Beveiliging

algemeen

Studiepunten	3
Aandeel PE/Examen	30% - 70%
Examen vorm	Mondeling met schriftelijke voorbereiding

De lessen zijn een combinatie van theorie en demo's. Aanwezigheid in de lessen is zeer aan te raden, omdat alle examenvragen wel eens zullen voorkomen.

De permanente evaluatie bestaat uit twee taken. De eerst is het digitaal onderteken van een email of JAR-file. De tweede taak is een mini-project over een door jou gekozen onderwerp, maar uiteraard moet het wel iets met beveiliging te maken hebben.

Het examen is theoretisch. Je moet je hacking-skills dus niet ten toon stellen. Je dient gewoon de gevaren en de oplossingen te kennen van de geziene beveiligings. Het is toegestaan de artikels op export af te drukken en mee te nemen naar het examen.

Lijst van technieken

Dit is een lijst van technieken die je kan gebruiken voor het kraken van allerhande beveiligingen, het saboteren van websites, etc. De lijst is zeker en vast niet volledig dus vul hem gerust aan. Indien je een van deze technieken, voor welke reden dan ook, wilt uitproberen. Zorg er dan voor dat je ZEKER EN VAST een getekende toestemming hebt van de eigenaar/verantwoordelijke van het systeem, of zet zelf een systeem op. Virtuele machines kunnen wonderen doen als je het bij jezelf wilt uitproberen. Je zal voor deze technieken wel zelf moeten opzoeken wat dat ze betekenen. Note: Als iemand tijd en zin heeft, mag die altijd beschrijvingen toevoegen :)

1. Portscanning
2. XSS exploits
3. CSRF (uitgesproken als seasurf) exploits
4. SQL injections
5. FTP server exploiten
6. DNS records veranderen
7. Smurf attack
8. Cookie stealing
9. Session hijacking (in browsers)

10. Log poisoning
11. E-mail spoofing
12. Phishing
13. ARP-Spoofing
14. Man in the middle attacks
15. Passive sniffing
16. Social engineering
    1. Even telefoneren...
    2. Dumpsterdiving
17. botnet

2011 januari examen

Groep 2

1. Er worden 5 weaknesses gegeven
    1. Zet ze in volgorde van erg naar minder erg.
    2. Als er nog geen update/patch voor handen is voor deze exploit, hoe zou je voorkomen dat er misbruik van wordt gemaakt?
2. Een vertrouwelijke mail
    1. Hoe kan ik aan deze mail geraken?
    2. Hoe beveilig ik tegen de voorgestelde methodes?
3. 3 waar of niet stellingen:
    1. SQL injection is enkel gevaarlijk in formulieren waar wordt ingevoegd of verwijderd.
    2. Een poortscan wordt steeds door een IDS opgemerkt
    3. XSS is niet gevaarlijk, enkel hinderlijk
4. Leg uit en geef voorbeelden:
    1. Risico / Risk
    2. In depth security

Groep 1

1. Er worden 5 security advisors gegeven (dit is een vraag die altijd terug komt)
    1. Zet ze in volgorde van erg naar minder erg. (dit moet je kunnen verdedigen. Een security adviser die meld dat een lokale gebruiker admin rechten kan krijgen is voor een systeembeheerder een groot probleem, maar voor een gebruiker op zijn thuiscomputer niet)
    2. Als er nog geen update/patch voor handen is voor deze exploit, hoe zou je voorkomen dat er misbruik van wordt gemaakt?
2. Een webmail
    1. Hoe kan een buitenstaander aan de inloggegevens geraken en geef een schaal van 1 op 10 naar moeilijkheid? (hier zou je er toch 7 tot 10 moeten op kunnen geven)
    2. Hoe beveilig ik tegen de voorgestelde methodes?
3. 3 waar of niet stellingen:
    1. Een portscan is een vorm van passieve verkenning
    2. Een webinterface waar het wachtwoord in een hash is bewaard met salting is onmogelijk om een bruteforce op te doen
    3. Welk van de 2 zal het meeste false positives genereren: anomaly detection of patroon detectie

4. Termen kunnen verduidelijken met voorbeelden (eigen voorbeelden worden het meest geapprecieerd, voorbeelden die in de cursus staat of tijdens de les zijn gegeven minder)
    1. least privileged
    2. Security through obscurity

2012 januari examen

Woensdag 25 januari 2012

1. Juist of fout + leg uit
    1. Wanneer je een IDS achter je firewall zet, geeft die minder false positives
    2. Met een botnet kan je alleen DDoS aanvallen doen
    3. Wanneer je geen bijlages opent, kan je geen malware krijgen via mail
2. Geef zoveel mogelijk manieren om (tijdelijk) te veranderen wat mensen op een pagina zien + geef oplossingen om deze tegen te gaan
3. Een lijst van vijf verschillende threats, je moet ze in de juiste volgorde zetten van ernstig naar minder ernstig
    1. Location Bar Spoofing
    2. POST data send to wrong site
    3. Crash & remote code execution
    4. Compromise of SSL-protected communication
    5. File stealing by changing input
4. 'Defense in depth' uitleggen a.d.h.v teksten of eigen voorbeelden
5. Project even bespreken
6. Zeggen welke teksten je het leukste vond en welke minder leuk

Maandag 16 januari 2012

1. Juist of fout + leg uit
    1. Als een certificaat niet geverifieerd kan worden, is het dan veiliger om deze op te slaan of niet? => ja, zo merk je veranderingen op (man in the middle bv)
    2. Als een pc achter een firewall zit die alle inkomende dingen blokkeert, kan hij dan nog deel van een botnet zijn. => Ja, besmetting via USB stick bv. Kan nogaltijd opdrachten uitvoeren zoals bv DDOS.
    3. Is Salting en hashing een vorm van Security by obscurity? Neen, geen verborgen of obscure algoritmes. (?)
2. Leg zoveel mogelijk manieren uit om aan een confidentiële email te geraken. Vertel ook hoe dit te voorkomen.
3. Een lijst van 5 verschillende bugs in antivirussen. Rangschik die van erg naar minder erg. Verzin voor elke bug een mogelijk aanvalsscenario en hoe ge dat scenario kunt tegengaan nog voordat de patch uit is.
4. Principle of least privilege uitleggen adhv de teksten

5. Project: "Vertel mij de problemen die ge ervaren hebt bij het maken van uw project" en "Was het leuk?" (Had bij mij hier niets over gevraagd, maar kans is wel groot)
6. Welke tekst vindt gij het leukst? Welke het minst? Welk hoofdstuk heeft u gelezen en wat vindt u hier het interessantste aan?

Vrijdag 13 januari 2012

1. True or false. Explain.
    1. Q: Making your SSH server listen on another port (not 22) is an example of "Security through Obscurity". A: T. Dit is sowieso een voorbeeld van security through obscurity. Het is immers heel makkelijk om even met een portscanner, eg: nmap, effe alle poorten te gaan scannen van het IP adress en dan de poorten waar niet sowieso aangegeven word dat het een bepaalde service draait, ie: "unknown" even naar te netcatten. Bij SSHd is het immers zo dat deze automatisch een welkomstboodschap, etc gaat geven. Het is dus een manier dat het systeem alleen maar ongebruiksvriendelijk maakt, men gaat immers niet de default poort gebruiken, en gaat maar een klein aantal malware/scriptkiddies weghouden.
    2. Q: Exploitation of a buffer overflow always results in root or administrator access to a system. A: F. Er zijn 3 soorten gevallen waarop men root rechten kan krijgen door een buffer overflow. De eerste is door een buffer overflow te gebruiken in een programma dat sowieso volledig als root draait (door slechte programmatuur, maar dit kom je maar zelden tegen op deftig gemaakte systemen), de tweede manier is als het ge-overflowde programma als root draait, terwijl dit nodig is (door een slechte of luie sysadmin...) of doordat je in een programmagedeelte kan springen dat als root gedraait wordt (dit is vaak de moeilijkste manier, maar vaak ook de enige bij goed gemaakte systemen die toch buffer overflows hebben)
    3. Q: If you suspect your network contains zombie clients belonging to some botnet, you can disable them easily by blocking the port for Communication&Control communication on your firewall. A: Kan iemand dit aanvullen? :) Zou in de tekst over command & control moeten staan; volgens mij is het antwoord F.
2. How would you disrupt a competitor's website ? What (if anything) could your competitor do to prevent these disruptions? Het belangrijkste hierbij is vooral zoveel mogelijk proberen op te noemen...een lijst van interessante technieken hiervoor zal ik toevoegen ergens op deze pagina :)
3. Rank the attached security advisories by their severity. Use 1 for the most urgent advisory, 5 for the least urgent one. For each advisory, provide a possible attack scenario and a workaround that can be used to prevent such an attack if no patch or fix is available.
    1. Winzip (versie x) authenticeert zijn update server niet, waardoor man-in-the-middle aanvallen mogelijk zijn.
    2. Een buffer overflow in software x zorgt voor root file system access voor lokale gebruikers (Edit: Dit ging niet over root file access, maar access tot een andere gebruiker, in dit geval kon dit ook een gebruiker zijn dat toegang had tot het

netwerk, daar het ging over een programma voor file uploading, niet persé root access dus)
    3. (iForgot) (Edit: Dit had te maken met directory transversal, waardoor je bv een edit kon doen van bestanden in andere folders)
    4. Idem b, maar dan met remote gebruikers
    5. Door een fout in McAfee (versie x) worden sommige archiefbestanden genegeerd (of zoiets, heb de vraag zelf eigenlijk niet begrepen).
4. Required Reading: Welke was meest/minst interessant + welk hoofdstuk uit boek gelezen en waar gaat het over?
5. Assignments

Donderdag 12 januari 2012

1. Juist of fout + leg uit
    1. Het is makkelijker om formulierloze dingen te beveiligen als andere (vraag kwam daar toch op neer)
    2. Biometrics system for verification is less accurate than for identification
    3. CSRF can be blocked by verifying HTTP Referer header
2. Geef zoveel mogelijk manieren om aan e-mails te komen voor bvb spamming en voor elke manier een oplossing
3. 5 exploits die ge in volgorde moet zetten
4. Iets van alle teksten die je gelezen zou moeten hebben
5. Iets over je projecten

Maandag 09 januari 2012

1. Juist of fout + leg uit
    1. Applying 'least privileged' prevents 'path traversal' vulnerabilities
    Antwoord: Waar, maar het is eigenlijk een principe als voorzorgsmaatregel, omdat de applicatie zelf path traversal zou moeten kunnen tegen gaan en niet het systeem waarop de applicatie draait. Hij vroeg dan ook hoe je met PHP een path traversal vulnerability kon exploiten op het mondeling. Dit kan door vb. include="../../anderepersoon/.htaccess" te schrijven.
    2. Signature based IDS's have a lower false positive rate than anomaly based IDS's
    Antwoord: Juist, signature based IDS's hebben een lijst met dingen die toegelaten zijn en het gebeurt feitelijk nooit dat iets een juiste signature heeft, maar toch niet toegelaten is. Anomaly based IDS's gebruiken patronen om abnormaal gedrag te melden. Die patronen zijn nooit perfect dus soms wordt toegelaten gedrag gemeld omdat het gewoon wat vreemd is.

3. Private/public keys are are always better than a password/passphrase
   Antwoord: Fout, met keys kan men niet meer inloggen als men op vakantie gaat en een andere computer gebruikt omdat niemand zich een key herinnert. Daarbij zorgen keys er ook voor dat als 1 systeem gehackt wordt, de andere ook meteen gehackt zijn. Als iemand zich vergeet uit te loggen kan iedereen bv aan de server van systeembeheer.
2. Leg zo veel mogelijk manieren uit om data te sniffen op een switched netwerk, zeg voor elke manier hoe doenbaar het is en hoe dat kan verijdeld worden.
   Antwoord: hier zijn heel veel mogelijke antwoorden op. Ik had er 9 geschreven en hij heeft er tijdens het mondeling zelf nog veel bij verteld toen ik er geen meer wist. Ik had er 4 met ARP spoofing, 1 met een hardware stuk tussen de host en de ethernet poort in de muur, malware installeren bij hosts, fysieke toegang tot de switch, zwak punt in netwerk topologie zoeken en telnetten naar switch en brute forcen. Toen vroeg hij of ik nog voorbeelden van laag 3 van het osi model kon geven aangezien ik er zoveel over laag twee (ARP) had gegeven ma da wist ik ni maar dat was blijkbaar ICMP redirects, valse DNS of DHCP advertisement om gateway te worden van een slachtoffer of meerdere slachtoffers.
3. Een lijst van 5 verschillende bugs in Debian. Rangschik die van erg naar minder erg. Verzin voor elke bug een mogelijk aanvalsscenario en hoe ge dat scenario kunt tegengaan nog voordat de patch uit is.
   1. Interne gebruikers konden code uitvoeren op de printserver via foute printjobs door gebruik van een slechte plugin
   2. Bug in apache waardoor de apache runt als root in plaats van de apache user wanneer een bepaalde waarde niet ingevuld wordt
   3. IMAP server crasht wanneer iemand een rare header stuurt en iemand met een threading plugin opent die mail zodat een aanvallen heel de mail daemon kan doen crashen
   4. DHCP clients met dhcp3 geinstalleerd zijn kwetsbaar voor DHCP boodschappen waardoor de DHCP server code kan uitvoeren bij de client. Een aanvaller kan dit door een rogue DHCP server op te zetten verkeerde input sanitization bij openoffice bij het importen van .lwp objecten. Die worden dus niet door een virusscanner tegengehouden maar kunnen wel code uitvoeren bij de client zodra die dat object importeert. Kheb geschreven dat dat het minst gevaarlijke was omdat een aanvaller toch al goe zijn best ga moeten doen om iemand zo ver te krijgen een '.lwp' bestand in openoffice te importen aangezien de meeste gebruikers hun bureaubladachtergrond niet eens kunnen veranderen en ge ze dan beter gewoon een .exe kunt sturen.
4. Hoofdstuk van het boek lezen. Ik las een van 46 paginas, waarschijnlijk is hij dan blijer dan wanneer ge er een van 16 leest en hij zegt gewoon 'vertel mij is over wa da gaat/wa ge ervan geleerd hebt'.
5. Project: "Vertel mij de problemen die ge ervaren hebt bij het maken van uw project" en "Was het leuk?"
6. Welke tekst vindt gij dat ik volgend jaar moet weglaten of welke vond ge het minst goed en waarom

2013 januari examen

26 Januari 2013

- Orden 5 verschillende aanvallen en leg je ordening uit.
- In een dokterskabinet staat een computer met patientengegevens, geef zoveel mogelijk manieren om deze gegevens te verkrijgen.
- Geef zoveel mogelijk voorbeelden (uit teksten of eigen voorbeelden) van hoe je de integriteit van code/tekst kan bewijzen
- Enkele statements met ja/nee en leg uit
  - Een computer met encryptie kan geen dataverlies hebben (Neen, aanvallen zijn nog mogelijk wanneer de computer uitstaat zoals de keys worden uit het werkgeheugen gehaalt, backdoors,...)
  - Encryptie zorgt voor integriteit (Neen, veel denken dit maar iets dat geencrypteert is zijn maar bytes wanneer integriteit net is dat je zeker bent dat alles er is ofzoiets)
  - Kan een IDS CSRF aanvallen detecteren (Neen, dit kan hij niet)
- Schrijf op de achterkant van dit blad wat je voor project hebt gemaakt, wat je hebt afgegeven en met wie je evt hebt samengewerkt.

Maandag 14 januari 2013

1. In een dokterskabinet staat een computer met patientengegevens, geef zoveel mogelijk manieren om deze gegevens te verkrijgen.
2. Zet de volgende 5 vulnerabilities in volgorde van minst naar meest gevaarlijk en hoe ze op te lossen.
3. Juist/fout:
   1. Voor een DOS aanval heb je meerdere computers nodig.
   2. Een IDS kan CSRF aanvallen detecteren.
   3. Een stuk code met een digitale handtekening moet altijd door de gebruiker handmatig gecontroleerd worden.
4. Geef zoveel mogelijk voorbeelden (uit teksten of eigen voorbeelden) van "Principle of least privilege"
5. Schrijf op de achterkant van dit blad wat je voor project hebt gemaakt, wat je hebt afgegeven en met wie je evt hebt samengewerkt.

Maandag 7 januari 2013

1. Geef zoveel mogelijk mogelijkheden om een website onbereikbaar te maken en zeg erbij hoe de eigenaar zich ertegen kan beschermen. Rangschik de technieken van minst naar

meest moeilijk.bvb:
   1. (D)Dos Voorkomen: Dos kan gedetecteerd worden, DDos is veel moeilijker
   2. Inbreken op webserver en afsluiten. Voorkomen: up to date houden, Firewall, IDS, ..
   3. DNS cache poisoning Voorkomen: DNSSec
   4. ARP poisoning Voorkomen: bvb statische MAC adressen instellen
   5. Fysiek onklaar maken: kabel uittrekken/oversnijden of electriciteit uitzetten. Voorkomen: serverrroom beveiligen en UPS
2. 5 exploits over Microsoft producten die je moet rangschikken op basis van meest belangrijkste eerst oplossen enwat doen als er nog geen patch beschikbaar is:
   1. attacker can execute remote code when user open specially crafted office file with embedded content. -> redelijk erg: kan bvb als attachment binnenkomen.
   2. attacker can execute remote code when user browses to dir with certain subfile/subdir with special name. -> voor interpretatie vatbaar
   3. On a SQLite server, certain custom made FTP packets may reveal information (ongeveer). -> niet zo leuk maar er wordt geen data aangepast
   4. XSS attack on SSRS page, user may elevate privilige mode and execute remote code as target user. -> zeer gevaarlijk. privileges zijn er voor een reden. Bovendien is 'SSRS' de admin pagina (volgens Gerben) dus kan bvb de admin cookie gestolen worden
   5. Remote desktop may execute remote code when certain custom made packets are received. Remote desktop is standard disabled under Windows. -> Hangt van situatie af. gebruikt bedrijf Remote Desktop? oplossen: whitelisting van RD gebruikers
3. juist/fout + uitleg
   1. een proces in een sandbox zonder rechten is nutteloos -> Niet waar, een process hoeft geen gebruik te maken van externe resources. (niet 100% zeker van antwoord, verificatie nodig)
   2. een certificaat dat niet ondertekend is door een CA is niet handig. -> Niet waar, bvb eigen certificaten of vreemde certificaten toevoegen om later MITM te voorkomen
   3. een site waar geen invoervelden zijn daar kan een hacker in het slechtste geval de hele databank op het scherm dumpen. -> Hangt ervan af: welke privileges heeft SQL-server? Stored procedures gebruikt? Welke rechten heeft de user: READ/WRITE/UPDATE?
4. geef zoveel mogelijk voorbeelden van slechte security door gebruikers/gebruiksvriendelijkheid
5. schrijf op de achterkant wat je project was en met wie je eventueel samenwerkte en wat je geüpload hebt. (en dan een paar vraagjes)

2014 augustus examen

1. Geef zo veel mogelijk manieren en rangschik deze van 1-10 (10 is minder haalbaar) om aan een mail te geraken die een concurrent naar een klant stuurde
2. Rangschikking van vijf exploits over Firefox
3. Juist of fout:
    1. Als je je harde schijf encyrpteert geraakt men niet meer aan de data
    2. Iets van dat je alleen aan de gegevens geraakt van de webpagina maar niet van OS via een browser
    3. SQL injecties zijn mogelijk op tabellen die worden gebruikt
    4. Door een extra wachttijd toe te voegen wordt de kans op een bruteforce aanval kleiner
4. Geef voorbeelden uit teksten of eigen voorbeelden of van uit de les van principle of least privelege en defense in depth

2014 januari examen

24 januari 2014

1. Geef zo veel mogelijk manieren om het mail- en webbrowseverkeer van een gebruiker te monitoren en wat je er tegen kan doen
2. Juist of fout:
    1. PIN code en Wachtwoord is een voorbeeld van tweevoudige authenticatie (false)
    2. Een VM is een voorbeeld van een sandbox (juist)
    3. Een plugin die javascript in de URL checkt en die pakketten tegenhoudt, beschermt je tegen XSS (false)
    4. Een algemen foutboodschap (bv "oeps er ging iets mis") is een voorbeeld van security through obscurity
3. Rangschikking van vijf exploits in Windows
4. Verduidelijk de moeilijke relatie tussen security en usability adhv enkele (ze hebben er liefst meer dan 10) voorbeelden
5. Required reading:
    1. Welke tekst vond je het moeilijkst, welk vrij te kiezen hoofdstuk heb je gelezen, ..
    2. Als je zou ontslagen worden, hoe zou je iets maken dat zo veel mogelijk schade berokkent aan je ex-werkgever?
6. Project:
    1. Wat heb je gedaan en hoe kan je voorkomen dat jouw experiment lukt?

20 januari 2014

1. Hoe kan je aan een correcte combinatie gebruikersnaam / paswoord komen, en geef wat er tegen te doen
2. juist of fout
    1. Signature based IDS's have a lower false positive rate than anomaly based IDS's
    2. Een firewall kan een drive by downlaod tegengaan
    3. Een sandbox zonder rechten is nutteloos
    4. Public / private encryptie is nutteloos zonder een CA
3. Rangschikking je kreeg 5 defecten van MCAfee toepassing, rangschik ze en geef een mogelijke oplossing wat er tegen te doen
4. Geef zo veel mogelijk voorbeelden van CIA(Confidentally, Integrety, Availability) uit teksten / eigen voorbeelden
5. Vragen over de required reading, zoals wat vond je goed, welke tekst minder? / enkele vragen over je project

13 januari 2014

1. Hoe kan je aan de gegevens van een laptop uit een dokterspraktijk geraken.
2. Juist of fout
    1. Je kan enkel op iemand zijn account geraken als je zijn wachtwoord steelt of raad
    2. Als je applicatie slechts enkele rechten heeft, moet je je als programmeur geen zorgen maken
    3. Een DoS aanval vergt veel computer of netwerk resources
    4. Cas is niet mogelijk in unsafe talen zoals C
3. Rangschikking
4. Principle of least privilege
5. Teksten en project

2015 januari examen

19 januari 2015 - nm

1. Er bestaat een pop met wifi ... Kinderen kunnen praten met de pop, die via wifi verbinding maakt met een systeem voor spraakherkenning in de cloud. De pop probeert de voorkeuren van haar gesprekspartners te onthouden en downloadt automatisch niruwe updates. Wat zou er kunnen mislopen, en hoe zou iemand met slechte bedoelingen de pop en/of de infrastructuur kunnen misbruiken? Welke verbeteringen zou jij dan aanbrengen?

2. Waar of niet waar. Verklaar je antwoord.

A. Apple-producten verkiezen boven Microsoftproducten omdat er minder virussen zouden zijn is een voorbeeld van security through obscurity

B. Je databank encrypteren voorkomt zogenaamde "data breaches" waaarbij gevoelige gegevens gestolen worden

C. Bij het gebruik van een bankkaart dient de kaart voor authenticatie, en de pincode voor authorisatie.

3. Geef zoveel mogelijk goede/slechte voorbeelden van het "principle of least privilege"

15 januari 2015 - vm

1. Stel dat je zoveel mogelijk spam wilt versturen en het zo moeilijk mogelijk wilt maken voor spamfilters. Geef zo veel mogelijk manieren om dit te doen. Hiernaast geef je telkens een oplossing

2. Waar of niet waar. Verklaar je antwoord.

A. Manier waarop permissions toegekend worden aan Android, is least privilege principe goed?

B. Xss issue geeft enkel problemen op de client,niet op de server.

C. Botnets worden enkl gebruikt voor DDOS.

3. Geef zoveel mogelijk voorbeelden van "security through obscurity"

4. Rangschik de security advisors volgens hun ernst

5. Project uitleggen

8 januari 2015 - namiddag

1. Mensen spelen wel eens een USB of laptop kwijt, en hun data kan zo in ongewenste handen terecht komen.Geef een aantal opties om dit probleem op te lossen en bijhorende voor- en nadelen.
2. Rangschikking van vijf router (residential) exploits
3. Juist of fout:
    1. SQL injecties zijn uitsluitend mogelijk via slecht ontworpen webformulieren/webpagina's
    2. Vingerafdruksystemen van de politie moeten een lagere false match rate hebben dan één die toegang geeft tot je smartphone
    3. Als je het slachtoffer bent van een DDoS aanval, kan je niets doen dan wahcten tot het voorbij is
4. Geef voorbeelden uit teksten of eigen voorbeelden of van uit de les van defense in depth
5. Licht je project toe

8 januari 2015 - Voormiddag

1. Wifi plug om electronica van op afstand te besturen (licht aan/uit). Hoe beveiligen en wat zijn de risico's?
2. Juist of fout:
    1. Backup's verminderen het risico van SQL Injecties. (Juist : Risico = kans * potentiële schade)
    2. Een trage encryptie-methode maakt het moeilijker paswoorden te vinden
    3. Voor een DoS aanval te kunnen uitvoeren heb je steeds een hoge bandbreedte nodig
3. Rangschikking van 5 exploits op VM ware.
4. Principle of least privilege aantonen met voorbeelden uit de les, documenten, ...
5. Licht je project toe

2016 januari examen

1. Geef aan zo veel manieren waarop je (een deel van) de klantenlijst van je concurrent zou kunnen stelen en hoe dat de concurrent je zou kunnen tegenhouden.
2. Order 5 problemen op de niveau van ernstigheid.
3. 1. Kan de firewall je beveiligen tegen XSRF? Leg uit.
   2. Is een wachtwoord veiliger dan biometrics?
   3. Geef zo veel mogelijke voorbeelden van security through obscurity.
4. Kan de risico van schade van een ransomware verminderd worden door een backup van je gegevens te maken of zoiets.
5. Bespreking project
6. vraag over welk hoofdstuk dat je gelezen hebt.

2019 januari examen

1. Order 4 problemen op de niveau van ernstigheid.

A. Cross-site scripting (XSS) vulnerability in the management interface for VMware ESX 2.5.x before 2.5.2 upgrade patch 2, 2.1.x before 2.1.2 upgrade patch 6, and 2.0.x
before 2.0.1 upgrade patch 6 allows remote attackers to inject arbitrary web script or HTML via messages that are not sanitized when viewing syslog log files.
CVE-2005-3619

B. The default configuration of VMware Workstation 6.0.2, VMware Player 2.0.x before 2.0.3, and VMware ACE 2.0.x before 2.0.1 makes the console of the guest OS accessible
through anonymous VIX API calls, which has unknown impact and attack vectors.
CVE-2008-1392

C. VMware Workstation 8.x before 8.0.2, VMware Player 4.x before 4.0.2, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 use an
incorrect ACL for the VMware Tools folder, which allows guest OS users to gain guest OS privileges via unspecified vectors.
CVE-2012-1518

D. Airwatch Agent for Android contains a vulnerability that may allow a device to bypass root detection. Successful exploitation of this issue may result in an enrolled
device having unrestricted access over local Airwatch security controls and data.
CVE-2017-4895

=> A < C < D < B

2. Attack Tree: Geef zo veel mogelijk manieren waarop je de klantenlijst van een bedrijf op de cloud kunt stelen.

3. Geef min. 6 voorbeelden uit teksten of eigen voorbeelden of van uit de les van multilevel/defense in depth

4. Bespreking project

5. Vraag over welk hoofdstuk dat je gelezen hebt.

2022 januari examen

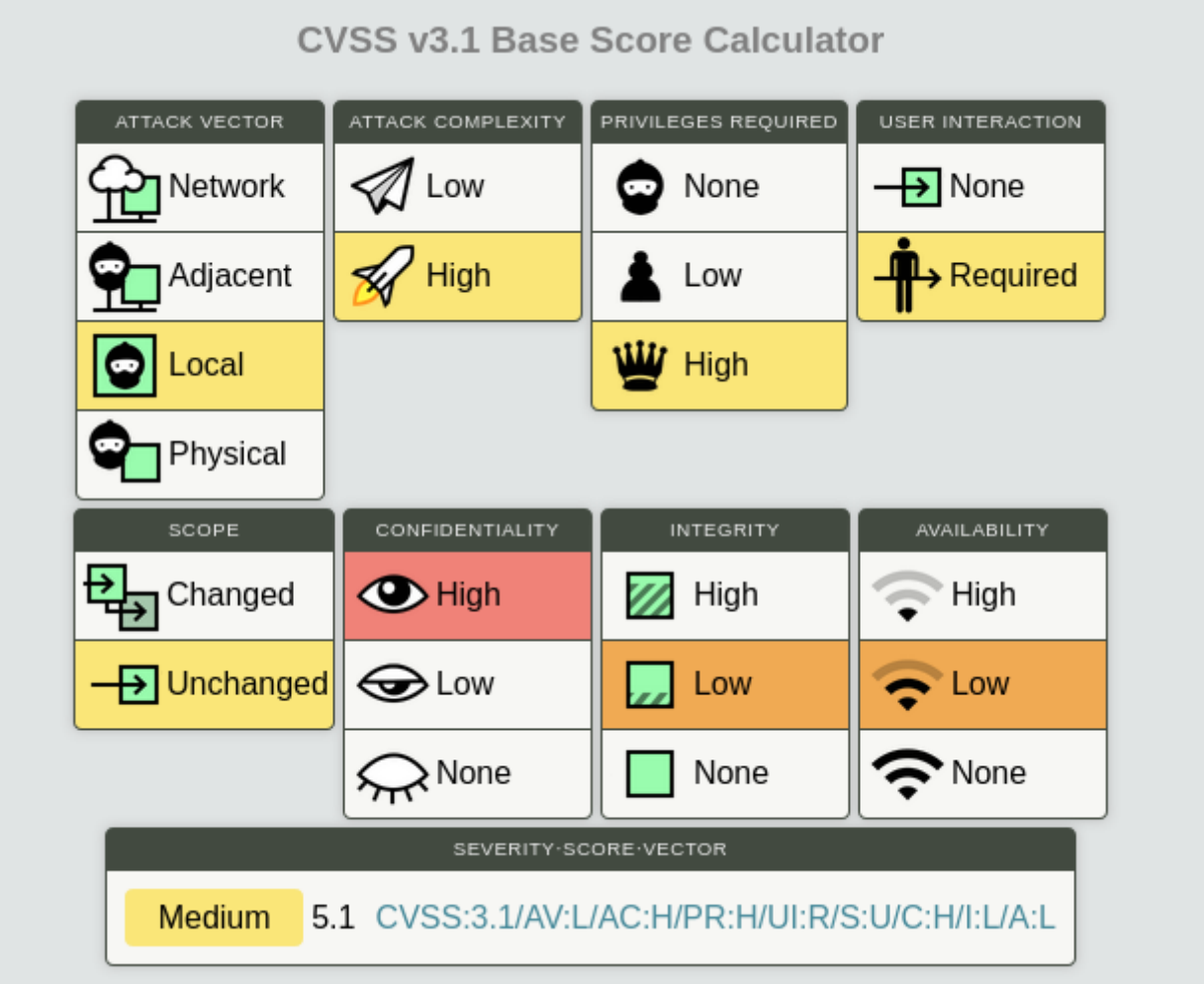
Het examen is open boek je kan dus alle PowerPoints en documenten van op Toledo gebruiken. Daarnaast is het ook nog een mondeling examen.

Vraag 1:

Je krijgt een aantal CVE's en jij moet de CVSS maken. Je kreeg een tabel waarin je elke eigenschap moet invullen. Zie hier een random voorbeeld. Bovenaan is de naam zoals *Attack Vector*, ...

AV	AC	PR	UI	S	C	I	A
L	H	H	R	U	H	L	L

Is het zelfde als dit:



Vraag 2:

Je moest een attack tree maken.

Vraag 3:

Een aantal stellingen waarbij je moest zeggen of die juist of fout waren.

Vraag 4:

Je moest van een principe een aantal voorbeelden geven. Bv "least privileged" of waar beveiligen ongemakkelijk zijn maar toch veel helpen met security.

Vraag 5:

Ging over de security tool PE-opdracht.