Les 5. Security

V1.0

ROC Horizon College

HORIZONCOLLEGE.NL ALKMAAR | HEERHUGOWAARD | HOORN | PURMEREND

HORIZON COLLEGE

Samen werk maken van je opleiding

Vandaag?

1. Vorige week Netwerkscan/gastspreker?
2. Waar doen wij het voor? “Het Examen”
3. Tools Windows in het examen? opdracht maken (ZenMap, Sysinternals, MBSA)
4. Status groepen?
5. Certificering!

Vorige week Netwerkscan/gastspreker?

Zenmap VS Nmap?!

Poorten

Poorten en poortnummers

Een poort is de in- of uitgang waarmee een computer of netwerk communiceert met de buitenwereld. In het kader van beveiliging is het noodzakelijk te weten dat uw PC's en netwerk communiceren met de buitenwereld via deze zogeheten 'poorten'.

Het poortnummer wordt door het netwerk gebruikt om te bepalen voor welk van de diensten data bestemd is. De poortnummers van uw netwerk zijn essentieel om u te verbinden met online diensten en websites.

Welke poorten zijn er en hoe kan je zien wat er aan dataverkeer in- en uitgaat via deze poorten?

Een overzicht van de meest bekende poorten:

- Poortnummer 70: Gopher
- Poortnummer 79: Finger
- Poortnummer 80: Hyper Text Transfer Protocol (http)
- Poortnummer 110: Post Office Protocol 3 (POP3)
- Poortnummer 119: Netwerk News Transfer Protocol (NNTP)
- Poort443 voor HTTPS,
- Poort20 en 21 voor FTP,
- Poort 22 voor SSH,
- Poort 25 voor SMTP, en anderen.
- Poorten vanaf 1024 zijn in de regel niet gereserveerd, en dus vrij te gebruiken.

Meerdere communicatie lijnen

Poorten en poortnummers zijn een essentieel onderdeel van de internetcommunicatie (TCP/UDP) tussen pc's. Poorten maken het mogelijk dat een pc meerdere communicatielijnen tegelijkertijd kan gebruiken. In dit artikel gaan we in op de belangrijkste poorten van je pc en hun specifieke functie.

In het kader van beveiliging van je pc is er een onderverdeling te maken tussen 'goede en slechte' programma's. De makers van slechte software (die onrechtmatig gebruik willen maken van de poorten op je pc) kunnen er immers kwade bedoelingen mee hebben. Je firewall maakt hen dat onmogelijk. Jouw poortnummers helpen bij het inrichten van firewalls en het geven van bepaalde rechten aan apps. Een pakketfilter-firewall leest het poortnummer uit van de afzender en de geadresseerde. Op basis van deze poortnummers reageert de firewall met het al dan niet actief maken van een firewall-beleidsregel. Om firewalls optimaal te kunnen configureren is enige basiskennis van poorten dan ook nodig.

- **Tool 1 - NetStat toont ingebruik zijnde poorten**

- Om te weten welke poorten actief zijn op je pc kun je gebruik maken van het commando netstat dat in Windows is ingebouwd. Het programma biedt weliswaar niet zeer veel opties maar kan toch een aardig beeld geven welke poorten open staan wanneer je met de pc werkt:

1. Kies **Start >> Uitvoeren**.
2. Typ **cmd** en druk op **Enter**.
3. In het geopende DOS-venster typ je achter de commandoprompt:

   C> netstat

Tool 2 - NbtStat toont de naamtabellen

Een andere ingebouwde Windows netwerkanalyse-tool is NbtStat. Dit programma start je op dezelfde manier als NetStat, dus ook via de command prompt. Het programma toont de protocolstatistieken van NetBIOS, zoals dat via TCP/IP (NetBT) wordt gebruikt. Zo zie je de naamtabellen van NetBIOS voor zowel de lokale pc als voor de remote computer en wordt ook de naamcache getoond van NetBIOS. Verder kan NbtStat deze naamcache opschonen.

Je ziet nu een venster zoals hierboven afgebeeld. NetStat toont een lijst van alle inbound en alle outbound netwerkconnecties, inclusief alle informatie van openstaande TCP- en UDP-poorten, IP-adressen en de status van een connectie. Het programma kent een aantal parameters. Om meer essentiëlere informatie uit NetStat te kunnen destilleren heb je deze parameters beslist nodig. Een overzicht van deze parameters kun je opvragen terwijl je werkt met NetStat door te typen:

NBtstat /?

Tool 3 - Essential nettools als Zwitsers legermes

http://www.tamos.com/download/main/

Het shareware-circuit biedt een aantal interessante programma's. Een van die programma's is Essential NetTools dat je kunt downloaden van Tamos (externe Engelstalige site). Het gaat hier om een set netwerk-tools om je netwerk te diagnosticeren. Helaas is het pakket niet in het Nederlands verkrijgbaar, maar uiteraard wel in het Engels. Het is het beste te vergelijken met een Zwitsers legermes en biedt talloze opties en mogelijkheden:

- **NetStat**
  Vergelijkbaar met de gelijknamige tool van Windows XP en Windows 2000. De Essential NetTools- versie kan ook aangeven welke applicatie de eigenaar is van een bepaalde verbinding.

- **NBScan**
  Dit is een krachtige en snelle NetBIOS-scanner. NBScan scant een netwerk binnen een bepaalde IP-range en geeft een lijst van de computers die NetBIOS en shares aanbieden. Daarnaast toont de utility de naamtabellen en MAC-adressen. Het is vergelijkbaar met de Microsoft-tool NbtStat, maar dan met een grafische gebruikersinterface. Hierdoor is het gebruikersvriendelijk. Een interessante optie is het parallel scannen: hierdoor kun je een netwerk in minder dan een minuut scannen.

- **PoortScanner**
  Dit is een TCP-poortscanner die het netwerk afzoekt naar actieve poorten. Je kunt zoeken naar poorten die een volledige connectie toestaan (conventionele poorten) of poorten die maar voor de helft open staan (stealth).

- **Shares**
  Het programma Shares verzorgt het monitoren en bijhouden van externe connecties naar de gedeelde bronnen van je computer. De optie toont lokale shares en biedt hulp bij het contact leggen met externe bronnen.

- **SysFiles**
  SysFiles is een eenvoudige editor voor de vijf belangrijkste systeembestanden: services, protocollen, netwerken, hosts en lmhosts.

- **NetAudit (NetBIOS Auditing Tool)**
  Deze tool kan je helpen om potentiële beveiligingslekken op te sporen.

- **RawSocket**
  Deze tool biedt je de mogelijkheid om een low-level TCP- and UDP-connectie op te zetten en zo de verschillende netwerk services te testen.

- **TraceRoute en Ping**
  Een handige utility om verbindingsproblemen te analyseren en op te lossen.

- **NSLookup**
  Een conversie-tool voor IP-adressen naar hostnamen en vice versa, het verkrijgen van aliassen, en het uitvoeren van geavanceerde DNS-queries zoals MX of CNAME.

- **ProcMon**
  Dit is wellicht het meest interessante onderdeel van de toolset. ProcMon toont alle actieve programma's met volledige informatie over de locatie van het programma, de leverancier, het ID van het proces en de actieve modules. Met ProcMon kun je verborgen applicaties ontdekken en ongewenste processen afsluiten, waardoor je de beschikbare bronnen van je pc beter kunt beheren.

ROC Horizon College

Barry P. · 1ste

alliander

Manager CISO Office Cyber Resilience Center | GSTRT GSOM CISSP

Waar doen wij het voor? “Het Examen”

P2-K2 Controleert de security

W1 Geeft security advies en verbetert

- Securityscans uitvoeren
- Analyse van de resultaten
- Verslag van de analyse

W2 Reageert op security incidenten

- Datalek vanuit de databaseserver
- Onderzoeksverslag

ROC Horizon College

HORIZON COLLEGE

Samen werk maken
van je opleiding

Status Groepen

39 studenten uit de3 A B klassen

7 groepjes van 5

1 groepje van 4

Beerepoot!!!

8-11