1. **Server16**
   1. **Nmap**

Wij zijn met nmap de Server gaan scannen om open poorten te vinden. Met het scannen hebben we dan gevonden dat de server zijn poorten gefilterd zijn. Hierna zijn we gaan zoeken of er een manier was om dit te omzeilen en hebben deze ook gevonden. We hebben dan dit commando uitgevoerd:

“sudo nmap -sS -v -v -Pn 192.168.0.247” (server16/nmap/screenshot\_2)

* -sS: TCP SYN/Connect()/ACK/Window/Maimon scans
* -v: Verhoog het breedsprakigheidsniveau (2 keer voor groter effect)
* -Pn: Gaat alle host als open beschouwen

Hiermee hebben we dan gewonden dat poorten 80 en 3389 open staan. Een poort op zich is nooit een vulnerability maar of het een zwak punt is hangt af van de service die naar de poort aan het luisteren is.

* 80:Deze poort heeft geen vaste applicatie die gebruikt maakt van hem dus ja kan niet met zekerheid zeggen dat dit een vulnerability is en zal dus moeten proberen uit te zoeken welke service deze poort aan het gebruiken is voor je hier gebruik van kan maken.
* 3389: Word gebruikt door RDP (Remote desktop protocol). Er zijn verschillende exploits die gebruik maken van deze poort maar ze lijden bijna allemaal tot hetzelfde resultaat en dat is dat de hacker je computer/server/mobile toestel kan besturen alsof hij achter je scherm zit. Er word hier gebruik gemaakt van bestaande permissies die normaal door de remote desktop gebruikt kunnen worden om uw apparaat te besturen.

Misschien nog wel het ergste is dat de meeste van deze exploits “wormable” zijn dit betekend dat ze automatisch van apparaat naar apparaat kunnen springen zo gouw dat er een toestel besmet is en zich zo dus zonder enige extra moete kan versprijden.

Deze vulnerability kan opgelost worden op 2 manieren. Je kan de poort dicht zetten en ja kan ja apparaat up to date houden zodat alle nieuwe bekende exploits met deze poort gepatcht zijn.

* 1. **Zap**

Met Zap hebben wij 2 vulnerability gevonden op de server deze 2 zijn dat de X-frame-options header is niet ingestet en dat de X-content-type-options header afwezig is. Deze 2 zorgen er voor dat er een paar exploits gebruikt kunnen worden

* X-frame-options Header not set (Server16/Zap/alert\_1):  
  Het fijt dat deze optie niet ingesteld is maakt uw gebruikers kwetsbaar voor een ‘Clickjacking’ aanval. Dit is een aanval die de gebruiker laat klikken op een webpage element dat onzichtbaar is of vermomd is als een ander element. Door op dit element te klikken wort er dan een malicieus actie uitgevoerd. Dit kan verschillende dingen inhouden zoals: malware downloaden, een link naar een malicieus site, gevoelige data vrijgeven, geld overdragen of een u een ongewenst product laten kopen.

Om dit op te lossen moet je simpel weg deze optie instellen

* X-content-type-options header missing (Server16/Zap/alert\_2):

Door deze optie niet in te stellen kunne oudere versies van internet explorer en chrome MIME-sniffing uitvoeren op de response body, wat kan zorgen dat de response body geïnterpreteerd en weergegeven wordt in een ander content type dan het ingestelde type.

De vulnerability van MIME-sniffing is dat het gebruikt kan worden om XSS aanvallen uit te voeren.

Deze vulnerability is redelijk gemakkelijk op te lossen ja moet de X-content-type-options header op “nosniff” zetten en de andere mogelijkheid is dat je probeert te zorgen dat de gebruikers en moderne webbrowser gebruiken en geen verouderde versie. Het beste kan je natuurlijk deze 2 opties allebei proberen uit te voeren.

* 1. **Nessus** (Server16/nessus)

Bij het scannen met nessus hebben we 5 medium vulnerabilities gevonden en 19 stukken info. Deze 5 hebben bijna allemaal met elkaar te maken en ze gaan over het SSL-certificaat.

* SSL Certificate Cannot Be Trusted/ SSL Self-Signed Certificate

Dit kan mensen afschrikken omdat dit meestal een melding geeft als je op de site gaat.

* TLS Version 1.0 Protocol Detection

Dit is een achterhaald protocol en heeft een aantal cryptografiece design flaws. De nieuwe protocollen hebben beschermingen tegen gekende zwaktes van TLS 1.0. Als je nog TLS 1.0 gebruikt ben je kwetsbaar voor downgrade aanvallen bij deze aanvallen makken hackers een connectie met uw server waarbij ze de server dwingen om oudere protocollen te gebruiken met bekende exploits.

Dit is zeer makkelijk op te lossen door te zorgen dat alle oude protocollen gedisabeld zijn op uw server en dat je alleen de nieuwe protocollen gebruikt.

* SSL Medium Strength Cipher Suites Supported (SWEET32)

Dit betekend dat de server medium sterkte voor encryptie gebruikt. Hiermee bedoelen ze encrypties met een sleutel lengte tussen 64 bits en 112 bits of als je de 3DES encryptie gebruikt.

De oplossing hiervan is het her configureren van de applicatie die deze sleutel gebruikt en deze dan instelt op een sterke sleutel.

* SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Dit geeft aan dat de server het gebruik van RC4 in 1 of meerder cipher suits ondersteunt. De RC4 cipher is heeft een grootte zwakte in zijn genereren van pseudo-random stream hierin worden een paar instellingen gevolgd waardoor de stream minder random is.

Voor het oplossen van deze zwakheid raden ze aan om de RC4 sipher te vermijden en deze te vervangen door TLS1.2 samen met AES-GCM suites.

1. **SimpleWin**
   1. **Nmap**

We zijn met nmap de windows client gaan scannen dit hebben we gedaan door het commando: “nmap 192.168.235.129”(Simple/nmap/nmap\_1) uit te voeren. Hier zagen we dan dat er best wel wat poorten open stonden deze zijn:

* 135: Word gebruikt door de msrpc service. Deze poort laten open staan zonder filter is best wel een grootte vulnerability het kan namelijk gebruikt worden voor meerder exploits. De meest bekende exploits zijn:
  + Popup message not send spam exploit:

Dit is het continu krijgen van pop-ups messages met de boodschap “message not send”

* + DoS aanval: Dit is mogelijk omdat er een fout in RPC zit. Deze fout zorgt er voor dat RPC faalt als deze een rekwest krijgt met bepaalde misvormde data. (Windows patch kan dit oplossen)
  + Worms zijn die zich verspreiden via deze poort.

Voor dit probleem kan je de poort niet zomaar sluiten want deze poort is nodig bij verschillende services vooral die van Microsoft zelf. Dus de beste oplossing is uw firewall het verkeer op deze poort te laten monitoren.

* 139: Word gebruikt door de netBios-ssn service. Dit is een protocol dat gebruikt word door File en print Sharing in alle huidige windows versies.

Het probleem hier is dat als je de standaard settings van File en Print Sharing gebruikt dit zich met alles verbind ook TCP/IP dus inplaats dat de gedeelde data alleen toegankelijk is in het lokale netwerk is deze ook toegankelijk vanuit het hele internet. Dit kan verholpen worden als je dit tegoei instelt.

De beste manier om deze zwakheid te voorkomen is het afzetten van File en Print Sharing of het blokkeren van poorten 135 tot 139. Als je dit toch wilt gebruiken raden ze je aan om 4 dingen te doen deze zijn: een sterk wachtwoord, een dollar teken achter je share naam te zetten, File en Print Sharing los te koppelen ven TCP/IP en NetBEUI in de plaats te gebruiken en het instellen van de poorten 135 tot 139 op je router/firewal.

Naast deze grootte zwakte is deze poort ook kwetsbaar door RPC van hierboven en kwetsbaar door een aantal Trojans/Backdoor aanvallen.

* 445: Word gebruikt door microsoft-ds service ook wel bekend als SMB (Server Message Block). Deze service wordt grotendeels gebruikt door Windows voor netwerk sharing en het remote uitvoeren van commando’s hierdoor is dit een heel populair aanvallen punt omdat dit de basisfuncties zijn die men bij de meeste aanvallen wilt gebruiken. Er zijn dus ook heel veel verschillende exploits die door de jaren heen zijn gevonden om deze poort te misbruiken als deze openstaat zonder enige bescherming.

Om dit tegen te gaan kan u best de poort dicht zetten of deze beschermen met een firewal.

* 1. **Zap** (Simple/Zap)

Met Zap hebben wij niet echt iets gevonden op SimpleWin we hebben enkel 2 files gevonden namelijk robots.txt en sitemaps.xml maar deze konden we niet opendoen.

* 1. **Nessus** (Simple/Nessus)

Bij het scannen van de SimpleWin met nessus hebben we 1 critical, 1 High en 2 medium vulnerabilities gevonden en ook nog 25 info bloken.

* + 1. Critical
       1. Unsupported Windows OS (remote): Dit houd in dat er een afwezige service pack is van de remote versie van windows of dat deze versie niet meer gesupporteerd word.

Dit is zeer gevaarlijk omdat voor alle nieuwe exploits die voor deze remote windows versie gevonden werden er geen patches worden gemaakt en deze exploits dus voor altijd zullen blijven werken.

De oplossing voor deze zwakheid is het upgraden naar een gesupporterde versie.

* + 1. High
       1. MS17-010: Security Update for Microsoft Windows SMB Server (4013389)(ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE)(ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialedcheck):

Dit betekend dat je een bepaalde update die u tegen verschillende vulnerabilities beschermt nog niet hebt gedaan en dat u dus kwetsbaar bent aan al deze exploits. Deze specifieke vulnerability bestaat in Microsoft server messaging block 1.0 door het verkeerd behandelen van een bepaald type rekwesten. De aanvaller kan dit gebruiken door een speciaal gemaakt pakket samen te stellen en dit te verzenden om dan zo bepaalde codes uit te voeren of om gevoelige data te verkrijgen.

De oplossing hiervoor is zo snel mogelijk deze updates uit te voeren zodat u niet meer kwetsbaar bent.

Als u op een niet gesupporteerde versie zit kan u best overschakelen naar een gesupporteerde versie maar als u dit niet wil zijn er ook enkel condfiguraties die u kan uitvoeren om het risico te verminderen. De 2 dingen die u dan best doet is het af zetten van SMBv1 en het blokkeren van de poort 445.

* + 1. Medium
       1. MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527)(Badlock) (uncredentialed check):

Dit is opnieuw een update die niet is uitgevoerd. De vulnerability die met deze update word opgelost is een elevation of privilege vulnerability in de SAM(Security Account Manager) en LSAD(Local Security Authority (Domain Policy)) protocollen doordat er slechte authenticatie level onderhandelingen zijn over de RPC chanels. Deze exploit kan gebruikt worden door een man-in-de-middel door de communicatie tussen de server en client te onderscheppen en dan een geforceerde authenticatie level downgrade te doen en zo een geauthentificeerde gebruiker na te kunnen doen.

Deze zwakte is simpel genoeg op te lossen door deze update uit te voeren.

* + - 1. SMB Signing not required: Dit betekent simpel genoeg dat er bij SMB geen validatie moet gebeuren over met wie u aan het communiceren bent. Dit maakt u kwetsbaar voor man-in-the-middle aanvallen omdat deze zich dan niet moet authentificeren.

De oplossing is ook redelijk simpel u moet gewoon aanzetten dat SMB signing verplicht is in uw configuratie.