Beperking van toegang tot machine voor poorten en telefoons

Inhoud

Inleiding

Dit document beschrijft een probleem dat is aangetroffen met Machine Access Bepertion (MAR) en biedt een oplossing voor het probleem.

Door de groei van persoonlijk in bezit zijnde apparaten is het belangrijker dat systeembeheerders ooit een manier kunnen bieden om de toegang tot bepaalde delen van het netwerk te beperken tot uitsluitend bedrijfsmiddelen. Het probleem dat in dit document wordt beschreven, betreft de manier waarop u deze aandachtsgebieden veilig kunt identificeren en ze kunt authentiseren zonder de gebruikersconnectiviteit te verstoren.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van 802.1x om dit document volledig te begrijpen. Dit document gaat ervan uit dat gebruikers 802.1x hun echtheidscontrole kennen en wijst op de problemen en voordelen die verbonden zijn aan het gebruik van MAR en meer in het algemeen op de authenticatie van machines.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van

elke opdracht begrijpen.

Probleem

MAR probeert in wezen een gemeenschappelijk probleem op te lossen dat inherent is aan de meeste van de huidige en populaire MAP-methoden (Extensible Verification Protocol), namelijk dat de authenticatie van machines en de gebruikersverificatie afzonderlijke, niet-gerelateerde processen zijn.

Gebruikersverificatie is een 802.1x-verificatiemethode die de meeste systeembeheerders bekend is. Het idee is dat de geloofsbrieven (gebruikersnaam/wachtwoord) aan elke gebruiker worden gegeven, en die reeks geloofsbrieven vertegenwoordigt een fysiek persoon (het kan ook tussen verscheidene mensen worden gedeeld). Daarom kan een gebruiker vanuit het netwerk inloggen met die referenties.

Een machinale echtheidscontrole is technisch hetzelfde, maar de gebruiker wordt doorgaans niet verzocht de geloofsbrieven (of het certificaat) in te voeren; de computer of machine doet dat op zichzelf. Hiervoor is nodig dat de machine al aanmeldingsgegevens heeft opgeslagen. De verzonden gebruikersnaam is **host/<MyPCHostname>**, mits de machine **<MyPCHostname>** als hostname heeft ingesteld. Met andere woorden, het stuurt **host/**gevolgd door uw hostname.

Hoewel dat niet direct met Microsoft Windows en Cisco Active Directory te maken heeft, wordt dit proces makkelijker weergegeven als de machine is aangesloten op Active Directory omdat de computer hostname is toegevoegd aan de domeindatabase, en de aanmeldingsgegevens zijn onderhandeld (en elke 30 dagen standaard verlengd) en opgeslagen op de machine. Dit betekent dat 'machine'-verificatie mogelijk is van elk type apparaat, maar het wordt veel gemakkelijker en transparanter gemaakt als de machine wordt aangesloten op 'Active Directory' en de aanmeldingsgegevens blijven verborgen voor de gebruiker.

MAR als oplossing

Het is makkelijk om te zeggen dat de oplossing is voor Cisco Access Control System (ACS) of Cisco Identity Services Engine (ISE) om de MAR te voltooien, maar er zijn voordelen en nadelen om te overwegen voordat dit wordt geïmplementeerd. Hoe dit te implementeren is het best beschreven in ACS of ISE gebruikershandleidingen, zodat dit document eenvoudig beschrijft of u dit al dan niet in overweging wilt nemen en een aantal mogelijke hindernissen.

De voors

De MAR is uitgevonden omdat de gebruiker- en machine-authenticaties totaal verschillend zijn. Daarom kan de RADIUS-server geen verificatie afdwingen waarbij gebruikers zich moeten aanmelden bij apparaten die eigendom zijn van het bedrijf. Met MAR dwingt de RADIUS-server (ACS of ISE, aan de Cisco-kant), voor een bepaalde gebruikersverificatie, dat er een geldige machine-verificatie moet zijn in de X-uren (doorgaans 8 uur, maar dit is configureerbaar) die de gebruikersverificatie voor hetzelfde eindpunt voorafgaat.

Daarom zal een machine-verificatie slagen als de machine-referenties bekend zijn bij de RADIUS-server, doorgaans als de machine is aangesloten bij het domein, en de RADIUS-server verifieert dit met een verbinding naar het domein. Het is volledig aan de netwerkbeheerder om te bepalen of een succesvolle machinetechtheidscontrole volledige toegang tot het netwerk biedt, of alleen een beperkte toegang; Meestal opent dit ten minste de verbinding tussen de client en de actieve map

zodat de client zulke acties kan uitvoeren als vernieuwing van het gebruikerswachtwoord of GPO's (Download Group Policy Objects).

Als een gebruikersauthenticatie afkomstig is van een apparaat waar de machineverantwoording in de voorafgaande paar uur niet heeft plaatsgevonden, dan wordt de gebruiker ontkend, zelfs als de gebruiker normaal geldig is.

Volledige toegang wordt alleen verleend aan een gebruiker indien de authenticatie geldig is en voltooid is vanaf een eindpunt waar de machineverantwoording in de afgelopen paar uur plaatsvond.

De Cons

In dit deel worden de voorwaarden voor het gebruik van de MAR beschreven.

MAR en Microsoft Windows Verkenner

Het idee achter de MAR is dat een gebruikersverificatie alleen succesvol is als de gebruiker over geldige aanmeldingsgegevens beschikt, maar dat ook een succesvolle machineverantwoording van die cliënt moet worden geregistreerd. Als daar een probleem mee is, kan de gebruiker niet authentiek verklaren. De kwestie die zich voordoet is dat deze optie soms per ongeluk een rechtmatige klant kan uitsluiten, wat de cliënt dwingt om opnieuw op te starten om toegang tot het netwerk te krijgen.

Microsoft Windows voert alleen machineverantwoording uit bij de start (wanneer het inlogscherm verschijnt); zodra de gebruiker de gebruikersreferenties invoert, wordt een gebruikersverificatie uitgevoerd. Als de gebruiker zich uitlogt (naar het inlogscherm terugkeert) wordt er ook een nieuwe machine-verificatie uitgevoerd.

Hier is een voorbeeldscenario dat laat zien waarom MAR soms problemen veroorzaakt:

Gebruiker X werkte de hele dag op zijn laptop, die aangesloten was via een draadloze verbinding. Uiteindelijk sluit hij gewoon zijn laptop en laat het werk. Dit plaatst de laptop in een hibernatie. De volgende dag komt hij terug op kantoor en opent zijn laptop. Nu is hij niet in staat een draadloze verbinding tot stand te brengen.

Wanneer Microsoft Windows verblijft, krijgt het een momentopname van het systeem in zijn huidige status, die de context van wie is ingelogd omvat. In één nacht, vervalt de MAR-gecached ingang voor de gebruikerslaptop en wordt gewist. Als de laptop echter wordt ingeschakeld, voert hij geen machineverantwoording uit. In plaats daarvan gaat het recht in op een gebruikersverificatie, want dat was wat de hibernatie registreerde. Dit kan alleen worden opgelost door de gebruiker uit te loggen of door zijn computer opnieuw op te starten.

Hoewel MAR een goede functie is, kan het netwerkverstoring veroorzaken. Deze verstoringen zijn moeilijk om problemen op te lossen tot u begrijpt hoe MAR werkt; wanneer u MAR toepast, is het belangrijk om de eindgebruikers te informeren over hoe zij computers goed kunnen sluiten en op het einde van elke dag kunnen afloggen.

MAR- en diverse RADIUS-servers

Het is gebruikelijk om meerdere RADIUS-servers in het netwerk te hebben voor taakverdeling en

redundantie. Niet alle RADIUS-servers ondersteunen echter een gedeeld MAR-sessiecache. Alleen ACS versies 5.4 en later, en ISE versie 2.3 en later ondersteunen MAR cache-synchronisatie tussen knooppunten. Vóór deze versies is het niet mogelijk een machineverantwoording uit te voeren tegen één ACS/ISE-server en een gebruikersverificatie tegen een andere, omdat zij niet met elkaar overeenkomen.

MAR- en bekabelde draadloze switching

Het MAR cache van veel RADIUS-servers is afhankelijk van het MAC-adres. Het is gewoon een tabel met het MAC-adres van laptops en het tijdstempel van hun laatste succesvolle machineverantwoording. Op deze manier kan de server weten of de client in de laatste X-uren geauthentiseerd is.

Maar wat gebeurt er als u uw laptop start met een bekabelde verbinding (en daarom een machine-verificatie van uw bekabelde MAC doet) en dan overschakelt op draadloos gedurende de dag? De RADIUS-server heeft geen middelen om uw draadloos MAC-adres te correleren met uw bekabeld MAC-adres en om te weten dat u in de afgelopen X-uren machinaal was bevonden. De enige manier is om uit te loggen en Microsoft Windows een andere machine authenticatie te laten uitvoeren via de radio.

Oplossing

Onder veel andere functies heeft Cisco AnyConnect het voordeel van vooraf geconfigureerd profielen die de verificatie van de machine en de gebruiker activeren. Dezelfde beperkingen die met Microsoft Windows Verkenner worden gezien, worden echter ook aangetroffen bij de verificatie van machines die alleen bij het uitloggen of opnieuw opstarten optreedt.

Ook is het met AnyConnect versies 3.1 en later mogelijk om met EAP-FAST te werken. Dit is in wezen één enkele authenticatie, waar je twee paar van geloofsbrieven tegelijk verstuurt, de gebruikersnaam/het wachtwoord van de machine en de gebruikersnaam/het wachtwoord. ISE controleert dus makkelijker of ze allebei succesvol zijn. Als er geen cache wordt gebruikt en geen vorige sessie hoeft terug te krijgen, is er een grotere betrouwbaarheid.

Wanneer de PC start, stuurt AnyConnect alleen een machine-verificatie, omdat er geen gebruikersinformatie beschikbaar is. Na inloggen van de gebruiker stuurt AnyConnect echter zowel de machine als de gebruikersinterface tegelijkertijd. Als u de kabel loslaat of uitkoppelt, worden zowel de machine als de gebruikersreferenties opnieuw verzonden via één EAP-FAST-verificatie, die verschilt van de eerdere versies van AnyConnect zonder EAP-koppeling.

EAP-TEAP is de beste oplossing op lange termijn, omdat het vooral ter ondersteuning van dit soort authenticaties wordt gemaakt, maar EAP-TEAP wordt op dit moment nog steeds niet ondersteund in de inheemse superieur van veel OS