OSY.SSI [2018] [13]

In the news...

- CIA comms compromised in Iran, 30 agents dead, using Google [link] [link]
- 44 years old Windows bug (e.g. `C:/con/con`) [link]
- Intel PortSmash side-channel attack [link]
- Not content with hacking into Belgacom, GCHQ sabotages the investigation [link]
- 81000 facebook accounts hacked [link]
- CVE-2018-9411: New critical vulnerability in Android [link]
- Critical vulnerability in Apple Mojave crypto [link]
- CVE-2018-4407: Kernel RCE on Apple ICMP stack [link]

In the last episode

Stack/heap overflow · ROP · spraying · UAF

Overall this course

- Look at technology with a new (and critical!) eye
- Test things beyond their normal/usual regimen
- Be curious and creative
- Put theories / metaphors / claims to the test
- Don't kill bugs, learn from them

And also the sorry state of technology

About today

A real-world operation.

Details were altered to conform to the contractual agreement between parties.

I'll try to illustrate as much as possible though.

Prelude and context

Prelude and context

- Contacted by a client following an incident

Prelude and context

- Contacted by a client following an incident
- A sensitive document (legal?) has leaked and the client wants to know how this was possible

Prelude and context

- Contacted by a client following an incident
- A sensitive document (legal?) has leaked and the client wants to know how this was possible
- So we start asking: what leaked exactly? where was it stored? what were the protections?

Prelude and context

- Contacted by a client following an incident
- A sensitive document (legal?) has leaked and the client wants to know how this was possible
- So we start asking: what leaked exactly? where was it stored? what were the protections?
- "We pay your for answers, not questions"

Prelude and context

- Contacted by a client following an incident
- A sensitive document (legal?) has leaked and the client wants to know how this was possible
- So we start asking: what leaked exactly? where was it stored? what were the protections?
- "We pay your for answers, not questions"... oooookayy

Prelude and context

- Contacted by a client following an incident
- A sensitive document (legal?) has leaked and the client wants to know how this was possible
- So we start asking: what leaked exactly? where was it stored? what were the protections?
- "We pay your for answers, not questions"... oooookayy
- Eventually they ask for a pentest, to figure out what went wrong and how the leak could happen.

Prelude and context

- Contacted by a client following an incident
- A sensitive document (legal?) has leaked and the client wants to know how this was possible
- So we start asking: what leaked exactly? where was it stored? what were the protections?
- "We pay your for answers, not questions"... oooookayy
- Eventually they ask for a pentest, to figure out what went wrong and how the leak could happen.

"Go as far as you can"

Let's go

Step 1:

Let's go

Step 1: Reconnaissance

Let's go

Step 1: Reconnaissance

- OSINT: Google, LinkedIn, registers, whois, domains, e-mails, contractors, phone numbers (Harvester)

Let's go

Step 1: Reconnaissance

- OSINT: Google, LinkedIn, registers, whois, domains, e-mails, contractors, phone numbers (Harvester)
- Call a few people's preious employers for "background check" and references

Let's go

Step 1: Reconnaissance

- OSINT: Google, LinkedIn, registers, whois, domains, e-mails, contractors, phone numbers (Harvester)
- Call a few people's preious employers for "background check" and references
- Google Maps, opening and closing hours, shodan (kamerka)
- Websites, webmails, different languages, 404, incorrect URLs

Recon: results

- A list of people, places, and their relationships
- An idea of where the legal team is working
- A list of public IPs for the company's webservers

Recon: results

- A list of people, places, and their relationships
- An idea of where the legal team is working
- A list of public IPs for the company's webservers

Need more info. Need to get closer.

Getting closer

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite
- Get closer to the physical building trying to get some Wifi

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite
- Get closer to the physical building trying to get some Wifi
- Notice any ingress and egress points that may be useful

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite
- Get closer to the physical building trying to get some Wifi
- Notice any ingress and egress points that may be useful
- Try to get a meeting with an employee to discuss a recent talk they gave

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite
- Get closer to the physical building trying to get some Wifi
- Notice any ingress and egress points that may be useful
- Try to get a meeting with an employee to discuss a recent talk they gave
  - Hopefully they'd bring their laptop and phone, badges. Note the models and manufacturers.

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite
- Get closer to the physical building trying to get some Wifi
- Notice any ingress and egress points that may be useful
- Try to get a meeting with an employee to discuss a recent talk they gave
  - Hopefully they'd bring their laptop and phone, badges. Note the models and manufacturers.
  - Keep note of specific clothing or items, get them to talk

Getting closer

- Run basic network tests (nmap, nessus, dnsnoop)
- Send carefully crafted e-mails (using personal info) to see if they'd bite
- Get closer to the physical building trying to get some Wifi
- Notice any ingress and egress points that may be useful
- Try to get a meeting with an employee to discuss a recent talk they gave
    - Hopefully they'd bring their laptop and phone, badges. Note the models and manufacturers.
    - Keep note of specific clothing or items, get them to talk

Need more info. Need to get closer.

Getting closer closer

- Get inside the building of interest during open hours. (video)

Getting closer closer

- Get inside the building of interest during open hours. (video)
- Observe and gather data, get a plan of the inside (matching Gmap).

Getting closer closer

- Get inside the building of interest during open hours. (video)
- Observe and gather data, get a plan of the inside (matching Gmap).
- There are a lot of computer systems inside, how are they connected? Model, maker, version? Traces of recent maintenance?

Getting closer closer

- Get inside the building of interest during open hours. (video)
- Observe and gather data, get a plan of the inside (matching Gmap).
- There are a lot of computer systems inside, how are they connected? Model, maker, version? Traces of recent maintenance?
- Take notice of open hours and typical ingress and egress flows. How many floors? How do people evolve in this space?

Getting closer closer

- Get inside the building of interest during open hours. (video)
- Observe and gather data, get a plan of the inside (matching Gmap).
- There are a lot of computer systems inside, how are they connected? Model, maker, version? Traces of recent maintenance?
- Take notice of open hours and typical ingress and egress flows. How many floors? How do people evolve in this space?
- How is the building guarded outside of business hours?

Getting closer closer

- Get inside the building of interest during open hours. (video)
- Observe and gather data, get a plan of the inside (matching Gmap).
- There are a lot of computer systems inside, how are they connected? Model, maker, version? Traces of recent maintenance?
- Take notice of open hours and typical ingress and egress flows. How many floors? How do people evolve in this space?
- How is the building guarded outside of business hours?
- Confirm clothing/branding

Getting closer closer

- Get inside the building of interest during open hours. (video)
- Observe and gather data, get a plan of the inside (matching Gmap).
- There are a lot of computer systems inside, how are they connected? Model, maker, version? Traces of recent maintenance?
- Take notice of open hours and typical ingress and egress flows. How many floors? How do people evolve in this space?
- How is the building guarded outside of business hours?
- Confirm clothing/branding
- Try to interact with other customers (discreetely)

Preparing for entry

Okay we may know enough to get further. We could

- Try to abuse the (insecure) webservers, which use an outdated TLS configuration (incl. for authentication)
- Send phishing e-mails with malware in it, since we know employees open them
- Try to get to the Wifi (WPA2) from outside, record, and decode later (cracking or getting Wifi key)
- Get branded shirts, get our tools, and go inside

Note: Up to this point, the risk was very minimal and we did not break any law (as we were mandated by the client)

Preparing for entry

Okay we may know enough to get further. We could

- Try to abuse the (insecure) webservers, which use an outdated TLS configuration (incl. for authentication)
- Send phishing e-mails with malware in it, since we know employees open them
- Try to get to the Wifi (WPA2) from outside, record, and decode later (cracking or getting Wifi key)
- Get branded shirts, get our tools, and go inside

Note: Up to this point, the risk was very minimal and we did not break any law (as we were mandated by the client)
Note bis: Do not risk your life to make a point.

Getting inside

- Ingress points: main door (to main room), garage door (remote clicker, elevator+badge)
- Main room guarded (2 persons visible, walking), under camera surveillance (+1 guard videowatching?)
- Guards arrive about 30 minutes before closure and depart 30 minutes after opening
- Guards go back and forth in about 1 minute

Getting inside

- Ingress points: main door (to main room), garage door (remote clicker, elevator+badge)
- Main room guarded (2 persons visible, walking), under camera surveillance (+1 guard videowatching?)
- Guards arrive about 30 minutes before closure and depart 30 minutes after opening
- Guards go back and forth in about 1 minute

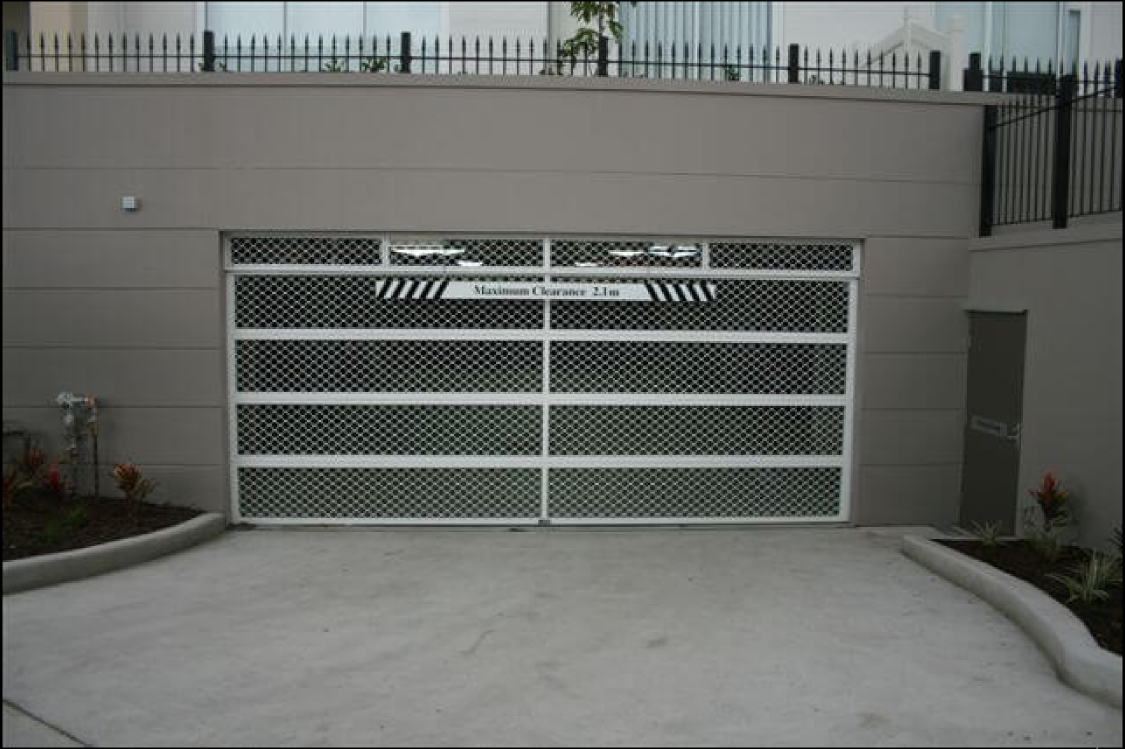
⇒ too short to check everything

Getting inside

- Ingress points: main door (to main room), garage door (remote clicker, elevator+badge)
- Main room guarded (2 persons visible, walking), under camera surveillance (+1 guard videowatching?)
- Guards arrive about 30 minutes before closure and depart 30 minutes after opening
- Guards go back and forth in about 1 minute

$\Rightarrow$ too short to check everything

$\Rightarrow$ floors -1, 1, 2 likely unguarded (?)


Maximum Clearance 2.1m

Getting inside

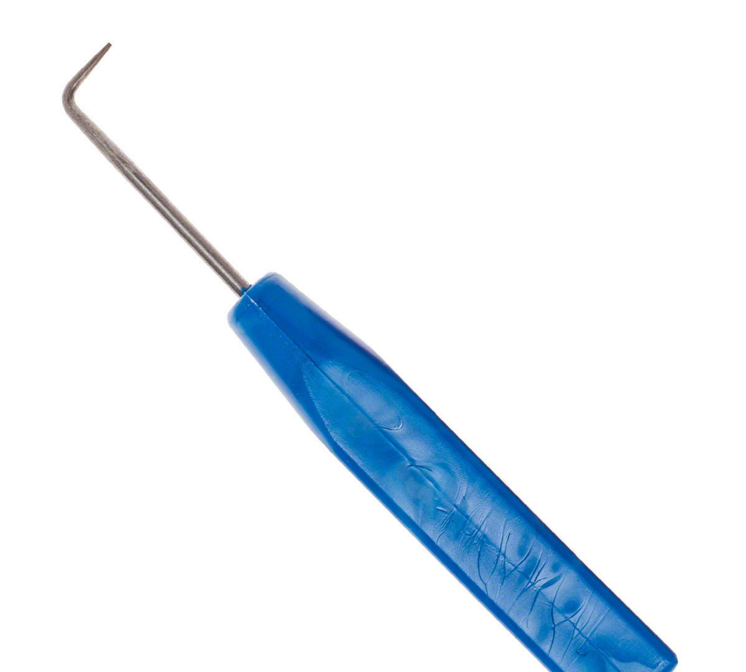
Garage door requires remote clicker + produces beeping sound when open...

Getting inside

Garage door requires remote clicker + produces beeping sound when open...

Noticed the door on the side?

Introducing: the Traveller's hook



Getting inside

Opening the door could have triggered an alarm.

Getting inside

Opening the door could have triggered an alarm. But it did not.

Getting inside

Opening the door could have triggered an alarm. But it did not.
(and if it did, we could have run away)

Getting inside

Opening the door could have triggered an alarm. But it did not.
(and if it did, we could have run away)

So here we are in the garage. A few cars.

Getting inside

Opening the door could have triggered an alarm. But it did not.
(and if it did, we could have run away)

So here we are in the garage. A few cars.

There are no cameras. We could cut the wires from the beeper and get vehicles in/out.
We could break into the cars there. We could draw obscene pictures on the windshield...

Getting inside

Opening the door could have triggered an alarm. But it did not.
(and if it did, we could have run away)

So here we are in the garage. A few cars.

There are no cameras. We could cut the wires from the beeper and get vehicles in/out.
We could break into the cars there. We could draw obscene pictures on the windshield...

Getting inside

Opening the door could have triggered an alarm. But it did not.
(and if it did, we could have run away)

So here we are in the garage. A few cars.

There are no cameras. We could cut the wires from the beeper and get vehicles in/out.
We could break into the cars there. We could draw obscene pictures on the windshield...

And we can continue. The only way in is the lift.

Getting inside...

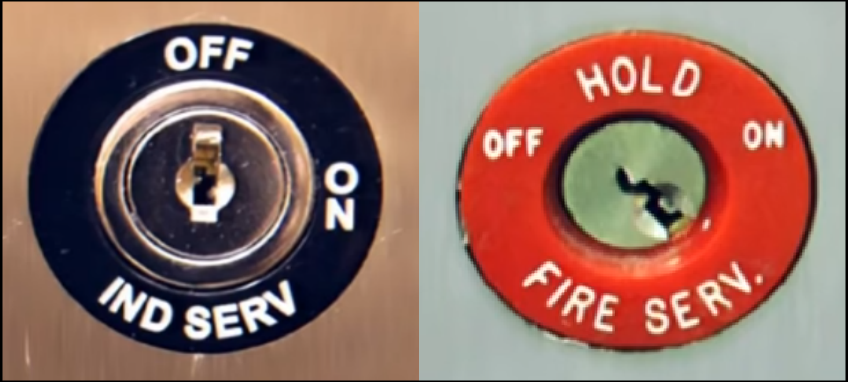
But the lift requires a badge...

Getting inside...

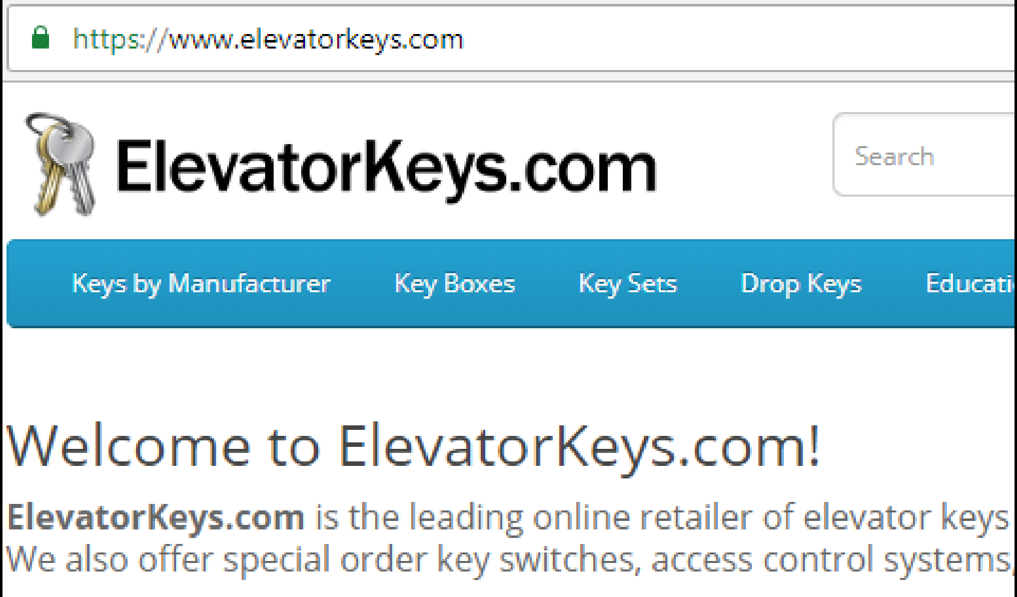
Did you notice the keyhole on the side?

Getting inside...

Did you notice the keyhole on the side?



Getting inside...



https://www.elevatorkeys.com

Welcome to ElevatorKeys.com!

ElevatorKeys.com is the leading online retailer of elevator keys
We also offer special order key switches, access control systems,

Getting inside

- We can get to any floor we want
- We set out sight to level 2

Getting inside

- We can get to any floor we want
- We set out sight to level 2
  - Guards certainly couldn't go all the way up there in time

Getting inside

- We can get to any floor we want
- We set out sight to level 2
  - Guards certainly couldn't go all the way up there in time
  - Most likely to have stairs down (and it's easier to run down if need be)

Getting inside

- We can get to any floor we want
- We set out sight to level 2
    - Guards certainly couldn't go all the way up there in time
    - Most likely to have stairs down (and it's easier to run down if need be)
    - Management typically prefers higher floors (compensation for something?)

Getting inside

- We can get to any floor we want
- We set out sight to level 2
  - Guards certainly couldn't go all the way up there in time
  - Most likely to have stairs down (and it's easier to run down if need be)
  - Management typically prefers higher floors (compensation for something?)
  - The elevator panel read "Management & IT, floor 2".

We're inside, now what?

2nd floor is essentially a corridor

- Several rooms on both sides, only some names on tags
- No camera surveillance in the corridor (so likely none in rooms either)
- All rooms are badge controlled. No keylocks, no easy unlock.
- One room had an extra padlock (certainly interesting).

We're inside, now what?

2nd floor is essentially a corridor

- Several rooms on both sides, only some names on tags
- No camera surveillance in the corridor (so likely none in rooms either)
- All rooms are badge controlled. No keylocks, no easy unlock.
- One room had an extra padlock (certainly interesting).

We estimate we have about 7 hours ahead of us.

We're inside, now what?

The padlocked room seems interesting, but let's keep it for later.

- We try getting into one of the rooms around, to test the under-door technique (video)

We're inside, now what?

The padlocked room seems interesting, but let's keep it for later.

- We try getting into one of the rooms around, to test the under-door technique (video)
- Once inside, we get a full fledged office space
  - Ethernet connection
  - Office computer
  - File cabinet...

We’re inside, now what?

The padlocked room seems interesting, but let’s keep it for later.

- We try getting into one of the rooms around, to test the under-door technique (video)
- Once inside, we get a full fledged office space
  - Ethernet connection
  - Office computer
  - File cabinet... with the keys still on...

We're inside, now what?

The padlocked room seems interesting, but let's keep it for later.

- We try getting into one of the rooms around, to test the under-door technique (video)
- Once inside, we get a full fledged office space
  - Ethernet connection
  - Office computer
  - File cabinet... with the keys still on...
  - Printer/Scanner
- We look through the file cabinet and take a few pictures that we e-mail ourselves
- Through the printer's log and resend functionality
- Plug a PC on the Ethernet port and `nmap` the internal network

We're inside, now what?

The padlocked room seems interesting, but let's keep it for later.

- We try getting into one of the rooms around, to test the under-door technique (video)
- Once inside, we get a full fledged office space
  - Ethernet connection
  - Office computer
  - File cabinet... with the keys still on...
  - Printer/Scanner
- We look through the file cabinet and take a few pictures that we e-mail ourselves
- Through the printer's log and resend functionality
- Plug a PC on the Ethernet port and `nmap` the internal network

Network is summarily segmented, a lot of redundancy, nothing obviously useable.
We are in the `mgmt` local network.

We're inside, now what?

- Just in case, power on the computer

We're inside, now what?

- Just in case, power on the computer actually it was just suspended

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords...

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up when we find a post-it under the keyboard (original)

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up when we find a post-it under the keyboard (original)
- Post-it password doesn't work.

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up when we find a post-it under the keyboard (original)
- Post-it password doesn't work.
- Paper bin contains, amongst other things, a crumbled post-it.

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up when we find a post-it under the keyboard (original)
- Post-it password doesn't work.
- Paper bin contains, amongst other things, a crumbled post-it. Password doesn't work either.

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up when we find a post-it under the keyboard (original)
- Post-it password doesn't work.
- Paper bin contains, amongst other things, a crumbled post-it. Password doesn't work either.
- However there is a similarity between the two and after some thinking I get the pattern.

We’re inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn’t have the tools
- Tried a few basic passwords... doesn’t work.
- We’re about to give up when we find a post-it under the keyboard (original)
- Post-it password doesn’t work.
- Paper bin contains, amongst other things, a crumbled post-it. Password doesn’t work either.
- However there is a similarity between the two and after some thinking I get the pattern.
- Good thing you can try as many passwords as you like on Windows.

We're inside, now what?

- Just in case, power on the computer actually it was just suspended
- We could have used all the advanced cold boot techniques, but didn't have the tools
- Tried a few basic passwords... doesn't work.
- We're about to give up when we find a post-it under the keyboard (original)
- Post-it password doesn't work.
- Paper bin contains, amongst other things, a crumbled post-it. Password doesn't work either.
- However there is a similarity between the two and after some thinking I get the pattern.
- Good thing you can try as many passwords as you like on Windows.
- We're in.

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)

We’re inside inside, now what what?

- Comparing username with our initial recon we realise this is the group’s CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.

We’re inside inside, now what what?

- Comparing username with our initial recon we realise this is the group’s CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.
- Many, many, many

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.
- Many, many, many many

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.
- Many, many, many many adult websites. Like a lot. Women. Men. Other things.

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.
- Many, many, many many adult websites. Like a lot. Women. Men. Other things.
- At this stage we could blackmail but that's not fun plus we haven't much time and other things to do.

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.
- Many, many, many many adult websites. Like a lot. Women. Men. Other things.
- At this stage we could blackmail but that's not fun plus we haven't much time and other things to do.
- Run mimikatz to get accounts info and a list of running and installed software (incl. antivir).

We're inside inside, now what what?

- Comparing username with our initial recon we realise this is the group's CSO computer (lel)
- Gmail, got it. LinkedIn, Wikipedia, Facebook... thank you dashlane.
- Go through recent documents and navigation history.
- Many, many, many many adult websites. Like a lot. Women. Men. Other things.
- At this stage we could blackmail but that's not fun plus we haven't much time and other things to do.
- Run mimikatz to get accounts info and a list of running and installed software (incl. antivir).
- Deactivate antivir, open an exception on the firewall and install Poison Ivy with keylogging on. Just in case.

We're inside inside, now what what?

Let's go back to the padlocked room.

- Similar door as all the rest, so we can probably open it the same way
- But extra layer of protection in the form of a Master padlock

We need a break.

At this point, we've been at it for 4 hours and it's time for a break.

Come back in 15 mins

Don't try this at home

Alcohol is dangerous and the leading cause of death for the 25–35.

The harmful use of alcohol can also result in harm to other people, such as family members, friends, co-workers and strangers. Moreover, the harmful use of alcohol results in a significant health, social and economic burden on society at large.

It is associated with mental and behavioural disorders, including dependence, major diseases such as liver cirrhosis, cancers and cardiovascular diseases, as well as injuries resulting from violence and road clashes and collisions.

Shimming (video)

We’re in in in. What do we do now now now ?

This is indeed an interesting room: the main network equipment room.

- Servers on racks (that we could just unplug and run away with)
- Alims (that we could just unplug and run away with)
- Routers (that we could... you get the idea)

We could in principle try to get inside the servers, run an Encase or a Volatility, to known about the info they are processing.

But we haven’t much time, and it’s unlikely to be high-value (and we can come back later anyway).

The Cisco in the room

One of the Cisco routers responded to a local nmap with an old version

The Cisco in the room

One of the Cisco routers responded to a local nmap with an old version
⇒ Google search confirms known vulnerabilities

The Cisco in the room

One of the Cisco routers responded to a local nmap with an old version

⇒ Google search confirms known vulnerabilities

⇒ Download and run appropriate exploit

The Cisco in the room

One of the Cisco routers responded to a local nmap with an old version
⇒ Google search confirms known vulnerabilities
⇒ Download and run appropriate exploit

(Minimal adjustments were needed to) get `root` access on that router.

Change configuration, set-up a connect-back tunnel to one of our IPs in Brazil.

Gotta catch'em all

At this point we are fairly confident that we have the bulk of the IT network under control, with RAT, keylogging, and untethered remote network acess.

We have physical access, and in all likelihood we can always come back.

We can explore the other parts of this building, which are certainly less protected.

Gotta catch'em all

At this point we are fairly confident that we have the bulk of the IT network under control, with RAT, keylogging, and untethered remote network acess.

We have physical access, and in all likelihood we can always come back.

We can explore the other parts of this building, which are certainly less protected.

Except...

Ground control to Major Tom

Ground floor is covered in cameras + armed guards.

Ground control to Major Tom

Ground floor is covered in cameras + armed guards.

Are the camera network-connected?

Ground control to Major Tom

Ground floor is covered in cameras + armed guards.

Are the camera network-connected? Yes they are! (thank you nmap)

Google-fu “D-Link DCS-7410” (shodan: dcs-lig-httpd)

Your Google-fu is strong

“It will execute any command you want” [CVE-2013-1599]

Craig Heffner, BlackHat USA 2013

Your Google-fu is strong

"It will execute any command you want" [CVE-2013-1599]

Craig Heffner, BlackHat USA 2013

```
http://192.168.1.101/cgi-bin/rtpd.cgi?reboot
```

Your Google-fu is strong

"It will execute any command you want" [CVE-2013-1599]
Craig Heffner, BlackHat USA 2013

```
http://192.168.1.101/cgi-bin/rtpd.cgi?reboot
```

```
http://192.168.1.101/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb
```

Your Google-fu is strong

"It will execute any command you want" [CVE-2013-1599]

Craig Heffner, BlackHat USA 2013

```
http://192.168.1.101/cgi-bin/rtpd.cgi?reboot
```

```
http://192.168.1.101/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb
```

⇒ Get the admin password in your browser

Your Google-fu is strong

"It will execute any command you want" [CVE-2013-1599]

Craig Heffner, BlackHat USA 2013

`http://192.168.1.101/cgi-bin/rtpd.cgi?reboot`

`http://192.168.1.101/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb`

⇒ Get the admin password in your browser

⇒ Get the video feed live in your browser

Your Google-fu is strong

“It will execute any command you want” [CVE-2013-1599]
Craig Heffner, BlackHat USA 2013

`http://192.168.1.101/cgi-bin/rtpd.cgi?reboot`

`http://192.168.1.101/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb`

⇒ Get the admin password in your browser
⇒ Get the video feed live in your browser

Oh and it’s RTP is UDP, so I can inject from anywhere in the network.

Peekaboo I see you

So now we know where the guards are (confirming $2 + 1$) and we can see what they see.

Peekaboo I see you

So now we know where the guards are (confirming 2 + 1) and we can see what they see.

We can also, in principle, inject a video stream or at least break it.

Peekaboo I see you

So now we know where the guards are (confirming 2 + 1) and we can see what they see.

We can also, in principle, inject a video stream or at least break it.

Also the guys are not leaving. If we had time and motivation, we'd go Captain Disillusion style

Ok back on track

At this point we can't go further without taking too much risks.

We already have quite a loot and the next step is figuring out how valuable this is.

Ok back on track

At this point we can't go further without taking too much risks.

We already have quite a loot and the next step is figuring out how valuable this is.

This is of course an educated guesstimate, we're not selling any of it.

Profit!!!

A rough estimation yields that

Profit!!!

A rough estimation yields that basically everything we got is more valuable than what was stolen.

Profit!!!

A rough estimation yields that basically everything we got is more valuable than what was stolen.

- Maybe the hackers were bad?

Profit!!!

A rough estimation yields that basically everything we got is more valuable than what was stolen.

- Maybe the hackers were bad?
- Maybe we don't know the whole story?

Profit!!!

A rough estimation yields that basically everything we got is more valuable than what was stolen.

- Maybe the hackers were bad?
- Maybe we don't know the whole story?
- Maybe it's not hackers to begin with.

Profit!!!

A rough estimation yields that basically everything we got is more valuable than what was stolen.

- Maybe the hackers were bad?
- Maybe we don't know the whole story?
- Maybe it's not hackers to begin with.

How likely is it that employees smuggled the info out?

Testing the theory

We know that employees click on their e-mail attachments (boo) but could they be manipulated into leaking company data?

- Set up a test with the company (we don't say which employee we'll target nor about what)

Testing the theory

We know that employees click on their e-mail attachments (boo) but could they be manipulated into leaking company data?

- Set up a test with the company (we don’t say which employee we’ll target nor about what)
- But the company gets handsy

Testing the theory

We know that employees click on their e-mail attachments (boo) but could they be manipulated into leaking company data?

- Set up a test with the company (we don't say which employee we'll target nor about what)
- But the company gets handsy ("do not click on any attachment today or you're fired")

Testing the theory

We know that employees click on their e-mail attachments (boo) but could they be manipulated into leaking company data?

- Set up a test with the company (we don't say which employee we'll target nor about what)
- But the company gets handsy ("do not click on any attachment today or you're fired")
- Someone sends the data anyway, and there's no access control besides badges

No protection against internal threats and no access logs + Successful experiment

⇒ Internal leak credible

We could have gone further

- Nothing prevented us from altering the hardware (or setting up cameras, microphones...). Hell we could have set the whole place on fire (no fire alarms).
- We could have gotten inside the network merely through e-mail manipulation, and perhaps wouldn't even need software
- The guards and cameras are guarding an empty room where nothing of value is stored
- The lawyer or contractor could simply be the author of the leak to begin with

Wrapping up

- Complete report on the many potential ways we could have gotten the info
- Complete report on the actual way we got some info, with proof
- Waited 1 week after the intrusion, to give them a chance to detect something (nope)
- Suggestions on improvements that would help make intrusion harder
- In particular: proper procedures and training, proper access control and logs, and rational use of resources
- Took about 2 years to implement the main suggested points

Wrapping up

Information security is not always only about computers

- Think globally and not just locally
- Play with technology, don't be mere users
- Have fun with the projects

And thank you so much for everything!

`remi.geraud@ens.fr`