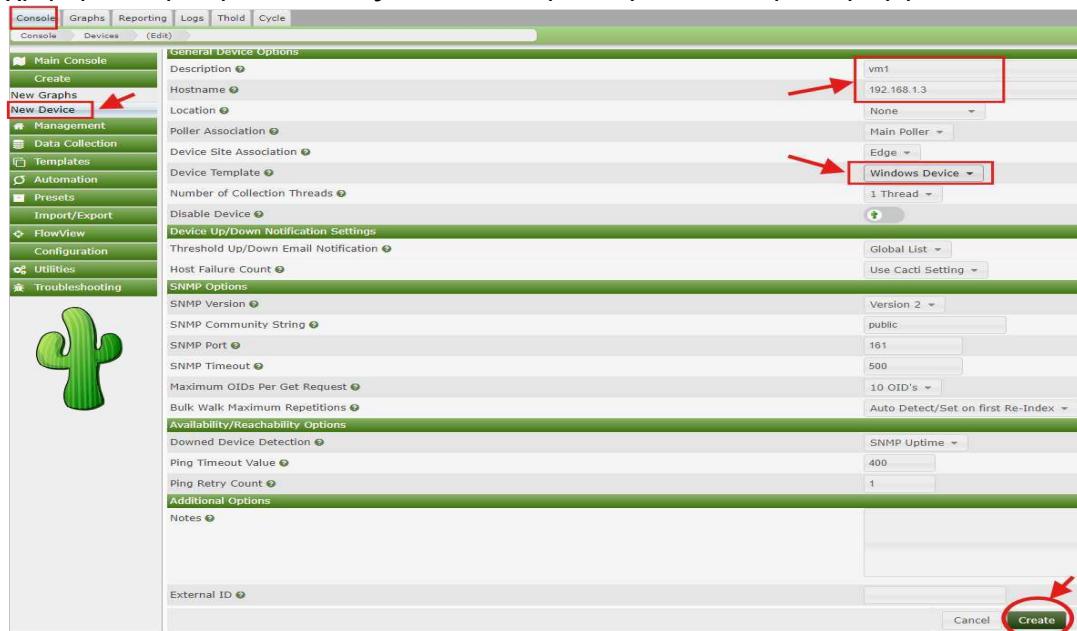
- Fatal error 404 : μπορεί να εμφανιστεί σε περίπτωση εγκατάστασης Cycle από tar αρχείου `plugin_cycle-4.1.tar.gz`.

Προσθήκη συσκευών

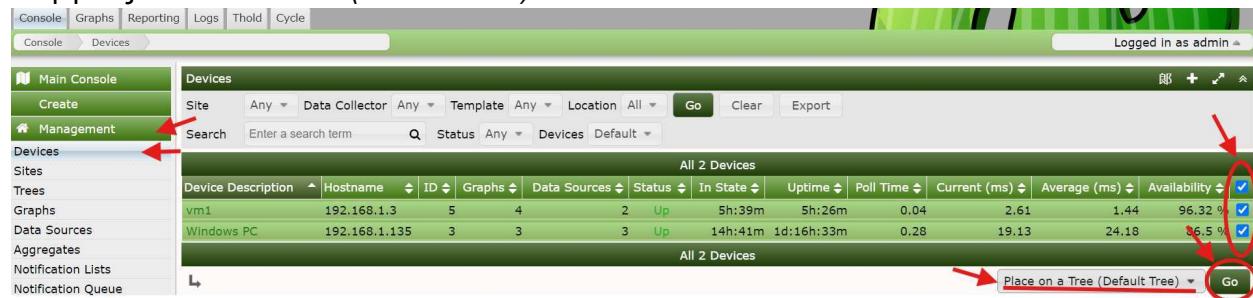
Αυτόματα από : Automation > Discovered Devices , επιλογή της προτεινόμενης συσκευής, της ενεργειας “Add Device” και Go.

Χειροποίητα από : Console > Create -> New Device

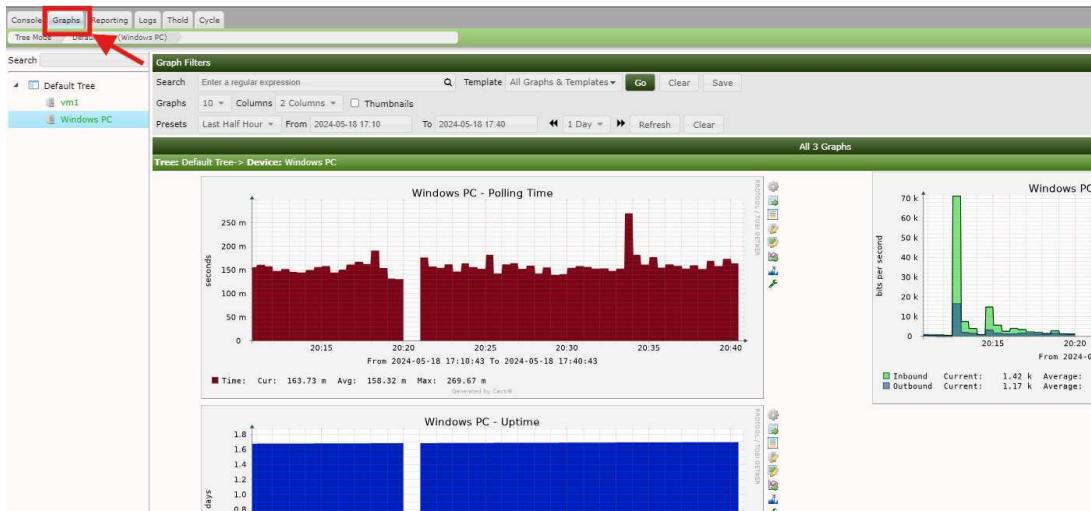
description: “Όνομα συσκευής”, Hostname “IP address” και device template “Τύπος συσκευής”. Η vm1 ,που δημιουργείται στην παρακάτω εικόνα, είναι ένα άλλο ubuntu server όπως η άλλες 3 εικονικές μηχανές ,των εφαρμογών διαχείρισης δικτύου που δημιουργήθηκαν στην αρχη, και θα χρησιμοποιηθεί για επιθέσεις. Με το ίδιο τρόπο γίνεται και η εισαγωγή του windows pc.



Στη συνεχεία : Console -> Management -> Device Επιλογή των καινούργιων συσκευών και της ενεργειας “Place on a Tree(Default Tree)” και Go.



Έτσι έχουμε εισάγη στο Graphs όλες της συσκευές σε ένα δέντρο και μπορούμε να έχουμε μια εύκολη πρόσβαση στα γραφήματα τους.



- **Σφαλματα:**

- Fatal error 505 ή αν λείπει το δέντρο : αλλαγή του URL link σε http://.....<IP>...../cacti/graph_view.php?action=tree ή Log out και μετά Log in ξανά.

Δημιουργία γραφημάτων

Για την ανάλυση επιθέσεων μεταξύ Windows PC και VM1 εικονική μηχανή, θα δημιουργηθούν οι παρακάτω τύποι του γραφήματος “SNMP - Interface Statistics”:

1. In/Out Bits: συνολική κίνηση δικτύου σε bits
2. In/Out Errors/Discards: Δίχνει σφάλματα ή απορρίψεις πακέτων. Είναι χρήσιμο γιατί σε περιπτώσεις επιθέσεων θα υπάρχει αύξηση στα σφάλματα ή στις απορρίψεις πακέτων λόγω της υπερβολικής κίνησης
3. In/Out Unicast: Τα unicast πακέτα είναι πακέτα δεδομένων που αποστέλλονται από έναν μόνο αποστολέα σε έναν μόνο παραλήπτη σε ένα δίκτυο

Η παρακάτω διαδικασία δημιουργίας γραφήματος είναι ίδια και για της 2, αλλάζοντας μόνο την συσκευή και των τύπο του γραφήματος “SNMP - Interface Statistics”: Console >Create>New Graph

1. στο Device επιλογή συσκευής
2. Ανανέωση του πίνακα Data Query [SNMP - Interface Statistics] από το πράσινο σύμβολο ανανέωσης και επιλογή της διεπαφής δικτύου που είναι συνδεδεμένο στο δίκτυο, δηλαδή την διεπαφή που έχει το ίδιο IP address με την επιλεγμένη συσκευή
3. Επιλογή του τύπου γραφήματος και Create , το ίδιο και για τους 3 τύπους In/Out Bits , In/Out Errors/Discards και In/Out Unicast.

The screenshot shows the Zabbix interface with the following details:

- Left Sidebar:** Contains links for Main Console, Create, New Graphs, New Device, Management, Data Collection, Templates, Automation, Presets, Import/Export, Configuration, Utilities, and Troubleshooting.
- Top Bar:** Shows 'Console', 'Graphs', 'Reporting', 'Logs', 'Thresholds', and 'Cycle'. The 'Console' tab is selected.
- Central Area:**
 - New Graphs for [vm1] (192.168.1.3 Windows Device):** The 'Device' field contains 'vm1'.
 - Graph Types:** Set to 'All'.
 - Search:** 'Enter a search term'.
 - Rows:** 'Default'.
 - Buttons:** 'Go', 'Clear', 'Save'.
 - Graph Template:** 'Select a graph type to create' with a 'Create' button.
 - Data Query [SNMP - Get Mounted Partitions]:** Shows 'No Items Found'.
 - Data Query [SNMP - Get Processor Information]:** Shows 'No Items Found'.
 - Data Query [SNMP - Interface Statistics]:** Shows 'All 2 Items' in a table:

| Index | Status | AdminStatus | Description | Name (IF-MIB) | Alias (IF-MIB) | Type | Speed | High Speed | Hardware Address | IP Address | IPv6 Address |
|-------|--------|-------------|-------------|---------------|----------------|------|-----------|------------|-------------------|-------------|--------------------------|
| 1 | Up | Up | lo | lo | | 24 | 10000000 | 10 | 127.0.0.1 | ::1 | |
| 2 | Up | Up | enp0s3 | enp0s3 | | 6 | 100000000 | 1000 | 08:00:27:48:BD:B9 | 192.168.1.3 | fe80::a00:27ff:fe48:bdb9 |
- Bottom Right:** 'Select a Graph Type to Create' dropdown set to 'In/Out Bits' with a 'Create' button.

Για την παρακολούθηση TCP καθυστερήσεων θύματος windows PC ,σε επιθέσεις από VM1, θα χρειαστεί η δημιουργία επιπλέων γραφήματος για το Windows PC από Console >Create>New Graph (όπως προηγουμένως) και στην καρτέλα New Graph Template επιλογή Select Graph type to create το “PING - Advanced ping” και Create. Στην επόμενη σελίδα επιλογή ping protocol ώρια 80 και τέλος Create.

- **Προειδοποίησης**

- Πριν την δημιουργία γραφήματος για συσκευές linux (Device Template: Local linux machine), πρέπει να προστεθεί από Management > Devices στην καρτέλα Associated Data Queries το SNMP - Interface Statistics, επιλέγοντας το στο Add Data query και κλικ στο Add για να προστεθεί.
- Χρειάζεται έλεγχος των step γραφημάτων αν γίνεται polling μικρότερα από 5 λεπτά. Management > Data Source για το καθένα κλικ και ενεργοποίηση το *Turn On Data Source Debug Mode. , *Turn On Data Source Info Mode. Έλεγχος της τιμής step και counter (heartbeat) στο Data Source Debug.

Για 30 seconds polling, το step πρέπει να είναι 30 και counter 60.

Αν δεν είναι εκτέλεση των εντολών Π.Χ.

```
sudo /usr/bin/rrdtool tune /usr/share/cacti/site/rra/pc_traffic_in_35.rrd --step 30
sudo /usr/bin/rrdtool tune /usr/share/cacti/site/rra/pc_traffic_in_35.rrd --heartbeat traffic_out:60
```

- Αν δημιουργηθεί 64-bit γράφημα, για κάποιες συσκευές μπορεί να μην εμφανίσει τίποτα το γράφημα. Για αυτό είναι καλύτερο να δημιουργηθούν τα απλά γραφήματα.

Δημιουργία Thresholds

Προσθήκη Trigger-Threshold για την ανίχνευση επιθέσεων όταν τα πακέτα έχουν απώλεια πάνω από 96%.

(Κανονικά το γράφημα έχει όνομα με μορφή “[device] - Advanced Ping” αλλά για ευκολεία πρόσθεσα στο τέλος και το “ - TCP ” από τις ρυθμίσεις Template)

1. Management > Thresholds κλικ στο “+” πάνω δεξιά

2. Επιλογή Create Type : Non Templatized, Device : Windows-PC, Graph : Windows-PC - Advance, Ping - TCP, Data Source: loss (απώλεια πακέτων) και κλικ στο Create.

3. Ρύθμιση όπως την παρακάτω εικόνα και Save:

4. Θα εμφανιστή στην καρτέλα Thold σε κατάσταση Ok

The screenshot shows a web-based monitoring interface with a green header bar. The top navigation bar includes links for Console, Graphs, Reporting, Logs, Thold (which is highlighted in blue), and Cycle. On the right side of the header, it says "Logged In as admin". Below the header is a search bar with fields for Search, Site, All, Device, and Any, along with Go and Clear buttons. There are also dropdown menus for Template (All), Data Template (All), Status (All), and Thresholds (Default). The main content area is titled "Threshold Status" and displays a table of thresholds. The table has a header row with columns: Actions, Name, External ID, Enabled, ID, Ack Detail, Type, Current, High, Low, Trigger, Duration, Repeat, Triggered, In State, Ack Required. A single threshold row is shown, indicating 1 threshold. The threshold details are: Name: Windows-PC - Advanced Ping - TCP [loss], Enabled: Yes, ID: 3, Type: High / Low, Current: 0 - / 96 - / - 1 Minute, Trigger: N/A Every Minute, Duration: N/A, Repeat: N/A, Triggered: No Since Created, In State: Ok, Ack Required: No. The status bar at the bottom of the table shows color-coded categories: Alert (red), Baseline Alert (orange), Warning (yellow), Notice (light green), Ok (green), Acknowledgment (purple), and Disabled (grey).

| Actions | Name | External ID | Enabled | ID | Ack Detail | Type | Current | High | Low | Trigger | Duration | Repeat | Triggered | In State | Ack Required |
|---------|---|-------------|---------|----|------------|------------|-------------------------|------|--------------|---------|----------|------------------|-----------|----------|--------------|
| | Windows-PC - Advanced Ping - TCP [loss] | | Yes | 3 | | High / Low | 0 - / 96 - / - 1 Minute | N/A | Every Minute | | | No Since Created | Ok | No | |

Αυτό το threshold πλέον θα γίνεται κόκκινο και θα εμφανίζει μήνυμα Alert όταν το γράφημα έχει απώλεια πακέτων πάνω από 96ms.

5.Zabbix

Το Zabbix είναι ένα εργαλείο λογισμικού ανοιχτού κώδικα για την παρακολούθηση υποδομών πληροφορικής όπως δίκτυα, διακομιστές, εικονικές μηχανές και υπηρεσίες cloud και πολλά άλλα, το οποίο ξεκίνησε την ανάπτυξή του το 2001 από τον Alexei Vladishev και γράφτηκε σε C (server, proxy, agent), Go (agent2), PHP (frontend) και Java (Java gateway).

Επιτρέπει την δωρεάν χρήση όλων των λειτουργιών του χωρίς την ανάγκη πρόσθετης άδειας. Αν και είναι λογισμικό ανοιχτού κώδικα, η ανάπτυξή του πραγματοποιείται ως κλειστό προϊόν από την εταιρεία Zabbix LLC με έδρα στη Λετονία και γραφεία στις ΗΠΑ, τη Βραζιλία, το Μεξικό και την Ιαπωνία.



Με την πάροδο των ετών, το Zabbix έχει εξελιχθεί σε ένα από τα πιο αξιόπιστα και ευέλικτα εργαλεία παρακολούθησης, επιτρέποντας στους διαχειριστές συστημάτων και δικτύων να διατηρούν την ομαλή λειτουργία των υποδομών τους και να προλαμβάνουν προβλήματα πριν αυτά επηρεάσουν τις επιχειρησιακές διαδικασίες.

Παρέχει πλούσια λειτουργικότητα, όπως αυτόματη ανίχνευση συσκευών, έτοιμες προσαρμοσμένες ειδοποιήσεις, διαχείριση συμβάντων, παρακολούθηση δικτύου από απόσταση και άλλα.

Προσφέρει συλλογή δεδομένων το λιγότερο κάθε 10 δευτερόλεπτα με Agent, SNMP, JMX και IPMI και αυτόματη δημιουργία γραφημάτων για κάθε πρότυπο συσκευής.

Παρέχει πανεύκολη εγκατάσταση χωρίς καμία χειροκίνητη διαδικασία και πολλές λειτουργίες χωρίς καμία προσθήκη επιπλέων plugin.

Η μακροχρόνια παρουσία του Zabbix έχει καλλιεργήσει μια μεγάλη και ενεργή κοινότητα χρηστών (www.zabbix.com/community). Υπάρχει εκτενής και κατανοητή τεκμηρίωση στην επίσημη ιστοσελίδα του Zabbix (www.zabbix.com/documentation) και στο GitHub (github.com/zabbix). Το επίσημο φόρουμ (www.zabbix.com/forum/) είναι ενεργό από το 2005, παρέχοντας ένα πλούσιο αρχείο αναρτήσεων και θεμάτων για την υποστήριξη των χρηστών. Επίσης υπάρχει μια πάρα πολύ μεγάλη ποσότητα πρότυπων κοινότητας στο github.com/zabbix/community-templates οπου μπορεί ο καθένας να κάνει import στο zabbix.

Εγκατάσταση (<https://www.zabbix.com/download>)

- `cd ~`
- Εγκατάσταση του αποθετηρίου Zabbix
`wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu24.04_all.deb`
- `sudo dpkg -i zabbix-release_6.4-1+ubuntu24.04_all.deb`
- Εγκατάσταση διακομιστή Zabbix, frontend, Agent
`sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent`
- Εγκατάσταση MySQL (αν δεν υπάρχει ήδη)
`sudo apt-get install mysql-server`
- Δημιουργία αρχικής βάσης δεδομένων
`sudo mysql -uroot -p`
 - `mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;`
 - `mysql> create user zabbix@localhost identified by 'password';`
 - `mysql> grant all privileges on zabbix.* to zabbix@localhost;`
 - `mysql> set global log_bin_trust_function_creators = 1;`
 - `mysql> quit;`
- Εισαγωγή του αρχικού σχήματος και των δεδομένων.
`sudo zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix`
- Απενεργοποίηση της επιλογής log_bin_trust_function_creators
`sudo mysql -uroot -p`
 - `mysql> set global log_bin_trust_function_creators = 0;`
 - `mysql> quit;`
- Διαμορφωση της βάσης δεδομένων για τον διακομιστή Zabbix
`sudo nano /etc/zabbix/zabbix_server.conf`
 - `DBPassword=123`
- `systemctl restart zabbix-server zabbix-agent apache2`
- `systemctl enable zabbix-server zabbix-agent apache2`
- Προβολή και αντιγραφή της διεύθυνσης ip : `ip addr`
- Επικόλληση στο πρόγραμμα περιήγησης το : `http://<ip address>/zabbix`
- Επιλογή γλώσσας και Next Step
- Έλεγχος των προαπαιτούμενων εάν όλα είναι εντάξει και Next Step
- Διαμόρφωση σύνδεσης DB εισάγοντας κωδικό και Next Step
- Ρύθμιση του ονόματος Zabbix server και Next Step

Προσθήκη συσκευών

Monitoring > Hosts > Create Host

The screenshot shows the 'Create host' dialog in Zabbix. On the left, the navigation menu is visible with 'Hosts' selected. The main form has the following fields:

- Host name:** vm1
- Visible name:** vm1
- Templates:** Linux by SNMP
- Groups:** Linux servers, Templates/Operating systems, Virtual machines
- Interfaces:**
 - Type: SNMP, IP address: 192.168.1.3, Connect to: IP, Port: 161, Default: checked
 - SNMP version: SNMPv2
 - SNMP community: \${SNMP_COMMUNITY}
 - Use bulk requests: checked
- Description:** (empty)

At the bottom right of the dialog are 'Add' and 'Cancel' buttons, with the 'Add' button highlighted by a red arrow.

Δημιουργία χάρτη δικτύου

The screenshot shows the 'Maps' page in Zabbix. The navigation menu has 'Maps' selected. A network diagram titled 'Local network' is displayed, showing the following components and their status:

- Zabbix server (127.0.0.1) - OK
- VM Virtual Box (vm1, 192.168.1.3) - OK
- Windows Laptop
- Wi-Fi Router
- windows pc (192.168.1.135) - 7 problems

At the top right of the map area is an 'Edit map' button, highlighted by a red arrow.

Διαμόρφωση dashboard

The screenshot shows the 'Global view' dashboard in Zabbix. The navigation menu has 'Dashboard' selected. The dashboard displays several monitoring panels:

- vm1: Interface enp0s3(): Network traffic**: Shows traffic over time for various interface metrics.
- win pc network traffic**: Shows network traffic for the windows pc host.
- vm1: Linux: CPU utilization**: Shows CPU utilization over time for the vm1 host.
- windows pc: Windows: CPU utilization**: Shows CPU utilization over time for the windows pc host.
- System information**: Displays system status metrics like availability and errors.

At the top right of the dashboard area is an 'Edit dashboard' button, highlighted by a red arrow.

Ρυθμιση του Polling σε 30 δευτερόλεπτα

Για κάθε συσκευή:

1. Configuration > Hosts , κλικ στο Discovery

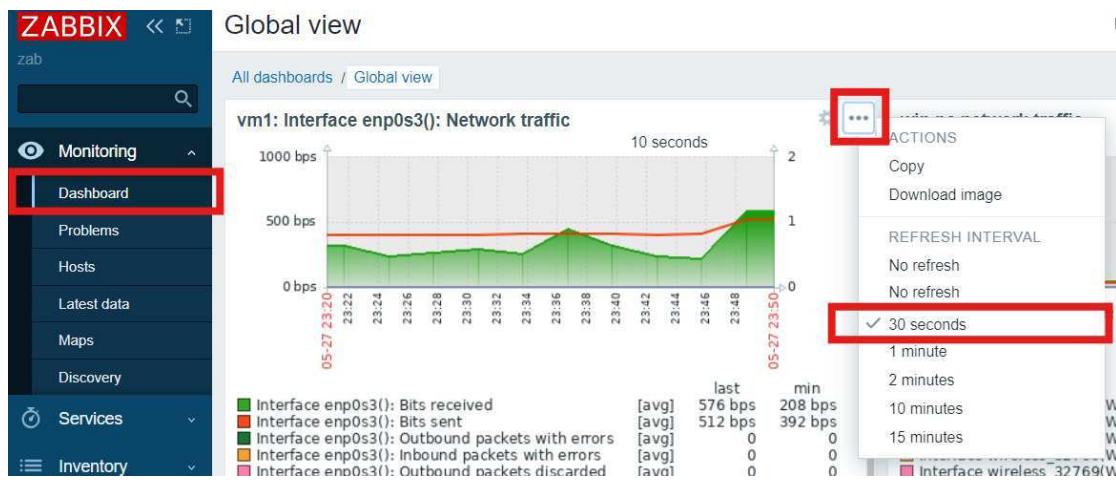
| Name | Items | Triggers | Graphs | Discovery |
|------------|-----------|--------------|-----------|-------------|
| vm1 | Items 59 | Triggers 24 | Graphs 11 | Discovery 5 |
| windows pc | Items 361 | Triggers 162 | Graphs 41 | Discovery 3 |

2. κλικ στο Network interfaces discovery και Αλλαγή του Update interval σε “30s”
3. κλικ πάνω δεξιά στο item prototypes, κλικ στο κάθε item και αλλαγή Update interval σε “30s”

Item prototypes

| Name | Key | Interval | History | Trends | Type |
|--|---|----------|---------|--------|------------|
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Bits received | net.if.in[ifHCInOctets.#SNMPINDEX] | 30s | 7d | 365d | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Bits sent | net.if.out[ifHCOutOctets.#SNMPINDEX] | 30s | 7d | 365d | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Inbound packets discarded | net.if.in.discards[ifInDiscards.#SNMPINDEX] | 30s | 7d | 365d | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Inbound packets with errors | net.if.in.errors[ifInErrors.#SNMPINDEX] | 30s | 7d | 365d | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Interface type | net.if.type[ifType.#SNMPINDEX] | 1h | 7d | 0 | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Operational status | net.if.status[ifOperStatus.#SNMPINDEX] | 30s | 7d | 0 | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Outbound packets discarded | net.if.out.discards[ifOutDiscards.#SNMPINDEX] | 30s | 7d | 365d | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Outbound packets with errors | net.if.out.errors[ifOutErrors.#SNMPINDEX] | 30s | 7d | 365d | SNMP agent |
| *** Linux by SNMP: Interface (#IFNAME)(#IFALIAS): Speed | net.if.speed[ifHighSpeed.#SNMPINDEX] | 30s | 7d | 0 | SNMP agent |

- 4.



6. Συγκριση

| Χαρακτηριστικό | Zabbix | Cacti |
|--------------------------|---|--|
| Εύρος και Χαρακτηριστικά | Προσφέρει παρακολούθηση με και χωρίς πράκτορα, αυτόματη ανακάλυψη, πλήρης συστήματος ειδοποιήσεων, οπτικοποίηση, αυτοματοποίηση, κλιμακωσιμότητα, ενσωμάτωση, επεκτασιμότητα, δυνατότητες Τεχνητής Νοημοσύνης | Επικεντρώνεται στη γραφική απεικόνιση και με χαρακτηριστικά για διαχείριση συσκευών, συλλογή δεδομένων, δημιουργία γραφημάτων, πρότυπα και πακέτα, απομακρυσμένη συλλογή δεδομένων, ανακάλυψη και αυτοματοποίηση, διαχείριση χρηστών, plugins, θέματα και επεκτάσεις |
| Ευκολία Χρήσης | Απαιτεί περισσότερη εξοικείωση λόγω πληθώρας χαρακτηριστικών | Προσφέρει απλότητα και ευκολία χρήσης για γρήγορη οπτικοποίηση |
| Κλιμακωσιμότητα | Κατάλληλο για μεγάλες εγκαταστάσεις με δυνατότητα κατανεμημένης παρακολούθησης | Κατάλληλο για μικρές έως μεσαίες επιχειρήσεις με περιορισμένες ανάγκες |
| Χρήσης | Κατάλληλο για επιχειρήσεις που χρειάζονται πλήρη παρακολούθηση και ειδοποιήσεις | Κατάλληλο για επιχειρήσεις που επικεντρώνονται στην απεικόνιση τάσεων δεδομένων |
| Άδεια και Τιμολόγηση | Δωρεάν και ανοικτού κώδικα, με δυνατότητες πληρωμένων υπηρεσιών | 100% Δωρεάν ανοικτού κώδικα |
| Κοινότητα & Υποστήριξη | Μεγάλη Ενεργή κοινότητα, καλή τεκμηρίωση και επαγγελματική υποστήριξη διαθέσιμη | Μεγάλη Ενεργή κοινότητα, καλή τεκμηρίωση |
| Αναφορές | Εκτεταμένες δυνατότητες δημιουργίας αναφορών | Βασικές αναφορές |
| Ρύθμιση | Από το web UI | Για κάποιες χειροποίητα από τα αρχεία |
| Επεκτασιμότητα & Plugins | Μεγαλύτερη | Μεγάλη |
| Αποθήκευση δεδομένων | MySQL, PostgreSQL, Oracle, SQLite | RRDTool (Round-Robin Database) με MySQL |
| Υποστήριξη Πλατφορμών | Υποστήριξη για Linux, Windows, και άλλα λειτουργικά συστήματα | Κυρίως Linux, υποστήριξη για Windows μέσω τρίτων εργαλείων |
| Συναγερμοί | Προηγμένο σύστημα συναγερμών με πολλαπλά κριτήρια | Βασικοί συναγερμοί (threshold) |

Τόσο το Zabbix όσο και το Cacti έχουν τη δυνατότητα να αντιμετωπίσουν ορισμένα από τα μειονεκτήματά ή ελλείψης τους μέσω plugins. Για παράδειγμα, το Cacti αρχικά δεν παρέχει τη δυνατότητα συλλογής δεδομένων με IPMI, JMX, SSH, ή Telnet αλλά αυτές οι λειτουργίες μπορούν να προστεθούν μέσω plugins. Επίσης για πολύ μεγάλα σε κλίμακα συστήματα το αρχικό cacti με cmd.php poller είναι αργό στη συλλογή δεδομένων, όμως με το spine poller αυτό

το μειονέκτημα αντιμετωπίζεται. Το ίδιο και για το zabbix με διάφορα plugins όπως παρακολούθηση αρχείου καταγραφής με Log , παρακολούθηση της MySQL και των fork της με MySQL plugin και άλλα.

Για αυτό δεν μπορούμε να πούμε ότι έχουν διαφορές πέρα από τις παρακάτω:

- **Λειτουργίες και Εγκατάσταση:**
 - Το Zabbix προσφέρει περισσότερες λειτουργίες ενσωματωμένες από την αρχή, κάτι που απαιτεί περισσότερους πόρους και καθιστά την εγκατάσταση πιο περίπλοκη.
 - Αντίθετα, το Cacti παρέχει μια απλούστερη και ταχύτερη διαδικασία εγκατάστασης. Ωστόσο, για να επιτύχει κάποιες επιπλέον λειτουργίες, ενδέχεται να χρειαστεί η εγκατάσταση plugins ανάλογα με τις συγκεκριμένες ανάγκες του χρήστη.
- **Χρήση και Διεπαφή:**
 - Το Cacti διαθέτει πιο κατανοητή χρήση και φιλική διεπαφή χρήστη,
 - ενώ το Zabbix μπορεί να είναι πιο περίπλοκο για νέους χρήστες.
- **Ακρίβεια Παρακολούθησης και Γραφήματα:**
 - Το Cacti παρέχει ακριβή παρακολούθηση και σαφής γραφήματα.
 - Αντίθετα, το Zabbix μπορεί να έχει καθυστερήσεις και να μην δείχνει ακριβώς τις ώρες που συνέβησαν συγκεκριμένα γεγονότα. Για παράδειγμα, κατά τη διάρκεια μιας επίθεσης SYN flood, το Zabbix δεν έδειχνε ακριβώς την ώρα που αυξήθηκαν τα εξερχόμενα πακέτα του VM1 κατά την επίθεση.
- **Υποστήριξη και Διαθεσιμότητα:**
 - Το Zabbix διαθέτει γραφεία και υποστήριξη σε πολύ περισσότερες χώρες από το Cacti, παρέχοντας μεγαλύτερη πρόσβαση σε επαγγελματική υποστήριξη και συμβουλευτικές υπηρεσίες.

Για τα παρακάτω σενάρια επιθέσεων επέλεξα να χρησιμοποιήσω το Cacti λόγο της διαφοράς που έχει με το Zabbix στην λειτουργία, εγκατάσταση, χρήση, διεπαφή, ακρίβεια παρακολούθησης και στα γραφήματα.

7. Επιθέσεις DoS και Αποτελέσματα

1. **SYN flood attack** : είναι μια μορφή επιθέσεων DoS (Denial of Service) και κατακερματίζει τους διαθέσιμους πόρους μεταξύ πολλών αιτημάτων TCP SYN. Η διαδικασία είναι ως εξής:

- a. Χειραψία TCP(Handshake): Ο επιτιθέμενος υπολογιστής στέλνει ένα SYN πακέτο (αίτηση σύνδεσης) στον στόχο.
 - b. Απάντηση SYN-ACK: Ο προορισμός απαντά με ένα SYN-ACK πακέτο (επιβεβαίωση SYN) προετοιμάζοντας τη σύνδεση.
 - c. Διακοπή σύνδεσης (Connection Teardown): Ο επιτιθέμενος δεν απαντά με ACK πακέτο για να ολοκληρώσει τη διαδικασία, αφήνοντας την σύνδεση σε μια κατάσταση αναμονής.
2. **Επίθεση slowloris:**
- Η επίθεση Slowloris είναι μια μορφή «χαμηλή και αργή» επίθεση άρνησης υπηρεσίας (DoS) που στοχεύει στη διακοπή της λειτουργίας ενός web server διατηρώντας πολλές ανοιχτές συνδέσεις TCP (sockets) ταυτόχρονα. Το κλειδί πίσω από ένα Slowloris είναι η ικανότητά του να προκαλεί πολλά προβλήματα με πολύ μικρή κατανάλωση εύρους ζώνης και για αυτό δεν θα δούμε αύξηση στην κίνηση του διαδικτύου συσκευών.
- Η διαδικασία είναι ως εξής:
- a. Δημιουργία Συνδέσεων:
 - i. Το εργαλείο Slowloris δημιουργεί πολλαπλές συνδέσεις TCP (sockets) προς τον στόχο web server.
 - b. Αποστολή Μερικών Αιτημάτων HTTP:
 - i. Για κάθε σύνδεση, το Slowloris στέλνει μερικές κεφαλίδες HTTP χωρίς να ολοκληρώνει το αίτημα, διατηρώντας τις συνδέσεις ανοιχτές.
 - c. Διατήρηση Συνδέσεων:
 - i. Σε τακτά χρονικά διαστήματα, το Slowloris στέλνει επιπλέον κεφαλίδες HTTP (keep-alive) για να αποτρέψει τον διακομιστή από το να κλείσει τις συνδέσεις λόγω αδράνειας.
3. **Slowhttptest:** είναι ένα εργαλείο που χρησιμοποιείται για να δοκιμάσει την αντοχή ενός ιστού απέναντι σε επιθέσεις slow HTTP. Δημιουργεί πολλαπλές συνδέσεις με τον ιστότοπο και στέλνει δεδομένα σε πολύ αργούς ρυθμούς, ελέγχοντας έτσι την απόκριση του ιστού σε αυτές τις συνθήκες. Είναι πιο ευέλικτο από slowloris και μπορεί να προσομοιώσει διάφορες μορφές επιθέσεων

Οι επίθεσης αυτές εκτελέστηκαν από την εικονική μηχανή VM1 ubuntu server (192.168.1.3), ενός windows laptop. Το θύμα αυτόν των επιθέσεων είναι ένα Windows PC (192.168.1.135).

7.1 SYN flood attack με Hping3

Το hping3 είναι ένα εργαλείο δικτύου που επιτρέπει την αποστολή προσαρμοσμένων ICMP/UDP/TCP πακέτων και την εμφάνιση απαντήσεων από τον στόχο. Υποστηρίζει τη διαχείριση κατακερματισμένων πακέτων και την αποστολή πακέτων με αυθαίρετο περιεχόμενο και μέγεθος. Επίσης μπορεί να χρησιμοποιηθεί για διάφορες Δοκιμές, Αναλύσεις, επιθέσεις Δικτύου και πολλά άλλα. Παρακάτω θα εκτελεστή SYN flood επίθεση με το Hping3.

Για περισσότερες πληροφορίες: <https://www.kali.org/tools/hping3/>

Εγκατάσταση : `sudo apt install -y hping3`

(Με το -y δεν ζητάει κάποια άδεια κατά την εγκατάσταση)

Δοκιμή του εργαλείου hping3 εκτελώντας, για 20 λεπτά, την εντολή :

```
sudo hping3 -c 10000 -d 10000 -S -p 80 192.168.1.135
```

Προέκυψαν τα παρακάτω γραφήματα μετά από 20 λεπτά:

- Επιτιθέμενος (VM1 ubuntu server)

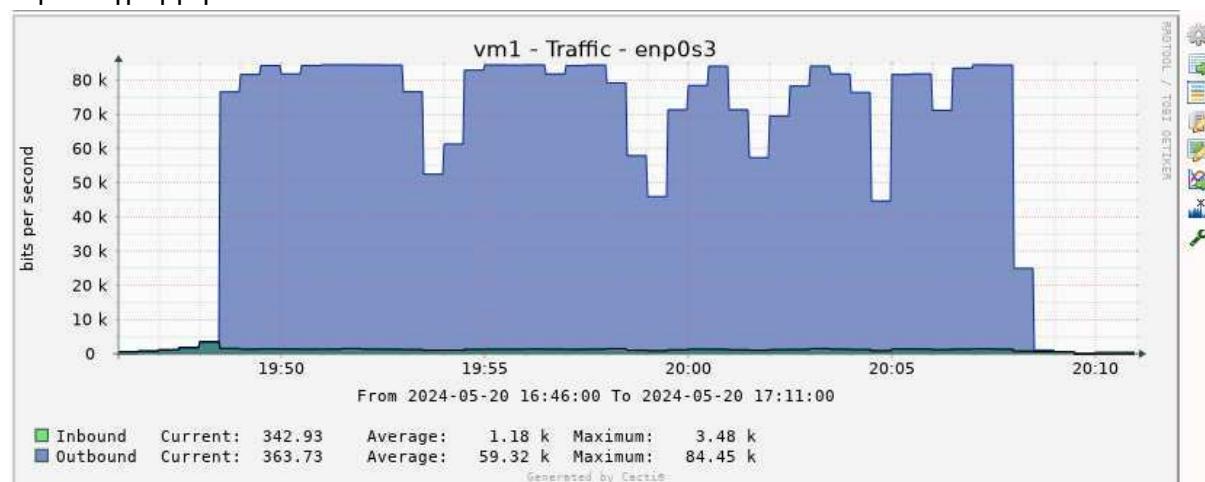
- Zabbix:

Η κόκκινη γραμμή είναι τα πακέτα που στέλνονται.



- Cacti :

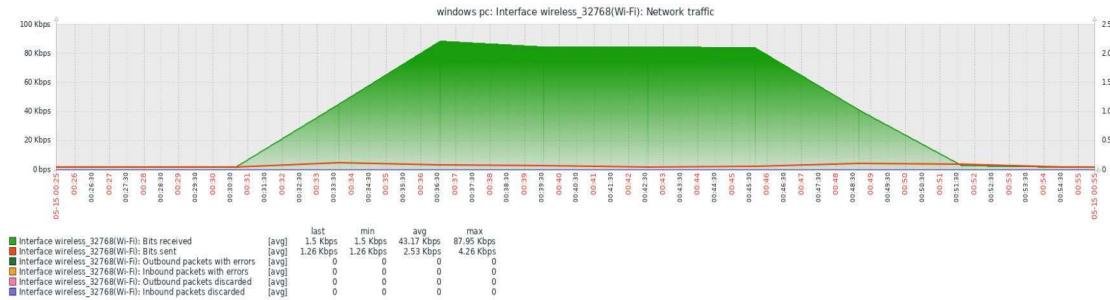
Η μπλε γραμμή είναι τα πακέτα που στέλνονται.



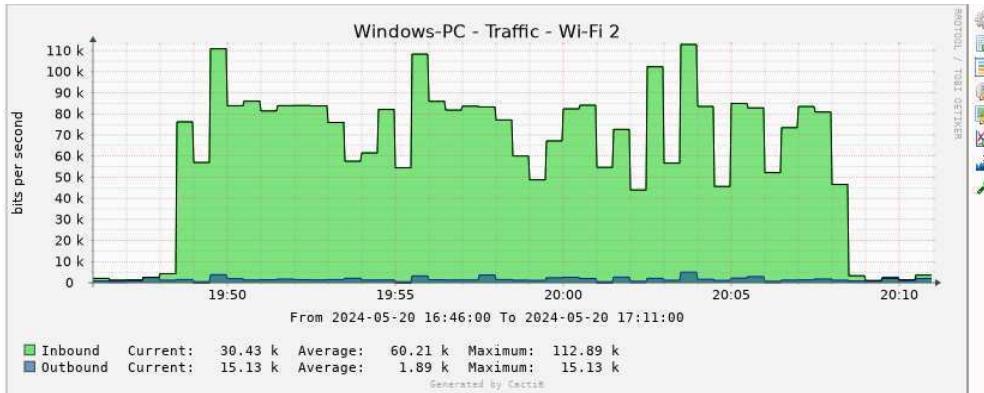
- Θύμα (Windows pc)

Η πράσινες γραμμές είναι τα πακέτα που λαμβάνονται.

- Zabbix



- Cacti



- Αποτέλεσμα: Δεν εμφανίστηκε καμία ανωμαλία από την παραπάνω εντολή αφού δεν ήταν κάτι παραπάνω από μια απλή και μικρή αποστολή TCP πακέτων.

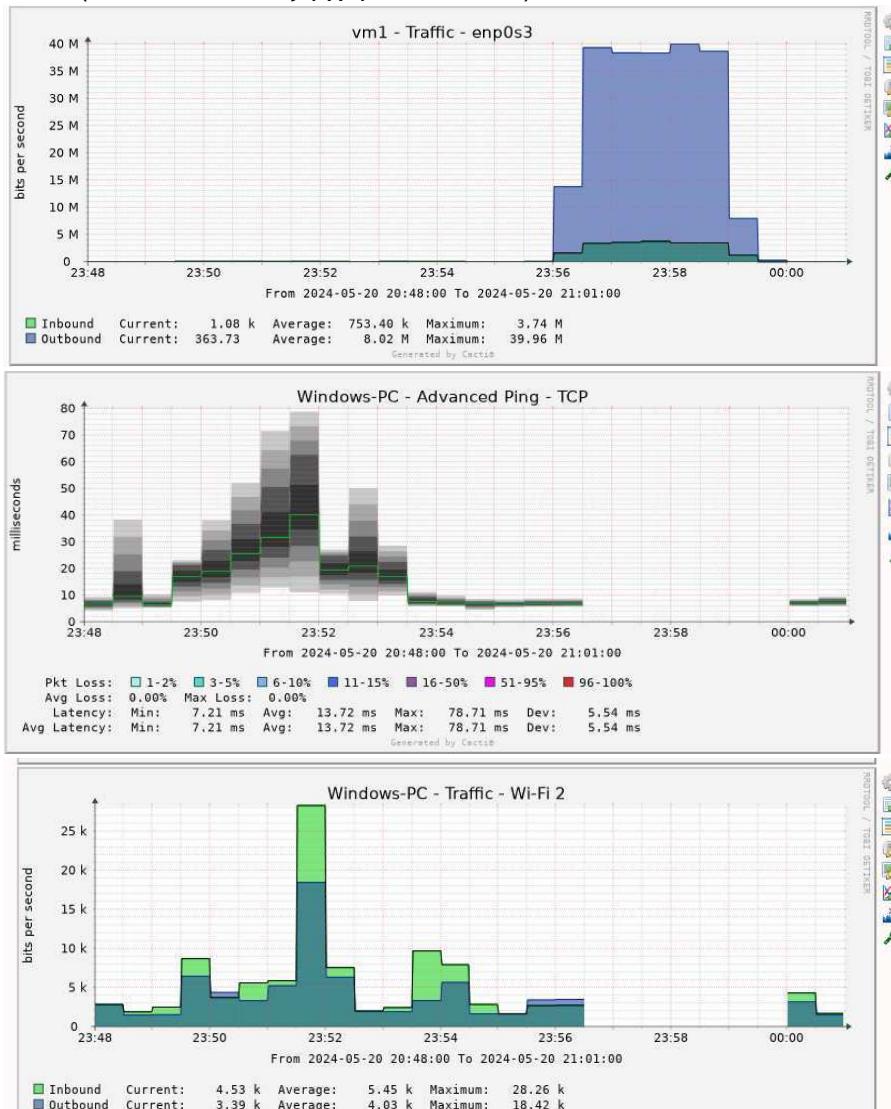
Επίθεση SYN flood attack εκτελώντας την εντολή:

```
hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood 192.168.1.135
```

- **-c** : αριθμός πακέτων, **-d**: μέγεθος πακέτων(bytes), **-S** : χρήση SYN, **-w**:TCP window size **-p**: Θύρα, **-flood**: γρηγορότερη αποστολή πακέτων
- Τερματισμός της εντολής πληκτρολογώντας CTRL-C

Μετά την επίθεση, προέκυψαν τα παρακάτω γραφήματα:

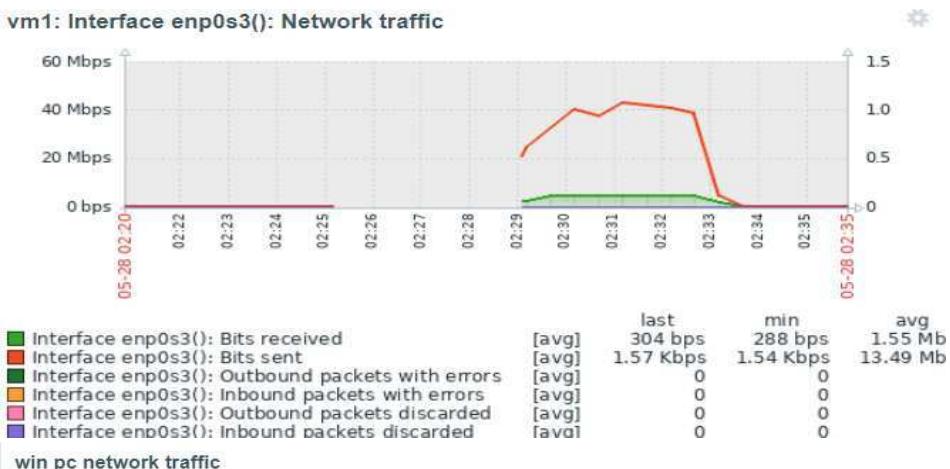
- Cacti (Μπλέ είναι τα εξερχόμενα πακέτα)



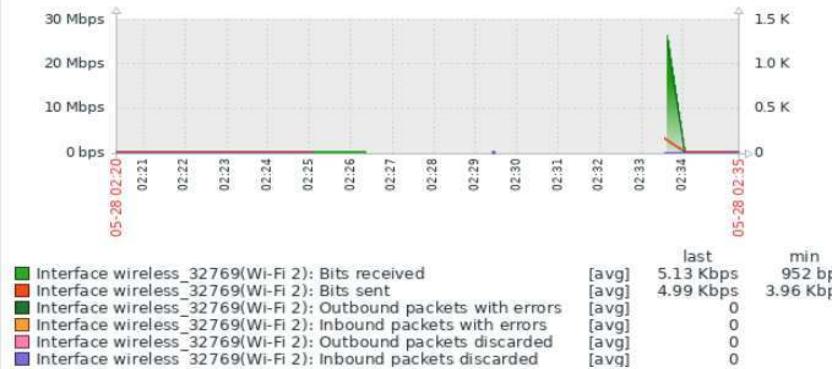
- Αποτέλεσμα: Στο γράφημα "Traffic" του vm1 παρατηρείται μια απότομη αύξηση και μείωση των εξερχόμενων πακέτων όταν ξεκινά και τελειώνει η επίθεση αντίστοιχα. Στο Windows PC, παρατηρείται ένας απότομος μηδενισμός των πακέτων στο "Traffic" και στο "TCP ping", που υποδηλώνει διακοπή της επικοινωνίας SNMP λόγω της επίθεσης. Με τη λήξη της επίθεσης, η επικοινωνία με το Windows PC αποκαθίσταται αμέσως κατά τον επόμενο κύκλο συλλογής δεδομένων (polling).

- Zabbix

vm1: Interface enp0s3(): Network traffic



win pc network traffic



windows pc: Windows: ICMP loss

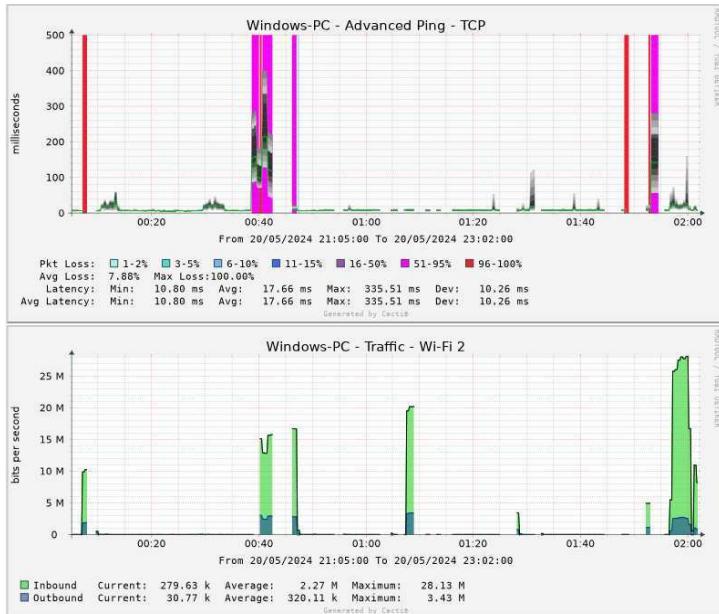


Problems

| Time | Info | Host | Problem • Severity | Duration | Ack. |
|----------|------|------------|---|----------|------|
| 02:30:33 | | windows pc | Windows: Unavailable by ICMP ping | 1m 48s | No |
| 02:33:38 | | windows pc | Interface wireless_1(Wi-Fi 2-Virtual WiFi Filter Driver-0000): High error rate (>2 for 5m) | 4m 37s | No |
| 02:33:38 | | windows pc | Interface wireless_32769(Wi-Fi 2): High error rate (>2 for 5m) | 4m 37s | No |
| 02:33:38 | | windows pc | Interface wireless_4(Wi-Fi 2-WFP 802.3 MAC Layer LightWeight Filter-0000): High error rate (>2 for 5m) | 4m 37s | No |
| 02:33:38 | | windows pc | Interface wireless_0(Wi-Fi 2-WFP Native MAC Layer LightWeight Filter-0000): High error rate (>2 for 5m) | 4m 37s | No |
| 02:33:33 | | windows pc | Interface wireless_3(Wi-Fi 2-QoS Packet Scheduler-0000): High error rate (>2 for 5m) | 4m 42s | No |

Επειδή διακόπτεται η επικοινωνία SNMP του windows PC με το Cacti κατά την επίθεση και δεν καταγράφεται τίποτα, προσπάθησα να εκτελέσω τις εντολές Hping κατά διαστήματα. Δηλαδή ξεκινούσα την επίθεση και αν το Cacti δεν μπορούσε να καταγράψει τίποτα ξανα εκτελούσα την επίθεση. Ετσι σε κάποιες περιπτώσεις, το Cacti πέτυχε να καταγράψει την κίνηση TCP πακέτων και του δικτύου κατά την επίθεση, αλλά για λίγο χρονικό διάστημα πριν διακοπή η επικοινωνία SNMP, όπως φαίνεται στα παρακάτω γραφήματα :

- Θύμα (windows pc)



- Επιπιθέμενος (VM1 ubuntu server)



- Αποτέλεσμα: Στο γραφήμα κίνησης δικτύου Traffic του vm1 υπάρχουν απότομες αύξησης πακέτων που σημαίνουν ότι εκτελέστηκε η επίθεση. Στο γραφήμα Traffic και TCP ping του windows pc φαίνεται οτι σε κάποιες από αυτές της επιθέσεις πέτυχε η

συλλογή δεδομένων.

Επίσεις στο γράφημα TCP ping υπάρχουν μωβ και κόκκινες γραμμές που δείχνουν την απώλεια TCP πακέτων σε ποσοστά, 51%-95% και 96%-100& αντίστοιχα, οταν το windows pc είναι υπό επίθεση.

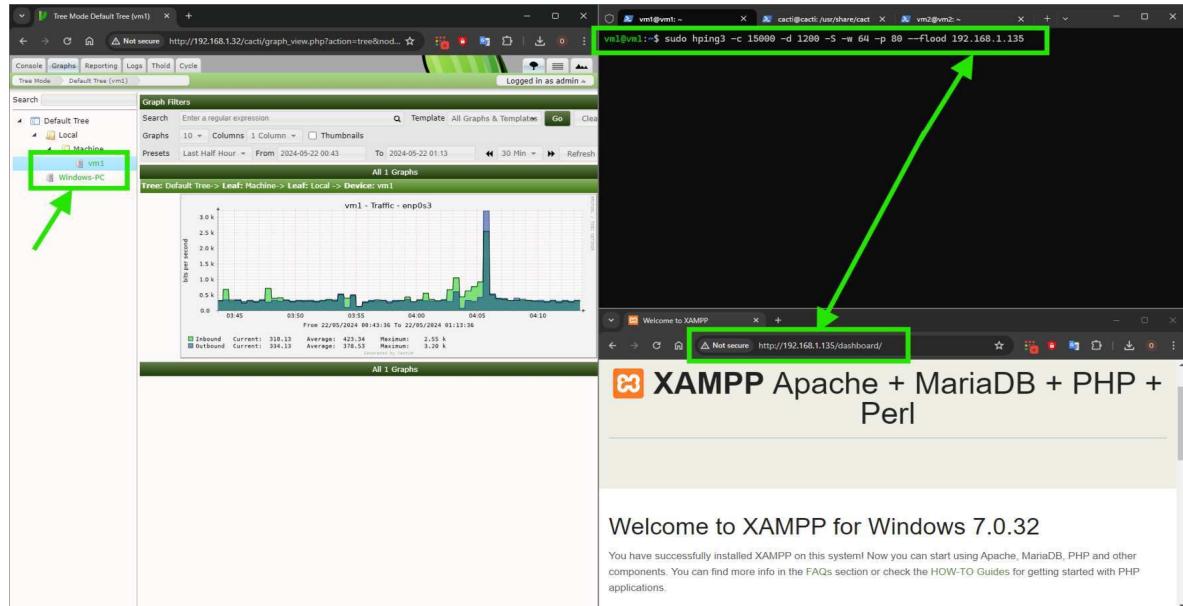
Παρακάτω φαίνεται μια καλύτερη εικόνα των επιπτώσεων της επίθεσης TCP SYN flood attack όπου υπάρχει μια μεγάλη απώλεια πακέτων TCP ping με ποσοστό 96-100%.



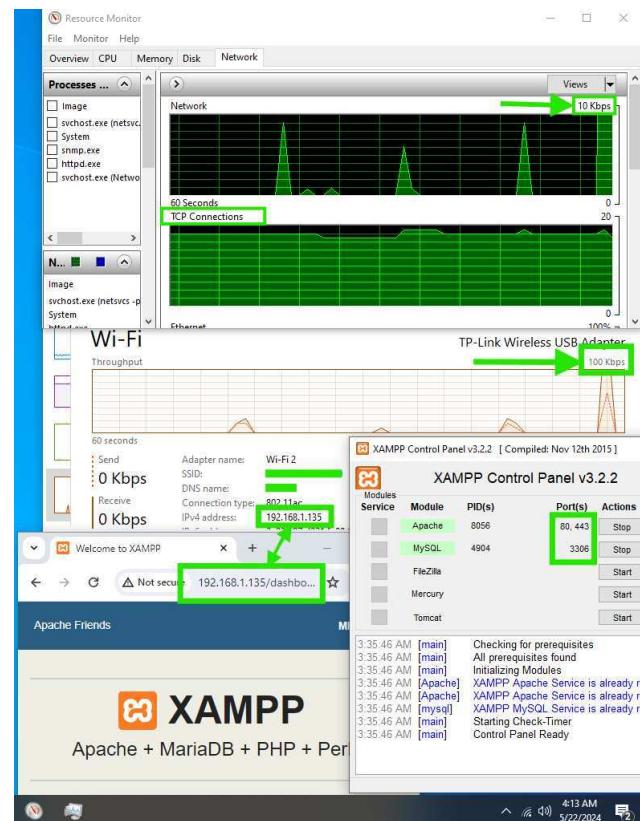
Παράδειγμα(Στιγμιότυπα οθόνης Windows laptop με εικονική μηχανή vm1 και από Windows pc)

Πριν την επίθεση:

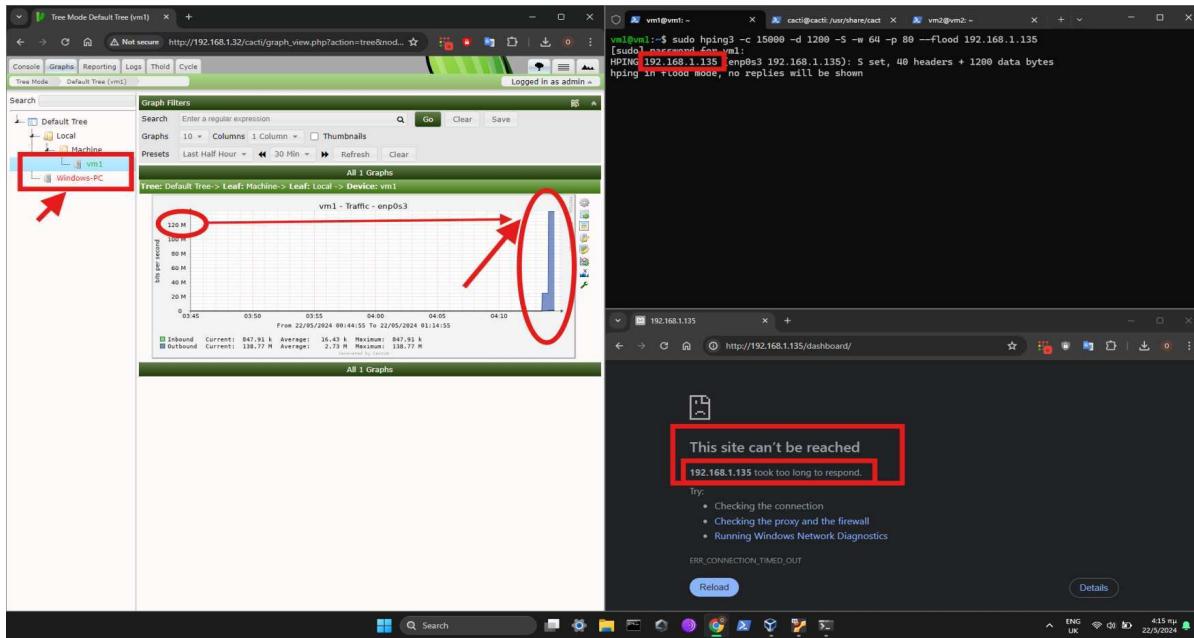
- Windows laptop:vm1(επιτιθέμενος) είναι έτοιμος για επίθεση, επιτυγχάνει πρόσβαση στην XAMPP Apache του Windows PC. To Cacti εμφανίζει το Windows PC με πράσινα γράμματα, υποδεικνύοντας επιτυχή επικοινωνία, ενώ το γράφημα Traffic(vm1) φτάνει μεχρι τα 3k bit/sec.



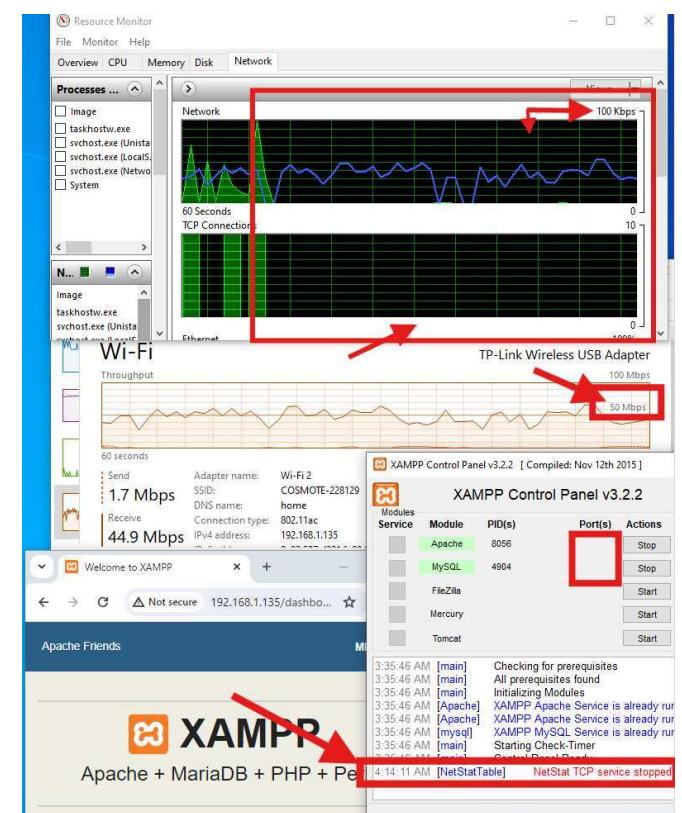
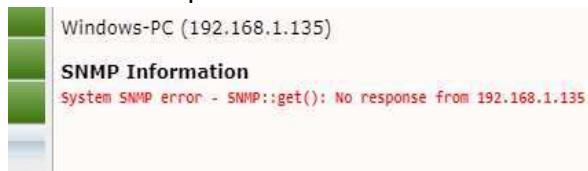
- Windows pc (Θύμα). Στο Resource Monitor, το γράφημα Network δείχνει μέγιστο 10 Kbps και το TCP δείχνει ενεργές συνδέσεις. Στο Task Manager, το γράφημα Wi-Fi φτάνει τα 100 Kbps και το XAMPP εμφανίζει τη θύρα του Apache server.



Μετά την επίθεση: Windows laptop: vm1 ξεκίνησε την επίθεση και μετά από λίγα δευτερόλεπτα η ιστοσελίδα εμφάνισε το μήνυμα “192.168.1.135 took too long to respond”. Αυτό σημαίνει ότι το Windows PC εξάντλησε τους πόρους του και δεν μπορεί να εξυπηρετήσει το Windows laptop. Στο Cacti, το PC εμφανίστηκε με κόκκινα γράμματα λόγω διακοπής της επικοινωνίας SNMP και μετά από ένα λεπτό το γράφημα Traffic του vm1 έδειξε απότομη αύξηση από 3k bits/sec σε 120M bits/sec.

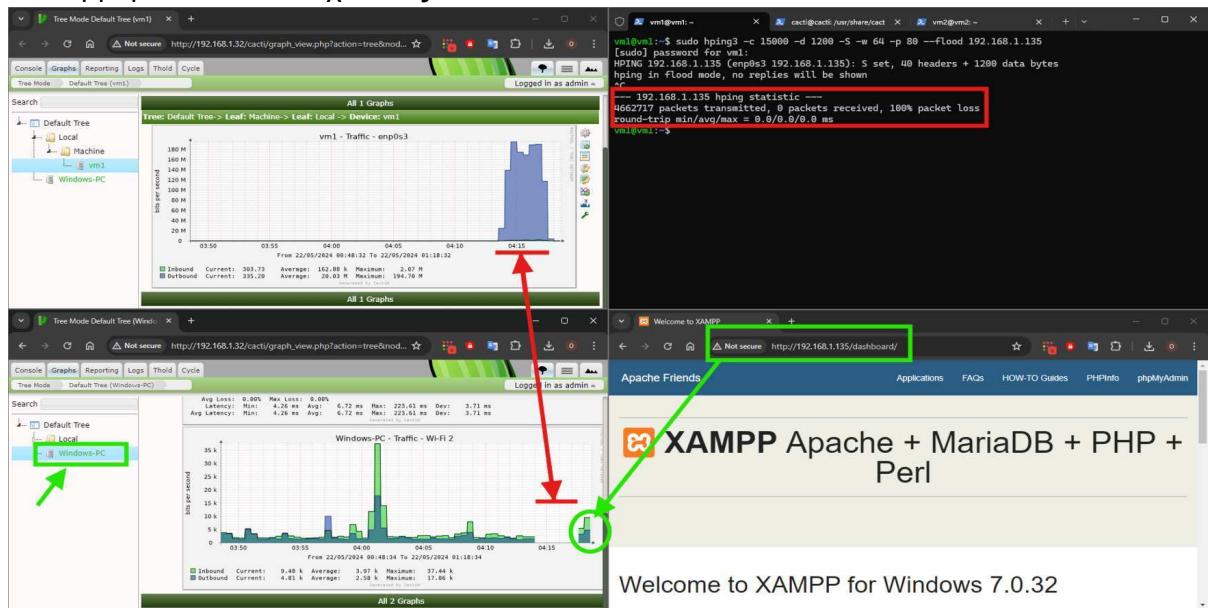


- Windows PC(Θύμα): Στο Resource Monitor, το γράφημα Network έφτασε τα 100 Kbps και το TCP δεν δείχνει καμία σύνδεση. Στο Task Manager, το γράφημα WI-FI άγγιξε το όριο του router στα 50 Mbps. Το XAMPP δεν εμφανίζει πλέον τη θύρα του Apache server και έδειξε το μήνυμα "NetStat TCP service stopped", υποδεικνύοντας ότι η υπηρεσία που διαχειρίζεται τις TCP συνδέσεις έχει σταματήσει να λειτουργεί. Επίσης το θύμα δεν είχε πρόβλημα πρόσβασης στην ιστοσελίδα του XAMPP apache server.



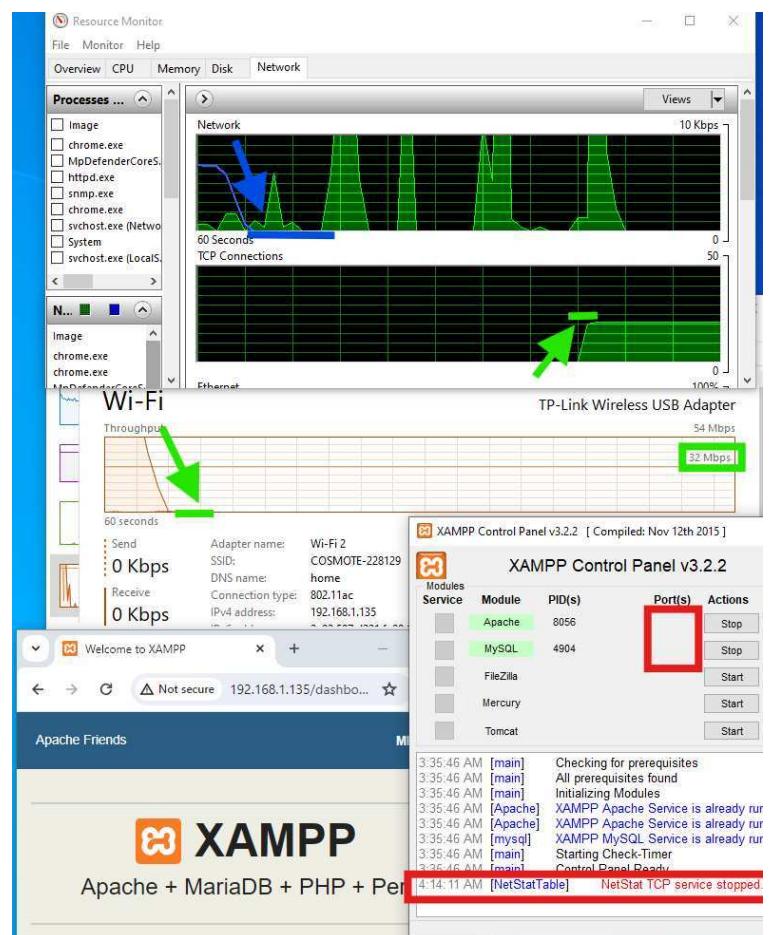
Τελος επίθεσης:

- Windows laptop: Η επίθεση τερματίστηκε με CTRL+C. Η ιστοσελίδα XAMPP επανήλθε και το Windows PC επανασυνέθηκε με το Cacti, το οποίο το εμφάνισε με πράσινα γράμματα. Στο επόμενο polling (30 δευτ.), το γράφημα Traffic του Windows PC ξαναεμφάνισε δεδομένα, ενώ το γράφημα του vm1 έδειξε απότομη μείωση από εκατομμύρια bits/sec σε χιλιάδες bits/sec.



- Windows PC(Θύμα):

Στο Resource Monitor εμφανίστηκε απότομη μείωση στο γράφημα Network, ενώ το TCP ξαναέδειχνε συνδέσεις. Στο Task Manager, το γράφημα WI-FI εμφάνισε επίσης απότομη μείωση στη χρήση του δικτύου. Μετά από επανεκκίνηση του XAMPP, ανακτήθηκαν οι θύρες και δεν είχε σφάλματα.

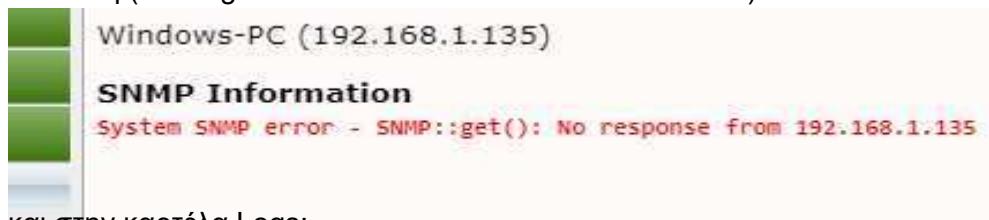


Συμπέρασμα

- Όπως φαίνεται και στα γραφήματα του windows pc υπάρχουν απότομες διακοπές που προερχονται από την αποσυνδεση του USB Αντάπτορα

Ασύρματου Δικτύου και την διακοπή επικοινωνίας snmp κατα την SYN flood επίθεση. Για αυτόν τον λόγο μια τέτοια SYN flood attack μπορεί να ανιχνευθεί αν παρατηρηθεί από τα γραφήματα που εμφανίζουν μηδενικές τιμές. Σε αυτήν την περίπτωση δεν χρειάζεται το threshold plugin επειδή το cacti αυτόματα εμφανίζει στην καρτέλα logs σχετικά μηνύματα.

Μετά την διακοπή επικοινωνίας με το SNMP εμφανίζοταν το παρακάτω μήνυμα στην συσκευή (Management > Devices κλικ στο Windows-PC):



και στην καρτέλα Logs:

- **ERROR: HOST EVENT: Device is DOWN Message: SNMP not performed due to setting or ping result, ICMP: Ping timed out**
- **SNMPAGENT WARNING: No notification receivers configured for event: cactiNotifyDeviceDown (CACTI-MIB), severity: high**

- **SNMPAGENT WARNING: No notification receivers configured for event: cactiNotifyDeviceFailedPoll (CACTI-MIB), severity: medium**

Με τον τερματισμό της επίθεσης, η snmp επικοινωνία επανέρχεται κατευθείαν και τα γραφήματα δουλεύουν κανονικά.

- Η επίθεση SYN flood αποστέλλει μια μεγάλη ποσότητα αιτημάτων TCP SYN στον στόχο με σκοπό την κατανάλωση των πόρων του. Καθώς ο στόχος απαντάει με SYN-ACK για κάθε αίτηση SYN που λαμβάνει, αλλά οι απαντήσεις αυτές δεν ολοκληρώνονται, οι ανοικτές συνδέσεις SYN παραμένουν στον πίνακα κατακερματισμού του στόχου. Αυτό οδηγήγει σε μια ξαφνική και απότομη αύξηση της κίνησης, καθώς ο στόχος προσπαθεί να αντιμετωπίσει το μεγάλο όγκο αιτημάτων SYN.
- Τα ίδια ισχύουν και για ICMP & UDP flood επιθέσεις.

7.2 Επίθεση slowloris

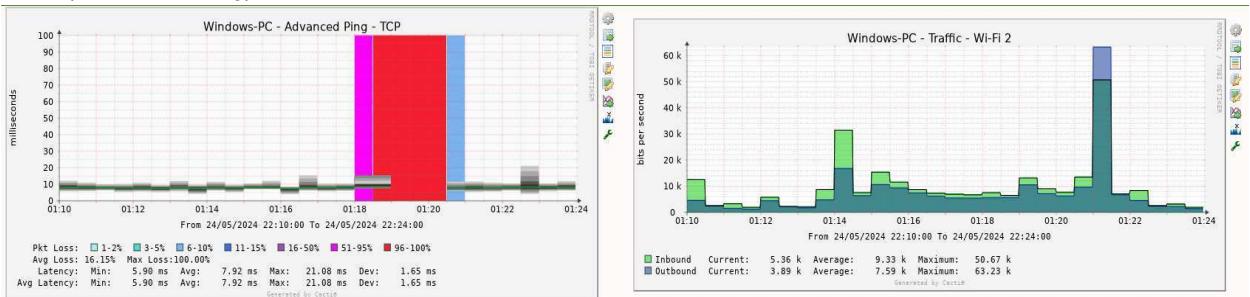
Εγκατάσταση:

1. `sudo apt-get install slowloris`

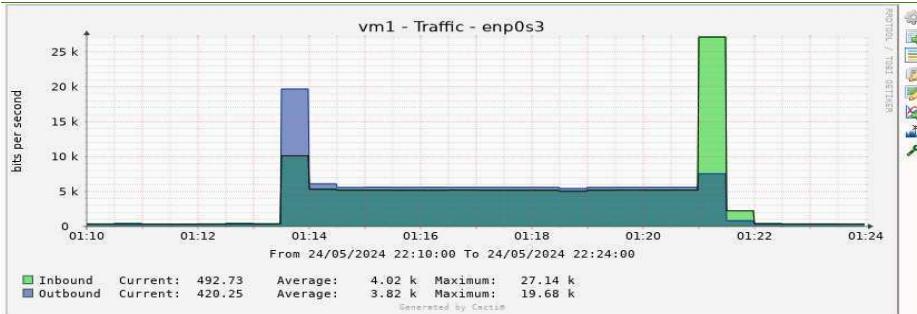
Επίθεση slowloris από vm1 σε windows pc: `sudo slowloris 192.168.1.135`

```
vm1@vm1:~$ sudo slowloris 192.168.1.135
[sudo] password for vm1:
[25-05-2024 01:13:54] Attacking 192.168.1.135 with 150 sockets.
[25-05-2024 01:13:54] Creating sockets...
[25-05-2024 01:13:56] Sending keep-alive headers...
[25-05-2024 01:13:56] Socket count: 150
[25-05-2024 01:14:11] Sending keep-alive headers...
[25-05-2024 01:14:11] Socket count: 150
[25-05-2024 01:14:26] Sending keep-alive headers...
[25-05-2024 01:14:26] Socket count: 150
[25-05-2024 01:14:41] Sending keep-alive headers...
[25-05-2024 01:14:41] Socket count: 150
[25-05-2024 01:14:41] Socket count: 150
```

• VIII (Επιμόρφωσης)



- windows pc (Θύμα)



- Αποτέλεσμα: Αυτή τη φορά, η σύνδεση SNMP του υπολογιστή με λειτουργικό σύστημα Windows δεν διακόπηκε. Το γράφημα TCP ping αποδείχθηκε χρήσιμο καθώς κατέγραψε τον χρόνο εκκίνησης, τον τερματισμό και τη διάρκεια της επίθεσης με επιτυχία. Η επίθεση αυτή καθυστέρησε περίπου 4 λεπτά πριν "ρίξει" τον διακομιστή Apache του Windows PC επειδή ο αριθμός των συνδέσεων TCP (socket) ήταν λίγες (προκαθορισμένα 150). Δεν παρατηρήθηκε ύποπτη αύξηση στην κίνηση δικτύου, καθώς η επίθεση slowloris επικεντρώνεται στη διατήρηση ανοιχτών συνδέσεων αντί στην αποστολή μεγάλου όγκου δεδομένων.

| Device | Time | Type | Event Description | Alert Value | Measured Value |
|------------|---------------------|-------------------|---|-------------|----------------|
| Windows-PC | 2024-05-24 22:21:01 | High / Low NORMAL | Windows-PC - Advanced Ping - TCP [loss] restored to Normal Threshold with value 0 | N/A | 0 |
| Windows-PC | 2024-05-24 22:20:03 | High / Low ALERT | Windows-PC - Advanced Ping - TCP [loss] is still above Threshold of 96.00 with 100.00 | 96 | 100 |
| Windows-PC | 2024-05-24 22:19:03 | High / Low ALERT | Windows-PC - Advanced Ping - TCP [loss] went above Threshold of 96.00 with 100.00 | 96 | 100 |

Παράδειγμα slowloris με 500 sockets : sudo slowloris 192.168.1.135 -s500

Πριν την επίθεση:

- Windows laptop :

vm1@vm1:~\$ sudo slowloris 192.168.1.135 -s500

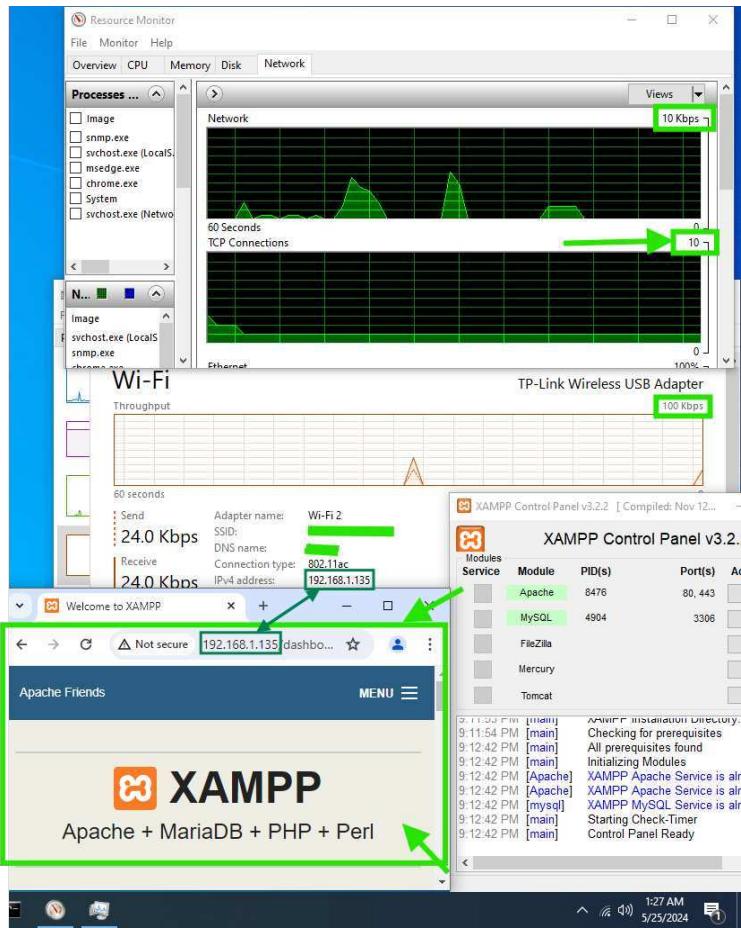
Welcome to XAMPP

http://192.168.1.135/dashboard/

XAMPP Apache + MariaDB + PHP + Perl

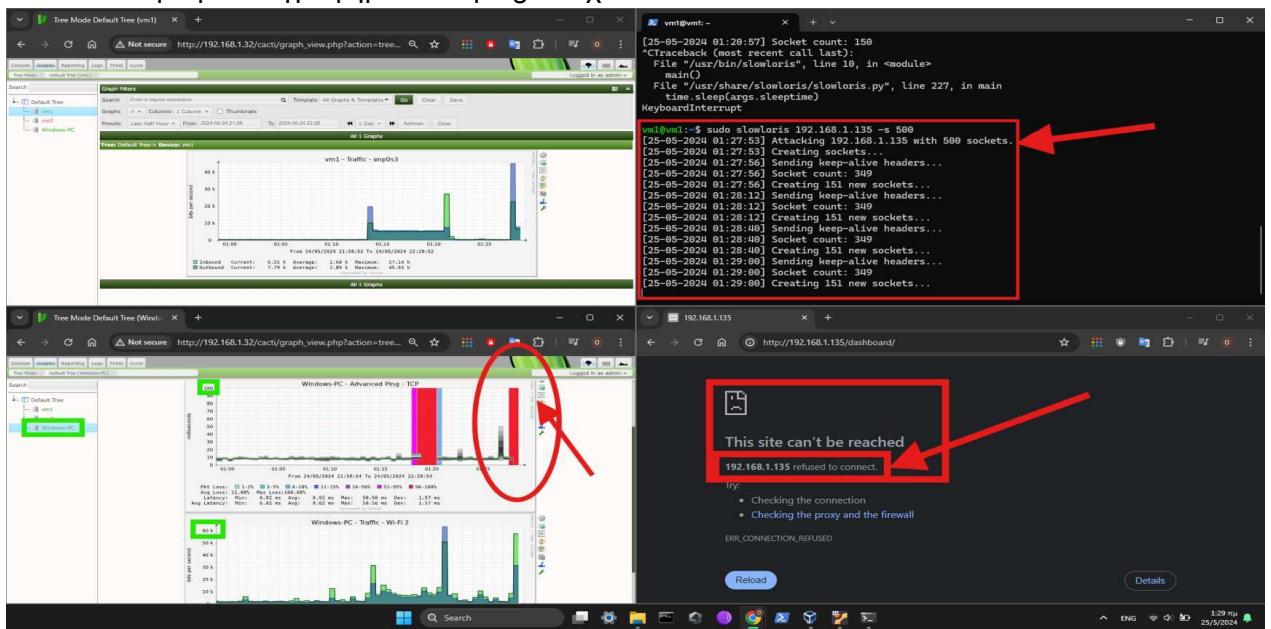
Welcome to XAMPP for Windows 7.0.32

- Windows pc :

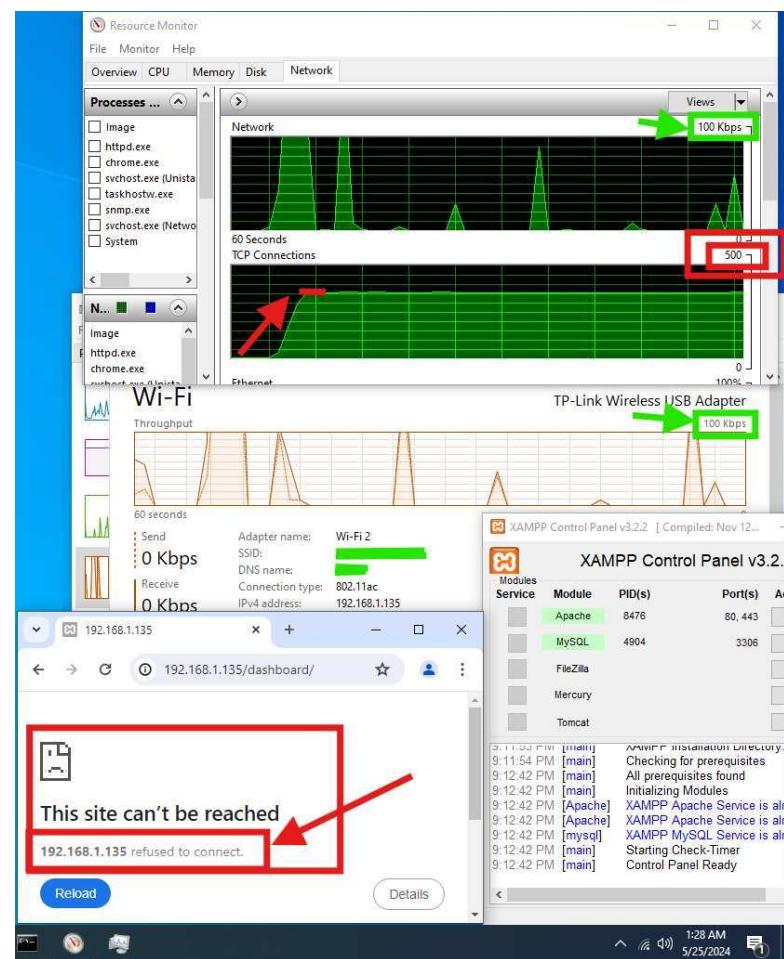


Μετά την επίθεση: Μέσα σε λίγα δευτερόλεπτα η ιστοσελίδα apache server “έπεσε”.

- Windows laptop : Το γράφημα TCP ping έδειχνε 96-100% απώλεια πακέτων TCP.

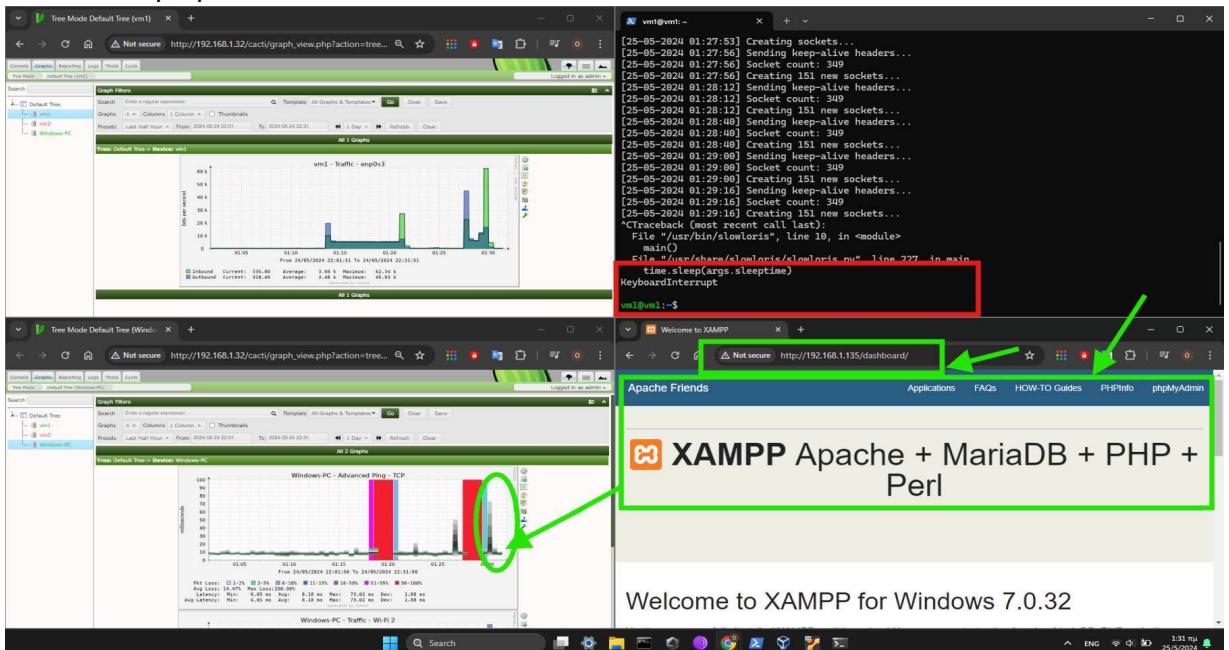


- Windows pc : Στο Resource Monitor, το γράφημα Network παρέμεινε κάτω από 100 Kbps και το TCP αυξήθηκε απότομα στις 350 συνδέσεις περίπου.



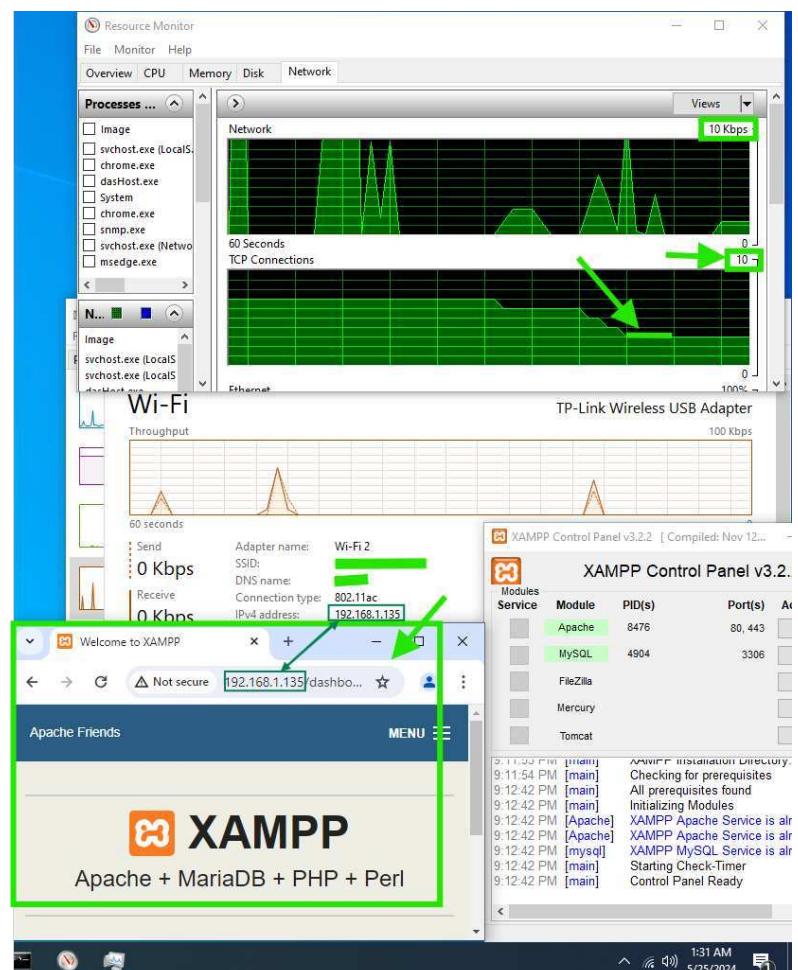
Τέλος της επίθεση:

- Windows laptop :



Welcome to XAMPP for Windows 7.0.32

- Windows pc : Στο Resource Monitor, το γράφημα TCP επανήλθε σε κάτω από 10 συνδέσεις και η ιστοσελίδα δούλευε κανονικά.

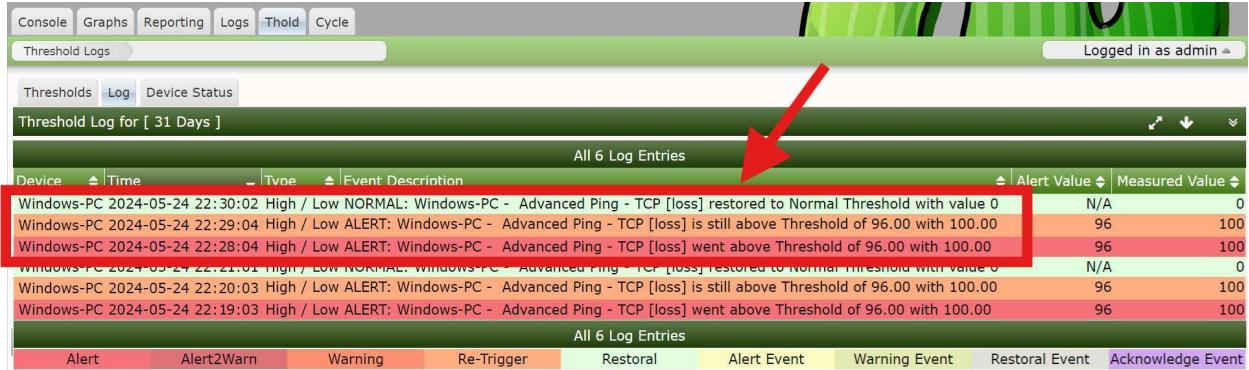


Συμπέρασμα:

- Όσο πιο πολλά είναι τα sockets που χρησιμοποιούνται στην επίθεση slowloris τόσο γρήγορα πέφτει το apache server.
 - Απαιτεί λιγότερους πόρους από την πλευρά του επιτιθέμενου και μπορεί να είναι πιο αποτελεσματικό σε περιπτώσεις που ο διακομιστής δεν είναι ρυθμισμένος για να αντιμετωπίσει τέτοιου είδους επιθέσεις.
 - Το Slowloris δημιουργεί πολλές ημιτελείς συνδέσεις και διατηρεί αυτές τις συνδέσεις ενεργές, στέλνοντας περιοδικά keep-alive headers. Καθώς αυτές οι συνδέσεις δεν ολοκληρώνονται ποτέ, ο Apache διατηρεί τα νήματα ανοιχτά και τελικά εξαντλείται ο αριθμός των διαθέσιμων νημάτων, προκαλώντας αυτό το παρακάτω μήνυμα σφάλματος.
- apache error log : AH00326: Server ran out of threads to serve requests. Consider raising the ThreadsPerChild setting.
- κατα την επίθεση SYN flood attack η ιστοσελίδα apache server ήταν προσβάσιμο στο θύμα, δηλαδή όταν ανανέωναι την σελίδα εμφανιζόταν κανονικά. Ενώ στην επίθεση slowloris ούτε το θύμα δεν είχε πρόσβαση στην ιστοσελίδα.
 - Κατά τη διάρκεια της επίθεσης SYN flood, η ιστοσελίδα του Apache server παρέμενε προσβάσιμη στο θύμα. Αυτό σημαίνει ότι, ακόμα και όταν η σελίδα ανανεωνόταν,

εμφανιζόταν κανονικά χωρίς προβλήματα. Αντίθετα, κατά την επίθεση Slowloris, το θύμα δεν μπορούσε να έχει πρόσβαση στην ιστοσελίδα καθόλου. Η σελίδα δεν φόρτωνε και ο διακομιστής φαινόταν να είναι μη διαθέσιμος. Αυτή η διαφορά αναδεικνύει τη διαφορετική φύση των δύο επιθέσεων: ενώ το SYN flood μπορεί να επηρεάσει κυρίως την απόδοση του δικτύου, το Slowloris στοχεύει άμεσα στους πόρους του διακομιστή, καθιστώντας τον ανίκανο να εξυπηρετήσει νέα αιτήματα.

- Επίσεις το threshold εμφάνισε τα παρακάτω μηνύματα στην εικόνα:



| Device | Time | Type | Event Description | Alert Value | Measured Value |
|------------|------------------------|-------------------|---|-------------|----------------|
| Windows-PC | 2024-05-24 22:30:02 | High / Low NORMAL | Windows-PC - Advanced Ping - TCP [loss] restored to Normal Threshold with value 0 | N/A | 0 |
| Windows-PC | 2024-05-24 22:29:04 | High / Low ALERT | Windows-PC - Advanced Ping - TCP [loss] is still above Threshold of 96.00 with 100.00 | 96 | 100 |
| Windows-PC | 2024-05-24 22:28:04 | High / Low ALERT | Windows-PC - Advanced Ping - TCP [loss] went above Threshold of 96.00 with 100.00 | 96 | 100 |
| Windows-PC | 2024-05-24 22:27:21:01 | High / Low NORMAL | Windows-PC - Advanced Ping - TCP [loss] restored to Normal Threshold with value 0 | N/A | 0 |
| Windows-PC | 2024-05-24 22:20:03 | High / Low ALERT | Windows-PC - Advanced Ping - TCP [loss] is still above Threshold of 96.00 with 100.00 | 96 | 100 |
| Windows-PC | 2024-05-24 22:19:03 | High / Low ALERT | Windows-PC - Advanced Ping - TCP [loss] went above Threshold of 96.00 with 100.00 | 96 | 100 |

7.3 slowhttptest

Εγκατάσταση: `sudo apt install slowhttptest`

Επίθεση slowhttptest από vm1 σε windows pc εκτελώντας την εντολή:

```
slowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200 -s 8192 -t FAKEVERB
-u https://192.168.1.135 -x 10 -p 3
```

- -c 1000: 1000 συνδέσεις.
- -B: Χρήση μπλοκαρίσματος.
- -g -o my_body_stats: Αποθήκευση στατιστικών σε αρχείο csv και html "my_body_stats".
- -i 110: Διάστημα ανάμεσα στα αιτήματα, 110 δευτερόλεπτα.
- -r 200: Ρυθμός αποστολής δεδομένων, 200 bytes ανά αίτημα.
- -s 8192: Μέγεθος σώματος αιτήματος, 8192 bytes.
- -t FAKEVERB: Χρήση μη υποστηριζόμενης μεθόδου HTTP.
- -u <https://192.168.100.4>: Διεύθυνση URL στόχου.
- -x 10: Αριθμός συνεχόμενων αιτημάτων ανά σύνδεση.
- -p 3: Παράλληλες συνδέσεις, 3.

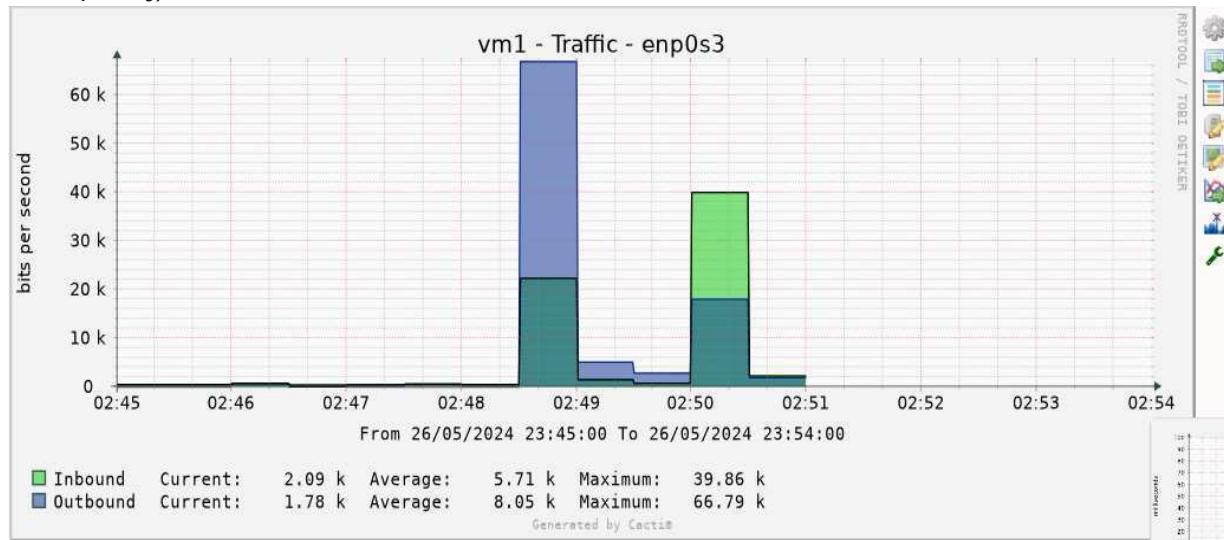
```

GNU nano 7.2
Seconds,Closed,Pending,Connected,Service Available
0,0,1,0,1000
1,0,2,151,1000
2,0,2,307,1000
3,127,2,350,1000
4,296,3,350,0
5,466,2,350,0
6,633,2,350,0
7,650,0,350,0

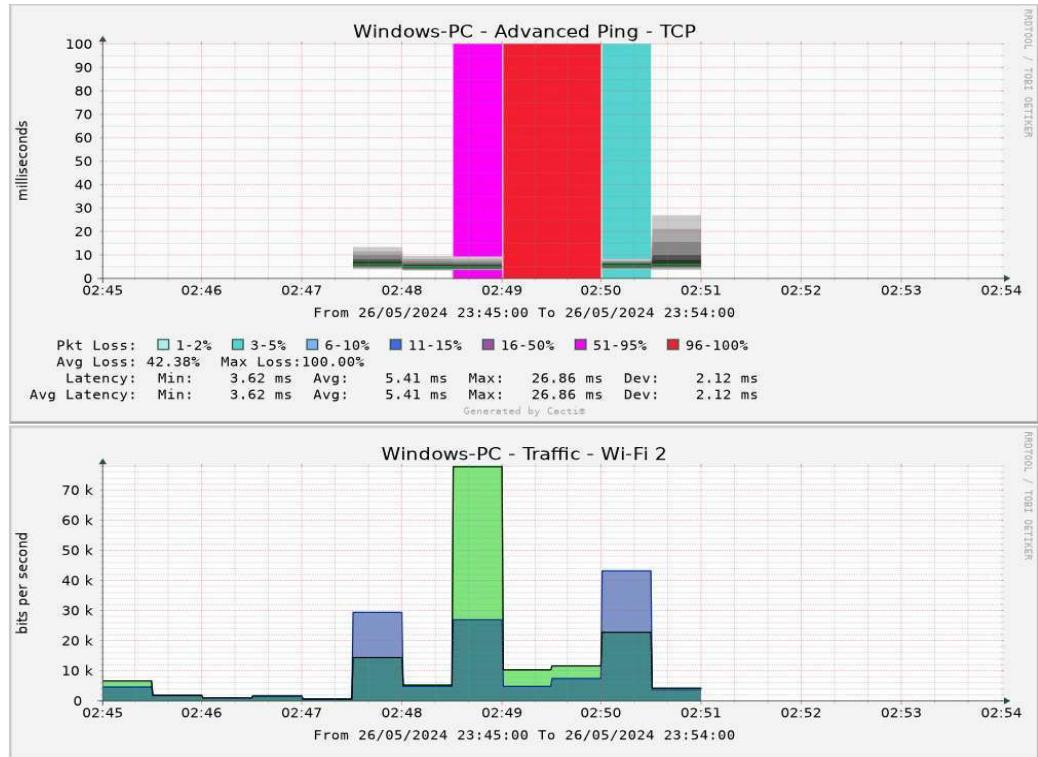
```

Προέκυψαν τα παρακάτω γραφήματα:

- vm1 (Επιπιθέμενος)



- windows pc (Θύμα)



Παράδειγμα επίθεσης slowhttptest:

Μετά την επίθεση:

- Windows laptop: vm1

vmt@vmt:~

```
Mon May 27 02:39:13 2024;
slowhttptest version 1.9.8
- https://github.com/shkyan/slowhttptest -
test type: SLOW BODY
number of connections: 1000
URL: https://192.168.1.135/
proxy: PROXYWEB
cookie: Content-Length header value: 8192
follow up status code: 200
idle time between follow up data: 118 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
total duration: 240 seconds
using proxy: no proxy
```

Mon May 27 02:39:13 2024;
slow HTTP test status on 100th second:

```
initializing: 0
pending: 0
connected: 348
error: 0
closed: 652
service available: NO
```

192.168.1.135

This site can't be reached
192.168.1.135 refused to connect.
Try:
• Checking the connection
Reload

Tree Mode Default Tree (Windows-PC)

Windows-PC - Advanced Ping - TCP

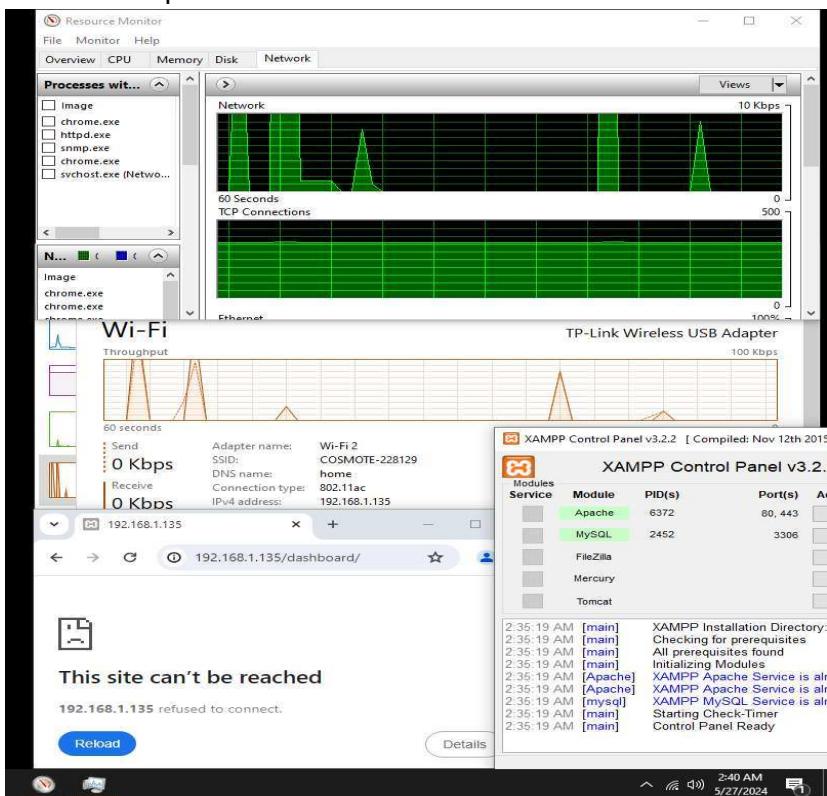
Windows-PC - Traffic - Wi-Fi 2

Tree Mode Default Tree (vm1)

All 1 Graphs

vm1 - Traffic - enp0s3

- Windows pc :



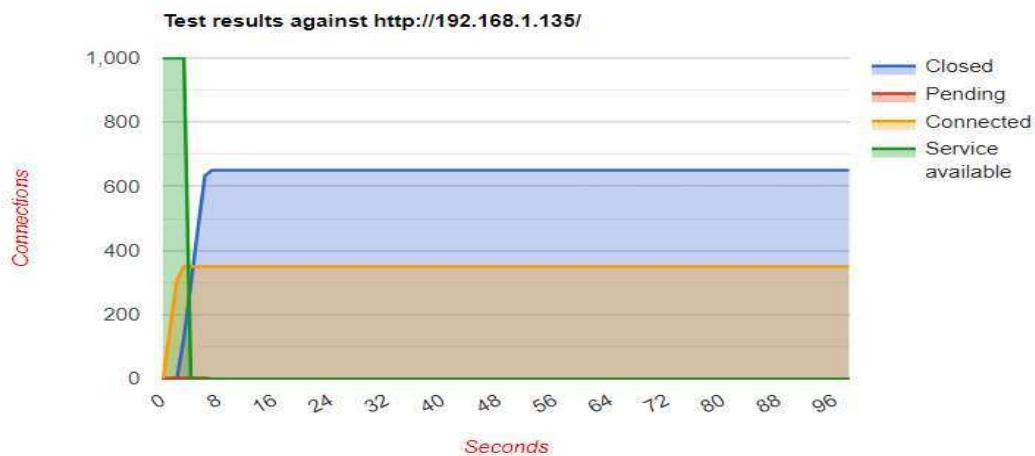
- csv αρχείο από slowhttptest:

```
vm1@vm1: ~          my_body_stats.csv
GNU nano 7.2
Seconds,Closed,Pending,Connected,Service Available
0,0,1,0,1000
1,0,4,158,1000
2,0,3,320,1000
3,140,3,348,0
4,312,2,348,0
5,484,2,348,0
6,652,0,348,0
7,652,0,348,0
182,652,0,348,0
183,652,0,348,0
```

- **HTML αρχείο** από slowhttptest:

Test parameters

| | |
|---------------------------------|-------------|
| Test type | SLOW BODY |
| Number of connections | 1000 |
| Verb | FAKEVERB |
| Content-Length header value | 8192 |
| Cookie | |
| Extra data max length | 22 |
| Interval between follow up data | 110 seconds |
| Connections per seconds | 200 |
| Timeout for probe connection | 3 |
| Target test duration | 240 seconds |
| Using proxy | no proxy |



Αποτέλεσμα: Παρόμοιο με το slowloris. Επίσεις το Slowhttptest παρέχει csv και HTML αρχείο με της καταγραφές κατα την επίθεση και δείχνει ότι το server έπεισε αφού δεν παρέμεινε διαθέσιμη υπηρεσία μετά από 3 δευτερόλεπτα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- ➔ Jian Ren and Tongtong Li, Michigan State University
<https://www.egr.msu.edu/~renjian/pubs/network-management.pdf>
- ➔ University of Oregon , Network Startup Resource Center
<https://nsrc.org/workshops/2020/ekiti-connect/netmgmt/en/welcome-intro/network-management.pdf>
- ➔ Medium.com , Devshan Liyanage-ISO framework for network management.
<https://medium.com/@devshanliyanage/iso-framework-for-network-management-b1c0ee33a2de>
- ➔ https://en.wikipedia.org/wiki/Network_management_software
- ➔ Cacti <https://www.cacti.net/> , [https://en.wikipedia.org/wiki/Cacti_\(software\)](https://en.wikipedia.org/wiki/Cacti_(software))
- ➔ Hping3 <https://www.kali.org/tools/hping3/>
- ➔ slowhttptest <https://github.com/shekyan/slowhttptest>
- ➔ Zabbix <https://www.zabbix.com/> , <https://en.wikipedia.org/wiki/Zabbix>
- ➔ SNMP <https://www.site24x7.com/network/what-is-snmp.html> ,
https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- ➔ Slowloris <https://github.com/gkbrk/slowloris> , <https://www.geeksforgeeks.org/slowloris-ddos-attack-tool-in-kali-linux>
<https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/>