Haavoittuvuuksien hallinta

Harjoitustyö 2

Antti Tammelin, TTV20S5

Tero Räsänen, TTV20S5

Elmeri Söderholm, TTV20S5

Eliel Taskinen, TTV20S5

Alex Rebiai AA5240, TTV20S5

Harjoitustyö
Kyberturvallisuuden hallinta TTC6020-3002, Jarmo Nevala
07.12.22
Tieto- Ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Tämä harjoitustyö on osa Kyberturvallisuuden hallinta -opintojaksoa, ja osa Kyberturvallisuuden hallinta TTC6020-3002 kurssia. Harjoitustyön aikana opimme tekemään Haavoittuvuuksien hallintaa ISO standardien mukaisesti. Sen lisäksi raportoimme riskiarvioinnin, ja mahdolliset korjausehdotukset.

2 Harjoitustyön tausta

2.1 Tehtävänanto

Harjoitustyön tehtävänantona oli tehdä Haavoittuvuuksien hallinta ISO standardien mukaisesti. Käytimme tarkemmin tiettyjä kohtia ISO standardeista, eli ISO 27001:2017 Taulukko A.12.6 (ISO 27001:2017. 2017) ja ISO 27002:2017 Kappale 12.6 (ISO 27002:2017. 2017). Tässä raportissa käymme myös läpi eri työkaluilla löydettyjä haavoittuvuuksia, riskiarvioinnin haavoittuvuuksista, ja mahdollisia korjausehdotuksia haavoittuvuuksiin. Sen lisäksi meillä oli harjoitustyön ohjeet, jota seurasimme (Harjoitustyön ohje. N.d.).

2.2 Yritys

DefendByVirtual, joka harjoituksen ajaksi on ympäristön omistaja, aloitti toimintansa 2021. Yrityksellä on monenlaisia puolustusmekanismeja, SIEM, SOAR, palomuuri. Meidät palkattiin vuonna 2022 auditoimaan ja saamaan pystyyn heitteille jätetty yritys. Yrityksellä ei ole yhtään rahaa, ja ei voi investoida enempiä resursseja kuin meidän ryhmältämme löytyy.

2.3 Ympäristö

Harjoitustyömme, ja koko moduuli, on toiminut VLE ympäristön sisällä. VLE, tai Virtual Learning Environment, on virtuaalinen ympäristö, missä on eri palveluihin suunnattuja virtuaalisia koneita. Liitteenä 1 on kuva ympäristöstä. Käytimme suurimmaksi osaksi Kali virtuaalista konetta, joka sijaitsi Admin-Netissä, mutta skannasimme Greenbone työkalulla kaikki muutkin ympäristössä olevat koneet.

2.4 Greenbone

Greenbone on maailman käytetyin avoimen lähdekoodin haavoittuvuuksien hallinnointityökalu. Greenbonen skannaus havaitsee järjestelmän haavoittuvuudet, arvioi niiden riskipotentiaalin sekä suosittelee korjaustoimenpiteitä. Näin voidaan huomata haavoittuvuudet ennen kuin niihin voidaan kohdistaa kyberhyökkäyksiä. Greenbone Vulnerability Management (GVM) on verkon skannaustyökalu, jossa on graafinen käyttöliittymä. GVM tunnettiin aikaisemmin nimellä Open Vulnerability Assessment System (OpenVAS). Greenbone on kehittänyt ohjelmaa vuodesta 2006. GVM on alun perin rakennettu nmap porttiskannerin päälle. (About Greenbone. N.d. ; Gentoo Linux. Greenbone Vulnerability Management. 2022).

Tässä harjoituksessa käytimme Greenbone Security Assistantin versiota 21.4.3. Greenbone Security Assistant on web-pohjainen GVM:n käyttöliittymä (ks. Kuvio 1).

Kuvio 1. Greenbone Versio.

3 Teknisten haavoittuvuuksien hallinta

Haavoittuvuuksien analysoinnin ja korjaamisen lisäksi yrityksen olisi hyvä huomioida riskienhallintaan liittyviä standardeja. Yritykselle pitää luoda aikataulu, jossa määritetään, kuinka useasti ympäristölle ja yritykselle tehdään riskianalyysi. Tämän lisäksi pitää luoda aikataulu, sille kuinka nopeasti reagoidaan eritasoisiin uhkiin ja haavoittuvuuksiin järjestelmissä. Haavoittuvuuksien

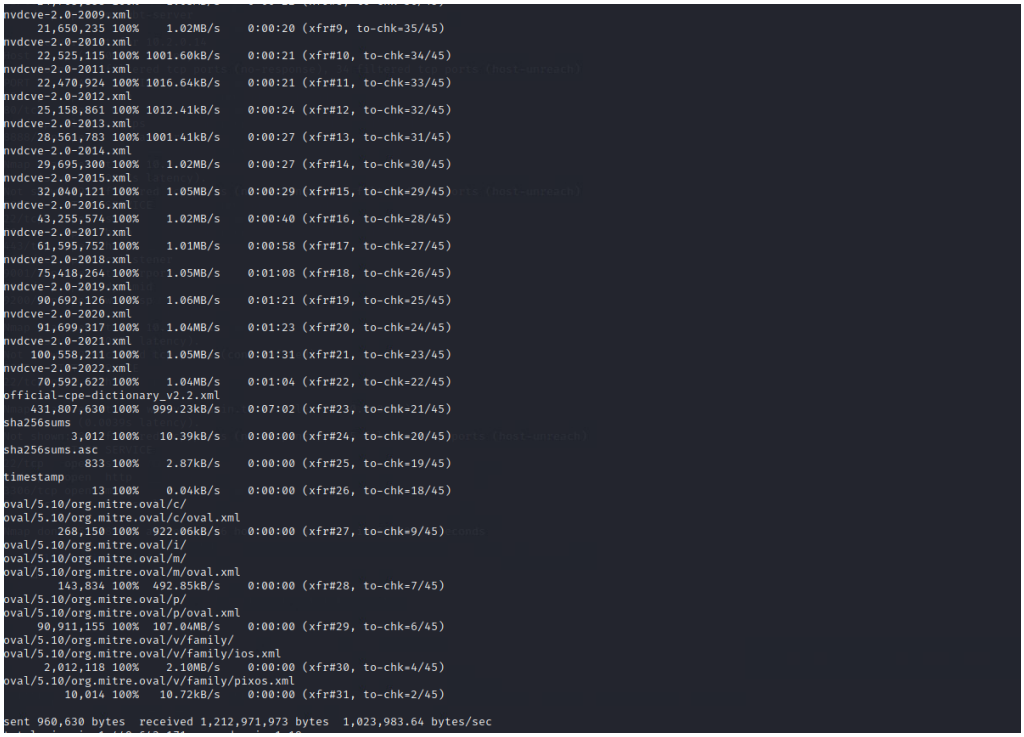
korjauksessa pitää ottaa huomioon, ettei korjaus tai korjaustiedosto aiheuta lisää uhkia ympäristölle. Korjaus pitää siis tutkia ja analysoida riskit etukäteen ennen paikkausta. Organisaatiossa olisi hyvä myös olla henkilö tai tiimi, jotka vastaavat riskienhallinasta. Riskienhallintaa varten pitää siis tehdä työn ja vastuiden jako.

Organisaatiolla pitäisi olla tapahtumaloki kaikista suoritetuista toimenpiteistä ja ennakoida riskejä tunnetuista haavoittuvuuksista. Haavoittuvuuksien hallintaprosessin pitäisi olla yhtenäinen hallintatoimenpiteiden kanssa.

4 Ympäristön skannaus

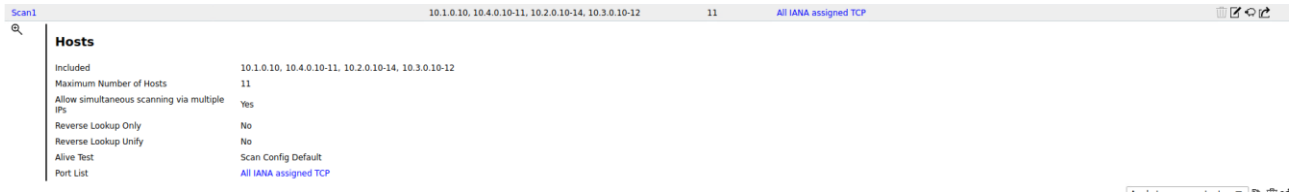
Tärkeä osa Haavoittuvuuksien hallintaa on haavoittuvuuksien löytäminen, ja kategorisointi. Käytimme tähän Greenbone työkalua, jolla pystyy skannaamaan kokonaisia ympäristöjä yhtä aikaa. Luultavasti emme löytäneet kaikki haavoittuvuuksia, jota olisimme voineet parantaa skannaamalla syvemmälle tai muuttamalla palomuurin asetuksia, että Greenbone pääsisi oikeasti toimimaan. Tulimme silti siihen päätökseen, että tällä normaalilla ja nopealla metodilla saa jo harjoitustyöstä paljon irti, joten kokeilimme vain nopeasti skannata.

Heti skannauksen alussa meidän piti päivittää tunnistetietokannat, sillä skannaus ei toiminut vanhentuneilla kannoilla. Se onnistui Kalin komentorivin kautta (ks. Kuvio 2).



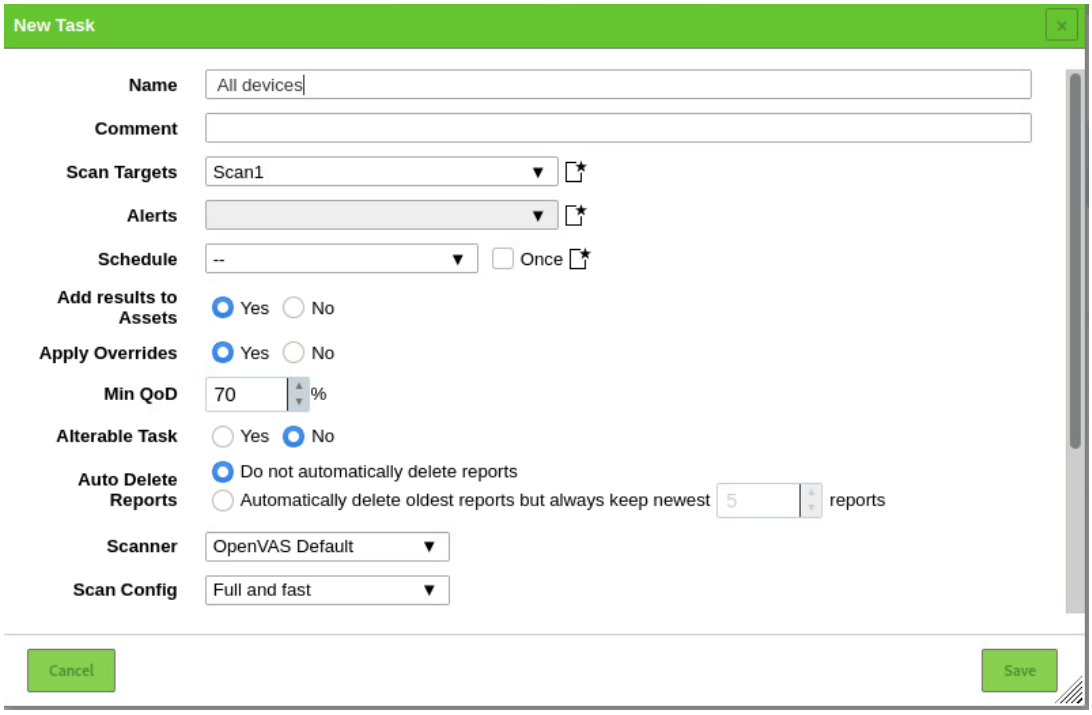
Kuvio 2. Tietokantojen päivitys

Sen jälkeen, kun olimme päässeet Greenboneen sisälle, teimme Greenbonen skannaukselle kohteen tai Targetin. Laitoimme meidän VLE ympäristön kaikki IP:t kohteiksi, ja jatkoimme seuraavaan osaan (ks. Kuvio 3).



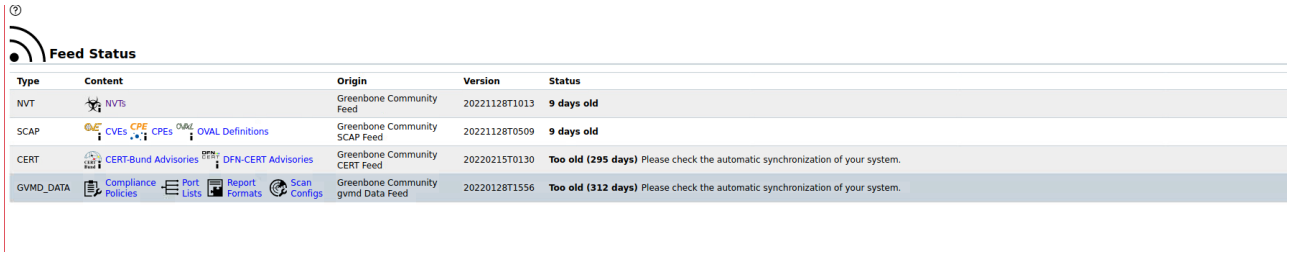
Kuvio 3. Skannauksen target

Sen jälkeen teimme uuden Taskin, jossa käytimme äsken tehtyjä Targetteita. Emme muita muuttaneet, eli käytimme OpenVAS Default Scanneria, ja Scan and Configissa Full and Fast optionia. Tämä on enimmäkseen kattava, ja nopeampi kuin muut skannit (ks. Kuvio 4).



Kuvio 4. Skannauksen luonti

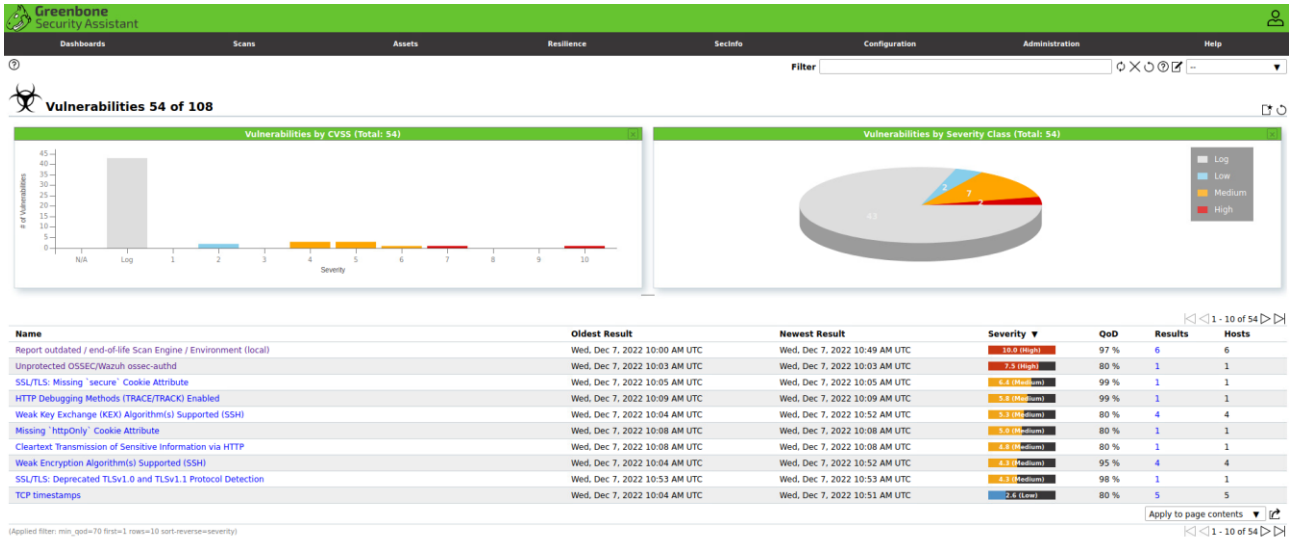
Sen jälkeen tarkistimme vielä, että haavoittuvuustietokannat olivat päivittyneet, ja aloitimme skannauksen (ks. kuvio 5).



Kuvio 5. Tietokannat

Skannauksesta tuli hyvin paljon tuloksia. Greenbone luokittelee eri haavoittuvuudet eri vakavuusasteisiin, yllä päivitettyjen tietokantojen mukaan. Käytimme tässä CVSS-tietokantaa, joka luokittelee haavoittuvuudet lowiin, mediumiin ja highin. Low tulokset ovat useimmin vain huomioita, joissa ehdotetaan erilaisia parannuksia. Medium tulokset ovat sellaisia haavoittuvuuksia, jotka pitäisi korjata ja joita voi itse priorisoida oman harkinnan mukaan. High tulokset ovat haavoittuvuuksia, jotka pitää heti korjata.

Käymme tässä raportissa läpi yhden high tuloksen ja sitten muutaman medium tuloksen. Menimme päivittämään tunnistetietokannan, joten pystyimme skannaamaan vain 6 hostia. Tämä tehtiin, koska olimme hämmentyneitä tehtävänannosta ja koska skannaaminen ei onnistunut ilman päivittämistä (ks. Kuvio 6).



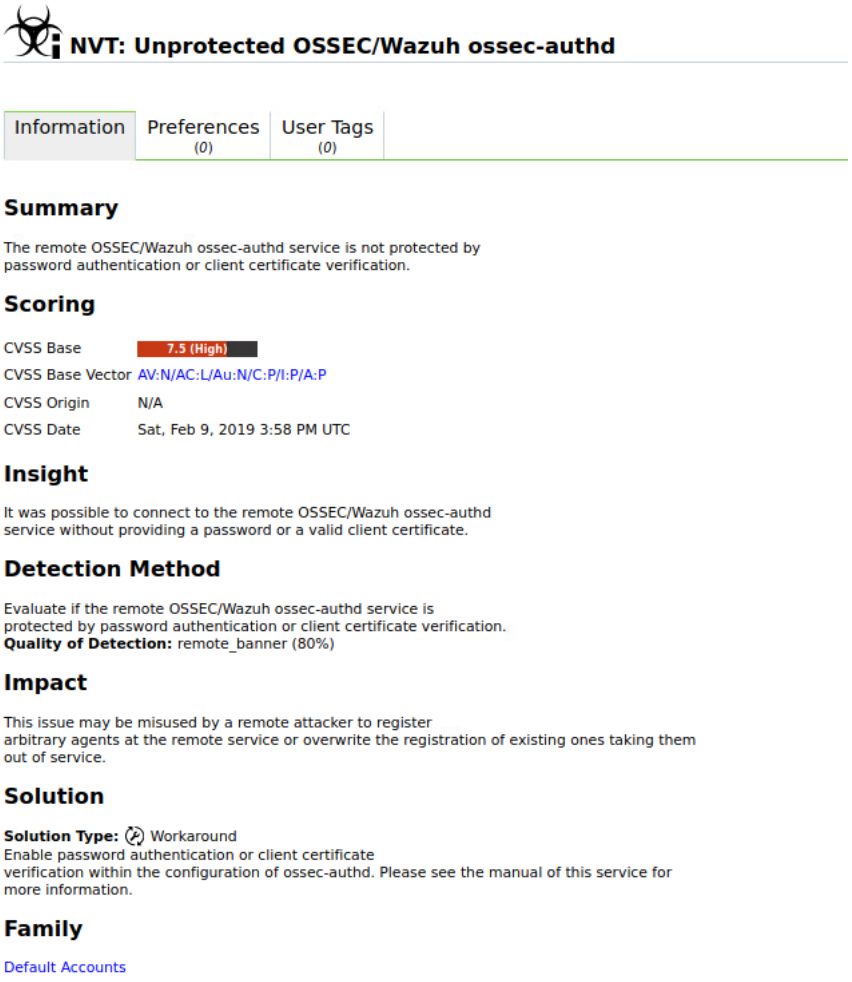
Kuvio 6. Skannauksen tulokset

5 Riskianalyysi

Riskianalyysi on tekniikka, jossa tunnistetaan yrityksen riskejä eri tasoilla. Sen avulla yritys pystyy toteuttamaan riskienhallinta suunnitelman. Riskejä voidaan tutkia monilla eri tasoilla esimerkiksi ulkoiset riskit. Riskien analysointiin voidaan myös käyttää työkaluja, joilla skannataan haavoittuvuuksia verkosta ja järjestelmistä, kuten meidän tapauksessamme. Riskien analysoinnilla voidaan minimoida yritykseen kohdistuvia uhkia ja havaita riskejä. Tämän avulla voidaan parantaa yrityksen turvallisuutta ja turvata tietoja.

Riskienanalysointia varten meidän piti pohtia, mitä järjestelmiä otamme mukaan riskianalyysiin. Päätimme skannata Greenbone Vulnerability työkalulla VLE ympäristön koneita, koska halusimme hyvän kokonaisuuden ympäristön haavoittuvuuksista. Riskianalyysiin otimme huomioon yli 5.3 CVSS tuloksen saaneet haavoittuvuudet, koska vakavat haavoittuvuudet olisi hyvä korjata nopeasti.

Skannauksessa tuli tosiaan vain yksi high haavoittuvuus, joka koski OSSEC/Wazuhia. Tällä palvelulla ei ole ollenkaan salasana tai certi -authentikaatiota ja se pitäisi enabloida (ks. Kuvio 7).



NVT: Unprotected OSSEC/Wazuh ossec-authd

Information | Preferences (0) | User Tags (0)

Summary

The remote OSSEC/Wazuh ossec-authd service is not protected by password authentication or client certificate verification.

Scoring

CVSS Base	7.5 (High)
CVSS Base Vector	AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Origin	N/A
CVSS Date	Sat, Feb 9, 2019 3:58 PM UTC

Insight

It was possible to connect to the remote OSSEC/Wazuh ossec-authd service without providing a password or a valid client certificate.

Detection Method

Evaluate if the remote OSSEC/Wazuh ossec-authd service is protected by password authentication or client certificate verification.
Quality of Detection: remote_banner (80%)

Impact

This issue may be misused by a remote attacker to register arbitrary agents at the remote service or overwrite the registration of existing ones taking them out of service.

Solution

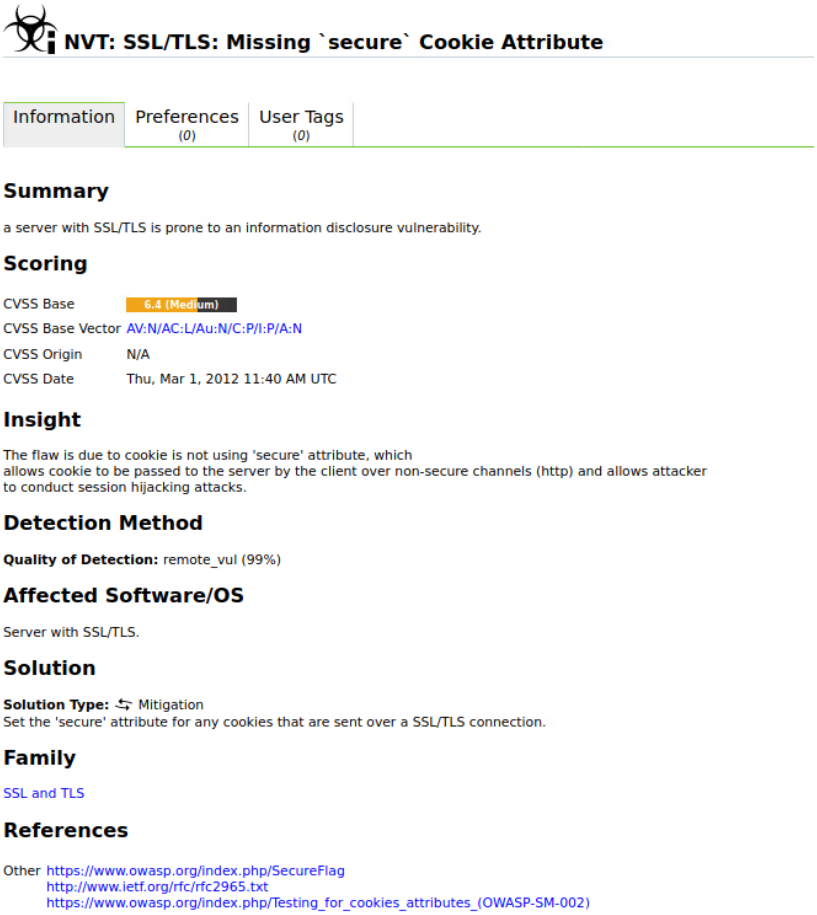
Solution Type: Workaround
Enable password authentication or client certificate verification within the configuration of ossec-authd. Please see the manual of this service for more information.

Family

Default Accounts

Kuvio 7. High haavoittuvuus

Ensimmäinen medium haavoittuvuus koski palvelinta, jossa on SSL/TLS käytössä. Evästeet pääsevät siis http-kanavia pitkin kulkemaan, ja ne eivät ole suojattuja. Tässä ei ole secure cookie attribuuttia käytössä ja se pitäisi laittaa päälle (ks. Kuvio 8).



NVT: SSL/TLS: Missing `secure` Cookie Attribute

Information | Preferences (0) | User Tags (0)

Summary

a server with SSL/TLS is prone to an information disclosure vulnerability.

Scoring

CVSS Base	6.4 (Medium)
CVSS Base Vector	AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Origin	N/A
CVSS Date	Thu, Mar 1, 2012 11:40 AM UTC

Insight

The flaw is due to cookie is not using 'secure' attribute, which
allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker
to conduct session hijacking attacks.

Detection Method

Quality of Detection: remote_vul (99%)

Affected Software/OS

Server with SSL/TLS.

Solution

Solution Type: Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Family

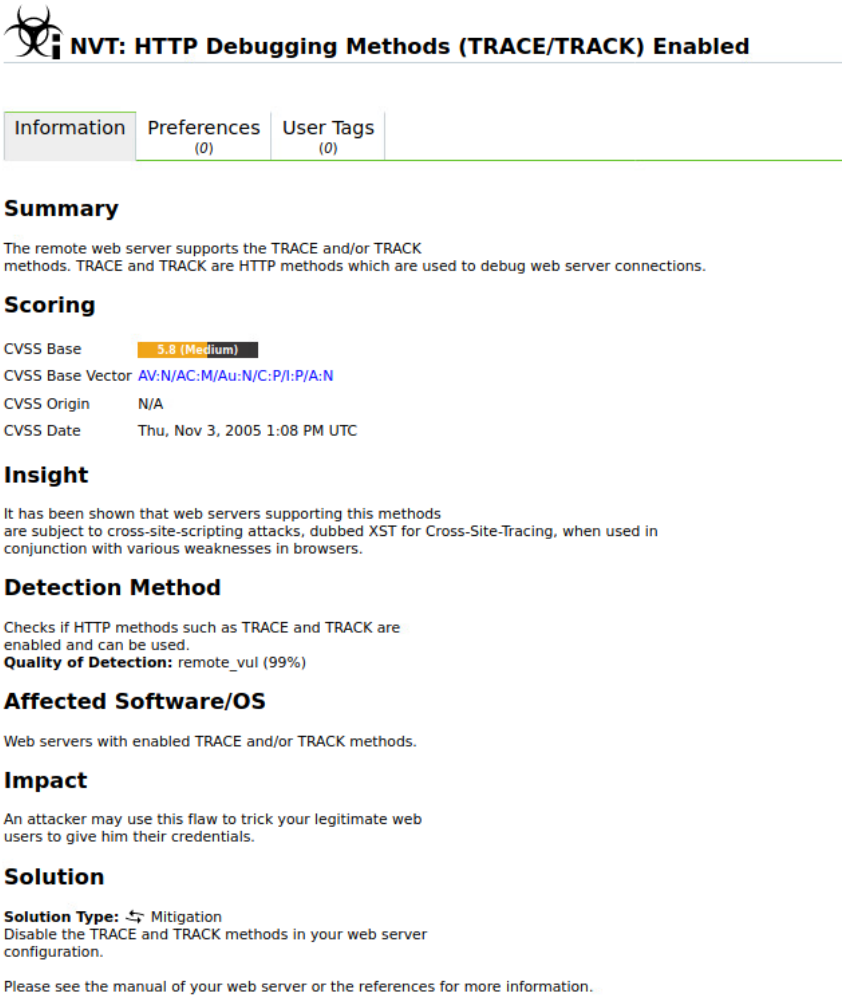
SSL and TLS

References

Other https://www.owasp.org/index.php/SecureFlag
http://www.ietf.org/rfc/rfc2965.txt
https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Kuvio 8. Medium haavoittuvuus 1

Toisessa medium haavoittuvuudessa on TRACE/TRACK päällä, jonka takia palvelimet ovat alttiita muun muassa skriptihyökkäyksille. Tämä haavoittuvuus korjaantuu ottamalla TRACE/TRACK metodin pois päältä webbipalvelimilta.



Kuvio 9. Medium haavoittuvuus 2.

Kolmas haavoittuvuus koski SSH-serveriä. Serveri tukee tällä hetkellä heikkoa key exchange- algoritmia. Tämä uhka sai arvion 5,3 eli medium. Miljoonat HTTPS, SSH ja VPN-serverit käyttävät samaa key exchangea. Aikaisemmin uskottiin, että tämä ei ole ongelma mutta on käynyt ilmi, että hyökkääjä voi tämän haavoittuvuuden takia katkaista yksittäisiä yhteyksiä. Ratkaisuna tähän haavoittuvuuteen on kytkeä heikot algoritmit pois päältä (ks. Kuvio 10).

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Information | Preferences (0) | User Tags (0)

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Scoring

CVSS Base 5.3 (Medium)
CVSS Base Vector CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS Origin Greenbone
CVSS Date Tue, Nov 23, 2021 10:58 AM UTC

Insight

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime

- ephemerally generated key exchange groups uses SHA-1

- using RSA 1024-bit modulus key
Quality of Detection: remote_banner (80%)

Impact

An attacker can quickly break individual connections.

Solution

Solution Type: Mitigation
Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Kuvio 10. Medium haavoittuvuus 3

Yleisesti emme löytäneet monia isoja haavoittuvuuksia, mutta tarpeeksi että meidän ympäristössämme on silti korjattavaa. Turvallisinta olisi päivittää kaikki ajan tasalle, ja varmistaa, että nämä High ja Medium haavoittuvuudet hoidettaisiin mahdollisimman nopeasti. Sen lisäksi laittaisin enemmän rahaa ja resursseja yleisesti kyberpuolustukseen, mutta se on myöhemmän ajan murhe.

6 Pohdinta

Kun aloitimme tehtävän, emme oikeastaan tienneet mitä meidän olisi pitänyt tehdä. Harjoitustyön ohjeissa luki, miten pitää vain seurata ISO standardeja, ja siitä ei ollut sitten enempää infoa tai ohjeita, miten haavoittuvuuksien hallintaa tehdään. Meidän piti itse etsiä ja kysellä muilta opiskelijoilta, miten he olivat tehneet. Kun vihdoinkin löysimme miten tämä pitäisi tehdä, eli tämän Greenbone työkalun avulla, niin senkin kanssa oli ongelmia, koska meillä ei ollut mitään tietoa, miten sitäkään käytetään. Kuitenkin opimme porukassa jotain, vaikka tämä prosessi olisi ollut helpompi, jos tähän olisi annettu enemmän neuvoja.

Lähteet

About Greenbone. N.d. Viitattu 7.12.2022. https://www.greenbone.net/en/about-greenbone/

Digiturvamalli. N.d. Viitattu 28.11.2022. https://www.digiturvamalli.fi/vaatimus/8-asset-management

Cortex 7.10.2022 https://github.com/TheHive-Project/Cortex/milestone/32

Gentoo Linux. Greenbone Vulnerability Management. 2022. Viitattu 7.12.2022. https://wiki.gentoo.org/wiki/Greenbone_Vulnerability_Management.

Harjoitustyö Ohje. N.d. Viitattu 07.12.2022. https://moodle.jamk.fi/pluginfile.php/805948/mod_resource/content/0/TTC6020-Harjoitusty%C3%B6_02.pdf.

ISO 27001:2017. 2017. Viitattu 07.12.2022. https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID6/2/493427.html.stx.

ISO 27002:2017. 2017. Viitattu 07.12.2022. https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID6/2/493421.html.stx.

TechTarget. What is risk analysis?. R.l. Viitattu 7.12.2022. https://www.techtarget.com/searchsecurity/definition/risk-analysis

Liitteet

Liite 1. Ympäristön kuvaus