APPENDIX ORIGINELE PENPI OPGAVE

Gebruik de raspberry pi om 1 of meerdere security-related zaken te automatiseren. Het ultieme doel (maar niet makkelijker haalbaar) zou een raspberry pi kunnen zijn die je eender waar kan plaatsen aan een (bedraad/draadloos) netwerk waarop deze automatisch een hele hoop security tests (penetration tests, identification, etc) uitvoert. Vervolgens kunnen er verschillende zaken gebeuren met de vergaarde data: de rpi mailt deze, de gebruiker logt in via ssh op de rpi, etc.

Zorg ervoor dat je rpi 1 of meerdere van volgende zaken kan:

- Automatische WEP-cracking 2:
    - De rpi zal automatisch alle, met WEP-beveiligde, draadloze netwerken detecteren en vervolgens trachten de WEP-sleutel te achterhalen. Telkens een WEP-key wordt gevonden zal de RPI een mail sturen met daarin het SSID en de WEP-key. Je werkt voort op de projecten van vorig jaar, gebruikmakend van wifite. De basis functionaliteit is er reeds, de volgende fase zou WPA hacking kunnen zijn of
- Automatische netwerk-analyse
    - De rpi zal automatisch het netwerk afscannen waarmee de rpi verbonden is (maw, vereiste is dat de rpi een geldig IP-adres van het netwerk heeft verkregen). Zoveel mogelijk scans zullen uitgevoerd worden (OS fingerpinting, portscans, etc) om een zo compleet mogelijk beeld te verkrijgen van het netwerk. Elke [x] minuten wordt dit rapport gemaild, aangevuld met extra vergaarde informatie.
- Automatische netwerkdata-analyse
    - Ook hier is vereist dat de rpi een geldig IP-adres heeft. De rpi zal alle netwerkdata capteren (hang rpi aan hub!) en een rapport genereren met daarin een netwerkanalyser (naar keuze; denk bv aan top 10 IP-adressen, meest voorkomende protocols, gesnifde paswoorden/usernames, etc) dat elk [x] minuten wordt gemaild.
- Automatische ????
    - Stel zelf een automatisatie voor (ideeën/pistes: keycrackers, social engineering met metasploit, sql injection, etc).