



Turning an Intrusion attempt Into a Waterloo disaster

Renaud Bidou
S³ EMEA



Smart Network. Smart Business.



Introduction

June 1815

Smart Network. Smart Business.

- Napoleon
 - **North Army** : 125.000
- Coalition, based in Belgium
 - **Prussians** : 120.000
 - **English** : 100.000
 - **Expected reinforcement**
 - Russians
 - Austrians
 - **Arrival by end of summer**

1. Attack before Russians & Austrians join
 - **June 14th** : North Army Crosses the border at Charleroi
2. Split English and Prussian armies
 - **June 15th – 17th** : 4-Bras Battle
3. Crush Prussian army
 - **June 17th** : Ligny Battle
4. Finish the brits !
 - **June 18th** : Waterloo Battle

Smart Network. Smart Business.

Brussels

Wellington

Blucher

Ney

Napoleon

Grouchy

Brussels

Wellington

Blucher

Ney

Ney

Napoleon

Grouchy

- 1 Take and hold 4-Bras position to prevent Brit reinforcement on Prussian Army

Brussels

Wellington

Ney

Napoleon

Grouchy

Blucher

- 2 Brake Prussian Army in two and crush the survivors with Drouet d'Erlon corp from Ney reserve

Brussels

Wellington

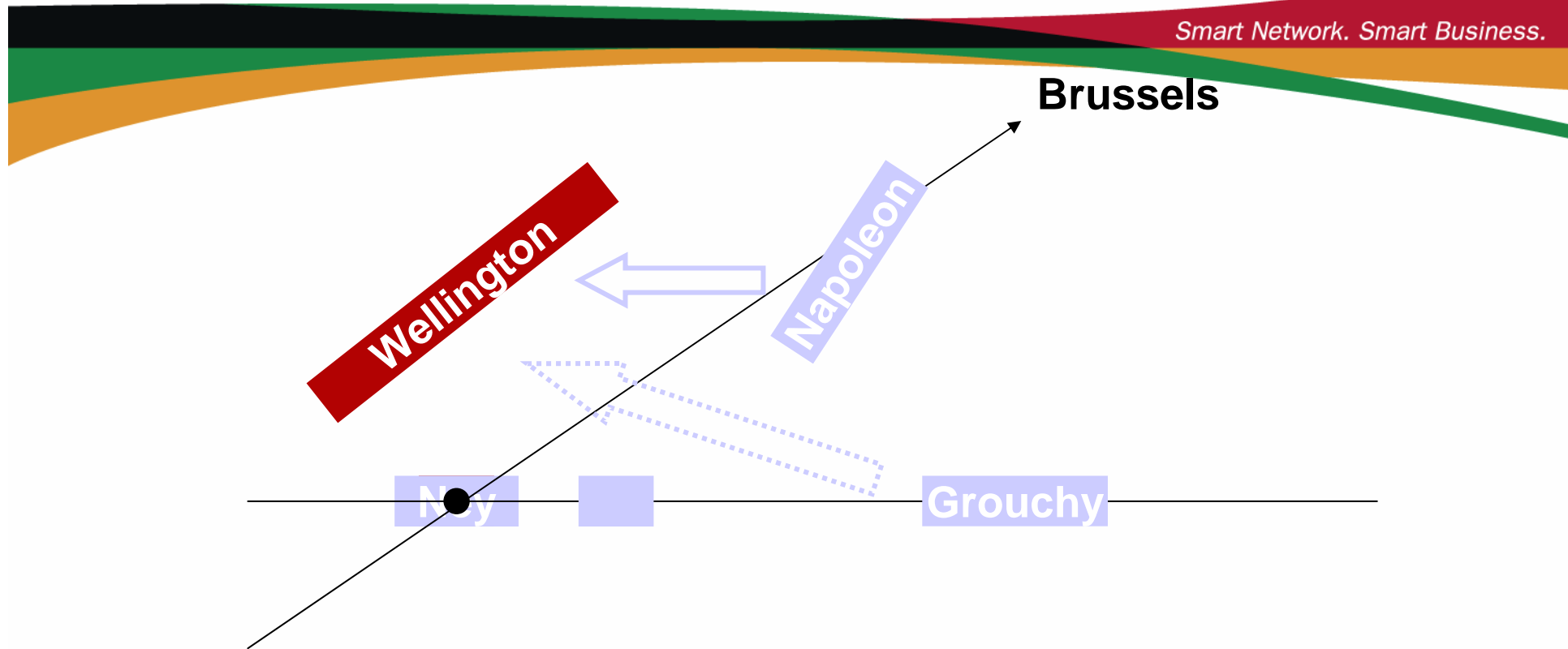
Napoleon

Noy

Grouchy

Blucher

3 Reorganize (during tea time 😊)



4 Terminate Brits

- Everything worked OK !
 - **4-Bras battle** : Ney army eventually took 4-Bras
BUT : Took too much time and Drouet d'Erlon couldn't support Napoleon the day after
 - **Ligny battle** : Napoleon beat Prussians
BUT : Without support from Ney's reserve he didn't manage to exterminate Blucher's army
 - **Waterloo battle** : Could have been won
BUT : Grouchy got lost and Blucher arrived in the back of French army

Know your enemy

Smart Network. Smart Business.



- Alone
 - against a full set of security tools / devices
 - against numerous and organized defenders
- Must go fast before
 - patches / updates are applied
 - detection ⇒ security reinforcement
- Its main goal is not known from defenders
 - and should remain secret as long as possible

- Take and hold position into the internal network
- ↔ 4-Bras Battle, June 15th – 17th
 - Easy
 - May take time but will be done anyway
 - Some intrusion vectors
 - direct : exploit, 0-day, L7 weakness
 - 2-tiers : via PDA or mobile phone compromise
 - the 5th column : WiFi / Physical access
 - human : social engineering, internal complicity

- Secure strategic position
- ↔ Secure 4-Bras, June 17th
 - Compromise the local environment
 - logging capabilities
 - environment variables
 - binaries and libraries
 - LKM insertion
 - system calls addresses (through system.map or /dev/kmem)
 - Prepare further accesses
 - backdoors, poor-man access
 - secure with encryption, authentication and portknocking capabilities

- Prepare reserve for next step
- ↔ Drouet d'Erlon division, June 17th
 - download additional tools from compromised hosts
 - rootkits to remain stealth on the local system
 - covert channels to avoid egress traffic detection

- Eliminate security support
- ↔ Ligny battle, June 17th
 - identify security devices
 - log management : destination can be determined from compromised host configuration
 - filtering : classical firewalking mechanism
 - intrusion detection / prevention : easy ☺ ... headers, response time, broadcast / multicast sensitivity etc.
 - evade or terminate
 - elimination : log flooding, DoS
 - confusion & substitution : tunneling, encryption, encoding
 - fragmentation : application level is the worst case
 - insertion : L3 (RST), L4 (checksum, seq numbers), L7 (\0)

- Prepare the final assault
- ↔ Napoleon, June 17th, evening
 - Get closer from the target
 - identify the path (usually long)
 - compromise hosts on the way
 - classical procedure : identify, qualify, attack, own
 - Identify the target
 - from multiple sources on the internal network

- Close the deal
- ↔ Waterloo, June 18th
 - should be straight forward now
 - as long as everything worked as expected ...



Defeating Napoleon

Smart Network. Smart Business.

1. You can loose a battle, sometimes you have to
2. Never underestimate your enemy
3. Time is on your side
4. Murphy's law
5. There is no rule at war

- A key point for victory
 - Protection and reaction capacities vary
 - Know where you are strong
 - And know your weaknesses
- Don't let initiative to the enemy
 - Mess his plans
 - Leave him in defensive mode
 - Slow its advances

- You cannot win this battle ...
 - One day somebody will get into your network
 - You don't know when, where and how
 - **But it will happen**
- ... But you can
 - Reduce the number of occurrences
 - Blocking common attacks : recent exploits, generic shellcodes, worms, typical misbehavior
 - Slow down intrusion process : anti-scanning, honeypots
 - Get ready
 - Suspicion : Anomaly detection and heuristic analysis
 - Early alerting : Scenario correlation

- Apply basic hygiene rules
 - Patch, even local privilege escalation vulnerabilities
 - Check and strengthen permissions (there are possibilities to define other accounts but *root* 😊)
 - *chroot* what you can
 - Setup appropriate logging
 - Perform integrity check
 - Don't store passwords in clear (even in memory)
- Effect
 - It will limit the impact of the first strike
 - And lower the power of the next attack

➤ Prevent reinforcement

- Secure egress traffic path
 - Firewall filtering must be applied for outgoing traffic
 - What about personal firewalls ?
 - Enforce the use of proxies
 - Ask for authentication and go for OTP
- Investigate and block tunnels
 - Tools signatures
 - Protocol anomaly detection
 - Layer 3 to 7 stateful analysis

- Another battle to be lost
 - Security tools can be bypassed
 - Techniques are known
 - Most easy and efficient are log flooding and DoS
 - Special award to RPC fragmentation
 - *Security is a process, not a product*
- Get ready for counter-strike
 - Go fast, time is critical
 - Identify tools misbehavior
 - Investigate and fix as fast as possible
 - It may be the key to victory
 - Your personal Blucher army that will hit the enemy in the back

- Limit the propagation of the intrusion
 - Define and enforce security zones
 - Each zone must be protected from others
 - Control traffic
 - Monitor and secure internetworking devices
 - Use honeypots to create fake networks
 - Patch me if you can
 - Don't leave systems unpatched
 - Or at least protect them... as much as possible
 - Don't trust anybody
- ⇒ It will make intruder progression harder

- How can we win the war
 - Reduce intruder capacity to attack
 - Limited access to the target
 - Insufficient resources to launch an effective attack
 - Hit in the back
 - Lack of time, took too long to get there
 - Enough time to find vulnerabilities and backdoors
 - **Terminate the rogue access**

- The best case : 99,999% of security
 - First-strike security : 90% blocked
 - Local security on the target : 90% blocked
 - Egress traffic filtering : 90% blocked
 - Internal security : 90% blocked
 - Quick response : 90% blocked
- The reality
 - First-strike security : easy
 - Local security : don't even dream about it
 - Tunnel investigation : easy
 - Internal security : always partial
 - Quick response : highly variable



Conclusion

Smart Network. Smart Business.

- Waterloo disaster is the consequence :
 - Of many tactical mistakes
 - Hackers does mistakes
 - We can have them make mistakes
 - Of bad timing
 - We can slow down the intrusion process
 - Investigation and response can be done in time
 - Of Murphy's law
- ⇒ **Of in depth protection**
 - Not so called at the time...