**Security Advanced– PE Opdracht**

**Algemeen**

De opdracht is een **open opdracht**: er wordt opgegeven wat de minimale vereisten zijn van de opdracht, maar er worden ook uitbreidingen voorgesteld om een hogere score te behalen. De studenten mogen zelf ook uitbreidingen voorstellen en implementeren, in overeenstemming met de begeleidende lectoren.

De opdracht is een **team opdracht**: er wordt in een team gewerkt van **4 studenten**. De lectoren zullen regelmatig de samenwerking en vordering van het project bij de teams nagaan. Een groepsopdracht betekent ook een groepscijfer, dat ook individueel kan aangepast worden. De PE opdracht staat op 60% van het eindtotaal, en is niet herneembaar voor 2de zit.

**Let op: deadline voor het doorgeven van de teamleden is 5/3/2020. Een student die dan nog niet bij een team hoort, is te laat om nog mee te doen met de PE → 0/60 voor de PE!**

Er zal tijdens de lessen steeds tijd voorzien worden om in team aan de opdracht verder te werken. De **verdediging** van de opdracht zal tijdens de laatste lessen van het OLOD plaatsvinden.

De opdracht zelf bestaat uit **3 aspecten (Yellow Team, Blue Team, Red Team)** die dan nog eens onderverdeeld zijn in **3 niveaus (C, B, en A(+))**. Deze niveaus zijn opbouwend: eerst wordt het laagste niveau C afgewerkt, waarna men niveau B kan behandelen, en daarna kan men evt zelfs nog verder gaan in dat aspect en niveau A topics aanpakken. Ieder team wordt verondersteld **alle aspecten op niveau C** af te werken, en **minstens 2 aspecten tot niveau B**. Omdat het een open opdracht is, kan men dus nog verder gaan en ook A niveau items gaan behandelen, of de 3 aspecten tot niveau B brengen… Men kan zelfs niveau A nog verder uitbreiden naar A+…

Voor het **Yellow Team (YT)-aspect**: voor het maken van het Crypto-programma, mag er vertrokken worden van bestaande code op het internet, mits **duidelijke referentie in de commentaar** + studenten moeten de code wel **goed begrijpen**. De bedoeling van het YT-aspect is immers niet puur het programmeren, maar wel het toepassen en begrijpen van security aspecten. Maak dus een eigen ‘shell’ rond deze code, maak er uw eigen applicatie van. Het onderling sharen van code tussen de teams is niet toegestaan (gebruik een private github).

Voor het **Blue (en Red) Team aspect**: hier wordt het best gestart met een VM met daarop het Kali of Parrot Security OS. De vulnerability scan wordt dan uitgevoerd vanuit Kali/Parrot naar een andere VM met het target OS op.

Om een Nessus scan te doen, wordt gebruikt gemaakt van de **gratis Nessus Essentials (vroeger de Nessus Home Feed plugin)**, die dan op de VM wordt geïnstalleerd.

***LET OP****: het uitvoeren van een vulnerability scan mag enkel op uw eigen hosts/netwerk! Wees er dus zeker van dat je de scan niet doet over het PXL netwerk, of op een host waarvoor je de toestemming niet hebt = cybercrime!*

**Opdracht Security Advanced – Yellow Team aspect:**

**Hybrid Crypto App**

**Algemeen:**

De bedoeling is om een applicatie te maken (of te vinden en het u eigen te maken), in een programmeeromgeving naar keuze, om een bericht veilig van persoon A naar persoon B te sturen, gebruikmakend van een combinatie van cryptografische functies (hybrid crypto: hashing + symmetrische + asymmetrische functions). Denk bv aan een secure chat applicatie, of een secure mail applicatie, waarmee je een bericht en/of file kan versturen.

Gebruik hiervoor bestaande security libraries, zodat je deze crypto componenten niet zelf moet coderen. Kijk wel in documentatie welke opties die componenten hebben, welke defaults, hoe je die het beste kan gaan gebruiken voor jullie applicatie.

Als men de principes van hybrid crypto correct toepast, kan men onderstaande statements garanderen:

* De ontvanger is zeker dat hij de enige is die de file terug kan decrypteren
* De ontvanger is zeker dat de file van A afkomstig is
* De ontvanger is zeker dat er niets veranderd is aan de file tijdens transport
* De zender kan niet meer ontkennen dat hij de file gestuurd heeft

*Note: In principe heb je voor het bovenstaande certificaten nodig om de linking te kunnen maken tussen een persoon A en zijn public key. Dit is voor de niveau C uitwerking geen vereiste.*

**Level C requirements:**

* Standalone applicatie (enkel local op uw eigen laptop) voor minstens 2 gebruikers, Alice en Bob
* Er moet geen inlog zijn. App mag opgestart worden als zijnde voor gebruiker A. Daarna sluiten. Terug openen als zijnde gebruiker B.
* Key generation en (local) storage voor symmetric / asymmetric crypto voor iedere gebruiker
* Het moet mogelijk zijn om zowel tekst, als een file, naar B te sturen, via hybrid principe
* Er moet een check gebeuren na ontvangst van hybrid principes (signature en hash check)

**Level B requirements:**

* Client / server applicatie (moet geen online server zijn, maar mag), aka front- en back-end. Liefst web front-end, maar geen vereiste (mag bv ook mobile of iets anders zijn)
* ‘new user’ en inlog module (en dus ook user authentication via bv password)
* OWASP Pro-Active Controls: definieer specifieke security requirements uit de OWASP ASVS standards waaraan jullie project zal moeten voldoen (pro-active, dus voor er mee te starten), en highlight bij de analyse fase die delen van jullie applicatie waar expliciet aandacht zal worden aan besteed volgens de top-10 pro-active controls. Highlight bij jullie verdediging dan ook specifieke delen die aangepast waren ten gevolge van deze guidelines.
  + Note: deze standards en guidelines zijn het meest toepasbaar op web-based front-ends, maar vele van deze issues gelden ook voor andere soorten front-ends

**Level A requirements:**

* Code quality is ook voor security doeleinden belangrijk. Bugs en flaws kunnen nefast zijn voor secure code. Buiten de OWASP Pro-Active guidelines, zijn er ook tools die automatisch kunnen scannen op coding best practices, code smell detection, (unit test coverage), maar ook automatische checks doen op vulnerabilities, o.a. gebaseerd op de OWASP guidelines. De meest gekende tool hiervoor is Sonarqube. Run je code base eens op sonarqube, en analyseer de resultaten.

**Level A+ requirements:**

* Sky is the limit…
* Verschillende manieren van authentication: (Google) 2FA module, fingerprint login of andere biometrics, Belgische eID login/certificaten…
* Online applicatie over https, met bv Let’s Encrypt certificaten
* Toevoeging van steganografie om encrypted file te verbergen in bv image om die door te sturen
* JWT tokens, OAuth,…

**Opdracht Security Advanced – Blue Teaming aspect: Vulnerability Analysis / Forensics**

**Algemeen Vuln.Analysis:**

Vooraleer een server live beschikbaar is via het internet, moet deze gecontroleerd worden op mogelijke vulnerabilities. Indien er kwetsbaarheden gevonden zijn, moeten deze eerst gepatched worden, zodat er geen exploits meer mogelijk zijn.

Veel gebruikte vulnerability scanners zijn: Nessus, Nexpose (van Rapid7 – company behind metasploit), OpenVAS, nmap, maar ook OWASP ZAP. OpenVAS, nmap en OWASP ZAP zijn open source, Nessus en Nexpose zijn betalend. Maar, Nessus Essentials is de gratis versie voor persoonlijk gebruik / educational doeleinde, en Nexpose heeft ook een gratis trial (check wel nodige resources).

**Level C requirements:**

* Zorg dat je een VM (bv Kali of Parrot) hebt waarop je minstens Nessus Essentials, nmap, en OWASP ZAP op geïnstalleerd is
* Zorg dat je een VM hebt met een Win7 (of iets gelijkaardigs op), en een VM waarop je Metasploitable 3 hebt geïnstalleerd. Deze OS’en zijn de targets.
* Scan deze targets met Nessus en nmap. Scan de WindowsOS ook eens zonder firewall. Analyseer de resultaten van deze scans, en zorg dat je de belangrijkste vulns begrijpt.
* Scan Metasploitable3 met OWASP ZAP en analyseer de resultaten

**Algemeen Forensics:**

Forensics, het klinkt recht uit een crimireeks...en dat is het deels ook. Letterlijk betekent het sporenonderzoek en dat is ook wat we doen, niet enkel de politie wil weten hoe iets is gebeurd. Als er een incident gebeurd is in een IT omgeving die we beheren, willen we ook weten WAT er juist gebeurd is en HOE het is kunnen gebeuren, dus dan gebruiken we deze technieken om er uit te leren, het te begrijpen en te zorgen dat het niet meer kan gebeuren (en soms ook om de schuldige aan te duiden).

Veelgebruikte tools in Forensische onderzoeken zijn Sleuthkit, Autopsy en Volatility frameworks. Dit zijn open source tools die we ook onderliggend terugvinden in commerciële producten zoals FTK en EnCase.

**Level B requirements:**

* Rick’s PC

<https://dubbadub.be/s/XD8Wnhtedc8mOvr>

passwoord: rFVoi8GZyd&xvUKvLFU3z6FrU5ZhY\*B9pRdG

We hebben een memory dump te pakken kunnen krijgen van Rick en weten dat het paswoord dat hij daar gebruikt hetzelfde is als op zijn werk. Kan jij het paswoord ontdekken?

De oplossing is natuurlijk niet enkel het paswoord: voor dit onderdeel van de PE verwachten we natuurlijk iets meer. Beschrijf de stappen die je ondernomen hebt om tot de oplossing te komen. Bespreek de technieken die je gebruikt hebt en licht dit alles zeker ook toe in je presentatie/verdediging.

**Level A(+) requirements:**

* Forensics open

Je hebt keuze genoeg uit voorbeeld images op sites als:

* + <https://digitalcorpora.org/corpora/disk-images>
  + <https://www.cfreds.nist.gov/>
* Nexpose en OpenVAS op andere OS’en (misschien nog een oude PC thuis staan?)

**Opdracht Security Advanced – Red Teaming aspect:**

**Ethical Hacking**

**Algemeen:**

Zowat het meest tot de verbeelding sprekende onderdeel van Security is het zelf aanvallen van omgevingen en machines, dat is waar dit onderdeel over gaat.

Begin bij het begin en gebruik publieke gegevens om binnen te raken in een bedrijf om daarna met alle gevonden informatie verder binnen te dringen in de data van dat bedrijf en toegang te krijgen tot gevoelige informatie.

Nog interessanter wordt het natuurlijk als we actief op zoek gaan naar fouten in applicaties en servers om echt toegang te krijgen tot machines om er volledige toegang (Root) tot te krijgen. Gebruik tools zoals Nmap om te scannen, Exploit-DB om naar kwetsbaarheden op zoek te gaan en MSF om ze uit te voeren….of doe het oldskool zelf in je terminal.

**Level C requirements:**

* Neem de resultaten van je scans op de Metasploitable 3 VM van de Blue team opdracht en ga hiermee aan de slag met Metasploit:
* Ga op zoek naar MSF modules die de gevonden vulns kan gebruiken en verkrijg toegang tot de machine. Zet een RDP sessie op naar deze machine met Administrator rechten.
* Er zitten 15 hidden flags in deze machine verborgen in de vorm van afbeeldingen van speelkaarten, vind er minstens een.

Beschrijf de stappen die je ondernomen hebt om tot de oplossing te komen. Bespreek technieken die je gebruikt hebt en licht dit alles zeker ook toe in je Presentatie.

**Level B requirements:**

* OSINT Challenge HTB - <https://www.hackthebox.eu/>
  + Infiltrated
  + We Have a Leak
  + Breach

Oplossing op HTB is enkel de flag, maar voor dit onderdeel van de PE verwachten we natuurlijk iets meer. Beschrijf de stappen die je ondernomen hebt om tot de oplossing te komen. Bespreek technieken die je gebruikt hebt en licht dit alles zeker ook toe in je presentatie.

* Log in op de HTB Labo en zorg dat je user en root rechten krijgt op minstens 1 van de volgende boxen: TBD

Voor deze machines zijn Write-ups beschikbaar op het internet, je kan deze gebruik **MAAR** we verwachten dat jullie ook in eigen woorden de stappen beschrijven en kunnen aantonen dat de gevolgde stappen begrepen worden.

**Dit onderdeel is pas beschikbaar vanaf April!**

Oplossing op HTB is enkel de flag, maar voor dit onderdeel van de PE verwachten we natuurlijk iets meer. Beschrijf de stappen die je ondernomen hebt om tot de oplossing te komen. Bespreek technieken die je gebruikt hebt en licht dit alles zeker ook toe in je Presentatie.

**Level A(+) requirements:**

* Verkrijg user en root rechten op een van de Active boxes op HTB

Oplossing op HTB is enkel de flag, maar voor dit onderdeel van de PE verwachten we natuurlijk iets meer. Beschrijf de stappen die je ondernomen hebt om tot de oplossing te komen. Bespreek technieken die je gebruikt hebt en licht dit alles zeker ook toe in je Presentatie.