

**UNIVERZITET U SARAJEVU**  
**ELEKTROTEHNIČKI FAKULTET SARAJEVO**

# **DOMACA ZADACA 3**

## **TEHNOLOGIJE SIGURNOSTI**

**Student: Mašović Haris**

**Indeks: 1689/17993**

**Odsjek: Računarstvo i Informatika**

**Datum:**

**07.12.2020**

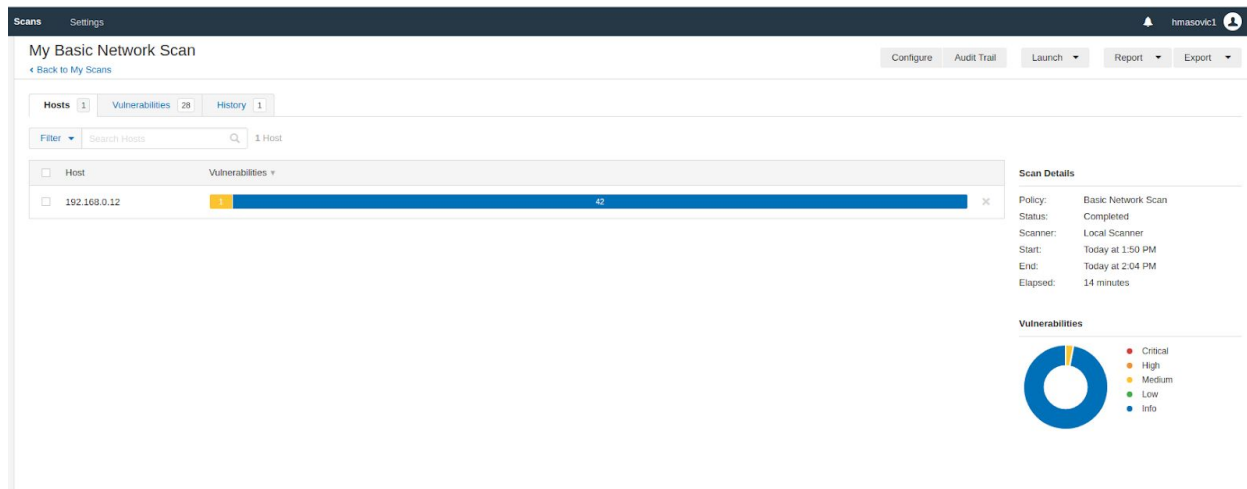
**Potpis:**

---

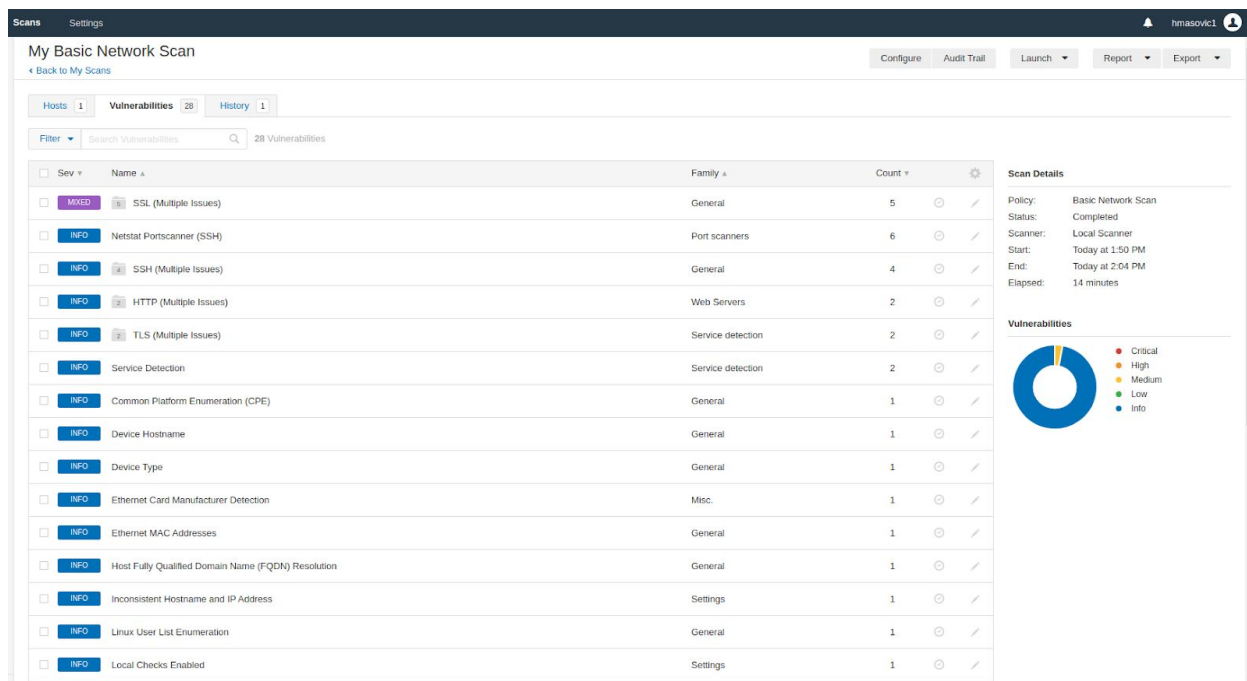
Potrebno je, koristeći Nessus alat za provjeru postojanja sigurnosnih propusta, pregledati vaš računar i napraviti izvještaj o rezultatima. Ovaj izvještaj je potrebno dostaviti putem Zamgera.

Rok za predaju zadaća je 10.12.2020.

Instaliran je nessus alat i izvršen basic scan. U nastavku su prikazani rezultati scan-a:



Svi rezultati skeniranja tj. rezultati ranjivosti su dati na sljedećim slikama:



<input type="checkbox"/>	INFO	Local Checks Enabled	Settings	1	⊙	/
<input type="checkbox"/>	INFO	mDNS Detection (Local Network)	Service detection	1	⊙	/
<input type="checkbox"/>	INFO	Nessus Scan Information	Settings	1	⊙	/
<input type="checkbox"/>	INFO	Nessus Server Detection	Service detection	1	⊙	/
<input type="checkbox"/>	INFO	Netstat Connection Information	General	1	⊙	/
<input type="checkbox"/>	INFO	OS Identification	General	1	⊙	/
<input type="checkbox"/>	INFO	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)	Misc.	1	⊙	/
<input type="checkbox"/>	INFO	SSL / TLS Versions Supported	General	1	⊙	/
<input type="checkbox"/>	INFO	Strict Transport Security (STS) Detection	Service detection	1	⊙	/
<input type="checkbox"/>	INFO	Target Credential Issues by Authentication Protocol - No Issues Found	Settings	1	⊙	/
<input type="checkbox"/>	INFO	Target Credential Status by Authentication Protocol - Valid Credentials Provided	Settings	1	⊙	/
<input type="checkbox"/>	INFO	Time of Last System Startup	General	1	⊙	/
<input type="checkbox"/>	INFO	Unix / Linux - Local Users Information : Passwords Never Expire	Misc.	1	⊙	/
<input type="checkbox"/>	INFO	Unix / Linux Running Processes Information	General	1	⊙	/

Kao sto se vidi na prethodnim slikama, vecina predstavlja INFO tip ranjivih propusta, dok jedan tip varijante (SSL) je MIXED tip. Shodno time detaljni prikaz te grupe propusta je dat u nastavku:

Hosts1

Vulnerabilities28

History1

Search Vulnerabilities

5 Vulnerabilities

<input type="checkbox"/>	Sev ▾	Name ▲	Family ▲	Count ▾	
<input type="checkbox"/>	MEDIUM	SSL Certificate Cannot Be Trusted	General	1	
<input type="checkbox"/>	INFO	SSL Certificate Information	General	1	
<input type="checkbox"/>	INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
<input type="checkbox"/>	INFO	SSL Cipher Suites Supported	General	1	
<input type="checkbox"/>	INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	

Vidimo da postoji SSL certifikat koji nije *trusted* i kojeg je nessus detektovao. Posto je ovaj tip propusta MEDIUM tipa, za njega je prikazana posebna slika u nastavku:

Hosts1

Vulnerabilities20

History1

MEDIUM

SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>  
<https://en.wikipedia.org/wiki/X.509>

Output

```

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=masha-unix
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

```

Port A

Hosts

8034 / tcp / www

192.168.0.12

Plugin Details

Severity:

Medium

ID:

51192

Version:

1.19

Type:

remote

Family:

General

Published:

December 15, 2010

Modified:

April 27, 2020

Risk Information

Risk Factor:

Medium

CVSS v3.0 Base Score:

6.5

CVSS v3.0 Vector:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS Base Score:

6.4

CVSS Vector:

CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Vidimo da u deskripciji ovog propusta je objasnjeno da serverski x.509 certifikat nije povjerljiv i da se treba ili kupiti ili generisati SSL certifikat za ovaj uredjaj. Vidimo da je CVSS score 6.5, te zbog toga ujedno je i postavljen kao MEDIUM prioritet.

Gledajući generalno, nema nekih bitnih propusta za istaknuti, vecinski su INFO tip, a i ovaj za certifikat ne predstavlja veliki problem, iako je MEDIUM tip.