SYSDREAM
IT Security Services

Grenoble INP
ENSIMAG

Set up of an Attack & Defense infrastructure

Jérémy Brun-Nouvion

Presentation

- Studied Computer Science at ENSEEIHT
- IT Security enthusiast -> 3rd year in M2 SCCI at ENSIMAG
- Internship in Sysdream, IT Security company (Paris)

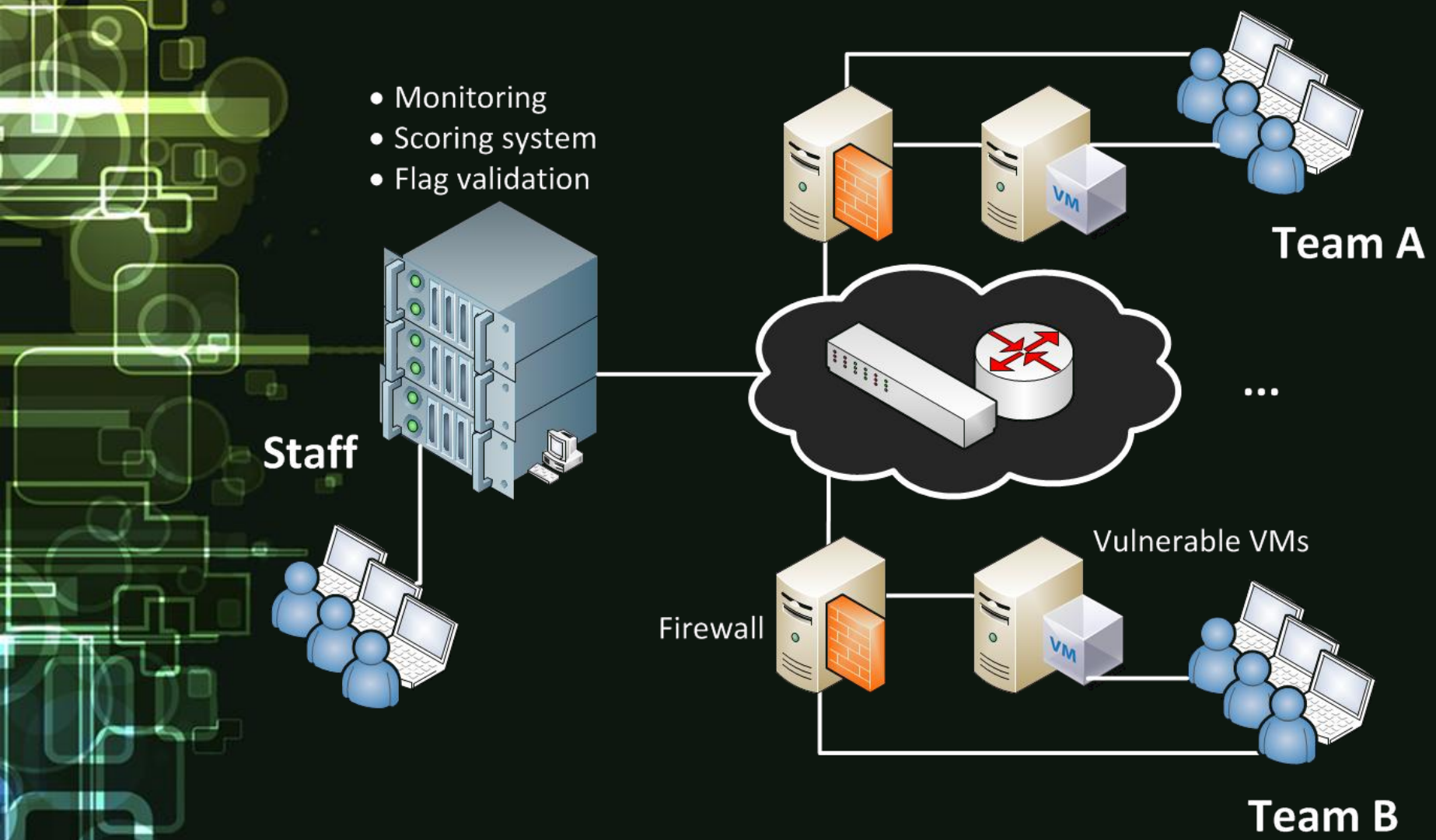
Internship topic

- Set up the infrastructure for the “Capture the Flag” of “La Nuit du Hack”

- Develop Security challenges (Windows)

Learn and experiment hacking techniques

Overview of the infrastructure



Windows Security Challenges

- Remote Buffer Overflow
  - > bypass some mitigation mechanisms
- Website vulnerable to MS SQL injection
  - > bypass filter + exploitation via SMB
- Vulnerable driver
  - > local privilege escalation

Exploitation using MOF files

- Inspired by exploitation of MS10-061 in Windows Printer Spooler by Stuxnet
- WMI is based on CIM classes, described in MOF files

DEMO

MOF File in action !

Platform: Windows 2003 Server SP2

Conclusion

- Good experience:
  - Team working
  - Ambitious and technical project
  - Windows security skills ++

- "Know your enemy": thinking as an attacker was essential to anticipate the possible exploitation methods

Thanks for your attention

Questions ?


Jeremy.brun@etu.enseeiht.fr


http://poppopret.blogspot.com


@Xst3nZ