

# 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 nog altijd 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) authenticceert 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 geïnstalleerd 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

