



Haavoittuvuuksien hallinta

Harjoitustehtävä 2

Aro Jesper, TTV21S1

Jalkanen Kalle, TTV21S2

Koivisto Ossi, TTV21S2

Salomäki Sini, TTV21S5

Harjoitustehtävä

Kyberturvallisuudenhallinta TTC6020-3006, Nevala Jarmo

xx.2.2024

Tieto- ja viestintätekniikka, insinööri (AMK)

Sisältö

1	Johdanto	3
2	Teknisten haavoittuvuuksien hallinta.....	3
2.1	Tunnistaminen.....	3
2.2	Arviointi.....	4
2.3	Käsittely.....	4
3	Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin	5
3.1	Tarkoitus.....	5
3.2	Asentaminen	6
4	Haavoittuvuuksien skannaus	6
4.1	WS ja ADMIN-net	6
4.2	DMZ	10
4.3	Servers-net	11
5	Riskianalyysi	12
5.1	Haavoittuvaisuudet	12
5.2	Suosittelut korjaukset.....	12
6	Pohdinta.....	13
	Lähteet	14

Kuviot

Kuvio 1 ohjelmistot	4
kuvio 2. Greenbone skannerin vertailu tietokantojen versiot.....	7
kuvio 3 greenbonen antamat avonaiset portit	7
kuvio 4 Greenbone ws tulokset	7
kuvio 5 nmap WS-net tulokset.....	8
kuvio 6 ws1 haavoittuvaisuudet	8
kuvio 7. Onion haavoittuvaisuudet	8
kuvio 8. SIEM haavoittuvaisuudet.....	9
kuvio 9 SOAR haavoittuvuudet	9
kuvio 10 rocky haavoittuvaisuudet	9
kuvio 11 Kalin haavoittuvaisuudet.....	10
kuvio 12. WWW havoittuvaisuudet	10
kuvio 13. NS1 haavoittuvaisuudet	11
kuvio 14. SRV01 haavoittuvaisuudet	11

kuvio 15. DC01 haavoittuvaisuudet	11
kuvio 16. Nmap skannaus wsus laitteesta	12

Taulukot

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

Taulukko 1 Laitteiden kriittisyys	5
---	---

1 Johdanto

Tässä harjoituksessa tavoitteena on muodostaa ISO standardin 27001 ja 27002 mukainen haavoittuvuuksien hallinta kuvitteelliselle organisaatiollemme. Hallinta suunnitelma pitää sisällään ISO standardin kohdan 8.8. mukaiset vaatimukset teknisten haavoittuvuuksien hallinnasta, kohdan 8.19 mukainen ohjeistus ohjelmistojen asentamisesta organisaation järjestelmiin, haavoittuvuuksien skannauksen Greenbone Vulnerabilityllä ja tulosten dokumentoinnin sekä riskianalyysin, jossa käy ilmi mitkä ympäristön haavoittuvuudet huomioidaan. Dokumentin tarkoituksena on selkeyttää organisaatiomme menettelytapoja haavoittuvuuksien tunnistamisessa, hallinnassa ja niiden ehkäisevissä toimenpiteissä.

2 Teknisten haavoittuvuuksien hallinta

Hallintakeinon tyyppi on ehkäisevä eli näillä toimilla pyritään ehkäisemään mahdollisimman paljon potentiaalisi uhkia. Tarkoituksena on etukäteen kerätä tietoa organisaation käytössä olevien tietojärjestelmien haavoittuvuuksista, jotta niitä voidaan tarkastella kunkin haavoittuvuuden tasolle sopivalla vakavuudella. Näin ollen voidaan estää teknisten haavoittuvuuksien hyväksikäyttö. (SFS-EN ISO/IEC 270032:2022, 102)

2.1 Tunnistaminen

Jotta tunnistamista voidaan tehdä, Organisaatiolla on ylläpidossaan ISO standardin kohtien 5.9–5.14 mukainen omaisuuserien luettelo. Omaisuuserien luettelossa luetellaan organisaation käytössä olevat ohjelmat, joiden lisäksi ohjelman toimittaja, nimi, versio, käyttötilanne ja vastaava henkilö organisaatiossa (kuvio 1). Omaisuuserien listaa tulee vastuuhenkilön päivittää sen mukaan, kun muutoksia tapahtuu (SFS-EN ISO/IEC 270032:2022, 102).

Ohjelmistot					
Nimi	versionumero	toimittaja	Käyttötilanne	Vastuu henkilö	
Windows 11	10.0.22631	Microsoft	Työasema käyttöjärjestelmä WS01	Ossi Koivisto, Tietoturva-asiantuntija	
Kali Linux	2022.04	Offensive Security	Työasema käyttöjärjestelmä Kali-WS	Ossi Koivisto, Tietoturva-asiantuntija	
Microsoft AD	88	Microsoft	ActiveDirectory käytössä DC01:ssä	Ossi Koivisto, Tietoturva-asiantuntija	
Palo Alto	10.1.3	PaloAlto Networks	Palomuuuri	Ossi Koivisto, Tietoturva-asiantuntija	
ElasticSIEM	8.3.3	Elastic	kerää lokeja, tunnistaa uhkia ja analysoi tapahtumia	Kalle Jalkanen, Tietoturva-asiantuntija	
Security Onion	2.3.140	Security Onion Solutions, LLC	auttaa tunnistamaan tietoturvapoikkeamia	Kalle Jalkanen, Tietoturva-asiantuntija	
Wazuh	4.3.6	Wazuh	Havaitsee tunkeutumista, joka pystyy tunnistamaan hostissa epäilyttävät toiminnot.	Kalle Jalkanen, Tietoturva-asiantuntija	
Greenbone	22.4	Greenbone	Haavoittuvuuksien skannaus	Kalle Jalkanen, Tietoturva-asiantuntija	
Shuffle	1.0	Shuffle Automation		Kalle Jalkanen, Tietoturva-asiantuntija	
ITop	3.0.1	ITop	Työkaluja IT palveluiden hallintaan ja seurantaan	Kalle Jalkanen, Tietoturva-asiantuntija	
TheHive	3.1.6-1	TheHive	auttaa tunnistamaan tietoturvapoikkeamia	Kalle Jalkanen, Tietoturva-asiantuntija	
Cortex	3.1.6-1	Cortex Technology	auttaa tunnistamaan tietoturvapoikkeamia	Kalle Jalkanen, Tietoturva-asiantuntija	
Misp	2.4.161	Misp	kyberturvallisuuden indikaattoreiden ja uhkien keräämiseen, tallentamiseen ja jakamiseen.	Kalle Jalkanen, Tietoturva-asiantuntija	

Kuvio 1 ohjelmistot

Kunkin ohjelmiston vastuuhenkilö tarkastaa viikoittain oman vastuualueensa ohjelmistojen turvallisuuden. Yrityksen tietoturvatimi seuraa myös aktiivisesti ajantasaisia tietoturvauutisia esimerkiksi kyberturvallisuuskeskuksen -sivuja (<https://www.kyberturvallisuuskeskus.fi/fi>) ja tutkii niissä ilmenneiden haavoittuvuuksien soveltuvuutta organisaatiomme ympäristöön. Toimittajan valinnassa tulee kiinnittää huomiota, että heillä on käytössä asianmukaiset raportointi ja tunnistus menetelmät haavoittuvuuksille. Lisäksi organisaatiossamme tulee olla ajantasaiset työkalut haavoittuvuuksien tunnistamiselle, organisaation käytössä on Greenbone Security scanner (versio 22.4.0), jokaisen haavoittuvuuden korjauksen jälkeen organisaation vastuuhenkilön on pystyttävä todentamaan, että korjaus on tehonnut.

2.2 Arviointi

Teknisiä haavoittuvuuksia koskeissa raporteissa kyseisestä ohjelmistosta tai ohjelmistoista vastaava henkilö tai henkilöt sekä tietoturvapäällikkö suorittavat raportin analysoinnin ja mikäli mahdollinen haavoittuvuus löytyy, on siihen liittyvät riskit yksilöitävä ja tehtävä tarvittavat toimenpiteet liiketoiminnan suojelemiseksi.

2.3 Käsittely

Organisaatiossa tunnustettuihin ja ilmoitettuihin haavoittuvuuksiin tulee reagoida vuorokauden sisässä. Mikäli haavoittuvuus on suuri tai merkittävä riski liiketoiminnalle reagoida täytyy välittömästi. Organisaatiossa on sovittu, että käytetään oletuksena kaikissa ohjelmistoissa automaattisia päivityksiä, mikäli ohjelmisto sen sallii. Haavoittuvuuden paikkaamiseen tulee käyttää vain luotettuja lähteitä ja korjausmenetelmiä, luotetut lähteet voivat olla niin organisaation sisäisiä kuin ul-

koisiakin esimerkiksi toimittajan tarjoamat ratkaisut, jotka yleensä ovat päivitys tai korjaustiedostoja. Mikäli haavoittuvuus koskee laajalti koko organisaation laitteita tai osaa niistä, on korjaus toimenpiteet aloitettava yritystoiminnalle kriittisimmästä laitteesta (taulukko 1).

Taulukko 1 Laitteiden kriittisyys

	Priority 1	Priority 2	Priority 3
Palvelimet	DC01 SRV01 WSUS PaloAlto	ns-1 www	Onion SIEM SOAR OVS
työasemat		Kali-WS (admin-net) Rocky-WS (admin-net)	WS01 (WS-net)

Mikäli tarjolla ei ole korjaus vaihtoehtoa tai sitä ei olla vielä julkaistu, organisatio ottaa käyttöön muun hallinta keinon, jotka on määritelty listassa järjestyksessä.

Hallintakeinot mikäli korjaus vaihtoehtoa ei ole saatavilla luotetusta lähteestä

- 1) Ohjelmiston toimittajan suosittelema kiertoratkaisu
- 2) Haavoittuneen palvelun pois käytöstä otto.
- 3) Haavoittuvuuden estäminen palomuurin kautta
- 4) Haavoittuneen kohteen suojaaminen haitalliselta liikenteeltä
- 5) Valvonnan ja viestinnän lisääminen, jotta voidaan havaita hyökkäys

3 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin

3.1 Tarkoitus

Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin on ehkäisevä hallintakeinon tyyppi, jolla hallitaan turvallisesti ohjelmistojen asentamista järjestelmiin. Asentamalla varmistetaan järjestelmien eheys ja estetään mahdollisten teknisten haavoittuvuuksien hyödyntämisen sekä ylläpidetään toimittajien tuki ohjelmistolle.

3.2 Asentaminen

Ohjelmien ja päivitettyjen versioiden asentamisessa kuuluu olla tiedossa ohjelmistoa edeltävät ohjelmat sekä versiot dokumentoinnin sekä mahdollisten palautusstrategioiden kannalta. Asennetut ohjelmat pitää sisältää vain hyväksyttyä suorituskelpoista koodia ja koulutetun pääkäyttäjän toimesta. Uusien versioiden käyttöönotossa pitää selvittää version turvallisuus sekä sen tietoturva-haavoittuvuuksien määrä.

Ennen ohjelmiston asennusta pitää ohjelmisto ja päivitykset testauttaa ympäristössä, mahdollisten haavoittuvuuksien, yhteensopimattomuuksien tai muiden ongelmien varalta. Lisäksi kaikki ohjelmistojen vanhat versiot arkistoidaan varatoimenpiteenä, tarvittavien tiedostojen sekä konfiguraatioiden kanssa, niin pitkään kun se on mahdollista. Tässä vaiheessa kuuluu myös päivittää kaikki vastaavat ohjelmistojen lähdekirjastot ja määritetään palautusstrategia, mikäli sitä tarvitaan.

Ohjelmistojen versioita on päivitettävä siten, että toimittajien tuki säilyy, sillä ohjelmisto, jonka tuki on päättynyt, on tietoturvallisesti heikompi sekä mahdollinen apu on tällöin olematon. Organisaation on myös otettava huomioon avoimen lähdekoodin ohjelmistojen käytön riskit ja tuen mahdollinen loppuminen tai puute. (SFS-EN ISO/IEC 27002:2022, 120, 121)

4 Haavoittuvuuksien skannaus
































Aloitimme skannaamaan Admin-net ympäristöä greenbone security scannerilla (versio 22.4.0) ja skannausparametrit ja vertailu tietokantojen versiot (kuvio 2).

4.1 WS ja ADMIN-net

Ajoimme skannit laite kerrallaan ympäristössämme ja ensimmäinen laite olikin WS01. Tuloksista näkyy, että laitteella oli 2 porttia auki greenbonen mukaan (kuvio 3) ja 4 porttia nmap:in mukaan (kuvio 4). Laitteella oli myös haavoittuvaisuuksia (kuvio 5). Seuraavaksi skannasimme Onion:in osoitteessa 10.2.0.10 ja löysimme haavoittuvaisuudet (Kuvio 6). Jatkoimme skannaamaan SIEM laitteen osoitteessa 10.2.0.11 (kuvio 8.). Seuraavaksi skannasimme SOAR:in osoitteesta 10.2.0.12, ja listasimme sen haavoittuvaisuudet (kuvio 9). Jatkoimme rocky-Ws:ään 10.2.0.14 ka

otimme haavoittuvaisuudet ylös (kuvio 10). Viimeinen laite Admin verkossa oli Kali-WS 10.2.0.13 ja sen haavoittuvaisuudet ovat (kuviossa 11.)

Greenbonen tuloksia tarkastelemalla selviää, että Admin-net:issä suurimmat haavoittuvaisuutemme ovat JQuery haavoittuvaisuuksia ja heikkoja avain algoritmeja. Aiomme jatkossa puuttua näihin organisaatio tasolla ja poistaa heikot algoritmit käytöstä. Aiomme myös varmistaa, että pidämme JQueryä ajan tasalla.

Name ▲	Family		NVTs		Actions
	Total	Trend	Total	Trend	
Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)	2	→	3	→	   
Discovery (Network Discovery scan configuration. Version 20201215.)	10	→	3164	↗	   
empty (Empty and static configuration template. Version 20201215.)	0	→	0	→	   
Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.)	56	↗	83717	↗	   
Host Discovery (Network Host Discovery scan configuration. Version 20201215.)	2	→	2	→	   
Log4Shell (Configuration with checks for Log4j and CVE-2021-44228. Version 20211227.)	10	→	29	→	   
System Discovery (Network System Discovery scan configuration. Version 20201215.)	5	→	30	→	   
<div> Apply to page contents ▼    </div>					

kuvio 2. Greenbone skannerin vertailu tietokantojen versiot

			<div> 1 - 2 of 2 </div>	
Port	Hosts	Severity ▼		
135/tcp	1	5.0 (Medium)		
3389/tcp	1	4.3 (Medium)		
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)			<div> 1 - 2 of 2 </div>	

kuvio 3 greenbonen antamat avonaiset portit

kuvio 4 Greenbone ws tulokset


```

(kali@kali-ws)-[~]
$ nmap -sV -Pn 10.2.0.10
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-20 13:11 EET
Nmap scan report for 10.2.0.10
Host is up (0.42s latency).
Not shown: 923 filtered tcp ports (no-response), 74 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http     nginx
443/tcp   open  ssl/http nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.52 seconds

```

kuvio 5 nmap WS-net tulokset

1 - 3 of 3							
Vulnerability		Severity ▼	QoD	Host IP	Name	Location	Created
DCE/RPC and MSRPC Services Enumeration Reporting	🔧	5.0 (Medium)	80 %	10.1.0.10		135/tcp	Tue, Feb 20, 2024 10:38 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	🔧	4.3 (Medium)	98 %	10.1.0.10		3389/tcp	Tue, Feb 20, 2024 10:38 AM UTC
TCP timestamps	🔧	2.6 (Low)	80 %	10.1.0.10		general/tcp	Tue, Feb 20, 2024 10:38 AM UTC

kuvio 6 ws1 haavoittuvaisuudet

Vulnerability		Severity ▼	QoD	Host IP	Name	Location	Created
CentOS: Security Advisory for bpftool (CESA-2022:5937)	🔧	5.5 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
CentOS: Security Advisory for bind (CESA-2022:6765)	🔧	5.0 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
CentOS: Security Advisory for device-mapper-multipath (CESA-2022:7186)	🔧	5.0 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
CentOS: Security Advisory for expat (CESA-2022:6834)	🔧	5.0 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
CentOS: Security Advisory for krb5-devel (CESA-2022:8640)	🔧	5.0 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
CentOS: Security Advisory for open-vm-tools (CESA-2022:6381)	🔧	5.0 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
CentOS: Security Advisory for rsync (CESA-2022:6170)	🔧	5.0 (Medium)	97 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:02 AM UTC
TCP timestamps	🔧	2.6 (Low)	80 %	10.2.0.10		general/tcp	Tue, Feb 20, 2024 11:01 AM UTC

kuvio 7. Onion haavoittuvaisuudet

Vulnerability		Severity ▼	QoD	Host IP	Name	Location	Created
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	↩	5.3 (Medium)	80 %	10.2.0.11		22/tcp	Tue, Feb 20, 2024 11:15 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	⚠	5.0 (Medium)	70 %	10.2.0.11		9200/tcp	Tue, Feb 20, 2024 11:18 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)	↩	4.3 (Medium)	95 %	10.2.0.11		22/tcp	Tue, Feb 20, 2024 11:15 AM UTC
TCP timestamps	↩	2.6 (Low)	80 %	10.2.0.11		general/tcp	Tue, Feb 20, 2024 11:15 AM UTC
ICMP Timestamp Reply Information Disclosure	↩	2.1 (Low)	80 %	10.2.0.11		general/icmp	Tue, Feb 20, 2024 11:15 AM UTC

kuvio 8. SIEM haavoittuvaisuudet

Vulnerability		Severity ▼	QoD	Host IP	Name	Location	Created
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	↩	5.3 (Medium)	80 %	10.2.0.12		22/tcp	Tue, Feb 20, 2024 11:17 AM UTC
SSL/TLS: Certificate Expired	↩	5.0 (Medium)	99 %	10.2.0.12		1515/tcp	Tue, Feb 20, 2024 11:18 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	⚠	5.0 (Medium)	70 %	10.2.0.12		1515/tcp	Tue, Feb 20, 2024 11:21 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)	↩	4.3 (Medium)	95 %	10.2.0.12		22/tcp	Tue, Feb 20, 2024 11:17 AM UTC
TCP timestamps	↩	2.6 (Low)	80 %	10.2.0.12		general/tcp	Tue, Feb 20, 2024 11:17 AM UTC
ICMP Timestamp Reply Information Disclosure	↩	2.1 (Low)	80 %	10.2.0.12		general/icmp	Tue, Feb 20, 2024 11:17 AM UTC

kuvio 9 SOAR haavoittuvuudet

Vulnerability		Severity ▼	QoD	Host IP	Name	Location	Created
jQuery < 1.9.0 XSS Vulnerability	⚠	6.1 (Medium)	80 %	10.2.0.14		general/tcp	Tue, Feb 20, 2024 11:39 AM UTC
jQuery < 1.9.0 XSS Vulnerability	⚠	6.1 (Medium)	80 %	10.2.0.14		general/tcp	Tue, Feb 20, 2024 11:39 AM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled	↩	5.8 (Medium)	99 %	10.2.0.14		80/tcp	Tue, Feb 20, 2024 11:39 AM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	↩	5.3 (Medium)	80 %	10.2.0.14		22/tcp	Tue, Feb 20, 2024 11:38 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	⚠	4.8 (Medium)	80 %	10.2.0.14		8888/tcp	Tue, Feb 20, 2024 11:38 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)	↩	4.3 (Medium)	95 %	10.2.0.14		22/tcp	Tue, Feb 20, 2024 11:38 AM UTC
TCP timestamps	↩	2.6 (Low)	80 %	10.2.0.14		general/tcp	Tue, Feb 20, 2024 11:38 AM UTC
ICMP Timestamp Reply Information Disclosure	↩	2.1 (Low)	80 %	10.2.0.14		general/icmp	Tue, Feb 20, 2024 11:37 AM UTC

kuvio 10 rocky haavoittuvaisuudet

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
jQuery < 1.9.0 XSS Vulnerability		6.1 (Medium)	80 %	10.2.0.13		general/tcp	Tue, Feb 20, 2024 11:55 AM UTC

kuvio 11 Kalin haavoittuvaisuudet

4.2 DMZ

Aloimme skannaamaan DMZ-verkosta haavoittuvaisuuksia ja ensimmäisenä laitteena olikin organisaation WWW palvelin (kuvio 12). Pääasialliset haavoittuvaisuudet olivat heikot KEX algoritmit ja itse www sivusta johtuneet varoitukset. Olemme aloittaneet jo kovennus toimenpiteet (kovennus kurssi 4. labra) ja tulevaisuudessa saammekin web sivujen turvallisuuden paremmaksi. Tällä hetkellä web palvelinta ajetaan Docker kontista, joten realistista riskiä koko järjestelmän kattavaan tietomurtoon ei synny.

NS1 laite ilmoitti myös heikoista avain algoritmeista (kuvio 13) , tulemme korjaamaan nämä haavoittuvaisuudet myöhemmin.

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)		5.3 (Medium)	80 %	10.4.0.11	www.group6.ttc60z.vle.fi	22/tcp	Tue, Mar 5, 2024 10:48 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)		5.0 (Medium)	70 %	10.4.0.11	www.group6.ttc60z.vle.fi	3306/tcp	Tue, Mar 5, 2024 10:52 AM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	10.4.0.11	www.group6.ttc60z.vle.fi	443/tcp	Tue, Mar 5, 2024 10:49 AM UTC
SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection		5.0 (Medium)	99 %	10.4.0.11	www.group6.ttc60z.vle.fi	443/tcp	Tue, Mar 5, 2024 10:49 AM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80 %	10.4.0.11	www.group6.ttc60z.vle.fi	80/tcp	Tue, Mar 5, 2024 10:49 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.3 (Medium)	98 %	10.4.0.11	www.group6.ttc60z.vle.fi	3306/tcp	Tue, Mar 5, 2024 10:49 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)		4.3 (Medium)	95 %	10.4.0.11	www.group6.ttc60z.vle.fi	22/tcp	Tue, Mar 5, 2024 10:48 AM UTC
TCP timestamps		2.6 (Low)	80 %	10.4.0.11	www.group6.ttc60z.vle.fi	general/tcp	Tue, Mar 5, 2024 10:48 AM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	10.4.0.11	www.group6.ttc60z.vle.fi	general/icmp	Tue, Mar 5, 2024 10:48 AM UTC

kuvio 12. WWW haavoittuvaisuudet

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	↶	5.3 (Medium)	80 %	10.4.0.10		22/tcp	Tue, Mar 5, 2024 11:07 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)	↶	4.3 (Medium)	95 %	10.4.0.10		22/tcp	Tue, Mar 5, 2024 11:07 AM UTC
TCP timestamps	↶	2.6 (Low)	80 %	10.4.0.10		general/tcp	Tue, Mar 5, 2024 11:07 AM UTC
ICMP Timestamp Reply Information Disclosure	↶	2.1 (Low)	80 %	10.4.0.10		general/icmp	Tue, Mar 5, 2024 11:07 AM UTC

kuvio 13. NS1 haavoittuvaisuudet

4.3 Servers-net

Viimeiseksi aloimme tutkimaan server-net verkkoa ja ensimmäisenä laitteena srv01:stä (kuvio 14). Heti alkuunsa löysimme kriittisen haavoittuvaisuuden, jonka aiomme korjata heti. Domain controllerista ei taas löytynyt niin paljoa haavoittuvaisuuksia (kuvio 15), pääasiassa vanhentuneita protokollia.

Valitettavasti jouduimme käymään WSUS laitteen läpi vain nmap portti skannauksella (kuvio 16), sillä ilmeisesti käyttämässämme greenbone skannerissa on yhteensopivuus ongelmia kyseisen laitteen kanssa. Näistä ei löytynyt mitään yllättävää

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Windows IExpress Untrusted Search Path Vulnerability	🔒	7.8 (High)	80 %	10.3.0.12		general/tcp	Tue, Mar 5, 2024 11:16 AM UTC
Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability	🔒	6.9 (Medium)	80 %	10.3.0.12		general/tcp	Tue, Mar 5, 2024 11:18 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	↶	5.0 (Medium)	80 %	10.3.0.12		135/tcp	Tue, Mar 5, 2024 11:18 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	↶	4.3 (Medium)	98 %	10.3.0.12		3389/tcp	Tue, Mar 5, 2024 11:17 AM UTC

kuvio 14. SRV01 haavoittuvaisuudet

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
DCE/RPC and MSRPC Services Enumeration Reporting	↶	5.0 (Medium)	80 %	10.3.0.10		135/tcp	Tue, Mar 5, 2024 11:20 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	↶	4.3 (Medium)	98 %	10.3.0.10		3389/tcp	Tue, Mar 5, 2024 11:20 AM UTC
ICMP Timestamp Reply Information Disclosure	↶	2.1 (Low)	80 %	10.3.0.10		general/icmp	Tue, Mar 5, 2024 11:18 AM UTC

kuvio 15. DC01 haavoittuvaisuudet

```

(kali@kali-ws)-[~]
$ nmap -sV 10.3.0.11
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-05 13:43 EET
Nmap scan report for 10.3.0.11
Host is up (0.0036s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc?
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

kuvio 16. Nmap skannaus wsus laitteesta

5 Riskianalyysi

5.1 Haavoittuvaisuudet

Skannaus tulosten perusteella suurin riski on servers-netin SRV01 laite. Tällä laitteella oli ympäristön ainut korkean riskin skannaus tulos ” Windows IExpress Untrusted Search Path Vulnerability” joka mahdollistaa koodin ajamisen järjestelmässä. Todennäköisimmin kuitenkin hyökkäyksen kohteena on www-palvelin, jossa on haavoittuvuus joka mahdollista DOS-hyökkäyksen. Palvelin myös käsittelee käyttäjiä, sekä salasanoja suojaamattomalla http-yhteydellä. Https yhteyden käyttöön-otto ratkoisi nämä ongelmat, ja sallisi esim. viestien ja tunnuksien salauksen (Digimarkkinointi nd).

Admin-net ympäristössä todennäköisin kohde voisi olla Onion. Se sisältää Cross-site scripting (XSS) haavoittuvuuden, jonka hyödyntäminen on kohtalaisen helppoa. Haavoittuvuus johtuu jQuery:n vanhentuneesta versiosta.

5.2 Suositellut korjaukset

Pidimme greenbone skannerista työkaluna, sillä mielestämme sen riskien pisteytys oli paikkansapitävää. Aiommekin alkaa korjaamaan ympäristöä pisteytyksien mukaan muodostuvassa prioriteetti järjestyksessä. Kriittisimpänä on saada SRV01 laite turvallisesti toimintaan. Tällä hetkellä olemme myös päivittämässä WWW palvelinta käyttämään https yhteyttä. Oletamme että näillä saamme kriittisimmät osuudet ajan tasalle.

Tämän jälkeen aiomme päivittää jokaisen ympäristön laitteen ajan tasalle ja tehdä uudet skannaukset. Oletamme että näillä saamme ympäristön hyvin toimintakuntoon.

6 Pohdinta

Mielestämme tehtävä sujui mukavasti ja tekeminen tuki hyvin kurssin oppimistavoitteita. Selkeän työnjaon ja tehtävänannon avulla emme kohdanneet juurikaan ongelmia. Materiaali tuki työskentelyä hyvin ja koemme oppineemme paljon tästä tehtävästä. Greenbone skannausten tekeminen oli osittain työlästä, sillä ympäristöä oltiin aiemmin kovennettu ja joudimme purkamaan kovenuksia, jotta skannaukset saatiin onnistumaan.

Lähteet

Digimarkkinointi. Kannattaako https ottaa käyttöön?. Viitattu 5.3.2024. <https://www.digimarkkinointi.fi/blogi/kannattaako-https-ottaa-kayttoon>

ISO/IEC 27002. 2022.Information security, cybersecurity and privacy protection — Information security controls. Oline SFS. Viitattu 20.2.2024.

