Ci-joint la liste des projets pour la validation de SR2I203.
Année scolaire 2017-2018
Ahmed Serhrouchni

Contact: ahmed@enst.fr

Ces projets peuvent être réalisés en binôme. A rendre au plutard le 07/02.
Je vous propose de me transmettre votre choix dès aujourd'hui (Lundi 27/11) par messagerie en choisissant 3 projets par ordre de priorité (votre premier choix sera attribué) . Utiliser svp comme objet dans votre message: SR2I203-Projet.
Trois rendus intermédiaires sont programmés pour le 19/12 (feuille de route et une première biblio), 10/01 (un premier état de l'art ou avancement avec une biblio bien établie), 23/01 (des premiers résultats avec des perspectives claires et établies).

Cette liste de projets n'est pas exhaustive, si vous avez un projet spécifique, vous pouvez le proposer.

1) Etude et mise en œuvre de la dernière attaque sur WPA2 (Krack).
2) Etude et mise en œuvre de l'attaque Wannacry.
3) Cartographie des services et réseaux de l'école.
4) Ecrire des scripts en Scapy pour le test de vulnérabilités (Audit) des applications Web.
5) Ecrire des scripts en Scapy (+nmap) pour identifier l'attaque shellshok.
6) Développement de script en Scapy en combinaison avec nmap pour le test de vulnérabilités.
7) Mise en œuvre à l'aide de Metasploit de l'attaque heartbleed sur le protocole TLS.
8) Mise en œuvre des attaques sur les applications WEB par Metasploit.
9) Etude et analyse des méthodes d'audit de vulnérabilités.
10) Aireplay application pour injecter des trames d'attaques sur le 802.11 (WIFI). Etudier, analyser et mettre en œuvre cette commande sous toutes ses formes.
11) Mise en œuvre d'attaques de types buffer overflow et mise en œuvre de contremesures.
12) Etude, analyse et mise en œuvre des attaques sur les cookies.
13) Etude et mise œuvre des attaques sur les documents PDF.
14) Etude et mise œuvre de l'outil BREACH (*Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext*) et SSLstrip.
15) Mise en œuvre de Burp Suite (ou Webscarab) pour des attaques notamment par fuzzing.
16) Etude et mise en œuvre d'Openvas pour la détection de vulnérabilités.
17) Etude et mise en œuvre de Nessus pour la détection de vulnérabilités.
18) Etude et mise en œuvre d'Ettercap, montage d'attaques autres qu'ARPspoofing.
19) Etude des outils de montage d'attaques de type SynFlooding.
20) Etude et mise en œuvre des attaques sur les mots de passe.
21) Mise en œuvre d'outils d'analyse de forensics sur des plateformes Windows Microsoft.
22) Mise en œuvre d'outils d'analyse de forensics sur des plateformes Linux.
23) Etude et analyse de la base de registre de Microsoft Windows et attaques potentielles.
24) Mise en œuvre d'attaques sur des sites de type "hackMe", "RootMe", etc.
25) Etude (attaque sur Dyn) et mise en œuvre des attaques sur le protocole DNS, étude du domaine flux et fast flux méthodes usuelles en combinaison avec les bootnets. http://www.networkworld.com/article/2886283/security0/top-10-dns-attacks-likely-to-infiltrate-your-network.html#slide1

26) Etude des attaques sur Bitcoin et la Blockchain.
27) Etude et mise en œuvre des attaques sur le CMS Wordpress.
28) Etude, analyse et mise en œuvre (état de l'art des outils) des attaques de types DDOS.
29) Etude et analyse des méthodes de PortScan (http://cseweb.ucsd.edu/~clbailey/PortScans.pdf).
30) Etude du langage d'écriture des règles de détection d'intrusion de ModSecurity. Validation par l'écriture d'une règle de défense et de sa mise en œuvre.
31) Etude, analyse et mise en œuvre (de Zeus ou Androrat) des Botnets (Ramnit botnet).
32) Etude et mise en œuvre des outils de type RAT (Remote Access Trojans) (*Sakula, Agent.BTZ/ComRat, KjW0rm, AlienSpy (OSX), Havex (ICS), Dark Comet, Heseber BOT, etc.).*
33) Etude et analyse des backdoors sur Android: Banker, SMSBot, MulDrop,Dridex, ...), http://sensorstechforum.com/types-of-trojan-attacks-2015-network-browser-exploits-and-security-essentials/ http://sensorstechforum.com/types-of-trojan-attacks-2015-network-browser-exploits-and-security-essentials/.
34) Etude et analyse des 5 grands attaques de grande envergure des ces 5 dernières années au plus. Cette analyse se fera sous l'angle des aspects techniques et de l'exploitation des vulnérabilités sous jacentes.
35) Etude, analyse des "faiblesses" des serveurs SMTP comme relais pour le Spam. Mise en œuvre de ces faiblesses pour spammer.
36) Etude et mise en œuvre des attaques sur le DNS.
37) Etude, analyse et mise en œuvre des attaques sur les Switch.
38) Etude, analyse et mise en œuvre des attaques sur les Vlan.