

Privacy en Beveiliging

1 Format

1. vragenronde over problemen / support en uitleg assignments
2. extra exercises bespreken / maken
3. discussie over een recent nieuwsartikel / podcast
4. security demo

2 Schedule tutorial

1. Week 1: assignment 1 + Write an essay, network structure + sniffing (wireshark)
2. Week 2: Write a summary, recap https + port scanning (nmap) and exploiting (buffer overflow vulnerability in tftp 0.4.2).
3. Week 3: Attack Trees, recap: Service Fingerprinting (nmap), Encryption (PGP), Password/Hashcracking (xhydra dictionary attack on mysql server, rcrack rainbowtables to crack the via mysql acquired forum md5 hash)
4. Week 4: Trojans and Post exploitation (metasploit meterpreter payload exe file, keystroke logging, remote packet sniffing, remote desktop enabling, user account adding etc.),
5. Week 5: SQL injection (wordpress 1.5 vulnerability in damn vulnerable linux) / XSS (cross site scripting in damn vulnerable linux exploitme005), Firefox NoScript, TOR and FreeNet
6. Week 6: VMWare, Virtualbox, iso disk files and images (how to do it yourself)

3 Possible topics thoughts

- -Basic network security + different attack vectors
- -Network vulnerability scanning
- -Wireshark: http sniffing, ftp sniffing
- -Botnet uitleg / beveiliging
- -Metasploit exploiting
- -Metasploit server / client remote code execution
- -SQL injection (high level)
- -Wireless protection cracking
- -Hashcracking (bruteforce vs dictionary)
- -RFID security (vergt hoop voorbereiding)
- -Man in the Middle attack
- -Public key encryption