

AUDIT REPORT

Company:

Pokemon LAN

Author:

Dauwe Matice

Disclaimer:

This pentest/network scan was provided in order of Howest Bruges. In no other case is it permitted to apply the following techniques to the company of 'pokemon lan'.

Table of Contents

Introduction 3

Summary 4

- Weak passwords 5
  - Risk(s) 5
  - Pentest 5
  - Prevention/suggestion(s) 5
- Remote Code Execution 6
  - Risk(s) 6
  - Pentest 6
  - Suggestions/prevention 7
- Command injection 8
  - Risk(s) 8
  - Pentest 8
  - Prevention/suggestions 8
- Vulnerable/outdated software 9
  - Risk(s) 9
  - Introduction 9
  - Pentest 9
  - Prevention/suggestions 9
- Pentesting Postgres 11
  - Risk(s) 11
  - Introduction 11
  - Pentest 11
  - Prevention/suggestions 11
- Zone transfer attack 13
  - Risk(s) 13
  - Pentest 13
  - Prevention: 13
- SMB Pentesting 14
  - Risk(s): 14
  - Introduction: 14
  - Pentest 14
  - Prevention/suggestions: 15

Conclusion 16

Introduction

We voerden als bedrijf een netwerk/system scan uit op voor het Pokemon bedrijf. We startten met het scannen van het netwerk. Zo beslissen we de scope van het onderzoek en zien we welke machines/computers er in eerste instantie op het netwerk aanwezig zijn. We kregen een dynamisch IP adres wat wijst op het feit dat er een DNS server draait op het netwerk. We berekenden de netwerkgegevens zoals 'subnet mask' en 'broadcast adress' om zo enkel op de eerste 100 IP adressen te scannen. We vinden 6 systemen op het netwerk inclusief onze eigen geconnecteerde machine. We zien direct al enkele hardware verkopers(VMware, HP, Dell) van bepaalde machines in het netwerk.

Vervolgens voerden we verschillende pentests uit en paste we bepaalde technieken toe om het netwerk en systeem te testen. We rangschikken de gevonden gegevens op basis van hun kwetsbaarheid. Zo komen de meest 'critical' pentests eerst aan bod. Hierop wordt voornamelijk de aandacht gelegd. Deze kwetsbaarheden moeten zo snel mogelijk aangepast worden om (verdere) toekomstige gegevensverliezen (data losses) te beperken/vermijden.

Verder vonden we ook nog minder kwetsbare gegevens. Deze hebben dan ook een ander label gekregen. Dit kan van 'medium' tot 'low' dringendheid gaan. Uiteindelijk is het wel de bedoeling dat alle kwetsbaarheden aangepast/gewijzigd worden. Per kwetsbaarheid worden door ons tips/suggesties meegegeven om dit te vermijden. Er zijn natuurlijk nog andere mogelijkheden, maar we hebben telkens de meest logische preventiemethodes genoteerd.

*Disclaimer: We hebben confidentiële gegevens zoals expliciete wachtwoorden, usernames vermeden in dit report. Op deze manier blijft bepaalde informatie binnen de bedrijfsmuren.

Summary

CRITICAL	HIGH	MEDIUM	LOW
2	3	1	1

We voorzien elke gevonden kwetsbaarheid van een label. Critical dient zo snel mogelijk opgelost te worden terwijl 'low' het systeem/netwerk minder kwetsbaar openstelt.

We voorzien de kwetsbaarheden ook van een 'risk score'. Deze geeft ook nog een duidelijk beeld van hoe kwetsbaar het gegeven is voor het systeem.

!Critical! :

1- Weak passwords
2- Remote code execution

High:

3- Command injection
4- Outdated software
5- Postgres injection

Medium:

6- Zone transfer attack

Low:

7- SMB pentesting

CRITICAL

Weak passwords

Risk(s)

Ongeoorloofde toegang tot een systeem.
Volledige besturing van het domein en/of alle systemen

Pentest

Tijdens de 'remote code execution' pentest stootten we op een zéér opmerkelijke kwetsbaarheid. We vonden namelijk een lijst met alle 'domain controllers' en ook een lijst met alle users van de computer in kwestie.

We probeerden remote op de 'Porygon' machine (192.168.*.10) in te loggen met een van de users. Als wachtwoord maakten we gebruik van diezelfde gebruikersnaam. Met 1 van de users kregen we op deze manier toegang tot de machine. Zo probeerden we ook op andere machines fysiek met deze user gegevens in te loggen. Met succes hadden we op deze manier toegang tot elke computer binnen het 'pokemon' bedrijf.

We verkregen op simpele wijze toegang tot het account van de systeem/domeinbeheerder. Als aanvaller/hacker heb je nu volledige kracht over het systeem. Dit is de grootste kwetsbaarheid die je als bedrijf kan ondergaan. Alle gegevens en/of gebruikers kunnen nu beperkt en/of verwijderd worden in het syteem.

Prevention/suggestion(s)

- Stel een wachtwoordpolicy op

  Stel als bedrijf een duidelijke regelgeving in verband met wachtwoorden op. Voeg zo bijvoorbeeld een minimumlengte en bepaalde complexiteit (implementeren van tekens zoals @ , _) toe. Op die manier vermijdt u als bedrijf het gebruik van makkelijk voorspelbare wachtwoorden. Een moeilijk te kraken wachtwoord biedt een gevoel van zekerheid.

- Invoegen van Tweestapsverificatie op computers binnen het bedrijf/netwerk

  Met Tweestapsverificatie bent u als gebruiker voorzien van een extra beveiliging laag. Indien het wachtwoord op een of andere manier toch geraden wordt, dient er nog altijd een tweede verificatiemethode ingegeven te worden.

  Tweestapsverificatie is eenvoudig te installeren door de domein/systeembeheerder op elke computer van het netwerk.

CRITICAL

Remote Code Execution

Risk(s)

Verspreiden van malware over het systeem.
Volledige controle over het syteem
Gegevensexploitatie

Pentest

In deze scan voerden we een script uit op het ‘alakazam’ systeem(192.168.**.60). Het script ging voor ons op zoek naar verouderde besturingsmodellen(os). Zo kwam we er uiteindelijk op uit dat de machine nog op ‘windows 7 Enterprise 6.1’ draait. Dit is een zeer verouderde versie als je weet dat er ondertussen al reeds 6 nieuwere modellen uitkwamen. Om gegevensverlies te vermijden, is er dus dringend een systeemupdate voor het ‘alakazam’ systeem noodzakelijk.

```
Host script results:
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Charmander
|   NetBIOS computer name: CHARMANDER\x00
|   Domain name: pokemon.lan
|   Forest name: pokemon.lan
|   FQDN: Charmander.pokemon.lan
|_  System time: 2023-06-13T20:27:36+02:00
```

Er zijn namelijk al reeds bekende kwetsbaarheden gevonden op dergelijke machineversies. ‘Eternal blue’ is hiervan een goed voorbeeld. Dit type kwetsbaarheid zorgde er in 2017 voor dat meer dan 100 000 computers werden geïnfecteerd met ransomware.

Ook hiervoor voerden we een scan uit. Nu bleek dat het systeem (Alakazam) dus ook kwetsbaar is voor ‘remote code execution’. Dit is een zeer hoge kwetsbaarheid. Aanvallers kunnen indien ze binnenraken, bijna het volledige systeem besturen. Dit dient dus ten allen tijden vermeden worden!

Via deze kwetsbaarheid kwamen wij ook binnen op het systeem. Al snel lijstten we alle gebruikers op.

```
 Directory of C:\Users

10/03/2023  15:00    <DIR>          .
10/03/2023  15:00    <DIR>          ..
14/03/2023  14:00    <DIR>          Administrator
01/03/2023  11:59    <DIR>          a
10/03/2023  15:00    <DIR>
01/03/2023  17:40    <DIR>
01/03/2023  12:00    <DIR>
14/07/2009  09:23    <DIR>
17/08/2017  15:36    <DIR>          User
               0 File(s)              0 bytes
```

Daarnaast vonden we ook alle domain control accounts met het commando ‘net user /domain’.

We kunnen hiermee dus praktisch alle gegevens/info over het domein ‘pokemon’ vinden. Dit is een zeer ernstige kwetsbaarheid!

Suggestions/prevention

- Update het systeem naar 1 van de laatste 2 nieuwste versies

  Nieuwe updates zorgen niet alleen voor een verbetering aan functionaliteiten op een systeem, maar ook voor extra beveiligingsmaatregelen. Het besturingssysteem dat nu gebruikt wordt, is zodanig verouderd dat er geen enkele garantie op een beveiligd systeem kan worden gegeven.

- Voorzie betere authenticatie op het ‘Alakazam‘ systeem

  Zorg er als bedrijf voor dat niet elke aanvaller toegang heeft tot systeeminformatie. Voorzie enkel voor geautoriseerde gebruikers zoals de systeembeheerder toegang tot deze informatie. Implementeer een extra authenticatie laag om te verzekeren dat enkel vertrouwde personen toegang hebben tot gevoelige gegevens en/of de machine/computer zelf.

HIGH

Command injection

Risk(s)

De aanvaller kan zo goed als alles doen op het verkregen systeem. Daarnaast kan er ook volledige controle verkregen worden.

Pentest

Wanneer we het volledige systeem scannen op de open netwerkpoorten, vinden we al snel een verdachte poort. Binnen de visie van het bedrijf is het redelijk vaag dat er op netwerk poort 25565, een service genaamd ‘minecraft?’ te vinden is. Vervolgens surften we naar het ip addess van desbetreffende machine(192.168.*.23) op poort 25565. Hier vonden we een ‘command line interface’ waarin we allerlei commando’s konden uitvoeren.



Prevention/suggestions

- Verwijder/sluit onnodige poorten op het systeem. Indien er geen gebruik meer wordt gemaakt van een poort, sluit deze connectie dan. Achterliggende open poorten zijn vaak de oorzaak van een datalek.

- ‘whitelisting’

  Dit is een term die alleen toegestane commando’s en invoer definieert. Dat wil zeggen dat de user enkel die bepaalde commando’s zal kunnen uitvoeren. Op deze manier is het systeem meer beveiligd tegen input die het systeem zou kunnen kapotmaken.

- Beperken van permissies voor gebruikers op het systeem

  Gebruikers hebben grotendeels niet alle rechten nodig. Voorzie deze daarom enkel van ‘read right’. Deze staat hun toe om de file/directory te kunnen lezen, maar niet te laten aanpassen of exporteren. Indien een user bijvoorbeeld niet meer in zijn account kan, zou het systeem alvast niet in gevaar mogen zijn door de weinige privileges van de user.

HIGH

Vulnerable/outdated software

Risk(s)

Verkrijgen van public en/of private keys van gebruikers. Met deze keys kan je digitale handtekeningen maken. Daarnaast kunnen deze sleutels ook als authenticatiemechanisme tot een systeem dienen. De combinatie van de 2 sleutels kan de identiteit van een gebruiker namelijk bevestigen.

Introduction

Verouderde software heeft als gevolg dat deze bepaalde kwetsbaarheden met zich meebrengt. Zo kwamen we snel te weten dat er op de machine 'alakazam' (192.168.*.60) een verouderde versie van 'elasticsearch' draait. Dit is software die gebruikt wordt voor het monitoren van grote hoeveelheden data. Doordat versie 1.1.1 nog op dit systeem draait, konden we allerlei gevoelige informatie vinden.

Pentest

We startten 'metasploit'. Dit is een tool waarin kwetsbaarheden van bepaalde systemen zichtbaar zijn. Zo vonden we voor versie 1.1.1 van elasticsearch een module. Uiteindelijk komen we op het punt dat er commando's kunnen worden ingegeven. We kunnen een nieuwe 'shell' aanmaken. Dit is een soort van sessie waarin we op het systeem(alakazam) allerlei commando's kunnen uitvoeren. Zo hadden we eigenlijk toegang tot de files van gebruiker 'ash'.

```
ls -al
total 36
drwxr-xr-x 5 ash  ash  4096 Mar 14 15:25 .
drwxr-xr-x 3 root root 4096 Mar 10 14:12 ..
-rw------- 1 ash  ash     5 Mar 14 15:25 .bash_history
-rw-r--r-- 1 ash  ash   220 Feb 24 11:27 .bash_logout
-rw-r--r-- 1 ash  ash  3526 Feb 24 11:27 .bashrc
drwxr-xr-x 3 ash  ash  4096 Feb 24 21:31 .local
-rw-r--r-- 1 ash  ash   807 Feb 24 11:27 .profile
drwx--r-- 2 ash  ash  4096 Mar  6 12:25 .ssh
drwxr-xr-x 2 ash  ash  4096 Mar 14 11:42 www
```

We kwamen dus in bezit van zowel de public als private key van de gebruiker 'ash'. Met de private key kunnen we zonder verkregen wachtwoord inloggen op het 'alakazam' systeem(192.168.*.60).

Prevention/suggestions

- Verwijder ongebruikte software

  Oude en niet-ondersteunde kan reeds bekende kwetsbaarheden bevatten die niet meer worden opgelost. Als bedrijf loopt u hier dus een onnodig risico.

- Organiseren van geplande, regelmatige software-updates

Dit soort updates zullen het systeem voorzien van de nieuwste beveiligingsmaatregelen. Software updates bevatten meestal 'bugfixes', die ervoor zorgen dat kwetsbaarheden uit vorige softwareversies, in deze versie niet meer voorkomen. Het is dus als bedrijf belangrijk om binnen een bepaalde tijdspanne zo'n software-update te laten uitvoeren. Software is iets dat constant zal evolueren. Vandaar dat u deze updates ook op regelmatige basis moet uitvoeren.

- Beperken van rechten op u systeem

  Als bedrijf is het aanbevolen om gebruikers niet te veel rechten toe te kennen. In dit geval konden we als aanvaller, door de verkeerd ingestelde rechten('read access for others'), de inhoud van de persoonlijke folder van een gebruiker bekijken. Rechten op bepaalde folders en bestanden dienen dus in vraag gesteld te worden door de systeembeheerder(s) van uw bedrijf.

HIGH

Pentesting Postgres

Risk(s)

Toegang tot de database. Wachtwoorden van gebruikers kunnen gekraakt worden. Eveneens kunnen gegevens verwijderd/aangepast worden.

Introduction

Postgresql is een 'object gerelateerde database systeem' die gebruikt maakt van SQL taal (= taal die gebruikt wordt voor het opstellen en aanpassen van databases) . Vaak kunnen dergelijke services makkelijk slachtoffer worden van een 'brute force' attack(=vele combinatiemogelijkheden op korte tijd zorgen er zo voor dat de server de juiste en/of alle waarden van de database zal teruggeven). Indien er zo'n waarde verschijnt, zal er hoogstwaarschijnlijk toegang tot het systeem aan verbonden zijn. Vandaar dus het grote gevaar.

Pentest

Allereerst voeren we een scan uit op de open poorten van de machine(192.168.*.60). Op poort 5432 draait een postgresql service. De default user van postgres is 'postgres'. Aan de hand van de hydra tool en 'pokemon.lst' die alle namen van gen1 pokemons bevat, gaan we nu een bruto force doen op die machine.
Uiteindelijk krijgen we een response waarin een wachtwoord(*****) te vinden is. Hierna startten we een postgres sessie.

Met de juiste postgres notatie komen we zo 2 users en hun wachtwoord(versleuteld) te weten.
Met de cracking tool 'hashcat' zien welke hash(encryptie) er gebruikt is. Uiteindelijk vinden we dus ook het wachtwoord *****) van gebruiker 'Brock'.

*het aantal sterretjes representeert niet het aantal karakters van het wachtwoord

Prevention/suggestions

- Monitoren van de database

  Implementeren van een logboek kan het opmerken van verdachte activiteiten versnellen/verduidelijken. Er kunnen zo bijvoorbeeld waarschuwingen gegeven worden indien er verdachte zaken zouden opduiken in de logbestanden.

- Regelmatig pentesten van de database

  Een pentest stelt uw bedrijf telkens op de hoogte van eventuele nieuwe kwetsbaarheden. Op die manier kunt u proactief te werk gaan en potentiële risico's uitsluiten.

- Implementeren van back-ups

Indien er gegevensverlies is opgetreden, bent u ervan verzekerd dat de gegevens niet verloren zijn gegaan. Kies hiervoor een veilige locatie, liefst zowel online als offline(fysieke locatie).

MEDIUM

Zone transfer attack

Risk(s)

- Verspreiding van interne netwerkinformatie
- DoS-aanvallen (grote hoeveelheden netwerkverkeer genereren op de zwakke plekken van een dns server). Kan leiden tot een platliggend DNS-systeem.

Pentest

Met “Dig axfr pokemon.lan 192.168.*.4” komen we te weten dat de dns machine (192.168.*.4) kwetsbaar is voor een ***zone transfer attack.***

Met toegang tot de DNS-zonegegevens kunnen er bijvoorbeeld ip-adressen gewijzigd worden. Dit houdt in dat er dan internetverkeerd naar valse websites/serves kan verstuurd worden. Met als gevolg dat er malware en phishing kan verspreid worden. Deze criminele feiten kunnen dan op hun beurt terug leiden tot het lekken van klantengegevens en/of schade aan de computers van klanten. Dit wil u als bedrijf natuurlijk te allen tijde vermijden.

Prevention:

- Beperk zone transfers: Configureer de DNS-server zodanig dat deze alleen zone transfers toestaat naar geautoriseerde DNS-servers. Hierdoor wordt voorkomen dat onbevoegde servers of aanvallers toegang krijgen tot de DNS-zonegegevens. Beperk de lijst met toegestane IP-adressen of domeinen voor zone transfers. Dit kan bijvoorbeeld door het implementeren van een ACL (acces control list). Zo bepaal je als bedrijf zelf welke gemachtigde IP-adressen toegang hebben tot deze zone transfers.

- Daarnaast stel je best een firewall in om verkeerd van en naar de DNS-server te blokkeren. Selecteer alleen de vereiste poorten (tcp poort 53) en protocollen.

- Tot slot verwijder je best onnodige en verouderde records van de DNS zone. Vermeld enkel wat essentieel is voor de nodige werking van het domein.

Dit zijn slechts enkele maatregelen die u als bedrijf kan treffen om de DNS-infrastructuur te versterken en de kans op een zone transfer aanval te verkleinen.

LOW

SMB Pentesting

Risk(s):

Documenten/gevoelige gegevens exporteren naar persoonlijke computers/machines.
Info over verouderde machines vinden om later verdachte acties op te kunnen uitvoeren.

Introduction:

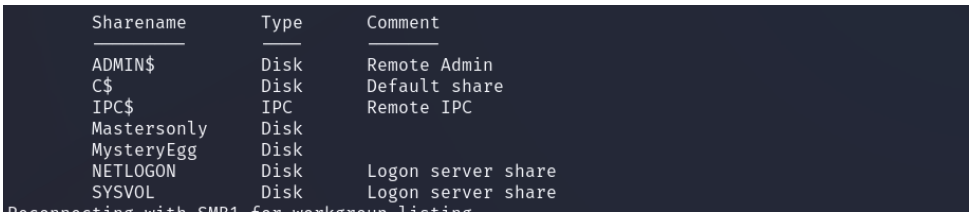
Met deze scan/pentest testen we de beveiliging van een systeem dat gebruik maakt van het SMB-protocol(Server Message Block). SMB wordt gebruikt voor het delen van bestanden, printers, poorten.. tussen computers in eenzelfde netwerk. SMB draait op poort 139(oudere versie) en 445. Daarom voeren we een scan uit op alle IP adressen van ons (pokemon) netwerk en zoeken we voor de open tcp poorten.

Pentest

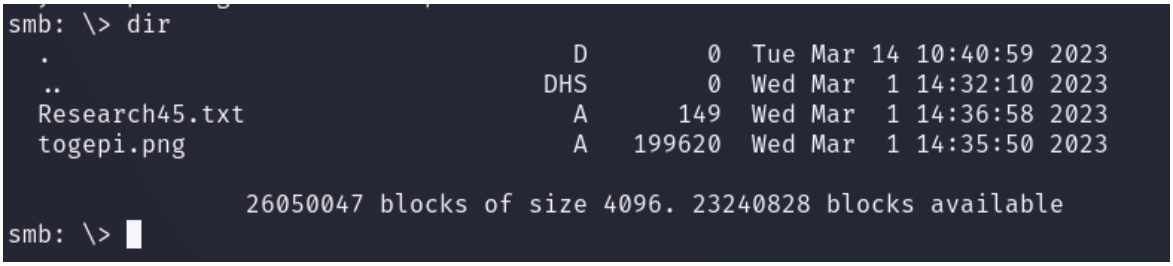
We voeren onderstaand commando uit op het volledige pokemon netwerk. We zoeken voor open SMB poorten met poortnummers 139 en 445.

Als snel zien we dat er 2 poorten open staan. Vervolgens maken we gebruik van de tool ‘smbclient’. Met deze tool proberen we toegang te krijgen gedeelde bronnen/gegevens op SMB servers.

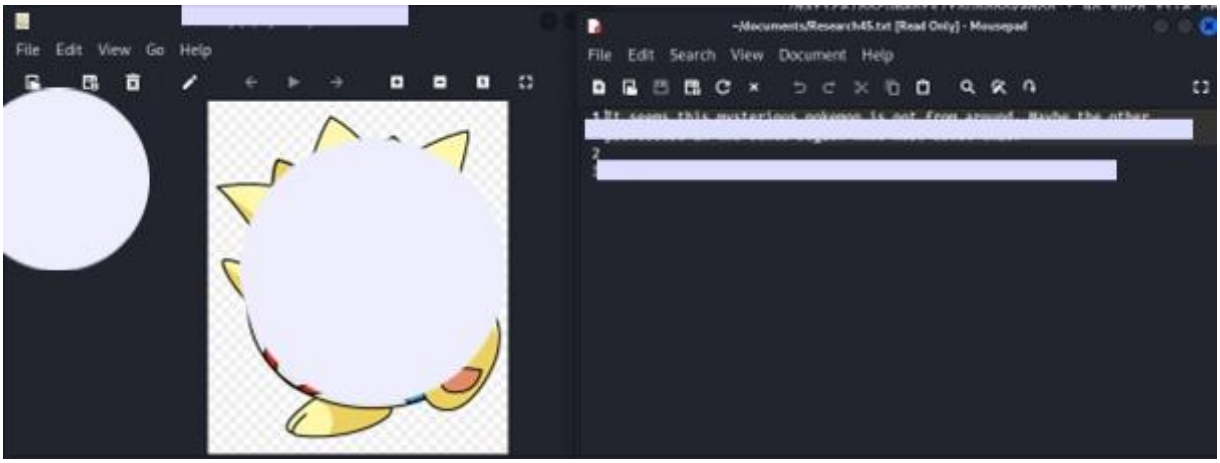
“smbclient -L \\192.168.*.4\\” toont ons een lijst met alle gedeelde gegevens(fileshares) en domain controllers. We hoefden in dit geval niet eens een passwoord mee te geven. Op enter duwen volstond om deze gegevens te kunnen zien.



In dit geval lijkt “MysteryEgg” het meest interessant. Om vervolgens in de ‘MysteryEgg’ disk binnen te raken maakten we terug gebruik van onze ‘smbclient’ tool.



We zitten nu op de disk en kunnen met een simpel commando als ‘dir’ of ‘ls’ alle files in verschillende directories oplijsten. We kunnen tijdens een smb-sessie geen documenten zomaar bekijken. Daarvoor exporteren we de gevoelige informatie naar onze persoonlijke computer.
We komen uiteindelijk uit op volgende gevoelige informatie:



Prevention/suggestions:

- Regelmatig uitvoeren van updates/patches
  Op die manier bent u, als bedrijf zijnde, zeker dat uw machines/computers van de laatste beveiligingsmaatregelen zijn voorzien.

- Toevoegen van authenticatiemechanismen
  Zorg ervoor dat u als bedrijf een sterke wachtwoordpolicy heeft opgezet. Een goed wachtwoord is namelijk moeilijk te kraken en zorgt ervoor dat indringers niet zomaar aan de gegevens van een folder kunnen. Het is ook aan te raden om regelmatig alle wachtwoorden te wijzigen.

  MFA (multifactor-authenticatie) kan in sommige systemen ook een mogelijkheid zijn. Zo implementeert u als bedrijf een extra authenticatielaag.

- Firewall configuratie aanpassen.
  Als bedrijf kan u de SMB-diensten enkel toegankelijk maken voor specifieke IP adressen en netwerken. Verder is het ook interessant om ‘ongeautoriseerd verkeer’ naar SMB-poorten (139, 445) te blokkeren.

Conclusion

We kunnen concluderen dat er zich in het systeem redelijk wat kwetsbaarheden bevonden. Iedere gevonden kwetsbaarheid werd gerangschikt volgens prioriteit. Zo kregen ‘Weak passwords’ en ‘Remote code execution’ een critical label. Dit wil zeggen dat ze zo snel mogelijk opgelost moeten worden. Deze gegevens zijn namelijk enorm schadelijk voor het systeem.

We vonden nog 3 ‘high value’ kwetsbaarheden. Deze dienen net zoals de criticals ook zo snel mogelijk verholpen te worden. Ze zijn namelijk nog steeds kwetsbaar voor het systeem alleen zijn de gevolgen net iets minder groot dan bij de criticals.

Een ‘zone transfer attack’ klasseren wij onder het ‘medium’ label. Dit is nog steeds een kwetsbaarheid, maar de risico’s hiervan zijn veel minder schadelijk voor het pokemon systeem. Netwerkinformatie is namelijk meestal redelijk publieke info, dus is het minder kwetsbaar. Bepaalde netwerkinformatie dient natuurlijk wel niet verspreid te worden, vandaar nog steeds het medium label.

Tot slot gaven we ‘SMB pentesting’ het ‘low’ label. Dit is namelijk een makkelijk te vermijden/oplosbare kwetsbaarheid. Meestal vereist dit een simpele (systeem)update. SMB wordt vaker vergeten als kwetsbaarheid omdat er meestal minder gevoelige data te vinden is. Vandaar dat wij hier dus de minste waarde aan hechtten.

Naast de vermelde kwetsbaarheden zijn er reeds nog andere gevoelige data gevonden op het systeem in de vorm van pokemons. Deze hebben we voor de ordelijkheid en privacy niet vermeld in het report.