

BRUGGE 27 SEPTEMBER 2018

SECURITY PROJECT

SEMESTER 5 – COMPUTER & CYBERCRIME PROFESSIONAL

TIJL DENEUT
HENDRIK DERRE
PARCIFAL AERTSSEN



howest.be

SECURITY PROJECT

- Situering

- Semester 5 – 3^{de} bachelor CCCP
=> Aanloop naar Stage/Bachelorproef

- Praktisch

- één dag/week + 2 projectweken
 - Week 1: 5/11 – 9/11
 - Week 2: 17/12 – 21/12
- **Deadline: 31/12**

Reminder: 6 STP = 150 uur...



VERLOOP ALGEMEEN



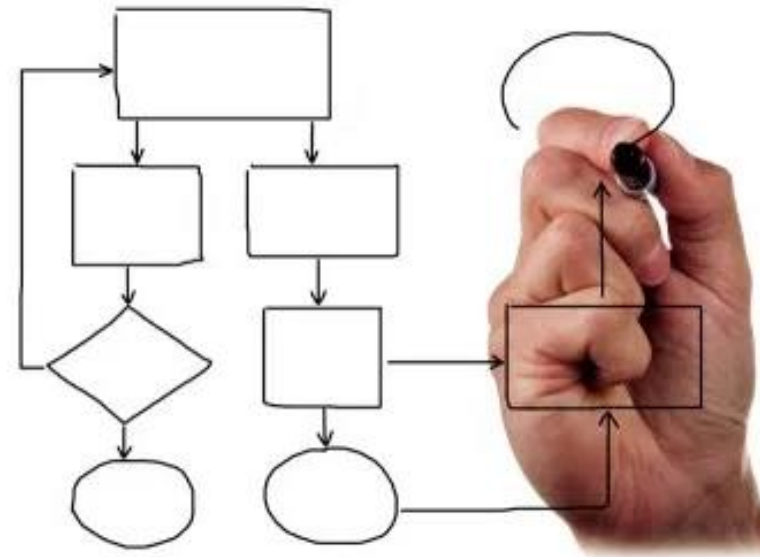
VERLOOP ALGEMEEN –FASE 1

Analyse project

- project grondig geanalyseerd en gedocumenteerd
- Duidelijk afbakenen scope
 - Info specifiek voor Security Audit, zie later
- Voorleggen aan begeleiders

! Project management !

- *Vrije keuze tools/methode*
 - Overzicht van de verschillende taken met tijdsinschatting
 - Toewijzing van de taken
 - Milestones/deadlines voor het project



VERLOOP PROJECT –FASE 2

Uitwerking project

“De studenten worden zelf verantwoordelijk geacht voor het opvolgen van het verloop van het project en tijdig contact op te nemen met de verantwoordelijke lectoren bij problemen.”

- Op regelmatige tijdstippen wordt de vooruitgang gerapporteerd aan de opdrachtgever en/of de coaches. (Vastgelegd tijdens analyse fase)
- Coaches zijn op elk van de voorziene project-tijdstippen aanwezig op de campus
 - Om vlotte begeleiding te garanderen (groot aantal groepen)

=> AFSPRAAK VASTLEGGEN

VERLOOP PROJECT –FASE 3

Verslaggeving

DEADLINE indienen security project: 31/12/2018

1 pdf document per groep waarin jullie volgende zaken rapporteren:

- Projectomschrijving (*analyse project*)
- Vooruitgangsverslag (*project management*)
- deliverable van het project
 - Bij audit => een 2^{de} pdf met het finale verslag voor de 'eindklant'
- Reflectie (*individueel!*)

VERLOOP PROJECT –FASE 3

Presentatie voor jury

Timing: einde van de examenperiode van januari

- Presenteren van zowel het proces als het finale product
 - *!! Indien er sprake is van 'gevoelige' informatie, afstemmen met coaches en opdrachtgever wat er mag gepresenteerd worden !!*
- Enkele tips:
 - Stel jullie zelf voor en de opdrachtgever
 - Respecteer het 'less is more' principe in jullie powerpoint.
 - Verzorg jullie voorkomen en kledij
 - Neem een open houding aan, reageer niet te defensief op vragen
 - Spreek rustig en duidelijk.

VERLOOP PROJECT – EVALUATIE

Evaluatie :

Niet enkel het finale product....

- **LEERRESULTAAT: Adviseren**

- “De professionele bachelor TI geeft advies over IT-oplossingen, -producten, -diensten en – technologieën voor verschillende domeinen en/of sectoren.”

- **LEERRESULTAAT: realiseren change management**

- “De professionele bachelor TI ondersteunt veranderingsprocessen in organisaties bij ingebruikname van IT-oplossingen.”

VERLOOP PROJECT – EVALUATIE

Evaluatie :

Niet enkel het finale product....

- **LEERRESULTAAT: Communiceren**
 - “De professionele bachelor TI communiceert op een professionele manier minstens in het Nederlands en het Engels, zowel mondeling als schriftelijk, aangepast aan het doelpubliek.”
- **LEERRESULTAAT: Projectmatig en teamgericht werken**
 - “De professionele bachelor TI kan zelfstandig en in een multidisciplinair en/of multicultureel team een opdracht op projectmatige wijze aanpakken. De professionele bachelor TI kan eenvoudig leidinggevende taken uitvoeren en een projectplan ontwerpen, interpreteren, uitvoeren, aanpassen en toelichten.”

VERLOOP PROJECT – EVALUATIE

Evaluatie :

Dit project wordt gequoteerd op 20 en elk onderdeel telt voor 1/3 mee:

Permanente evaluatie tijdens het projectwerk (o.a. opdrachtgever):

- Niveau van communicatie tijdens het project
- Behalen van milestones en deadlines
- Feedback van opdrachtgever
- Indien groepswork: peer review

Projectdocument (Coach):

- Niveau van (schriftelijke) communicatie
- Kwaliteit van het afgeleverde werk

Presentatie (Jury):

- Niveau van communicatie
- Inhoud van presentatie
- Correctheid antwoorden bij bevraging

KEUZE PROJECT



PROJECT: SECURITY AUDIT



PROJECT: SECURITY AUDIT

Doelstelling:

Het uitvoeren van een professionele security audit voor een externe opdrachtgever. Dit omvat zowel het security technische aspect alsook het beveiligingsbeleid.

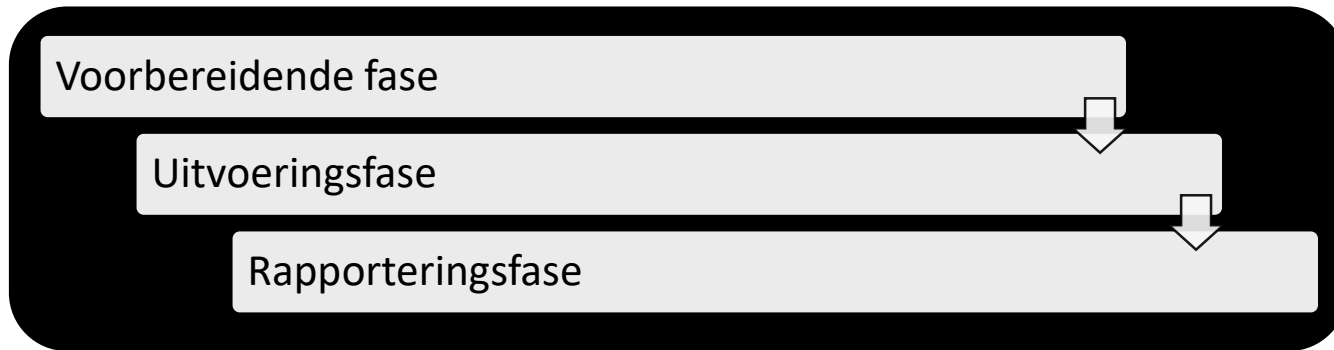
Opdrachtgever:

- Student brengt zelf audit aan en legt dit ter goedkeuring voor aan de projectcoaches. (vb. eigen bedrijf).
- Toewijzing project door Howest.



PROJECT: SECURITY AUDIT

Verloop Security audit:



Hou rekening met deze fases voor het projectmanagement!

- Tijdsinschatting van alle fase met sub-taken
- Definiëring van deadlines of milestones
- Eventueel toewijzing taken aan teamleden

PROJECT: SECURITY AUDIT

Afspraken met opdrachtgever

Inplannen initiële meeting met opdrachtgever:

- Voorleggen verschillende audit mogelijkheden.
- Definiëren en documenteren van scope. *
- Definiëren en documenteren van project timeline. *
- Ondertekenen van NDA (indien van toepassing). *

** Van deze documenten een kopie aan Howest bezorgen.*

Vorbereiding audit

- Literatuurstudie (vb. wetgeving, specifieke technologieën, ...)
 - Hieronder zit ook de Reconnaissance fase
- Updaten en testen van nodige tools (software & hardware)
- Stel uw pentest-kit samen (netwerk kabels, wifi/netwerk dongles, ...)

PROJECT: SECURITY AUDIT

Scope definitie; deze zaken niet vergeten

- Uiteraard de standaard zaken als subnets en websites
 - Let op: als een bedrijf de website host bij bijv. Combell is toestemming van Combell nodig voor een audit!
 - Bij websites: enkel de applicatie of ook de webserver?
- DHCP-range wel of niet? Sniffen wel of niet?
- Soorten toestellen wel of niet (AP, Printers, Switches)?
- Brute Force en/of dictionary attack? Enkel bepaalde services? Bepaalde duurtijd? Bepaalde tijdssloten?
- Bij toegang tot workstations: persoonlijke gegevens? Gebruiken?
- Social engineering? “Praatjes” of “papieren aan de muur” gebruiken?
 - Aansluitend: phishing campaign?
- **Aangeraden:** bevraging personeel. Bijv. ondervraag minstens 5 werknemers naar hun kennis van het ICT beleid, de toepassing ervan en hun awareness naar phishing (zie voorbeeld vragenlijst)
- Meldingsplicht? (erge inbreuken meteen melden i.p.v. wachten op het rapport)
- ...

Vragenlijst voor security audit:

Volgende vragen moeten voorgelegd worden aan minimaal drie werknemers (meer mag) als onderdeel van de security audit. Werknemers blijven volledig anoniem en worden enkel voorgesteld met WN1 (werknemer 1) tot WN_x (werknemer x).

Vraag	WN1	WN2	WN3
Persoonsgegevens durf ik al eens in de papiermand te gooien zonder te versnipperen	Y/N	Y/N	Y/N
Ik neem soms persoonsgegevens op een onbeveiligde USB stick mee naar huis of ik stuur die via onbeveiligde kanalen door (bijvoorbeeld e-mail)	Y/N	Y/N	Y/N
Ben je ingelicht over het gebruik van wachtwoorden?	Y/N	Y/N	Y/N
Wachtwoorden die ik thuis gebruik, gebruik ik ook op het werk en visa versa	Y/N	Y/N	Y/N
Als ik mijn werkpost voor enkele minuten verlaat zorg ik er voor dat de schermbeveiliging aan staat.	Y/N	Y/N	Y/N

Je krijgt een verdachte e-mail van iemand die je blijkbaar kent. Wat doe je?	WN1	WN2	WN3
Ik klik op de hyperlink maar open de bijlage niet			
Ik doe niets en contacteer de ICT helpdesk			
Ik doe niets en verwijder de e-mail			
Ik open de bijlage maar klik niet op de hyperlink			

PROJECT: SECURITY AUDIT

AUDIT <> PENTEST

Zie lesinhouden van “Web Pentesting” en “Network & System Pentesting”

- Scanning & enumeratie: Krijg een beeld van het netwerk/applicatie
 - Veruit het belangrijkste onderdeel
 - Verkennen van de omgeving, verzamelen informatie
 - Welke (sub)netten, welke programmeertalen, welke technologieën?
 - In 90% van de gevallen is hier reeds duidelijk hoe veilig een omgeving is
 - Vergeet de *obvious ones* niet!
 - SNMP, File Shares, routers, switches, airco's, access points ...
- Grote uitdaging: **verwerken van de verkregen info**
 - Dit is persoonlijk, zoek/bedenk een systeem dat voor u werkt
 - Bijv. Excel met een werkblad per subnet
 - Het is niet de bedoeling om tijdens de (bijv.) 2 dagen toegang tot het systeem er 4 uur verloren gaat aan overtypen van data of hernoemen van TXT bestanden ...

PROJECT: SECURITY AUDIT

Zie lesinhouden van “Web Pentesting” en “Network & System Pentesting”

- Scanning & enumeratie: Krijg een beeld van het netwerk/applicatie
- Exploitatie:
 - Use *Extreme Caution* bij het uitvoeren van (third-party) exploits!
 - Altijd veiliger om zo dicht mogelijk bij de “normale” gang van zaken te blijven
 - Bijv.: het is veiliger om SQL Injection te verifiëren m.b.v.
‘OR select “TEST” --
dan met ‘OR DROP schema # of ‘OR 1=1 ---
- Kans is zeer groot dat toegang met admin / admin o.i.d. mogelijk is
- Of dat er sprake is van *misconfiguraties* (ingelogde phpmyadmin pagina)
- Ook “exploitation”: een post-it opmerken aan de onderkant van een toetsenbord met username *contoso\pieterjan* & password *Contoso8940-!*
 - En vervolgens deze gegevens gebruiken m.b.v. psexec/cme/winrm/ ...
- Draai eventueel het onderzoek om: kies een populaire exploit en scan het netwerk i.p.v. elk toestel te scannen op kwetsbaarheden

PROJECT: SECURITY AUDIT

Zie lesinhouden van “Web Pentesting” en “Network & System Pentesting”

- Scanning & enumeratie: Krijg een beeld van het netwerk/applicatie
- Exploitatie: Extreme Caution
- Post-exploitatie: Gevoelig!
 - Na het verschaffen van toegang komt de *ethische* kant: verzamelen van data
 - **Bespreek dit reeds bij de scope**
 - Bij persoonlijke laptops: mag de (persoonlijke) dropbox bekeken worden. Wat bij het ontdekken van “*wachtwoorden-contoso.xlsx*”
 - Wat bij toegang tot de mailbox?
- Post exploitation is belangrijk, maar vergeet de “AUDIT” zelf niet:
 - De bedoeling is vooral om de kwetsbaarheden te detecteren en niet “hoe ver je geraakt”

PROJECT: SECURITY AUDIT

Zie lesinhouden van “Web Pentesting” en “Network & System Pentesting”

- Scanning & enumeratie: Krijg een beeld van het netwerk/applicatie
- Exploitatie: Extreme Caution
- Post-exploitatie: Gevoelig!
- Documentatie: belangrijk!
 - Documentatie is het enige **bewijs** van uw werk t.o.v. de opdrachtgever.
 - Bijlages met resultaten van scan tools mogen, maar benadruk dat deze resultaten niet allemaal hetzelfde risico meedragen:
 - Bijv. CVE-2015-1635 (MS15-034, IIS Remote Code Execution) is zeer kritisch maar slechts een minderheid van de hackers heeft de nodige skills om effectief code uit te voeren
 - Opletten met gevoelige data in rapporten
- Interessant: SANS document “[Writing a Penetration Testing Report](#)” (bevat voorbeeld pentest rapport)

PROJECT: ICS SECURITY



PROJECT: ICS SECURITY

Doelstelling:

Het uitvoeren van een professionele security audit op industriële hard- en/of software.

- *Schneider Electric PLC*
- *Allen Bradley PLC*
- *Siemens IoT Gateway*
- *Sinema Remote Connect*
- *MB Connect*
- ...

=> Focus hier op technisch in de diepte te gaan



Opdrachtgever:

- Onderzoeksgroep Xiak UGent
- Locatie: Kortrijk

PROJECT: NETWORK SECURITY MONITORING



PROJECT: NETWORK SECURITY MONITORING

Doelstelling:

Het uitbouwen van een State-of-the-Art (netwerk) monitoring systeem die dienst zal doen als benchmark voor de vergelijkende studie met AI gestuurde systemen.

- *Network Based*
- *Host Based*
- *Signature & Anomaly Detection*

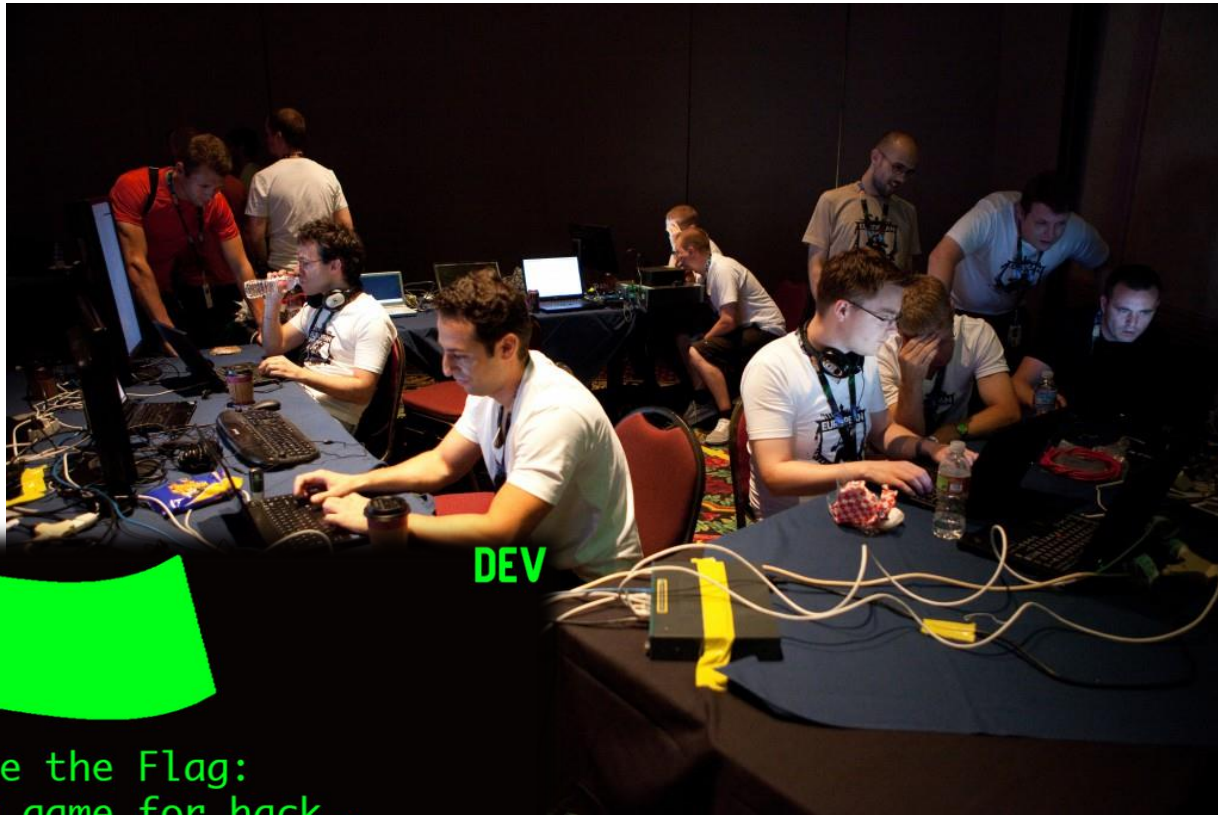


Opdrachtgever:

- Onderzoeksgroep Security&Privacy Howest
- Locatie: Brugge



PROJECT: CTF MONITORING



DEV

Capture the Flag:
It's a game for hack..
I mean security professionals

PROJECT: CTF MONITORING

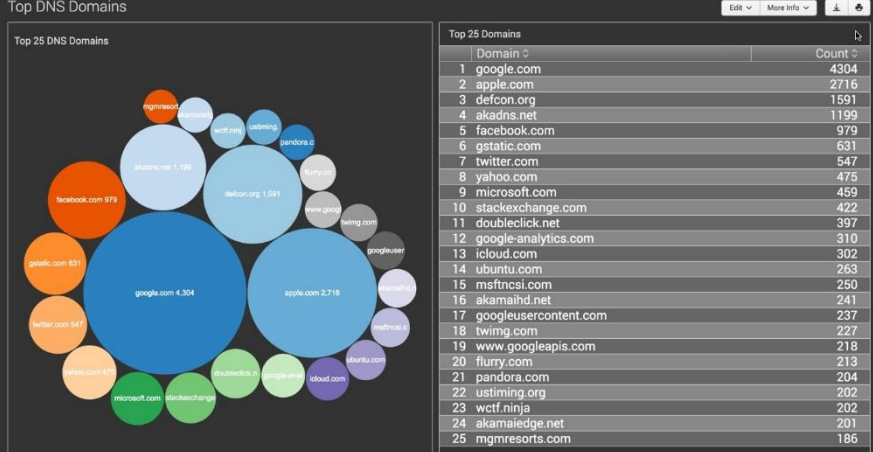
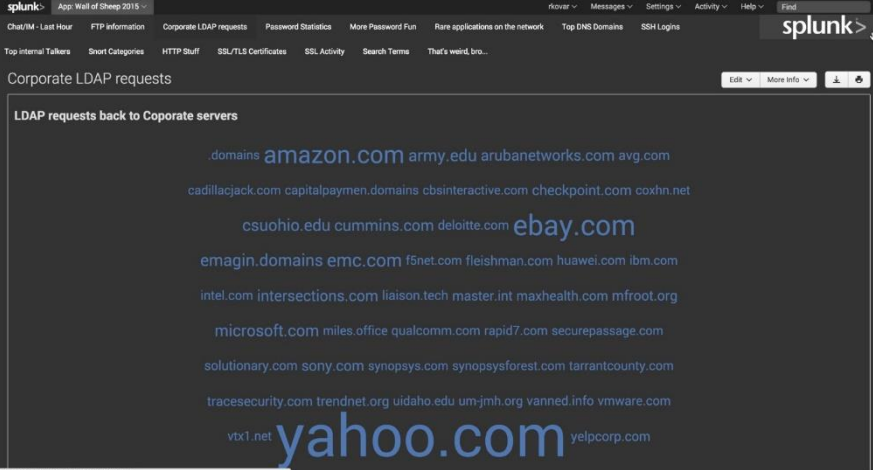
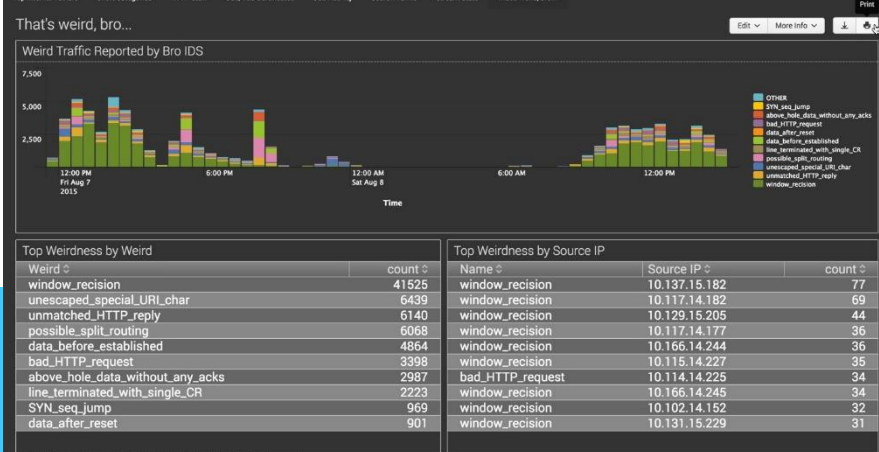
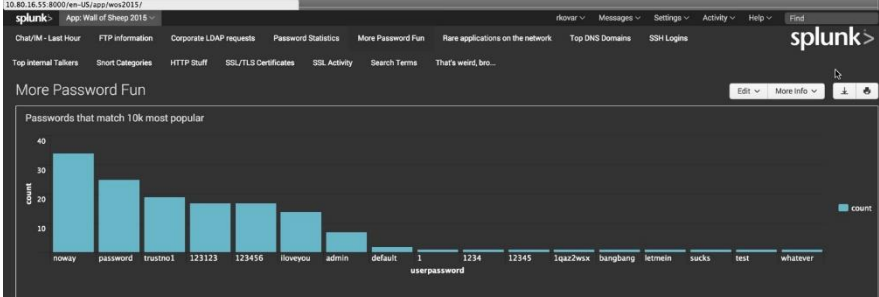
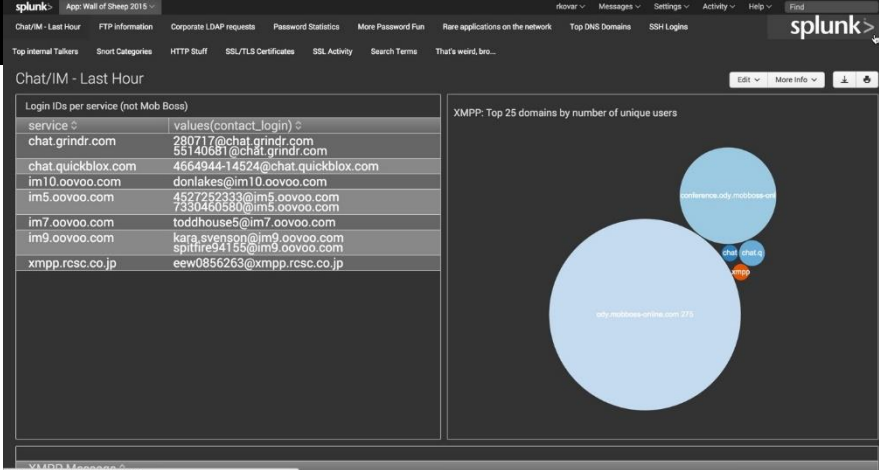
Doelstelling:

Het uitbouwen van een (netwerk) monitoring systeem die specifiek aangepast is om dienst te doen tijdens security events zoals Capture The Flag wedstrijden


- **General network monitoring** (oa. statistieken, Wall of sheep, wifi probes,..)
- **CTF challenge monitoring for admins**
 - Network Based monitoring
 - Host Based monitoring (challenge VM's)
 - Live visualisatie van de challenges attempts ([vb](#))

Opdrachtgever:

- Onderzoeksgroep Security&Privacy Howest
- Locatie: Brugge



PRO

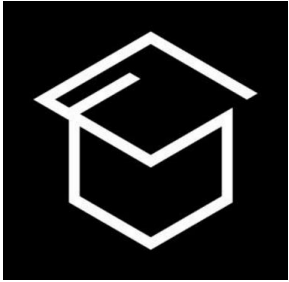


Wall of Sheep

login	pass	domain ip	application
h00p	tdc*****	65.154.34.164	HTTP
voltage_spike@fastmail.fm	tha*****	66.111.4.52	IMAP
Jennifer.lee@post.harvard.edu	poc*****	184.73.159.65	foursquare
demblew	MIC*****	137.52.224.216	pop
wencevdm	Sla*****	128.242.245.20	Twitter (on Android)
Nokia-osso-rx-49	JOS*****	207.114.197.94	HTTP
computicu	lof*****	128.242.245.116	Twitter
reuhelix	fay*****	128.242.245.116	Twitter
vishakn@yahoo.com	hea*****	184.73.159.65	foursquare
em2827891836	622*****	207.114.197.95	HTTP
rossknapp@gmail.com	863*****	184.73.159.65	foursquare
imylongs	tes*****	128.242.245.43	TWITTER
crissti	int*****	128.242.245.148	Twitter
6062191197	pre*****	184.73.159.65	foursquare
ptkrisnan	4li*****	128.242.245.20	twitter
	fen*****	184.73.159.65	4square

PROJECT: SECURE DATA TRANSFER

How to back-up decentralised confidential data in a deprived setting



Name	1st Term Test										2nd Term Test										3rd Term Exam									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
2	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
3	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
4	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
5	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
6	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
7	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
8	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
9	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
10	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
11	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
12	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
13	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
14	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
15	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
16	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
17	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
18	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
19	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
20	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
21	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
22	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
23	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
24	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
25	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
26	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
27	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
28	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
29	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51
30	58	57	41	51	51	51	51	51	51	51	48	57	41	66	46	61	65	45	57	6	58	51	51	51	51	51	51	51	51	51

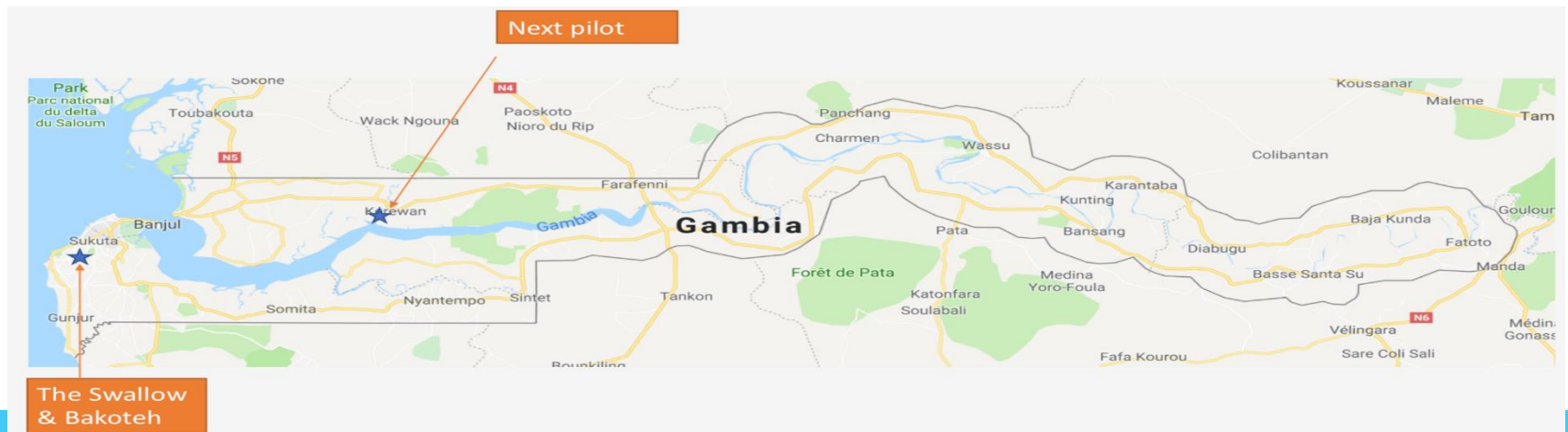
KUBO					
Dashboard My students Tests Exams Term results Chinyere					
Mathematics Term 1 results					
Search: <input type="text"/>					
Name	Decimals /100	Subtraction /100	Addition /100	Exam	Total
Tobiloba Segunmaru	70	53	88	58	81
Tobiloba Nojeem	85	94	85	80	82
Tililayo Ndukuwu	71	90	88	66	70
Tari Esther	64	86	54	77	75
Rasheedah Yaqub	86	62	90	83	82
Rasheedah Emmanuel	58	62	86	55	58
Lolade Omobolaji	53	59	89	75	73
Kubura Haniffat	91	93	86	55	84
Isioma Isokun	59	50	57	68	65
	67	90	61	70	71
	53	58	92	68	68
	72	73	78	92	87
	62	81	57	66	66
	73	60	61	76	73
	90	94	88	77	80
	58	83	55	88	82
	88	92	50	56	63
	57	72	54	78	74
	67	92	79	61	66



PROJECT: SECURE DATA TRANSFER

Prioriteiten:

1. versleutelde lokale backups
2. gecentraliseerde backups (droplet in USA)
3. Incrementele backups
4. Geaggregeerde data -> privacy?
5. Sneakernet: backups via stick naar een andere locatie, vanuit welke ze geupload worden. Moet veilig kunnen verlopen



PROJECT: BLOCKCHAIN SECURITY



BLOCKCHAIN

PROJECT: BLOCKCHAIN SECURITY

Doelstelling:

Verkennen van Blockchain Security en uitvoeren van smart contract auditing

- *Smart Contract Auditing*
- *Protocol Analysis*
- ...

=> Focus op onderzoeksaspect

Opdrachtgever:

- Onderzoeksgroep Security&Privacy Howest
- Locatie: Brugge



PROJECT: AUTOMATED SECURITY TESTING TOOL



PROJECT: AUTOMATED SECURITY TESTING TOOL

Doelstelling:

Ontwerpen van een geautomatiseerde tool op basis van een raspberry Pi om een initiële security scan/audit uit te voeren zonder menselijke interventie.

Globaal idee:

- Initiële audit uitvoeren bij opdrachtgever zonder personeel ter plaatste of remote toegang.
- Raspberry Pi als blackbox opsturen naar klant om lokaal met netwerk te verbinden.

Opdrachtgever:

- Onderzoeksgroep Security&Privacy Howest
- Locatie: Brugge

PROJECT: EIGEN VOORSTEL



IDEA

KEUZE PROJECT

- **Security Audit**
- **Industrial Security**
- **Network Monitoring Systemen**
- **CTF Monitoring**
- **Secure Data Transfer**
- **Blockchain Security**
- **Automated Testing**
- *Eigen Voorstel?*

KEUZE PROJECT

Praktisch:

- Voorkeur type project opgeven via Canvas voor 07/10
- Project zal verder gedefinieerd worden tijdens de week van 08/10
 - Eerste meeting met 'projectgroep' en coaches 11/10
- Je werkt in groep met +-3 personen
 - Groepen toegewezen a.d.h.v. gekozen projecten door coaches

Vragen? Opmerkingen?

