

Pentest Agreement

Cyber Security - Fontys Hogeschool - &RANJ



16 november 2017

Bart Beekwilder Wesley van Gogh Jelle Houwen
John Meerten Bas van Montfort

Inhoudsopgave

Inleiding	3
Wat is een pentest	4
Wie zijn wij?	5
Opdrachtomschrijving	6
Scope	Fout! Bladwijzer niet gedefinieerd.
Planning	Fout! Bladwijzer niet gedefinieerd.
Verwachte documenten	9
Testplan	10
Communicatieplan	11
Wettelijke vereiste	Fout! Bladwijzer niet gedefinieerd.
Afronding	13

Inleiding

In dit document zal onze agreement tussen ons (Fontys Cybersecurity CS31 groep C) en &RANJ worden beschreven. Hierbij leggen we uit wat precies onze scope is, ons plan van aanpak, ons schema en de afspraken die we in een eerdere meeting hebben gemaakt. (2-11-2017).

Wat is een pentest

Een pentest is een toets van een of meerdere computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Een pentest vindt normaal gesproken om rechtmatige redenen plaats, met toestemming van de eigenaars van de systemen die getest worden, met als doel de systemen juist beter te beveiligen. Indien het niet zonder toestemming van eigenaars van systemen, is er sprake van een inbraak, zelfs als de bedoeling van de persoon die de test uitvoert opbouwend bedoeld is.

Wie zijn wij?

Wij zijn 5 studenten van de Fontys Hogeschool in Eindhoven met veel interesse voor Cyber Security en alles wat hierbij hoort. Hierbij hebben we een uit eenlopende hoofdrichting van ICT & Software Engineering, Media Design en Technology, waardoor wij een veelzijdige groep zijn met ieder zijn pluspunten. Afgelopen weken hebben we ons voorbereid op een pentest als deze, waardoor wij nu gaan kijken of in de praktijk deze kennis kunnen omzetten in handelingen. Deze opdracht die wij gekregen hebben van Fontys Hogeschool houdt in dat we een pentest opstellen voor security-gerelateerde bedrijven en hierna ook uitvoeren. Nadat we de beschrijving hadden gelezen van &RANJ kregen we een goed gevoel, waarbij de kern van de opdracht de meeste groepsleden beviel, waardoor de keuze snel gemaakt was.

Hierbij hopen we dat wij uiteindelijk van uw bedrijf kunnen leren en uw bedrijf van ons.

Natuurlijk hopen we op een goede samenwerking tussen beide partijen, waarbij er gehouden wordt aan de afspraken in dit bestand.

Opdrachtoomschrijving

Omschrijving vanuit &RANJ:

“&RANJ heeft een nieuw information security-beleid. Graag kijken wij, samen en op een leuke manier, of dit goed wordt nageleefd. Hoe zit het met Social Engineering, beveiliging, hardware, onze infrastructuur, etc? Ik wil graag het menselijke component laten terugkomen en een nul-meeting laten uitvoeren op alle het digitale voor de hele organisatie. Daarbij zou ik een log willen bijhouden van alle te nemen stappen. Dat log kunnen wij als input gebruiken om een cyber security game te maken.”

Scope

Locatie: Rotterdam, wij houden dochter bedrijven buiten beschouwing.

Network Penetration Test

Wij gaan proberen om het netwerk te penetreren. Dit gaan we doen binnen de gevraagde ip-ranges.

Wij gaan proberen devices te penetreren denk hierbij aan printers en andere devices die aan het internet verbonden zijn.

Wireless Network Penetration Test

Wij gaan proberen door middel van password cracking in het netwerk te komen.

Web Application Penetration Test

Wij gaan kijken of we eventuele webserver kunnen penetreren.

Social Engineering

Wij gaan een aantal phishing mails sturen om te kijken welke werknemers hier allemaal op klikken.

Wij gaan kijken of we een usb-stick in een computer kunnen doen.

Wij gaan kijken of er mensen zijn die hun computer niet locken wanneer ze de computer verlaten wordt.

Een gedetailleerd plan volgt nog. Zodra we meer informatie hebben over ip-adressen en webserver.

Planning

Contactmomenten

Datum*	Werkzaamheden	Overige informatie
2 november 2017	Eerste gesprek voor maken van pentest	Opstellen van scope, wat mag wel, wat niet, bijzonderheden gedeeld
30 november 2017	Pentest 1	Onder voorbehoud
14 december 2017	Pentest 2	Onder voorbehoud
11/12 januari 2017	Resultaten laten zien	Onder voorbehoud (mogelijkheid om bij Fontys of &RANJ te presenteren)

*voorkeur voor donderdag of vrijdag i.v.m. lesdagen van Cyber Security

Verwachte documenten

Er zijn een aantal documenten die wij na onze periode gaan leveren. Ten eerste uiteraard het pentest rapport waarin wordt beschreven wat we precies hebben gedaan, hoe veilig de infrastructuur precies is en hoe we het proces hebben doorlopen.

Daarnaast is er vanuit &RANJ behoefte om een document te maken waarin allerlei vragen staan die je kan stellen vanuit ons process dat we doorlopen hebben.

Bijvoorbeeld: “is het veilig om een onbekende link te klikken in een e-mail?”.

Ook zal er een logboek per persoon worden bijgehouden met de activiteiten die er verricht zijn, dit wordt ook verzocht in de opdrachtomschrijving.

Testplan

Wij gaan ons opdelen in 3 groepen.

De eerste groep gaat beginnen met de 'Network Penetration Test'. En de tweede groep gaat van start met de 'Wireless Network Penetration Test'. De derde groep werkt in zijn eentje en gaat aan de slag met 'Social Engineering', denk hierbij vooral aan phishing mails. Als de derde groep eerder klaar is (wat wel verwacht wordt) zal hij aansluiten bij groep 1 of 2. Zodra groep 1 of 2 klaar is wordt er verder gegaan met de 'Web Application Penetration Test'.

Terwijl elke groep bezig is met zijn taak. Zullen we ook kijken of er medewerkers zijn die hun computer unlocked laten staan, of kijken of we misschien ergens een usb in de computer kunnen stoppen.

Een gedetailleerd plan volgt nog. Zodra we meer informatie hebben over ip-adressen en webservers.

Elke taak die iedereen uitvoert zullen we per 'case' noteren, dit ziet er als volgt uit:

Naam: Piet

Activiteit: Penetreren ip address: 127.0.0.1

Tijd/ datum: 1-1-2018 12:09

Bevindingen: Elke poort staat open, niet veilig!

Communicatieplan

De communicatie gaat vooral via Rogier. Technische en/of netwerk vragen kunnen ook aan René of Perry worden gesteld. De communicatie verloopt altijd via de officiële fontys mail (@student.fontys.nl).

Alle testen die we gaan doen worden altijd vooraf met Rogier gedeeld zodat Rogier altijd op de hoogte is en kan aangeven wanneer iets niet kan of te ver gaat.

Telefonisch contact is niet handig aangezien Rogier vaak vergaderingen heeft en toch vaak zijn mail checkt.

Officiële e-mailadressen van studenten:

Bart:

b.beekwilder@student.fontys.nl

Bas:

b.vanmontfort@student.fontys.nl

Jelle:

jelle.houwen@student.fontys.nl

John:

j.meerten@student.fontys.nl

Wesley:

w.vangogh@student.fontys.nl

Mails die niet komen van deze officiële e-mails kunnen onderdeel zijn van een test!

Wettelijke vereisten

De volgende punten zijn alleen toegestaan in opdracht van en op uitdrukkelijk verzoek van de opdrachtgever.

- Het analyseren van een geautomatiseerd systeem van de opdrachtgever
- Het binnendringen van een geautomatiseerd systeem van de opdrachtgever
- Het analyseren van de beveiliging van het geautomatiseerd systeem van de opdrachtgever
- Het doorbreken van de beveiliging van het geautomatiseerd systeem van de opdrachtgever

Deze punten kunnen uitgevoerd worden door middel van valse signalen, valse sleutels of door een valse hoedanigheid aan te nemen, zoals bedoeld in Artikel 138a Wetboek van Strafrecht. Wij mogen dit alleen doen met toestemming van Rogier.

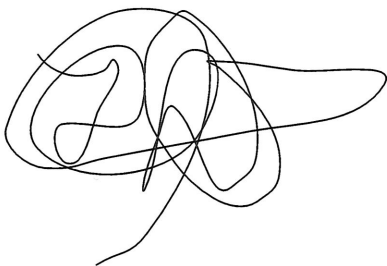
Verder is ook het verzenden van computervirussen en/of Trojan Horses naar e-mailadressen en systemen binnen de organisatie van de opdrachtgever, beperkt tot door de opdrachtgever aangegeven onderdelen van het geautomatiseerd werk. Deze computervirussen en/of Trojan Horses mogen nooit schade aanrichten aan een systeem.

Afronding

Studenten van Fontys Hogeschool te Eindhoven en het bedrijf &RANJ uit Rotterdam accepteren hierbij deze pentest agreement, waarbij beide partijen zich moeten houden aan afspraken die te vinden zijn in dit document.

Eindhoven, 9 november 2017

Handtekening Studenten (Fontys)



Wesley V. Gogh



Bart

John

Handtekening &RANJ



&RANJ
RANJ SERIOUS GAMES
LLOYDSTRAAT 21M
3024 EA ROTTERDAM
COG: 24290770
VAT: NL 8077.07.804.B.01