# **Log management, SIEM en Privacy**

Logs worden altijd doorgestuurd naar een centrale server, die logs werden daar gewoon bij gehouden en daar werd een backup zelfs van bijgehouden. Deze werden gebackupped op een non rewritable disk. Waarom? Stel der was een intruder en die heeft iets gestolen, dan raagt de rechtbank geef mij u logs eens. Waarom non rewritable, het eerste dat je als hacker leert is u eigen maskeren zodat ge de logs omzeilt.

Logs copien, u shit doen, dan logs terug zetten. Daarmee non rewritable.

Standaard loging systeem + een 2de logging systeem (Third party / TTP)

Er moet een standaard logging gezet wordne op elk device 🡪 SYSLOG, zo is het makkelijker om te analyseren.

(side note: kiwi syslog solarwinOS, is de meest gebruikte logging server)

Protocol: regels van communicatie

Standaard: 1 is de beste, meest gebruikte, da is de standaard

**SIEM** (Security Information and Event Management)

Examen: een siem server bestaat uit 2grote onderdelen:

1. Een SIM

Security information Management: LM Server (logging): historische analyse

1. Een SEM

Event Management: Een analyse maken van de logging, maar die analyse is realtime 🡪 enorme CPU power

Hier ben je meestal ook over Dashboards bezig.

Er worden niet enkel syslogs gebruikt maar ook randinfo, app logs, adds logs,…

Examen: Je gaat 2 stappen aan’t ondernemen:

Alle data eerste normaliseren ( de nuttige info uithalen zodat die in een formaat zit dzodat u systeem er makkelijk mee kan rekenen 🡪 Key Value Paires uithalen) zodanig dat

Stap 2: je corralaties (A.T) kunt aanleggen (coraleren is samenvoegen) (ADDS logs samen met gewone logs bv)

**Big Data SIEM**

Je gaat er niet enkel security events uithalen, maar je bent bezig met Organizational inteligence, hierin heb je echt alles staan.

(Side note: Meest gebruikte big data engine is Splunk

Veel plugins instaleren voor CPU monitoring , harde schijf monitoring, logs monitoring,…. )

1 van de meeste gebruikte SIEM’s is AlienVault.

# **Privacy**

Gaat vooral rond cookies draaien (of in mijn geval op eten xd )

Als je surft naar een website dan krijg je een klein plaatske op de pc en die mag daar info op zetten, die cookies gebruikt ge dan om te zien voor welke links er al geklikt zijn enz.

**SAME ORIGIN PRINCIPLE (EXAMEN)**

Enkel scripts van joske.be mogen aan de cookie van joske.be. Dus nienke.be mag daar niet aan.

Nu houden ze in de cookie een soort van ID / barcode plaatsen, om te identificeren wie gij zijt en dan houden ze een grote file bij op de server zelf en zo kunnen ze zien van waneer ge op die link klikt en dit dat hebt.

Hoe komt het nu dat als je op bol.com gaat dat je op facebook relame krijgt van bol.com

Aah nu komt de kikker

De meeste website verkopen banner advertenties, zo een abnner is altijd een image met een href code aan, waar de de image staat. Ge surft naar nienke.be als die href code van joshke.be gaat ge ni enkel met joshke.be contact legt, maar ook met nienke.be

Ik surf nu naar david.be , die heeft ook verschillende banners, die maakt contact met joshke.be, die laat dan iets staan waardoor ge de beste reclame krijgt.

Collusion is een plugin die bijhoudt hoeveel site ge eiegenlijk hebt bezicht op 1ne dag.

Stap verder, techniek van vroeger: tegenwoordig webbugs, op u website verkoopt gij een 1x1 pixel transparant. Hierdoor maak je connectie nog altijd met sites.

Ghostery plugin tracked dit. Dit is zeer moelijk te omzielen, en facebook en google verdienen zo geld.

(side note: Ze hebben zoveel info over ons, europese unie zegt dus dat ge moet zeggen dat ge cookies gebruikt, anders moogde ni verder. De nieuwste ideen zijn van canvas fingerprinting. Daar kunnen ze alles uithalen. )

Authentication cookies: Als een cookie een soort van ID tag is, waarom kan je die niet gebruiken om daarmee in te loggen. Da is natturlijk leuk voor een hacker. Dus we gaan nu cookies telen (Watch out cookie mmonster here I COME !!! )

Bv blackboard authentication cookie stelen: Cross Side Scripting (XSS)

Script : stuur cookie bb.pxl.be naar hacker.

2 meest gebruikte manieren:

1. Stored manier (persistent)

Als je slechte filtering doet, bv een script los in u forum kunnen inladen.

1. Reflected manier (non persistent)

PXL.be heeft een sreach veldje, dat search veldje heeft mss gene goeie check naar filtering toe, als je nu in dat ding script code paste, en laat zoeken, dan lees die browser dat in.

Dit moet je je gebruiker laten doen, hoe doe je dit. Spearphishing attack. Achter een URL kunt ge verbergen wat je wilt.