گزارش جرم شناسی

مسابقه ی کشف شواهد رایانه ای دانشگاه صنعتی شریف

زمستان 1393

فهرست:

به نام خدا

نکات اولیه:

در صورت نگفتن معیار زمانی زمان بر حسب زمان ایران میاشد زیرا هم سیستم باب و هم الیس بر حسب همین زمان است.

در صورت ذکر نکردن تاریخ روز ، منظور روز 17 NOV 2014 است زیرا بیشتر رویدادها در این روز اتفاق افتاده.

همچنین با بررسی cache file های فایرفاکس سیستم الیس میتوان حدودا درست بودن ساعت آن با وب سرور های معتبر تایید کرد. و با استفاده از تبادل بین وب سرور سیستم باب و سیستم الیس میتوان صحیح بودن ساعت باب را تایید کرد(البته با 2 دقیقه خطا)

از آنجا که هارد سیستمها به صورت مجازی است با کپی گرفتن و کار بروی نسخه کپی شده جلوی هر گونه از دست رفتن اطلاعات و تغییر اطلاعات سیستم را میگیریم!

در ابتدا مورارد مورد اهمیت بررسی و گزارش شده، و در انتها نتیجه گیری و تایم لاین حمله بیان شده است

بررسی سیستم الیس:

نوع سیستم عامل:

Windows 7 professional 32-bit

هارد مجازی

TimeZone سیستم عامل:

Tehran - iran

بررسی لاگ فایلهای (EVENT VIEWER):

- Securty:

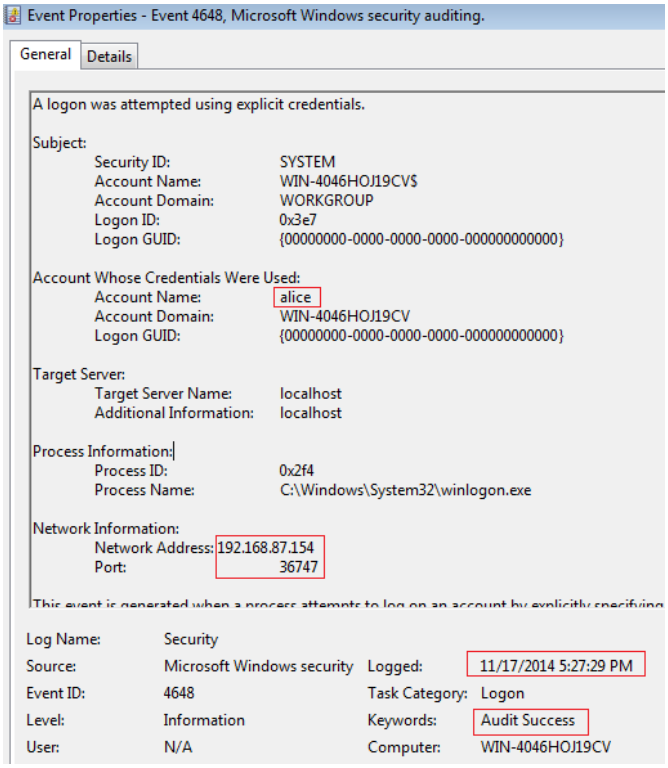
در لاگهایی securty میتوان زمان ورود و خروج یوزرها را به دست آورد، در لاگ ها ،آنهایی که logon type شماره 10 است مربوط به لاگین های به صورت rdp است و 2 نشان دهنده ورود فیزیکی است.

بازه های وقایع مهم به صورت زیر است:

username	logon type	زمان اولین اتفاق	زمان آخرین اتفاق	IP	توضیح
Alice	10	5:13:44 PM	5:27:29 PM	192.168.87.154	در این بازه زمانی تعداد زیادی تلاش ناموفق برای ورود از طریق RDP انجام شده که نشان دهنده حمله بروت فرس است. تا اینکه در تایم 5:27:29 اولین ورود موفق انجام میشود!
Alice	10	5:27:30 PM	-	192.168.87.154	اولین اتصال از بد از بروت فرس و رسیدن به پسورد صحیح با client name hydra که تایید کننده حمله بروت فرس است و تولز مورد استفاده مهاجم هم مشخص میکند که hydra است . این اتصال لحظه ای بد از بروت فرس توسط hydra برای بررسی صحیح بودن پسورد پیدا شده انجام میشود.
Alice	10	7:27:51 PM	7:47:24 PM	192.168.87.154	در این بازه زمانی session با نام kali به RDP برقرار بوده که سیستم

عامل فرد مهاجم را میتوان حدس زد که kali است					
Login و logout یوزر بصورت فیزیکی(interactice)	-	7:49:33 PM	7:49:29 PM	2	Alice
در این بازه زمانی session با نام kali به RDP برقرار بوده ، همزمان با اتمام session به صورت فیزیکی لاگین انجام شده که احتمالا به این دلیل session بسته شده!	192.168.87.154	8:00:16 PM	7:51:23 PM	10	Alice
لاگین به صورت فیزیکی	–	–	8:00:16 PM	2	Alice

از انجا که محدودیت session برای هر یوزر وجود دارد ، در هر لحظه یا کاربر پشت سیستم خود به صورت فیزیکی در حال استفاده از یوزر است یا از طریق RDP !



اولین اعتبار سنجی موفق هکر

- windows firewall :

در لاگ فایلهای windows firewall اتفاقتی که برای فایروال افتاده مثل غیرفعال یا فعال کردن و .. ثبت میشود که تنها اتفاق ثبت شده تاثیر گذار به صورت زیر است:

توضیح	زمان
غیرفعال شدن فایروال برای شبکه های Public	5:11:45 PM
غیرفعال شدن فایروال برای شبکه های Private	5:11:45 PM

بررسی prefetch فایلها :

در فایل های prefetch اطلاعات زیر حائز اهمیت بیشتری بود (اطلاعات به وسیله برنامه WinPrefetchView استخراج شده است):

Filename : FIREFOX.EXE-E60C0AA7.pf
Created Time : 11/17/2014 7:22:00 PM
Modified Time : 12/2/2014 5:03:11 PM
Process EXE : FIREFOX.EXE
Process Path : F:\PROGRAM FILES\MOZILLA FIREFOX\firefox.exe
Run Counter : 6
Last Run Time : 12/2/2014 5:03:08 PM
==========
Filename : WBPV.EXE-7C66A475.pf
Created Time : 11/17/2014 7:44:22 PM
Modified Time : 11/18/2014 9:19:34 AM
Process EXE : WBPV.EXE
Process Path : F:\Users\alice\AppData\Local\Temp\wbpv.exe
Run Counter : 3
Last Run Time : 11/18/2014 9:19:29 AM
==========
Filename : CMD.EXE-89305D47.pf
Created Time : 11/17/2014 12:43:42 PM
Modified Time : 11/18/2014 9:13:52 AM
Process EXE : CMD.EXE
Process Path : F:\Windows\System32\cmd.exe
Run Counter : 14
Last Run Time : 11/18/2014 9:13:41 AM
==========
Filename : NETSTAT.EXE-6D34D712.pf
Created Time : 11/17/2014 8:11:59 PM
Modified Time : 11/18/2014 9:13:56 AM
Process EXE : NETSTAT.EXE
Process Path : F:\Windows\System32\NETSTAT.EXE
Run Counter : 3
Last Run Time : 11/18/2014 9:13:55 AM

Filename : REG.EXE-26976709.pf
Created Time : 11/17/2014 10:28:45 PM
Modified Time : 11/17/2014 10:28:45 PM
Process EXE : REG.EXE
Process Path : F:\Windows\System32\reg.exe
Run Counter : 1
Last Run Time : 11/17/2014 10:28:45 PM

==========
Filename : REGEDIT.EXE-4748FE01.pf
Created Time : 11/17/2014 7:56:57 PM
Modified Time : 11/17/2014 9:29:14 PM
Process EXE : REGEDIT.EXE
Process Path : F:\Windows\regedit.exe
Run Counter : 4
Last Run Time : 11/17/2014 9:29:04 PM
==========
Filename : W.EXE-4CD5B5A5.pf
Created Time : 11/17/2014 7:44:00 PM
Modified Time : 11/17/2014 8:03:15 PM
Process EXE : W.EXE
Process Path : F:\Users\alice\AppData\Local\Temp\w.exe
Run Counter : 4
Last Run Time : 11/17/2014 8:03:02 PM
==========
Filename : RDPCLIP.EXE-A3424091.pf
Created Time : 11/17/2014 7:28:03 PM
Modified Time : 11/17/2014 7:51:34 PM
Process EXE : RDPCLIP.EXE
Process Path : F:\Windows\System32\rdpclip.exe
Run Counter : 2
Last Run Time : 11/17/2014 7:51:24 PM

همچنین فایلهای لود شده توسط w.exe به صورت زیر است:

Filename	Created Time	Modified Time	File Size	Process EXE
W.EXE-4CD5B5A5.pf	11/17/2014 7:44:00 PM	11/17/2014 8:03:15 PM	10,722	W.EXE

Filename	Full Path	Device Path	Index
NC.EXE	F:\Users\alice\AppData\Local\Temp\nc.exe	\DEVICE\HARDDISKVOLUME1\US...	22
W.EXE	F:\Users\alice\AppData\Local\Temp\w.exe	\DEVICE\HARDDISKVOLUME1\US...	5
WBPV.EXE	F:\Users\alice\AppData\Local\Temp\wbpv.exe	\DEVICE\HARDDISKVOLUME1\US...	23

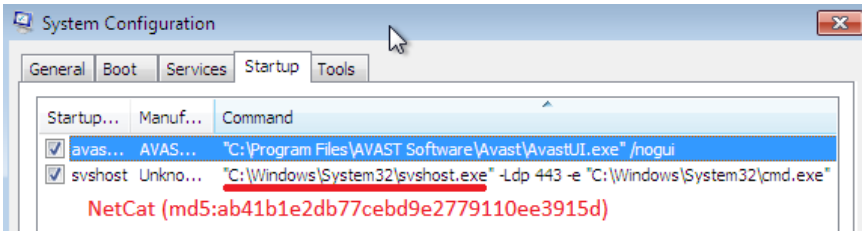
که با توجه به کاربرد فایل w.exe که جلوتر توضیح داده شده میتوان حدس زد اینها (nc.exe و w.exe و wbpv.exe) فایلهای دانلود شده توسط w.exe است.

تایم های highlight شده به رنگ سبز،در بخش نتیجه گیری استفاده شده است.

بررسی فایل ها یی که در startup ویندوز قرار دارند:

فقط در مسیر "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr entVersion\Run"

دو فایل برای startup قرار داده شده که در msconfig هم به صورت زیر قابل مشاهده اند:



در دایکرتوری های دیگر startup فایل دیگری نیست.

بررسی دایرکتوری Temp :

در فایلهای موجود در temp علاوه بر لاگ فایل های مربوط به vmware که اهمیت ندارد! میتوان فایل های زیر را یافت که در قسمتهای بعد بطور کامل بررسی میشود ....

Created Time	FileName	Md5
7:43:40 PM	w.exe	dbe287eb8d58e6322e9fb67110ed7122
7:44:00 PM	Wbpv.exe	aba9ed05edd515feb7ff7e79d1a51960
7:45:09 PM	Wbpv.cfg	
7:46:22 PM	Nc.exe	ab41b1e2db77cebd9e2779110ee3915d

بررسی فایرفاکس:

در پسورد های ذخیره شده یوزر پسورد جیمل alice وجود دارد.

Site	Username	Password	Last Used	Last Changed
https://accounts.google.com	alice00002014	1001251125	Nov 17, 2014, 7:23 PM	Nov 17, 2014

فایل w.exe در ساعت 7:37:17PM (با توجه با created time فایل) توسط فایرفاکس دانلود شده و در دایرکتوری downloads یوزر الیس ذخیره شده.در history فایرفاکس نیز ضبط شده.

*در cache فایلهای فایر فاکس میتوان بخشی از http request هایی که توسط فایر فاکس انجام شده را پیدا کرد (با کمک برنامه ی MozillaHistoryView) که در این میان درخواست زیر مهم است:

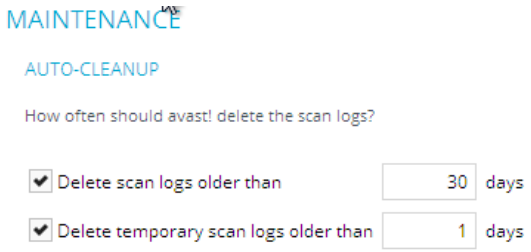
https://program.avast.com/api/?action=2&p_aas=0&p_adc=0&p_adi=-1&p_adp=0000&p_age=0&p_chr=1&p_cid=101393409&p_cnm=WIN-4046HOJ19CV&p_cpu=4.5&p_cpv=150996957&p_elm=7&p_fib=-1&p_geo=0&p_hid=3dfea1c3-a115-48d1-be98-6630093d5738&p_iex=8&p_inf=0&p_lan=1033&p_lci=1033&p_let=24&p_lex=483&p_lic=03354d7e-6000-4055-82ed-5b093dba097b&p_lid=en-us&p_lit=12&p_lng=en&p_lqa=1&p_lqe=0&p_lst=0&p_lsu=36&p_man=0&p_mdc=0&p_osv=6.1&p_pro=2&p_ram=1023&p_reh=600&p_rew=800&p_rid=3161&p_slcs=0&p_sllex=-16391&p_sllp=0&p_sllst=0&p_sllt=0&p_tzo=0&p_vbd=2013&p_vep=9&p_ves=0&p_wdc=0&p_wei=1.0&p_wnf=0&p_vir=Win32:Turkojan-AB%20[Trj]&p_prc=C:\Users\alice\AppData\Local\Temp\w.exe&p_obj=http://192.168.87.154/srv.exe

که در زمان 8:04:24PM فرستاده شده. (Date: Mon, 17 Nov 2014 16:33:24 GMT)

هچنین در جواب از سرور تایم سرور 8:03:24PM بوده که میتوان فهمید ساعت سیستم الیس حدود یک دقیقه خطا دارد.

بررسی Avast :

نکته مهمی که در مورد avast وجود دارد تنظیمات مربوط پاکسازی خودکار لاگها است که تا 30 روز گذشته را فقط نگه میدارد، برای از دست ندادن اطلاعات میتوان قبل اجرای سیستم عامل ساعت را به زمان مناسبی مثل 3 dec ببریم یا در فایلهای xml کانفیگ تنظیمات را تغییر دهیم یا ...



از آنجا که پنل خود avast گزارش خوبی از لاگفایلها نمیدهد با بررسی فایلها از مسیر C:\ProgramData\AVAST Software بررسی خود را ادامه میدهیم.

- از فایلهای موجود در Avast\report\ زمان فعال بودن بعضی از سرویسهای حفاظتی و ... را میتوان فهمید:

Name	from	to	توضیح
FileSystemShield	AM 11:27:54	PM 12:44:46	بازه فعال بودن سرویس
FileSystemShield	PM 5:00:26	PM 5:11:13	بازه فعال بودن سرویس
FileSystemShield	PM 7:47:05	PM 7:51:04	بازه فعال بودن سرویس
FileSystemShield	PM 8:02:29	PM 8:07:27	بازه فعال بودن سرویس
FileSystemShield	PM 8:10:18	PM 8:12:19	بازه فعال بودن سرویس
EmailShield	AM 11:27:54	PM 12:44:45	بازه فعال بودن سرویس
EmailShield	PM 5:00:26	PM 5:11:13	بازه فعال بودن سرویس
EmailShield	PM 7:47:05	PM 7:51:04	بازه فعال بودن سرویس
EmailShield	PM 8:02:29	PM 8:07:26	بازه فعال بودن سرویس
EmailShield	PM 8:10:18	PM 8:12:19	بازه فعال بودن سرویس
WebShield	AM 11:27:55	PM 5:11:13	بازه فعال بودن سرویس
WebShield	PM 7:47:05	PM 7:51:04	بازه فعال بودن سرویس
WebShield	PM 8:02:29	PM 8:12:20	بازه فعال بودن سرویس
WebShield	PM 8:03:18	–	تشخیص ادرس مخرب http://192.168.87.154/srv.exe (0) [L] Win32:Turkojan-AB [Trj]

- Avast\log\UITracking.log این فایل اتفاقات واسط گرافیکی را لاگ میکند که خط زیر نشان دهنده alert است:

Mon Nov 17 20:03:33 2014 - [IDR_HTM_TASKBAR_POPUP_VIR_FOUND] {button} app:virus_details

- Avast\log\aswAr.log لاگ فعالیت سیستم تشخیص روتکیت است که بدلیل روند این عملیات لیستی از پروسسها و سرویسهای فعال در زمان اسکن را دارد.

بازه زمانی اسکن:

Scan started: Monday, November 17, 2014 8:22:59 PM

Scan finished: Monday, November 17, 2014 8:23:33 PM

پروسس زیر تنها پرسس مهمی است که مانیتور شده است:

[1912] Process C:\Windows\System32\svshost.exe

- Avast\log\EventLog.log اطلاعات مفیدی که از این فایل استخراج میشود وضیعت سرویس فایر وال در زمان های خاصی است:

2014/17/11	11:28:01AM	[00000D00] Firewall enabled 1
2014/17/11	12:38:56PM	[00000E04] Firewall enabled 1
2014/17/11	5:01:54PM	[00000978]Firewall enabled 1
2014/17/11	5:11:13PM	[000006F4] Firewall enabled 0
2014/17/11	7:47:06PM	[000009FC] Firewall enabled 1
2014/17/11	7:51:04PM	[0000096C] Firewall enabled 0
2014/17/11	8:02:29PM	[00000B50] Firewall enabled 1
2014/17/11	8:11:52PM	[00000A30] Firewall enabled 1
2014/17/11	8:12:19PM	[00000E9C] Firewall enabled 0
2014/17/11	8:12:20PM	[00000EA4] Firewall enabled 0
2014/18/11	9:39:41AM	[00000B68] Firewall enabled 0

که میتوان حدود بازه های فعالیت سرویس فایروال را به صورت زیر برداشت کرد:

12:38:56 PM → 5:11:13 PM

7:47:06 PM → 7:51:04 PM

8:02:29 PM → 8:12:19 PM

- Avast\fw\NetProfiles.xml این فایل حاوی اطلاعاتی در باره شبکه هایی است که الیس در آنها حضور داشته که به صورت زیر است:

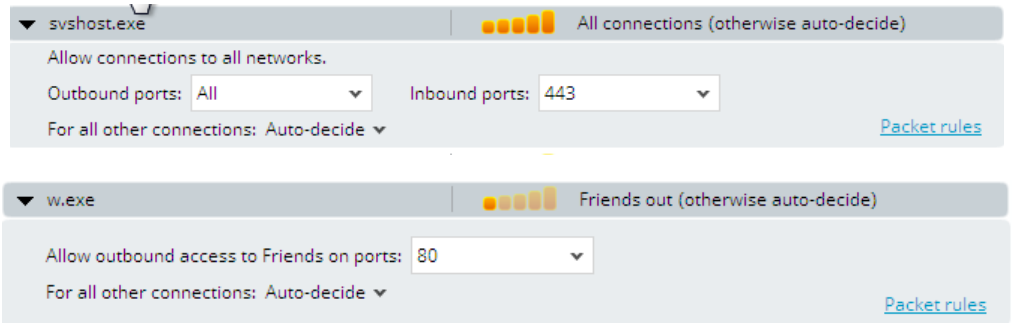
```
FARHANG AZMA COMMUNICATIONS COMPANY LTD (Intel(R) PRO/1000 MT, IR)
HwAddress="00-0C-29-E0-C8-FD"
IpAddress="fe80::fde5:aadf:4230:fa76"
Isp"=FARHANG AZMA COMMUNICATIONS COMPANY LTD"

TELECOMMUNICATION COMPANY OF TEHRAN (Intel(R) PRO/1000 MT, IR)
HwAddress ="00-0C-29-AA-94-FA"
IpAddress ="fe80::499:a33f:4d68:ce63"
Isp ="TELECOMMUNICATION COMPANY OF TEHRAN"

TELECOMMUNICATION COMPANY OF TEHRAN (Intel(R) PRO/1000 MT, IR)
HwAddress ="00-0C-29-AA-94-FA"
IpAddress ="fe80::499:a33f:4d68:ce63"
Isp ="TELECOMMUNICATION COMPANY OF TEHRAN"
```

- Avast\fw\rules.xml حاوی rule هایی که برای فایروال تعریف شده

این فایل اخرین زمان تغییرش(modified time) در 8:09:48PM بوده و این یعنی رولهای اضافه شده به فایروال قبل از این زمان اضافه شده!

که رولهای مهم به صورت زیر است:

Program	direction	port
\Users\alice\AppData\Local\Temp\w.exe	out	80
\Windows\System32\svshost.exe	in	443



- Avast\Fw.db\ دیتابیسی از نوع sqlite است که حاوی اطلاعات مربوط به کانکشنهای بلاک شده و ... است، اطلاعات مربوط به کانکشنهای بلاک شده در جدول Packet موجود است و دو بازه ی زمانی مهم میتوان از آن پیدا کرد:

از 7:47:05PM تا 7:50:56PM کانشنهایی به پورت 3389 که مربوط به rdp است بلاک شده که همه از سمت ایپی 192.168.87.154 (c0a8579a) بوده.

Time	Remote address	Remote port	Local address	Local port	Protocol
11/17/2014 5:08:05 PM	192.168.87.2	53	192.168.87.157	61591	UDP
11/17/2014 5:11:13 PM	192.168.87.2	53	192.168.87.157	56501	UDP
11/17/2014 7:47:05 PM	192.168.87.154	58395	192.168.87.157	3389	TCP
11/17/2014 7:47:24 PM	192.168.87.154	58395	192.168.87.157	3389	TCP
11/17/2014 7:47:25 PM	192.168.87.154	58395	192.168.87.157	3389	TCP

از 8:06:20PM تا 8:10:10PM کانکشنهایی به پورت 443 که مربوط به svshost.exe است بلاک شده که همه از سمت ایپی 192.168.87.154 (c0a8579a) بوده.

Time	Remote address	Remote port	Local address	Local port	Protocol
11/17/2014 8:02:36 PM	192.168.32.1	138	192.168.32.255	138	UDP
11/17/2014 8:06:20 PM	192.168.87.154	38555	192.168.87.157	443	TCP
11/17/2014 8:06:21 PM	192.168.87.154	38555	192.168.87.157	443	TCP
11/17/2014 8:06:23 PM	192.168.87.154	38555	192.168.87.157	443	TCP
11/17/2014 8:06:27 PM	192.168.87.154	38555	192.168.87.157	443	TCP

نکات دیگر:

- فایل system32/svshost.exe (md5:ab41b1e2db77cebd9e2779110ee3915d) برنامه ی netcat است که به صورت backdoor در startup ویندوز قرار داده شده است. زمان ایجاد فایل 7:55:41 PM میباشد.

(http://www.offensive-security.com/metasploit-unleashed/Persistent_Netcat_Backdoor)

- از انجا که یورز administrator رمز ندارد به راحتی میتوان در سطح ادمین دستورات را اجرا کرد!

بررسی pagefile.sys و hiberfil.sys:

این فایلها حاوی بخشهای از مموری بوده و میتوان حاوی اطلاعات باقی مانده در مموری باشد ، برای بررسی این فایلها با کمک برنامه ی bulk extractor اطلاعات که میتواند مهم باشد را استخراج میکنیم ، در این بین میتوان به ایپی ها و url هایی رسید که میتواند مهم باشد

http://192.168.87.154/srv.exe
http://192.168.106.1:49572/RootDevice.xml
http://localhost:80/WSMAN
192.168.87.2

بررسی استحکام رمز الیس:

به صورت لوکال رمز را کرک میکنیم تا سطح استحکام پسورد را بفهمیم ؛ که به راحتی توسط دیکشنری رمز پیدا میشود و نشاندهنده ضعیف بودن کلمه عبور است.

http://www.computersecuritystudent.com/SECURITY_TOOLS/PASSWORD_CRA/CKING/lesson2

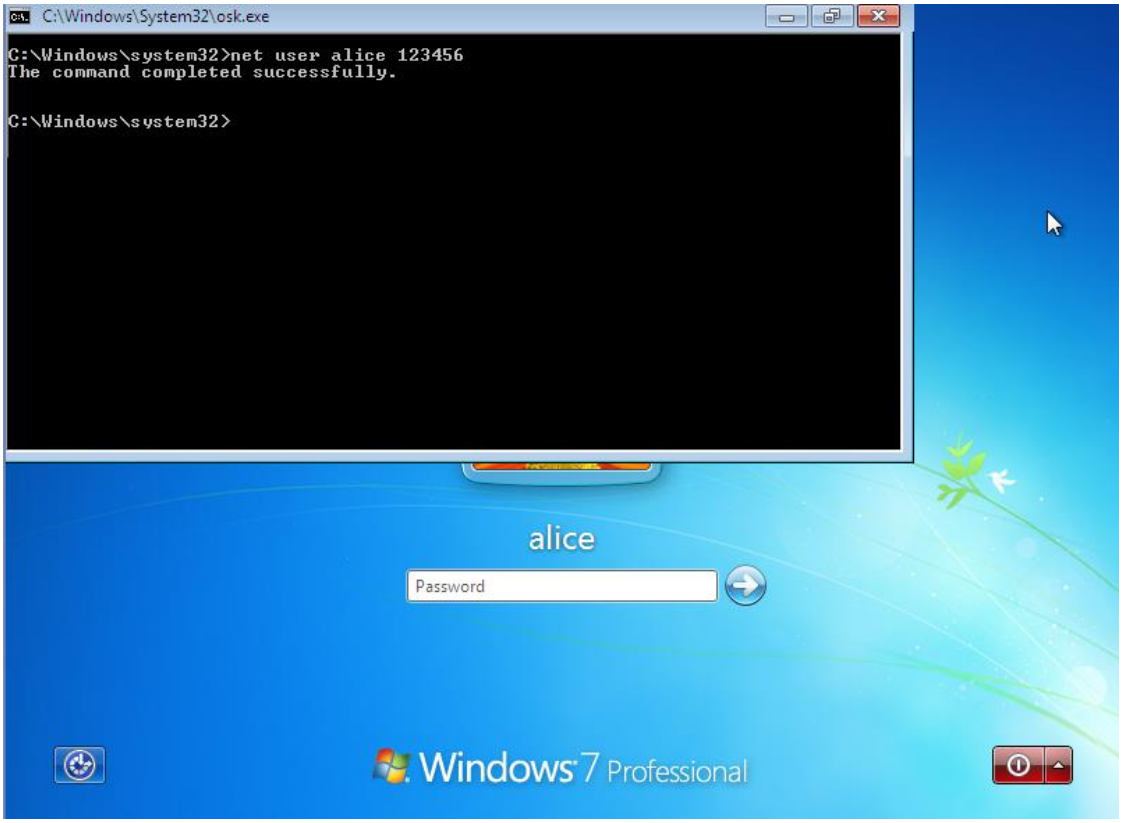
```
root@kali:/media/0A80FB3080FB20BD/Windows/System32/config# john /tmp/hash -format=nt2 -user=alice
Loaded 1 password hash (NT MD4 [128/128 SSE2 intrinsics 12x])
1q2w3e           (alice)
guesses: 1  time: 0:00:00:00 DONE (Tue Dec 23 06:55:14 2014)  c/s: 27100  trying: 1q2w3e - blazer
Use the "--show" option to display all of the cracked passwords reliably
```

مراحل تغییر رمز سیستم الیس برای ورود اولیه(ویندوز):

ابتدا با یک سیستم عامل دیگر به فایل های سیستم الیس دسترسی پیدا میکنیم و با رفتن به دایرکتوری system32 فایل osk.exeرا پاک کرده و به جای آن cmd.exe را با نام osk.exe کپی میکنیم.

فایل osk.exe در واقع فایل اجرایی کیبرد مجازی سیستم عامل ویندوز است و کیبرد مجازی به عنوان یکی از برنامه هایی است که در صفحه ورود ویندوز و قبل ورود قابل اجراست! ☺

بعد از ریست کردن و رفتن به صفحه ورود سیستم الیس با اجرای کیبرد مجازی cmd.exe در بالاترین سطح دسترسی(system) برای ما اجرا میشود که به راحتی با دستور net user alice 123456 پسور یوزر الیس را به 123456 تغییر میدهیم.



بررسی سیستم باب:

نوع سیستم عامل:

Ubuntu 14.04.1 LTS

```
Linux ubuntu 3.13.0-39-generic #66-Ubuntu SMP Tue Oct 28 13:31:23 UTC 2014 i686
i686 i686 GNU/Linux
```

هارد مجازی

TimeZone سیستم:

Asia/Tehran

تنظیمات شبکه:

در فایل /etc/network/interfaces تنظیمات کارت شبکه وجود دارد.

که ایپی سیستم به صورت دستی روی 192.168.87.154 ست شده است.

```
iface eth0 inet static
address 192.168.87.154
network 192.168.87.0
netmask 255.255.255.0
broadcast 192.168.87.255
```

بررسی لاگ ها:

- /var/log/apache2

در این دایرکتوری accesslog مهم است که حاوی اطلاعات درخواست هایی که به وب سرور شده است میباشد:

```
192.168.87.157 - - [17/Nov/2014:19:36:19 +0330] "GET /w.exe HTTP/1.1" 200 333107 "-" "Mozilla/5.0 (Windows NT 6.1; rv:33.0) Gecko/20100101 Firefox/33.0"
192.168.87.157 - - [17/Nov/2014:19:43:02 +0330] "GET /wbpv.exe HTTP/1.0" 200 353171 "-" "Wget/1.10.2"
192.168.87.157 - - [17/Nov/2014:19:45:03 +0330] "GET /nc.exe HTTP/1.0" 404 499 "-" "Wget/1.10.2"
192.168.87.157 - - [17/Nov/2014:19:45:24 +0330] "GET /nc.exe HTTP/1.0" 200 61745 "-" "Wget/1.10.2"
192.168.87.157 - - [17/Nov/2014:20:02:19 +0330] "GET /srv.exe HTTP/1.0" 200 110899 "-" "Wget/1.10.2"
```

باتوجه به اینکه زمان دانلود w.exe در سیستم 7:37:17 بود ،میتوان گفت حداکثر ساعت سیستم باب یک دقیقه عقبتر از سیستم الیس است پس سیستم باب هم حداکثر دو دقیقه خطا دارد.

- /var/log/apt

به کمک این فایلها میتوان زمان نصب برنامه ها را فهمید که سه برنامه روبرو اهمیت بیشتری دارد:

```
Start-Date: 2014-11-17 16:57:23
Commandline: apt-get install hydra
End-Date: 2014-11-17  16:57:53

Start-Date: 2014-11-17 19:34:11
Commandline: apt-get install apache2
End-Date: 2014-11-17  19:34:26

Start-Date: 2014-11-18  10:03:00
Install: iptables-persistent:i386 (0.5.7)
End-Date: 2014-11-18  10:03:04
```

- /var/log/auth.log

این فایل حاوی وقایع مربوط به سرویس ssh است.

از ایپی 192.168.87.156 در بازه ی زمانی 15:22:58 تا 16:53:43 تعداد زیادی تلاش ناموفق برای ورود به یوزر bob از طریق ssh انجام شده که نشان دهنده حمله بروت فرس است، و در لحظه 16:53:52 اولین ورود موفق از انجام شده که نشان دهنده موفقیت حمله است.

همچنین قسمتی از خطوط لاگ فایل به صورت زیر است که نشان دهنده بخشی از دستورات اجرا شده است:

```
Nov 18 10:00:39 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/sbin/iptables -t nat -L
Nov 18 10:02:27 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/usr/bin/aptitude install iptables-persistent
Nov 18 10:04:25 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/bin/mv /etc/iptables-up.rules /etc/iptables/rules.v4
Nov 18 10:04:45 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/usr/bin/vim /etc/network/interfaces
Nov 18 10:05:13 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/sbin/iptables-restore
Nov 18 10:05:21 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/sbin/iptables -L
Nov 18 10:05:26 ubuntu sudo:     bob : TTY=tty1 ; PWD=/home/bob ; USER=root ;
COMMAND=/sbin/iptables -t nat -L
Dec  2 11:18:53 ubuntu sudo:     bob : TTY=pts/2 ; PWD=/home/bob ; USER=root ;
COMMAND=/usr/bin/vim /root/.bash_history
Dec  2 11:19:13 ubuntu sudo:bob : TTY=pts/2 ; PWD=/home/bob ; USER=root ;
COMMAND=/usr/bin/vim /root/.bash_history
```

که دستورات مروبوط به کانفیگ iptable و تغییر bash_history. است!

مشکلی که وجود دارد اجرای اکثر کامند های مربوط به تغییر تنظیمات iptable سیستم باب با tty انجام شده که نشانگر تغییرات به وسیله یوزری است که به صورت فیزیکی پشت سیستم است...

- last :

```
bob      tty1                          Tue Dec  2 12:20 - down   (00:00)
reboot   system boot  3.13.0-39-generi Tue Dec  2 12:20 - 12:21  (00:00)
bob      tty1                          Tue Dec  2 11:21 - down   (00:00)
bob      pts/2        192.168.87.1     Tue Dec  2 11:17 - 11:19  (00:02)
bob      pts/1        192.168.106.1    Tue Dec  2 11:11 - down   (00:10)
bob      tty1                          Tue Dec  2 10:48 - 11:19  (00:31)
reboot   system boot  3.13.0-39-generi Tue Dec  2 14:17 - 11:22  (-2:-55)
bob      pts/0        192.168.106.1    Tue Nov 18 10:10 - 10:11  (00:01)
bob      tty1                          Tue Nov 18 10:06 - down   (00:05)
bob      tty1                          Tue Nov 18 10:05 - 10:06  (00:00)
bob      tty1                          Tue Nov 18 10:00 - 10:05  (00:05)
reboot   system boot  3.13.0-39-generi Tue Nov 18 09:50 - 10:11  (00:21)
bob      tty1                          Tue Nov 18 09:45 - down   (00:01)
bob      tty1                          Tue Nov 18 09:20 - 09:45  (00:24)
reboot   system boot  3.13.0-39-generi Tue Nov 18 09:19 - 09:46  (00:27)
bob      pts/1        192.168.87.156   Mon Nov 17 16:54 - down   (04:52)
bob      tty1                          Mon Nov 17 15:12 - down   (06:34)
reboot   system boot  3.13.0-39-generi Mon Nov 17 15:11 - 21:47  (06:35)
bob      tty1                          Mon Nov 17 13:19 - down   (00:00)
reboot   system boot  3.13.0-39-generi Mon Nov 17 13:18 - 13:19  (00:00)
```

که به وضوح بازه زمانی session ها و ip ها و نوع را مشخص کرده.

اتصال فیزیکی tty

اتصال از راه دور pts (ssh)

بررسی فایلها و دایرکتوریهای مهم:

- /etc/iptables/rules.v4

این فایل که حاوی رولهای فایروال سیستم عامل است،که رول نوشته شده باعث میشود کل ترافیک ورودی به پورت 3389 یا همان rdp (remote desktop) به پورت 3389 اپی 192.168.87.157 فروارد شود و سیستم نقش پروکسی را بازی کند.

همچنین اخرین زمان تغییر فایل 2 dec 11:15 بوده.

```
*nat
:PREROUTING ACCEPT [7:546]
:INPUT ACCEPT [7:546]
:OUTPUT ACCEPT [1:328]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 3389 -j DNAT --to-destination
192.168.87.157:3389
-A POSTROUTING -j MASQUERADE
COMMIT
```

- /home/bob/.bash_history

این فایل حاوی دستوراتی است که یوزر اجرا کرده و مشخص است که شامل همه دستورات نیست و بیشترش پاک شده.

```
sudo shutdown -h now
ifconfig
sudo shutdown -h now
```

- /home/bob/.viminfo

این فایل حاوی اطلاعاتی درباره فایهای تغییر داده شده توسط دستور vi است.

که در قسمت Registers میتوان مقادیری که در هنگام تغیرات فایل کپی یا کات شده اند مشاهده کرد

که ظاهرا در اینجا بخشی از دستورات .bash_history است که به صورت دستی تغییر داده شده!

```
whoami
ifconfig
ifup eth0
ifdown eth0
vim /etc/network/interfaces
ifconfig
ifup eth0
shutdown -h now
```

همچنین در بخش File marks میتوان فایل هایی که مورد تغییر واقع شده را دید

که تایید کننده این مطب است که فایل های .bash_history دچار تغییر شده!

```
/root/.bash_history
~/.bash_history
~/.bashrc
/etc/network/interfaces
/etc/hostname
/etc/hos
/etc/network/interfaces
```

- /root/.bash_history

```
vim /etc/network/interfaces
/etc/init.d/networking restart
ifconfig
ifdown eth0
```

- /root/.viminfo

: Registers

```
gateway 192.168.87.254
# Completed on Tue Nov 18 09:41:53 2014
# Generated by iptables-save v1.4.21 on Tue Nov 18 09:41:53 2014
poweroff
grep -Era 192.168.87.* /var/log
grep -Era 192.168.87.* /
nc 192.168.87.157 443
nc
nc 192.168.87.157 443
```

که بخشهایی از فایل /etc/iptables/rules.v4 و دستوراتی که احمالا در .bash_history سیستم بوده مشاهده میشود.که در این بین دستورات اتصال به در پشتی سیستم الیس و از همه مهمتر دستور grep است که نشاندهنده ی اهمیت ایپی های رنج 192.168.87 در لاگ فایلها برای هکر است که با دستور grep محتویات تمام لاگ فایلها را به دنبال ایپی خود میگردد ، نکته ای که وجود دارد این است که توسط این دستور محتویات فایلهایی مثل lastlogاکه به صورت encode شده اطلاعات را نگه میدارد جستجو نمیشود و میتوان به خروجی دستور last که محتویات این فایل را نشان میدهد اعتماد بیشتری کرد...

: File marks

```
/etc/network/interfaces
/etc/network/interfaces
/etc/iptables/rules.v4
/etc/iptables/rules.v4
~/.bash_history
/etc/network/interfaces
~/.bash_history
/var/log/auth.log
~/.bash_history
```

علاوه بر کانفیگ ها شبکه و فایروال،لاگ فایل های مهم تغییر پیدا کرده...

- /var/www/html/

این دایرکتوری حاوی فایلهای است که در روت وبسرور قرار دارد که هریک جلوتر بررسی میشود.

```
iepv.exe    (md5: 0f289098cc579d3cf22ff6368ed72c37)
index.html  (md5:c32ad802df5abca941d784abf642e7fd)
nc.exe      (md5:ab41b1e2db77cebd9e2779110ee3915d)
srv.exe     (md5:21560eef1794773c102c5a72efa08e38)
wbpv.exe    (md5:1960aba9ed05edd515feb7ff7e79d1a5)
w.exe       (md5:dbe287eb8d58e6322e9fb67110ed7122)
```

بررسی استحکام رمز باب:

به صورت لوکال رمز را کرک میکنیم تا سطح استحکام پسورد را بفهمیم ؛ که به راحتی توسط دیکشنری رمز پیدا میشود و نشاندهنده ضعیف بودن کلمه عبور است.

/http://www.binarytides.com/cracking-linux-password-with-john-the-ripper-tutorial

```
root@kali:/media/01e11a8$-32d8-4bb3-a606-60906f4fb5ca# john --wordlist=/usr/share/john/password.lst ~/ftc
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [32/32])
q1w2e3           (bob)
guesses: 1  time: 0:00:00:02 DONE (Tue Dec 23 06:10:11 2014)  c/s: 384  trying: oregon - random
Use the "--show" option to display all of the cracked passwords reliably
```

مراحل تغییر رمز سیستم باب(لینوکس):

پس از دسترسی گرفتن به فایلهای سیستم باب با سیستم عامل دیگری و تغییر سطر مروبوط به یوزر root در فایل shadow پسورد دلخواه را جاگذین میکنیم.

نکات دیگر:

از انجا که یوزر root پسوردی ندارد ،یوزر باب به راحتی میتواند سطح دسترسی خود را به روت ارتقا دهد.

یک ابهام(/var/lib/dhcp/) :

با بررسی فایلهای /var/lib/dhcp/ میتوان بخشی از اپپی هایی که سیستم از dhcp گرفته را مشاهده کرد، با بررسی این فایل ها که علاوه بر کار اصلی حالت لاگ فایل دارند میتوان متوجه ی اپپی سیستم در چند بازه زمانی شده که به شرح زیر است:

زمان شروع	زمان پایان	Dhcp server	router	ip
17/11/2014 16:15:14	17/11/2014 18:41:12	192.168.87.254	192.168.87.2	192.168.87.155
18/11/2014 06:45:48	18/11/2014 06:58:29	192.168.106.254	192.168.106.2	192.168.106.129
02/12/2014 11:01:31	02/12/2014 11:13:53	192.168.106.254	192.168.106.2	192.168.106.129

این اتطلاعات بیانگر این است که سیستم الیس توسط باب bruteforce نشده زیرا اپپی سیستم باب در آن زمان 192.168.87.155 بوده! در حالی که تمام موضوعات دیگر بیانگر خلاف این موضوع است، و این مشکل را میتوان گفت یا صحنه سازی هکر است یا ردپای تیم طراحی!

بررسی فایلها های ناشناس:

W.exe (md5:dbe287eb8d58e6322e9fb67110ed7122)

این فایل نسخه ویندوزی wget لینوکس است و برای دریافت اطلاعات بر روی پروتکل های مختلف از جمله http به صورت کامندی استفاده میشود. کد فایل به صورت opensource موجود است و الودگی ایجاد نمیکند

Nc.exe یا svshost.exe (md5:ab41b1e2db77cebd9e2779110ee3915d)

این فایل همان نتکت معروف است که ابزار پرکاربرد شبکه کاران و همپنین هکرهاست و به دلیل کاربرد بیشتر مفیدش از دید انتی ویروس ها و ... فایل تمیز و بیخطری است،از نتکت میتوان برای ایجاد backdoor و اجرای دستورات از راه دور و مخفیانه استفاده کرد.

(http://www.offensive-security.com/metasploit-unleashed/Persistent_Netcat_Backdoor)

Wbpv.exe (md5:aba9ed05edd515feb7ff7e79d1a51960)

نسخه 1.56 برنامه WebBroserPassView است

(http://www.nirsoft.net/utils/web_browser_password.html)

این برنامه پسورد های ذیره شده در مرورگرهای مختلف را از فایلهای مرورگر استخراج میکند ،

همچنین قابلیت اجرای کامندی نیز دارد!

Wbpv.cfg

فایل کانفیگ WebBroserPassView است که بعد از اجرای برنامه به صورت خودکار ساخته میشود

iepv.exe (md5:0f289098cc579d3cf22ff6368ed72c37)

نسخه 1.32 برنامه IEPassView است.

http://www.nirsoft.net/utils/internet_explorer_password.html

این برنامه رمزهای ذخیره شده در مرورگر IE را استخراج میکند.

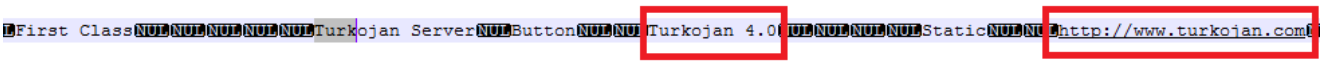
Srv.exe (eef1794773c102c5a72efa08e3821560)

این فایل تروجان معروفی که اکثر انتی ویروسها آن را شناسایی میکنند.

با برسی داینامیک فایل میتوان فهمید که تروجان سعی دارد به ایپی 192.168.87.152 پورت 15963 وصل شود.

Prot...	Local Address	Remote Address	State
TCP	192.168.1.8:49161	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49162	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49163	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49164	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49165	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49166	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49167	192.168.87.152:15963	SYN_SENT
TCP	192.168.1.8:49168	192.168.87.152:15963	SYN_SENT

همچنین بعد از اجرا با دامپ گرفتن از پروسس و بررسی استرینگ های موجود به موارد زیر میرسیم:



که میتوان از استریگ ها و شماره پورت فهمید تروجان به نام turkojan 4.0 است و ایپی c&c تروجان 192.168.87.152 است!

این تروجان قابلیت کیلاگر ، تصویر گرفتن از صفحه و ... را دارد.

نتیجه گیری:

برای تصیح حدودی خطا تایم های سیستم الیس یک دقیه افزایش یافته.

برای تصیح حدودی خطا تایم های سیستم باب دو دقیه افزایش یافته.

هکر ابتدا بدلیل پسورد ضعیف یوزر باب به سیستم باب نفوذ میکند و با استفاده از سیستم باب حمله ای را روی سیستم الیس انجام میدهد که باز بدلیل ضعف پسورد و غیر فعال بودن فایروالها با موفقیت انجام میشود همچنین در مراحل بعد از سیستم باب برای انتقال فایل و وصل شدن به در پشتی استفاده میکند همچنین با پروکسی قرار دادن سیستم باب اتصال ریموت دسکتاب به الیس را برقرار میکند(هم میتوان با ssh session پروکسی استفاده کرد و هم با کانفیگ iptable).در کل تمام اتصالات انجام شده هکر با سیستم الیس توسط سیستم باب بوده و فقط برای تروجانی که قصد اجرا داشت اپیی دیگر استفاده کرده بود.

در اتصال اول به سیستم الیس با تولزی که روی سیستم دانلود میکند پسورد جیمیل الیس را به دست می آورد سپس به وسیله فایروال سیستم الیس اتصال هکر قطع میشود ، در اتصال دوم هکر با استفاده از نتکت backdoor در سیستم الیس فعال میکند ، با ورود الیس به سیستمش اتصال ریموت دسکتاب هکر دوباره قطع میشود و هکر بوسیله در پشتی در مرحله بعد سعی میکند در زمانی که الیس پشت سیستم است تروجانی بروی سیستم الیس دانلود کند که با شناسایی آن توسط avast پیغام اخطاری به الیس نشان داده میشود که الیس هم با رفتن با لینک مربوط به تروجان که avast ایجاد کرده به این پیغام اهمیت میدهد و چند لحظه بعد با فعال کردن فایروال دسترسی هکر برای مدتی بسته میشود،اما از آنجا که بازه زمانی کمی فایر وال فعال است امکان ورود مجدد هکر زیاد است.

هکر در مرحله بعد با پاک سازی سیستم باب و تغییر در چند لاگ فایل سعی میکند رد پای خود را پاک کند،همچنین با تنظیم کردن iptable سیستم باب را برای اتصال به ریموت دسکتاب الیس به عنوان پروکسی اماده میکند.

از آنجا که در سیستم باب لاگ فایل ها دچار تغییر شده اند نمیتوان اعتماد کامل به لاگ فایل ها کرد.

اما اپیی های هکر میتواند موارد زیر باشد:

192.168.87.156 در بازه ی زمانی 21:48 تا 16:54 روز 17 nov (انجام حمله به باب و اتصال به سیستم)

192.168.87.152 که در فایل تروجان به عنوان c&c استفاده شده است.

192.168.106.1 و 192.168.87.1 که در روزهای بعد حمله به سیستم باب وصل شده و مشکوک به ایجاد تغییر در لاگ فایلها هستند.

همچنین کامندهایی در ارتباط با iptable به صورت فیزیکی پشت سیستم باب اجرا شده و با توجه به غیرعادی بودن کانفیگ نهایی میتواند خود یوزر باب نیز با هکر همکاری داشته باشد!!!

دو اپیی اول که در رنج 192.168.87 هستند مهمتر هستند به دلیل اینکه دستوراتی(grep -Era 192.168.87.* /var/log) در سیستم باب اجرا شده که به دنبال اپیی های این رنج در لاگ فایل ها بوده.

TimeLine بازه ی زمانی اصلی انجام جرم که در روز 17 NOV بوده باجزیات:

۱۵:۲۴:۵۸
۱۶:۵۵:۴۳
- انجام حمله موفق bruteforce به سیستم باب از ایپی ۱۹۲.۱۶۸.۸۷.۱۵۶ بر روی یوزر باب.

۱۶:۵۹:۲۳
- تصب برنامه ی hydra بر روی سیستم باب که برای حمله بروت فرس استفاده میشود

۱۷:۱۲:۴۵
- غیر فعال کردن فایروال ویندوز توسط الیس که باعث اسیب پذیر شدن سیستمش شد

۱۷:۱۴:۴۴
۱۷:۲۸:۲۹
- انجام حمله bruteforceموفق به سیستم الیس از ایپی ۱۹۲.۱۶۸.۸۷.۱۵۴ با برنامه ی hydra که احتملا این حمله از سمت سیستم باب بوده.

۱۹:۲۸:۵۱
- ورود هکر به سیستم الیس بوسیله ی سیستم عامل kali و با پروکسی کردن سیستم باب توسط پروتکل remote desktop

۱۹:۳۶:۱۱
- نصب وب سرور apache بر روی سیستم باب برای انتقال فایلهای هکر به سیستم الیس

۱۹:۳۸:۱۷
- دانلود w.exe به وسیله ی فایرفاکس که یک دانلودر کامندی است از وبسرور باب بر روی سیستم الیس توسط session ایجاد شدهی rdp .

۱۹:۴۵:۰۰
- دریافت wbpv.exeاز روی وب سرور باب بر روی سیستم الیس به وسیله w.exe

۱۹:۴۵:۲۲
- اجرای wbpv.exe و پیدا کردن پسورد های ذخیره شده در مرورگرهای سیستم توسط هکر، از جمله پسورد جیمیلی که برروی فایرفاکس سیو شده و دسترسی هکر به رمز جیمیل الیس!

۱۹:۴۷:۲۲
- دریافت netcatبر روی سیستم الیس از وبسرور باب

۱۹:۴۸:۲۴
- قطع اتصال rdp با فعال شدن فایروال avast سیستم الیس و بلاک کردن اتصالات ورودی به پورت 3389.

۱۹:۵۰:۲۹
۱۹:۵۰:۳۳
- ورود و خروجی بسیار کوتاه به صورت فیزیکی به سیستم الیس!!!

۱۹:۵۲:۰۴
- غیر فعال شدن فایروال avast ،شاید بخاطر سهل انگاری الیس یا اینده نگری هکر!

۱۹:۵۲:۲۳
- ورد مجدد هکر با rdp بعد از غیر فعال شدن فایروال avast

۱۹:۵۶:۴۱
- کپی کرن netcatدانلود شده به دایرکتوری system32الیس و تغییر نام ان به svshost.exe که باعث جلب توجه نشود

۱۹:۵۷:۵۷
- طبق prefetch ها در این زمان regedit اجرا شده ، که احتمالا هکر با استفاده از netcat که در سیستم مخفی کرده و ست کردن keyمربوطه در ریجستری درپشتی در startup سیستم الیس ایجاد کرده که بتواند بعدا از آن استفاده کند.

۲۰:۱:۰۶
- با ورود فیزیکی الیس به سیستمش session هکر قطع شده

۲۰:۴:۲۹
- هکر بوسیله در پشتی که ایجاد کرده سعی میکند تروجانی (srv.exe) بر روی سیستم الیس دانلود کند .

۲۰:۴:۳۳
- بعد از تلاش هکر برای دانلود تروجان، avastبا شناسایی تروجان جلوی دانلود آن را میگیرد و پنجره ی اخطاری برای الیس باز میکند

۲۰:۰۵:۲۴
- الیس با فایرفاکس به لینک مربوط به اخطار میرود که این نشاندهنده اهمیت موضوع برای الیس است

۲۰:۷:۲۰
- با فعال شدن فایروال avast احتمالا توسط الیس با جلو گیری از ارتباط با پورت ۴۴۳ سیستم یعنی پورتی که برای درپشتی استفاده شده ، مانع استفاده هکر از در پشتی میشود.