**Spear Fishing attacks**

Checken op facebook, zeggen hey je zag me op dat feestje , als je meer info wilt klik hier 🡪 malicious website 🡪 geinfecteerd

Examen: Wat is de meest gebruikte poort scanner?

Nmap: die gaat gewoon een target scannen

Portscan en portsweep

Gaat ge alle poorten afgaan en kijken welke reageert, of een poort selecteren en die op alle hosts checken

Stuurt een SYN op poort 80, stuurd gij iets terug dan weet ge da ge daar iets op hebt draaien

Volgende stap:

Vulnerab. Scanner:

Meest gebruikte is Nessus of OpenVas

Waaruit bestaan deze scanners? (Examen)

1. Port scanner

Die moet niet enkel bepalen welke poort open staat maar die moet ook kijken wat op die poort draait.

Dit gebeurd met Banner Grabbing technieken, en in die banner staat welke versie en welke service het is. (bv met apache) RegularExpressions a.k.a regex

1. Vurnibility databaes, die wordt gevuld met CVE’s

Dit zijn common Vulnerabiliets of Exposures

1. Raportage mechanisme , dit bepaalt hoe goed uwe scanner is

Als dit dieje poort open is , hoe losde da op.

Je werkt hier met een confussion matrix.

Examen: intrusion

Oldschool : Misbruik detectie

- Host IDS systemen

Tripwire / OSSEC

🡪 logs/events 🡪 werkt met agents

🡪 hashchecks van belangrijke files met server controleren 🡪 centrale server = SIEM

Ge gaat bepaalde patronen zien en die dan blokken.

Je kan dit enkel met attacks doen die je van te voren al kent, als je Zero Day attacks hebt, kunde da loggen maar ge kunt niks detecteren.

- En netwerk IDS

Snort 🡪 sniffer gaat da zijn (op’t examen moet dan ook nog een sniffer uit leggen (promiscious mode netwerk kaart))

Probleem hierbij is positie, waar gaat ge de sniffer zetten, de meest gebruikte positie voor die te zetten is bij de gateway. Je gaat deze bij belangrijke servers zetten. Niet bij de eind gebruiker anders ga je de patronen niet zien.

Newschool : AI based

- Host IDS (intrusion detection) systemen

Fuzzy logic, trainen end an detecteren

- En netwerk IDS