WESSI 2014

ARCHITRACE
L'apprentissage de la sécurité du SI par les « logs »

Véronique Legrand (insa-lyon)
Omar Gaouar (insa-lyon)
Pierre Parrend (ecam-strasbourg)

TC

Sommaire

1. Une nouvelle approche pour apprendre la sécurité ?
2. Le problème de l'apprentissage des systèmes complexes ?
3. Que nous apprennent les traces ?
4. Principe du projet ARCHITRACE.
5. Bilan et perspectives.

Contexte et objectifs

- ✓ **Nouveaux modèles d'enseignement :**
  - Des cartographies des connaissances télécoms et informatiques,
  - Un modèle pour apprendre le fonctionnement de systèmes complexes,
  - une méthode pour concevoir des scenarii et obtenir l'adhésion des enseignants.
- ✓ **Comprendre les grands systèmes complexes**
  - Cartographies des infrastructures pour visualiser les architectures globales,
  - Cartographies logicielles pour identifier liens clients-serveurs,
  - Cartographies des protocoles pour identifier les dépendances.
- ✓ **Fédérer le savoir d'équipes pédagogiques transverses**
  - Requiert la coopération des enseignants du monde du réseau, des services et des applications logicielles,
  - Divers briques de l'enseignement informatique,
  - Scenarii de portée globale : petites et grandes entreprises.
- ✓ **Maintien de la qualité de la formation d'ingénieur**
  - Résolution de problème inverse : l'atout des futurs ingénieurs

Public concerné

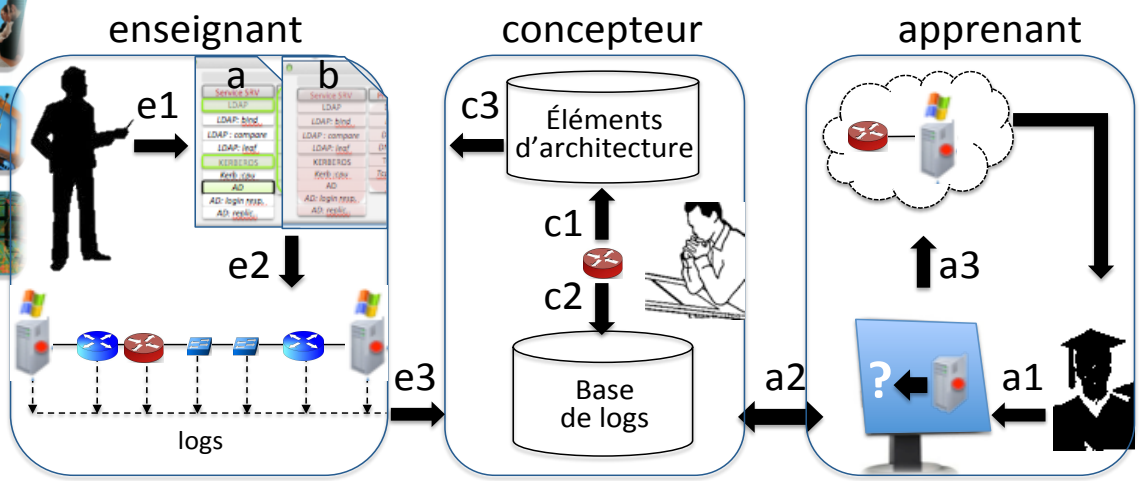
- ✓ **Entités :**
  - Formation d'ingénieur,
  - Mastère spécialisé,
  - Filière Apprentissage,
  - Formation continue.

- ✓ **Public**
  - Etudiants et enseignants de toute matière : informatique, réseaux et télécoms,
  - TP, TD, auto-formation.
- ✓ **Contenu**
  - Enseignement des systèmes complexes : architectures mobiles et de type « cloud »,
  - Impact des protocoles de sécurité.

Entrainer différentes formes de raisonnements

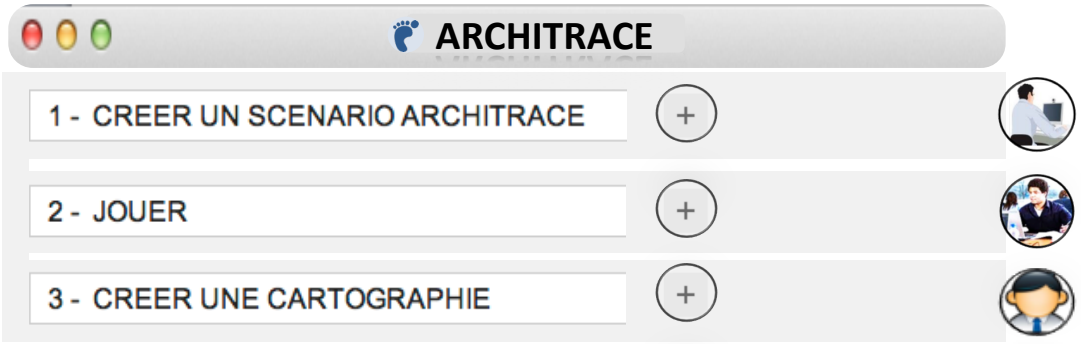
	Ce que je connais :		*Ce que j'apprends :*
Déduction	Règle 1 Règle 2	→	Comportement (trace)
Induction	Comportement (trace) Règle 1	→	Règle 2
Abduction	Comportement 1 (trace 1) Comportement 2 (trace 2)	→	Règle 1

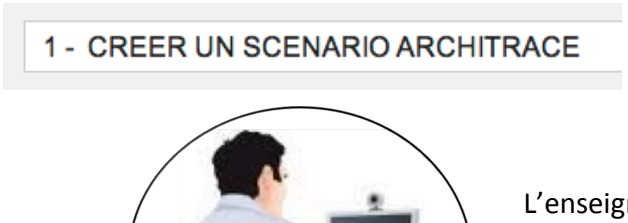
Principe général du projet



Le projet

✓ **Trois fonctions principales pour 3 acteurs :**





L'enseignant

4 étapes

1 –Problème (posé par l'enseignant)

ARCHITRACE - Enseignant

Entreprise Licoste

« *Diagnostic du temps de réponse entre la station de travail située en Roumanie et le site de l'application Active Directory à Paris due à un dns poisonning* »

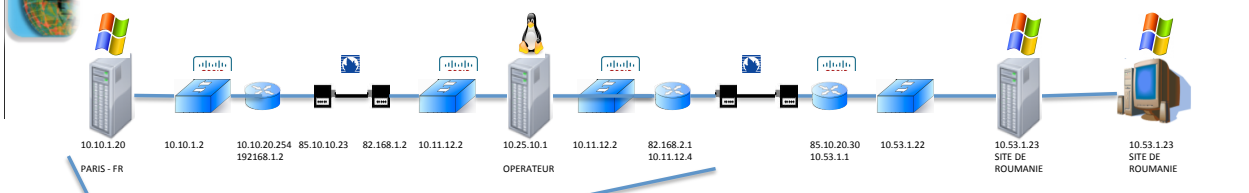
SERVEUR – END SYSTEM				INTERMEDIATE SYSTEM			CLIENT – END SYSTEM			
Service SRV	Protocole SRV	Matériel SRV	Data SRV	Level 3	Level 2	Level 1	Service CLT	Protocole CLT	Matériel CLT	Data CLT

1-L'enseignant choisit le menu pour élaborer le scenario
2-L'enseignant rédige le descriptif
3-L'enseignant choisit l'architecture globale

2 – Choix de l'architecture

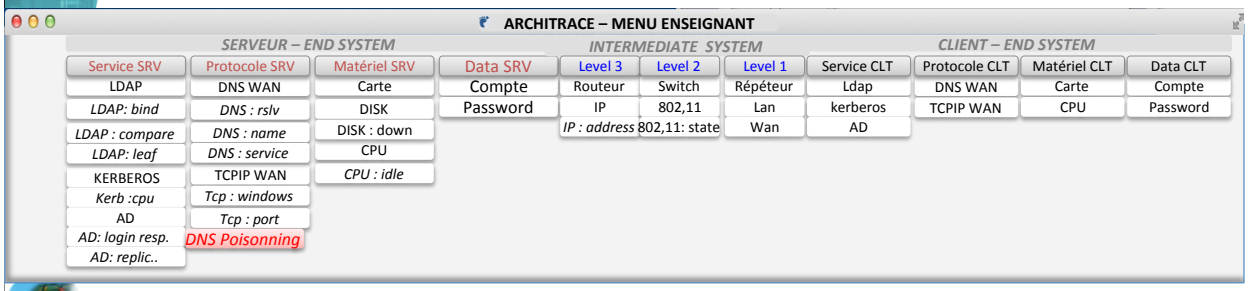
ARCHITRACE – MENU ENSEIGNANT

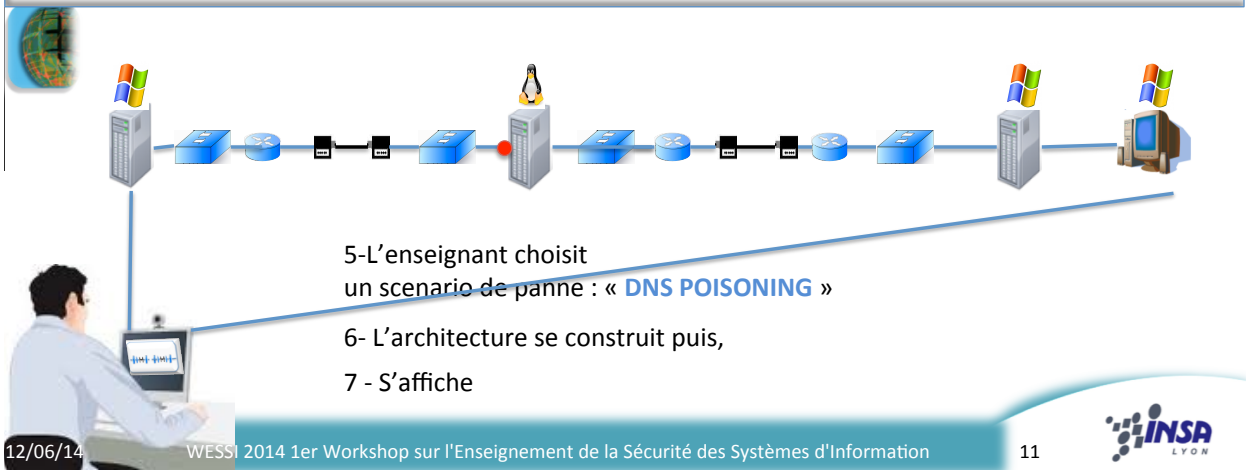
SERVEUR – END SYSTEM				INTERMEDIATE SYSTEM			CLIENT – END SYSTEM			
Service SRV	Protocole SRV	Matériel SRV	Data SRV	Level 3	Level 2	Level 1	Service CLT	Protocole CLT	Matériel CLT	Data CLT
LDAP	DNS WAN	Carte	Compte	Routeur	Switch	Répéteur	Ldap	DNS WAN	Carte	Compte
LDAP: bind	*DNS : rslv*	DISK	Password	IP	802,11	Lan	kerberos	TCPIP WAN	CPU	Password
LDAP : compare	*DNS : name*	DISK : down		*IP : address*	802,11: state	Wan	AD			
LDAP: leaf	*DNS : service*	CPU								
KERBEROS	TCPIP WAN	*CPU : idle*								
Kerb :cpu	*Tcp : windows*									
AD	*Tcp : port*									
AD: login resp.										
AD: replic..										



4-L'enseignant choisit l'architecture détaillée du scenario : « **active directory** »

3 – Création de l'incident



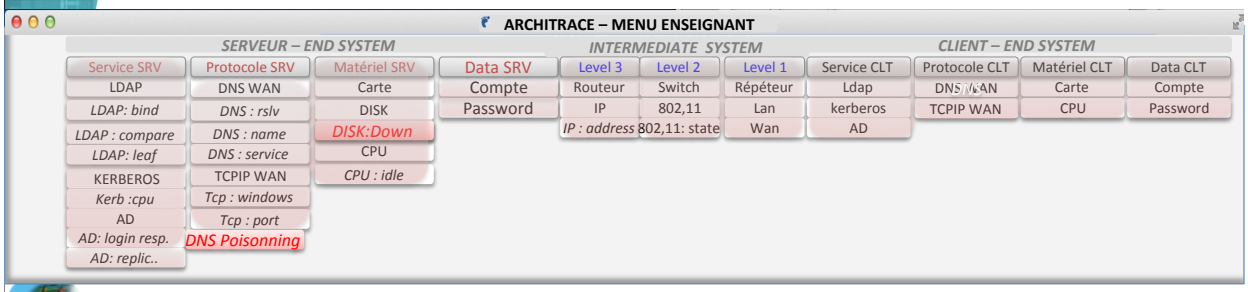


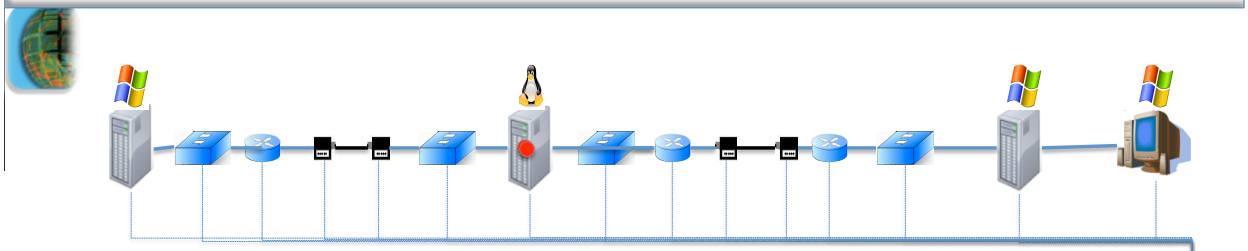
5-L'enseignant choisit
un scenario de panne : « **DNS POISONING** »

6- L'architecture se construit puis,

7 - S'affiche

4 – Génération des « logs » de l'incident





8-L'enseignant déclenche les « logs » du scenario

9-Le système affecte un poids à chaque « logs » qui constituera le **point gagné** par l'étudiant

2 - JOUER

L'apprenant

1 – Choix du jeu
2 – Progression de l'apprenant

Entreprise Licoste

« *Diagnostic du temps de réponse entre la station de travail située en Roumanie et le site de l'application Active Directory à Paris* »

4	AD- ROU	Performance	Test Server AD-ROU : Ping Remote depuis station ROUMANIE	Temps de réponse server	s	2 s	3 s	1s
7	AD-WAN	Performance	**Microsoft Windows DNS Server Cache Poisoning Vulnerability**	Temps de réponse server	s	2 s	3 s	>16s

1-L'étudiant choisit un scenario d'apprentissage : « active directory »

2-L'étudiant lit la question, le poste de travail et le serveur apparaissent

3-Le premier indice apparaît sous forme de « log »

4-L'étudiant propose un serveur active Directory AD-ROU sur le site de Roumanie….

5-Il a raison et le système lui attribut 1 point

6-L'étudiant clique pour obtenir un nouvel indice

7-L'étudiant propose un serveur active Directory AD-WAN sur le site de Roumanie….

8-Le système lui attribut 1 point

9 - L'étudiant clique pour obtenir un nouvel indice

10-L 'étudiant propose l'origine du probleme : le DNS poisoning

x-L 'étudiant propose la chaine de liaison complète pour augmenter son nombre de points à l'aide des logs

3 - CREER UNE CARTOGRAPHIE

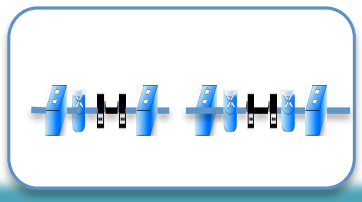
Processus d'acquisition des connaissances supervisé par l'Admin

SERVEUR – END SYSTEM				INTERMEDIATE SYSTEM			CLIENT – END SYSTEM			
Service SRV	Protocole SRV	Matériel SRV	Data SRV	Level 3	Level 2	Level 1	Service CLT	Protocole CLT	Matériel CLT	Data CLT
LDAP	DNS WAN	Carte	Compte	Routeur	Switch	Répéteur	Ldap	DNS WAN	Carte	Compte
LDAP: bind	*DNS : rslv*	DISK	Password	IP	802,11	Lan	kerberos	TCPIP WAN	CPU	Password
LDAP : compare	*DNS : name*	DISK : down		*IP : address*	802,11: state	Wan	AD			
LDAP: leaf	*DNS : service*	CPU								
KERBEROS	TCPIP WAN	*CPU : idle*								
Kerb :cpu	*Tcp : windows*									
AD	*Tcp : port*									
AD: login resp.										
AD: replic..										

Cartographie

logs

acquisition



Architecture physique

Enseignement projeté

✓ **Un véritable outil d'aide aux TP/TD/ complexes pour :**

- Département :TC/IF/IMSSI
- Cycle : 3/4/5
- Matières : orientées réseaux et protocoles

ANNEE	CYCLE	MATIERE	Durée	nb Group	TC (h)	IF (h)	IMSSI (h)	TC (h)
2014-2015	1	ARCHISI	4	1			4	4
	3	TEL	4	3	12			24
		RE	4	3		12		
	5	ARS	4	3	12			24
	5	OT	4	3		12		
							année 1 Architrace	52

ANNEE	CYCLE	MATIERE	Durée	nb Group	TC (h)	IF (h)	IMSSI (h)	TC (h)
2015-2016	1	ARCHISI	4	1			4	4
	3	TEL	4	3	12			
		RE	4	3		12		
	3	NET	4	3	12			36
	4	MACR	4	2	8			
	4	RE	4	3		12		20
	5	ARS	4	2	8			
		CDVI	4	2	8			
		OT	4	3		12		
		ARC	4	2	8			36
							année 2 Architrace	96

adhésion espérée minimale

Bilan : Architrace

- Un pas vers l'apprentissage de la vison globale d'architectures complexes d'aujourd'hui et de demain,
- En école d'ingénieur,
- Une aide pour l'enseignement de ce savoir,
- Des moyens adaptés et une « roadmap » par étape pour atteindre l'objectif.

Perspectives

- Apprendre à comprendre les systèmes complexes dans leur globalité
- Développer les mécanismes d'apprentissage par reverse engineering
- Aider l'enseignant à la conception d'enseignements scénarisés : MOOC
- Aider à comprendre les mécanismes de sécurité

Merci !

Questions