# Ispitivanje kibernetičke sigurnosti brodskog radara

**Kukec, Matej**

**SVEUČILIŠTE U RIJECI**
**POMORSKI FAKULTET**

**MATEJ KUKEC**

# ISPITIVANJE KIBERNETIČKE SIGURNOSTI BRODSKOG RADARA

**DIPLOMSKI RAD**

Rijeka, 2022.

**SVEUČILIŠTE U RIJECI**
**POMORSKI FAKULTET**

# ISPITIVANJE KIBERNETIČKE SIGURNOSTI BRODSKOG RADARA

# A SHIPBOARD RADAR CYBER SECURITY TEST

**DIPLOMSKI RAD**

Kolegij: Sigurnost informacijskih sustava
Mentor: prof. dr. sc. Boris Sviličić
Studen: Matej Kukec
Studijski smjer: Elektroničke i informatičke tehnologije u pomorstvu
JMBAG: 0112073415

Rijeka, rujan 2022.

Student: Matej Kukec

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112073415

**IZJAVA O SAMOSTALNOJ IZRADI DIPLOMSKOG RADA**

kojom izjavljujem da sam diplomski rad s naslovom

**ISPITIVANJE KIBERNETIČKE SIGURNOSTI BRODSKOG RADARA**

izradio samostalno pod mentorstvom prof. dr. sc. Borisa Sviličić.

U radu sam primijenio metodologiju izrade stručnog/znanstvenog rada i koristio literaturu koja je navedena na kraju diplomskog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u završnom radu na uobičajen, standardan način citirao sam i povezao s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Suglasan sam s trajnom pohranom završnog rada u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta Sveučilišta u Rijeci te Nacionalnom repozitoriju Nacionalne i sveučilišne knjižnice.

Za navedeni rad dozvoljavam sljedeće pravo i razinu pristupa mrežnog objavljivanja:

a) rad u otvorenom pristupu

**b) pristup svim korisnicima sustava znanosti i visokog obrazovanja RH**

c) pristup korisnicima matične ustanove

d) rad nije dostupan

Student

Matej Kukec

Student: Matej Kukec

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112073415

IZJAVA STUDENTA – AUTORA

O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

Izjavljujem da kao student – autor diplomskog rada dozvoljavam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta.

U svrhu podržavanja otvorenog pristupa diplomskim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskog fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja mog diplomskog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/

Student – autor

## SAŽETAK

Brodski je radar jedna od glavnih komponenti sigurne navigacije broda. U ovome radu je provedeno kibernetičko testiranje sigurnosti radara Navi Sailor 4000 na školskome brodu Kraljica mora. Prikazani su rezultati testiranja kibernetičke sigurnosti brodskog radara pomoću vodećeg industrijskog alata, Nessus Professional. Analizirane su detektirane prijetnje od strane implementiranih komponenata implementiranog broskog radara.



Ključne riječi: kibernetička sigurnost u pomorstvu, radar, kibernetičke ranjivosti, skeniranje kibernetičkih ranjivosti



## SUMMARY

The ship's radar is one of the main components of a ship's safe navigation. In this paper, cyber security testing of the Navi Sailor 4000 radar was conducted on the training ship Kraljica Mora. The results of cyber security test of the shipboard radar using the leading industry software tool Nessus Professional were presented. The detected vulnerabilities, caused by implemented components of the shipboard radar, were analysed.



Keywords: maritime cyber security, radar, cyber vulnerabilities, cyber vulnerability scanning

# SADRŽAJ

# 1. UVOD

Brodska radarska oprema predstavlja značajnu pomoć u navigaciji posljednjih sedam desetljeća, omogućujući brodskoj posadi sigurnu i brzu plovidbu. Proteklih godina, kako se razvijala radarska tehnologija, ista je postala obvezan navigacijski alat potreban na bilo kojem brodu od 300 BT i više. Navedena se tehnologija počela koristiti za identifikaciju, praćenje i pozicioniranje plovila kako bi se poboljšalo izbjegavanje sudara i sigurno upravljalo brodom. Značajan napredak u računalnoj tehnologiji u posljednja dva desetljeća također je utjecao na razvoj radara, koji je doveo do složenih računalnih sustava.

S druge strane, upotreba računala svakodnevna je karakteristika ljudskoga života. Kroz povijest, računala su implementirana u gotovo svaku vrstu poslovanja, kako bi se omogućila veća učinkovitost i efikasnost. Također, razvoj interneta omogućio je komunikaciju između udaljenih uređaja, kao i njihovo upravljanje na daljinu.

Upravo zbog navedenih razloga, pomorska se industrija uvelike okrenula korištenju računalih tehnologija. Uvođenje računala u pomorsku industriju omogućilo je pomorcima i pomorskim kompanijama jednostavnije upravljanje brodskim sustavima i navigacijom. Međutim, postoji i negativna strana napretka računalne tehnologije, a to su kibernetički napadi. Uz pomoć modernih tehnika, računalni napadači postavili su pomorsku industriju kao značajni izvor prihoda. Zbog nedostatka računalnog razumijevanja, računalni napadači već u početku same problematike posjeduju značajnu prednost u odnosu na pomorsku industriju.

Posljednjih sedam desetljeća, razvoj radara rezultirao jest sustavom koji se temelji na računalnim sustavima, stoga se javila i potreba za zaštitom pomorstva i navigacije od kibernetičkih prijetnji. Kibernetička sigurnost jesu postupci i metode pomoću kojih se štite računala, web poslužitelji te mobilni uređaji od zlonamjernih napada. „NotPetya“ primjer je kibernetičkog napada koji je pogodio pomorsku industriju 2017. godine. Pomorska danska kompanija A.P. Moller-Maersk pretrpjela je novčanu štetu u iznosu od 300 milijuna američkih dolara.

2017. godine, Međunarodna pomorska organizacija (IMO, engl. *International Maritime Organization*) objavila je dokument „*Guidelines on maritime cyber risk management*“, kojim se usmjerava pozornost na važnost kibernetičke sigurnosti, kao i na važnost kibernetičkih propusta i ranjivosti. Objavljeni dokument sadrži smjernice za upravljanje pomorskim

kibernetičkim rizicima, u svrhu zaštite pomorskog prometa od strane kibernetičkih prijetnji i slabosti.

U ovome diplomskom radu provedeno je testiranje kibernetičke sigurnosti brodskog radara Wärtsilä Transas Navi Sailor 4000, koji je instaliran na školski brod Kraljica mora. Provedbom testiranja radara, prikazani su rezultati testiranja istoga pomoću vodećeg alata na području testiranja kibernetičke sigurnosti, Nessus Professional-a. Opisano je 12 detektiranih ranjivih točaka sustava te su ponuđena potencijalna rješenja istih. Također, analizirane su tri kritične detektirane prijetnje od strane implementiranih komponenata Transasova radara Navi Sailor 4000.

# 2. POMORSKI RADAR

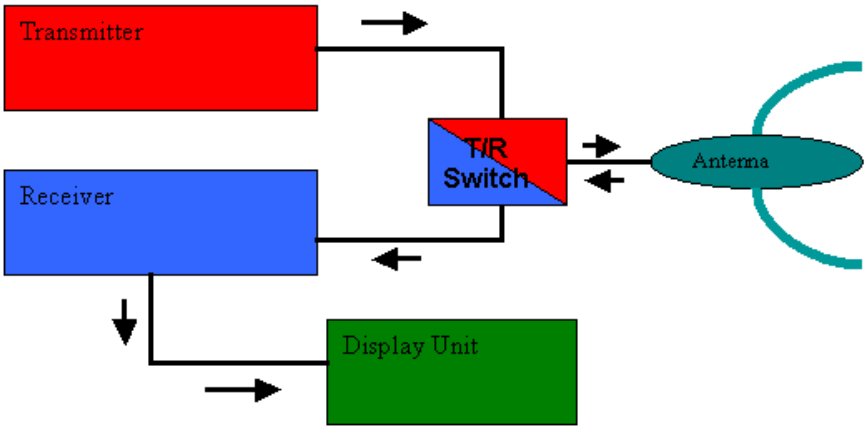
Radar predstavlja uređaj koji služi za otkrivanje objekata te mjerenje njihove udaljenosti pomoću radio valova. Riječ „RADAR“ zapravo je skraćenica engleskih riječi: RAdio Detecting and Ranging. Radar odašilje vrlo kratke impulse elektromagnetske energije u okolni prostor, koji se zatim odbijaju od objekta te se vraćaju do radarskog prijamnika. Povratak impulsa ukazuje na prisutnost određenog objekta u blizini vlastitog broda, dok vrijeme proteklo od odašiljanja impulsa do prijema istih proporcionalno je udaljenosti između broda i određenog objekta. Upravo je to razlog zašto se brodski radari nazivaju i „impulsnim radarima“ [1].

## 2.1. PRINCIP RADA POMORSKOG RADARA

Radar se sastoji od pet glavnih komponenti:

- Odašiljač (engl. *transmitter*)
- Prijemnik (engl. *receiver*)
- Pokazivač (engl. *display*)
- Antena (engl. *scanner*)
- T/R sklopka

Odašiljač je zadužen za odašiljanje impulsa elektromagnetske energije. T/R sklopka (engl. *Transmit/Receive*) predstavlja sklop koji omogućuje anteni da odašilje, odnosno prima impulse elektromagnetske energije. Prijemnik detektira, pojačava (engl. *amplifies*) te transformira primljene signale u vidljivi format koji se kasnije prikazuje na pokazivaču. Na slici 1 prikazane su komponente radara.




*Slika 1 Komponente radara*

Izvor: http://www.bom.gov.au/australia/radar/about/what_is_radar.shtml

Dvije su glavne karakteristike radara:

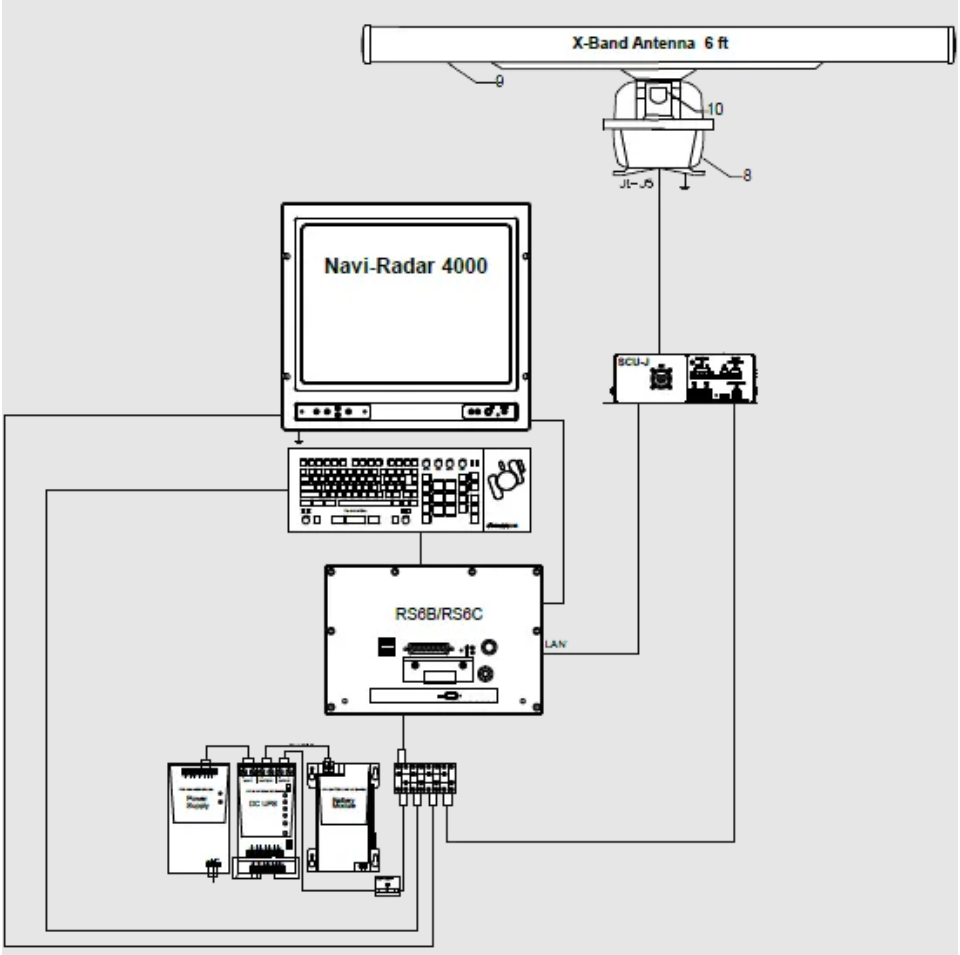
- Reflektivnost radara (engl. *reflectivity*)
- Brzina radara (engl. *velocity*)

Reflektivnost predstavlja mjeru koja nam govori koliko je odaslanih impulsa vraćeno (reflektirano) radarskom prijemniku nakon što su udarili u određeni objekt. Brzina radara predstavlja brzinu koja je bila potrebna da odaslani impulsi stignu do objekta te brzinu impulsa koja je bila potrebna da odaslani impulsi stignu do radarskog prijemnika. Kako bi se mjerile navedene brzine, potreban je Dopplerov radar.

Dopplerov radar bazira se na principu Dopplerovog efekta. Dopplerov efekt ili učinak jest pojava promjene u frekvenciji zvuka zbog relativnog gibanja izvora zvuka od slušatelja ili prema slušatelju. Kao popularni primjer Dopplerovog efekta uzimaju se vozila hitne pomoći te njihove sirene. Kada se vozila približavaju slušatelju, zvuk sirene je sve jači, odnosno kada se vozila udaljavaju od slušatelja zvuk postaje sve slabiji. Uz pomoć teorije Dopplerovog efekta, moguće je izračunati brzinu kretanja vozila hitne pomoći uz pomoć promjene frekvencije zvuka sirene. Istu princip rada koristi i Dopplerov radar, gdje se računa brzina potrebna da odaslani impulsi stignu do objekta te brzina impulsa koja je potrebna da odaslani impulsi stignu do radarskog prijemnika [1].

## 2.2. WÄRTSILÄ TRANSAS NAVI SAILOR RADAR 4000

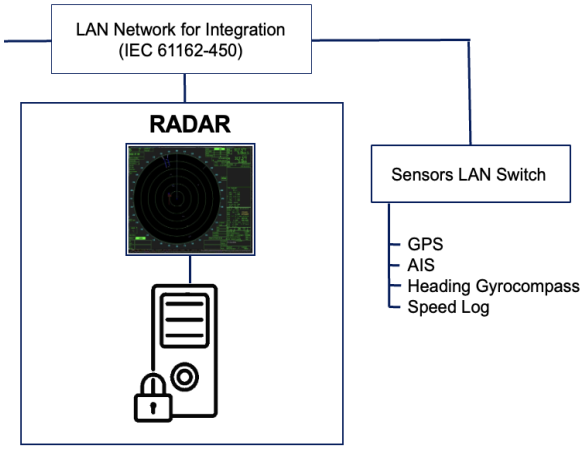
Navi Sailor Radar 4000 integrirani je radarski računalni sustav te je sastavni dio Wärtsilä Transas 4000 sustava. Navedeni je X-band radar implementiran na školski brod Kraljica mora, brod nad kojim je provedeno istraživanje. Navi Sailor radar računalni je sustav koji je standardiziran od strane Međunarodne pomorske organizacije 2016. godine (IMO, engl. *International Maritime Organization*), dok je na brod ugrađen 2019. godine. Na slici 2 nalazi se konfiguracija Wärtsilä Transas radara Navi Sailor 4000, dok su u tablici 1 prikazane specifikacije te sučelja instaliranog brodskog radara [2].




*Slika 2 Navi Sailor Radar 4000*

Izvor: https://www.wartsila.com/voyage/integrated-vessel-control-systems/navi-radar

Na slici 3 nalazi se arhitektura Navi Sailor radara. Radar je umrežen sa serijskom LAN (engl. *Local Area Network*) sklopkom. Navedena se sklopka koristi kao jedinica za prikupljanje podataka od strane NMEA (engl. *National Maritime Electronics Association*) senzora, putem serijske komunikacije. Podaci prikupljeni s primarnih senzora (pozicija, smjer i brzina) te podaci prikupljeni s dodatnih senzora, kao što su AIS (engl. *Automatic Identification System*) i NAVTEX (engl. *Navigational Telex*), šalju se radaru putem Ethernet mreže [3].




*Slika 3 Arhitektura Navi Sailor radara*

Izvor: Sviličić B., Bacasdoon J., Tawfik A.K., Pecota S., Towards a Cyber Secure Shipboard ECDIS, 2022.

| | | |
|---|---|---|
| RADAR | Proizvođač | Wärtsilä Transas |
| | Model | Navi Sailor 4000 |
| | Datum odobrenja | Srpanj, 2016. |
| | Datum ugradnje | Ožujak, 2019. |
| SUČELJE | Serijska NMEA | IEC61162-1 |
| | Serijska najveća brzina | IEC61162-2 |
| | Ethernet | IEC61162-450 |
| | Ažuriranje | USB sučelje |

*Tablica 1 Specifikacije i sučelja instaliranog radara*

## 2.3. KRALJICA MORA

U svrhu ovoga diplomskog rada, testiranje kibernetičke sigurnosti brodskog radara provedeno je na školskome brodu Kraljica mora. Navedeni je brod namijenjen za educiranje učenika srednjih škola te studenata Pomorskih fakulteta, dok je isti u vlasništvu Ministarstva mora, prometa i infrastrukture. Riječ je o jedrenjaku s dva jarbola koji je dugačak 35 metara, širok 8.55 metara, dok njegov gaz iznosi 2.65 metara. Tonaža Kraljice mora iznosi 298, dok postiže maksimalnu brzinu od 6 čvorova ukoliko koristi jedra, odnosno postiže brzinu od 11 čvorova ukoliko koristi motorni pogon. Navedeni brod posjeduje kapacitet od 28 učenika/studenata, četvero nastavnika te sedmero članova posade. Porinuće broda dogodilo se 2009. godine, dok je 2013. godine hrvatska kompanija Jadrolinija odgovorna je za upravljanje istim. Na slici 4 prikazan je školski brod Kraljica mora [4].

*Slika 4 Kraljica mora*

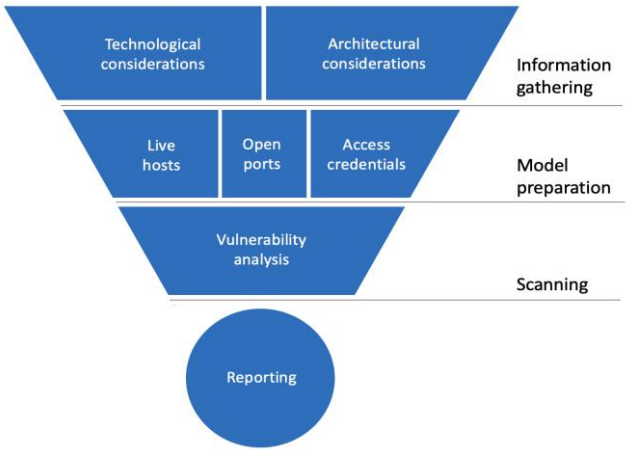
Izvor: https://morski.hr/2021/03/05/nasukao-se-skolski-brod-kraljica-mora/

# 3. SKENIRANJE RANJIVOSTI

Kibernetičko skeniranje ranjivosti radara predstavlja proces testiranja radarskog sustava u svrhu detekcije, klasifikacije te izvještaja o sigurnosnim nedostacima i ranjivostima. Navedeno se skeniranje provodi koristeći računalni softver koji je instaliran na prijenosno računalo, gdje je prijenosno računalo povezano s radarskim sustavom. Skeneri ranjivosti koriste bazu podataka kako bi se usporedili rezultate skeniranja s već otkrivenim nedostacima i ranjivostima. Unutar spomenutih baza podataka nalaze se informacije o nedostacima i ranjivostima pomoću kojih računalni napadači mogu pristupiti osjetljivim i privatnim informacijama. Nakon provedenog skeniranja, prikazuju se rezultati istoga te se ujedno nude i moguća rješenja detektiranih nedostataka i ranjivosti [3].

## 3.1. PROCES KIBERNETIČKOG SKENIRANJA RANJIVOSTI

Proces kibernetičkog skeniranja ranjivosti započinje prikupljanjem relevantnih informacija o određenom sustavu (u ovome slučaju, radarskom sustavu). Informacije o sustavu se prikupljaju putem razgovora s posadom, odnosno korištenjem tehničke dokumentacije radarskog sustava. Sljedeća je faza priprema modela skeniranja, koji se sastoji od tri koraka: utvrđivanje aktivnih sustava, pronalazak aktivnih priključaka i servisa te stjecanje ovlasti s korisničkim podacima za pristup sustavu. Posljednja jest faza skeniranje sustava [3].



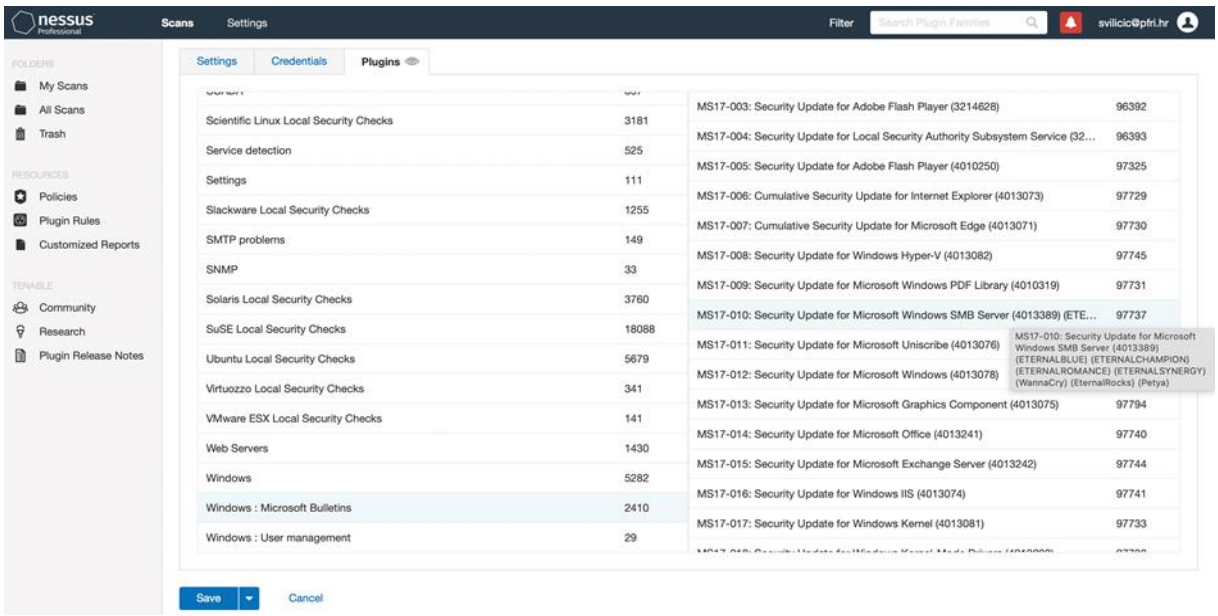

*Slika 5 Proces kibernetičkog skeniranja ranjivosti*

Izvor: Sviličić B., Bacasdoon J., Tawfik A.K., Pecota S., Towards a Cyber Secure Shipboard ECDIS, 2022.

### 3.2. NESSUS PROFESSIONAL

Testiranje sigurnosti provedeno je uz pomoć računalnog programa Nessus Professional. Nessus Professional posjeduje mogućnost skeniranja sustava na Unix, Linux te Windows platformama. Također, Nessus Professional podržava skeniranje sustava na daljinu. Verzija u trenutku testiranja radara te pisanja ovog diplomskog rada jest 8.15.2. [5]. Navedeni je program bio instaliran na prijenosno računalo te se ispitivanje sigurnosti provelo u trenutku kada je brod bio na vezu. Testiranje se provelo na način da se prijenosno računalo priključilo na brodsku lokalnu mrežu.

Detektirani sigurnosni propusti prikazuju se pomoću pripadajućih *plugin-ova*. Kako su ranjivosti otkrivene te objavljene u javnosti, kompanija Tenable Research razvija programe (*plugin-ove*) koji spomenute ranjivosti detektiraju. Navedeni programi razvijeni su skriptnome jeziku Nessus Attack Scripting Language. Razvijeni programi koriste se kao izvor informacija o ranjivosti te kao programski paket koji koristi algoritme za ispitivanje prisutnosti sigurnosnih ranjivosti. Tijekom pisanja ovog diplomskog rada, kompanija Tenable Research je objavila 172907 *plugin-ova* [6]. Slika 6 prikazuje dio *plugin-ova* koji se koriste tijekom „Basic Network Scan“ modela skeniranja.




*Slika 6 Basic Network Scan: dio korištenih plugin-ova*

Izvor: Sviličić B., Bacasdoon J., Tawfik A.K., Pecota S., Towards a Cyber Secure Shipboard ECDIS, 2022.

### 3.3. ZAJEDNIČKI SUSTAV BODOVANJA RANJIVOSTI

Sigurnost informacijskih sustava primarni je cilj, ali i problem svake kompanije. Značajna se količina novca, kao i vremena, ulaže u postizanje zadovoljavajuće razine sigurnosti informacijskih sustava. CVSS (engl. *Common Vulnerability Scoring System*) značajan jest faktor u povećanju razine sigurnosti informacijskih sustava.

CVSS predstavlja industrijski standard za ocjenjivanje ozbiljnosti sigurnosnih ranjivosti informacijskog sustava. Značajan broj kompanija koristi navedeni sustav tijekom uspostave razine ozbiljnosti određene ranjivosti u odnosu na ostale slične ranjivosti. Na taj se način određuju prioriteti i određuje hitnoća kod uklanjanja određenih ranjivosti sustava. CVSS omogućuje precizna mjerenja, kao i njihovo ponavljanje. Rezultati mjerenja bazirani su na mnoštvu provedenih mjerenja te stručnim procjenama. Upravo je zato CVSS prikladan sustav mjerenja za industrije, kompanije i vlade gdje su potrebni točni i nepromjenjivi rezultati utjecaja ranjivosti.

CVSS jest rješenje problema nekompatibilnih bodovnih sustava (npr. CERT-ov sustav bodovanja ranjivosti, SANS-ov sustav bodovanja ranjivosti te Microsoft-ov sustav bodovanja itd.). Izgradnja zajedničkoga jezika, odnosno sustava bodovanja od iznimne je važnosti za mnoštvo kompanija te donosi veliku dobit menadžerima, analitičarima ranjivosti te proizvođačima sigurnosne opreme i aplikacija. Dakle, navedeni se standard koristi u svrhu računanja ozbiljnosti ranjivosti koja je pronađena u sustavu te određivanja prioriteta uklanjanja ranjivosti.

S druge strane, svaka je kompanija osjetljiva na različite ranjivosti te određeni sigurnosni propusti nisu jednako kritični za svaku kompaniju. Svaka kompanija CVSS tumači na svoj karakterističan način te ih prilagođavaju vlastitim potrebama, odnosno potrebama politike kompanije.

Primjeri korisnika koji koriste CVSS:

- Isporučitelji izvješća o ranjivostima: u besplatnim izvješćima o ranjivosti, isporučitelji objavljuju CVSS rezultate bodovanja ranjivosti. Unutar izvješća nalaze se informacije o ranjivostima kao što su datumi otkrivanja ranjivosti, ugroženi sustavi te preporučeni načini uklanjanja ranjivosti.
- Isporučitelji programskih aplikacija: isporučitelji programskih aplikacija korisnicima omogućuju prikaz CVSS rezultata. Time je omogućen bolji uvid u ozbiljnost

sigurnosnih propusta koji se mogu pronaći u njihovim proizvodima. Na taj način korisnici mogu učinkovito upravljati sigurnosnim rizicima.

- Skeniranje i upravljanje ranjivostima: kompanije čiji je zadatak pronalaženje i upravljanjem ranjivostima skeniraju mrežu, kako bi detektirali propuste u računalnim sustavima. Korisnici skenera ranjivosti koriste dobivene rezultate za učinkovitije donošenja odluka na području sigurnosne politike. Gubici se tako pokušavaju reducirati te se izvodi zaštita od računalnih prijetnji.
- Upravljanje sigurnosnim rizicima: kompanije čiji je zadatak upravljanje sigurnosnim rizicima također koriste CVSS rezultate bodovanja ranjivosti. Takve kompanije koriste CVSS kao ulaznu vrijednost prilikom izračuna razine rizika ili prijetnje [29].

## 3.4. NACIONALNA BAZA PODATAKA RANJIVOSTI

Nacionalna baza podataka ranjivosti predstavlja repozitorij s podacima o računalnim ranjivostima. Nacionalnom bazom podataka ranjivosti upravljan je od strane Nacionalnog instituta za standarde i tehnologiju Sjedinjenih Američkih Država. Repozitorij se ažurira svakodnevno te sadrži informacije o gotovo 12000 računalnih ranjivosti. Isti omogućuje korisnicima pretraživanje ranjivosti te filtriranje rezultata prema: nazivu proizvoda (npr. Microsoft Office), nazivu proizvođača (npr. Microsoft) te CVE (engl. *Common Vulnerabilities and Exposures*) identifikatoru [30].

## 3.5. IDENTIFIKACIJSKI SUSTAV RANJIVOSTI I IZLOŽENOSTI

CVE predstavlja identifikacijski sustav ranjivosti (bazu podataka), gdje svaka ranjivost posjeduje jedinstveni identifikator, kratko obrazloženje ranjivosti te CVSS vrijednost. CVE jest praktičan i pouzdan način za proizvođače, kompanije te razne akademije i sveučilišta da razmjenjuju informacije o kibernetičkim propustima. Prije uvođenja CVE-a, proizvođači su imenovali sigurnosne propuste na različite načine, što je administratorima sustava stvaralo značajne probleme kod praćenja propusta te ažuriranja sustava. CVE je omogućio da se za svaki propust uvede jedinstveni identifikator u formatu CVE-<godina>-<broj>. Proizvođače se poziva na korištenje CVE standarda, kako bi se reducirali potencijalni nesporazumi koji se odnose na proizvoljno imenovanje sigurnosnih propusta [31].

# 4. PROVEDBA ISPITIVANJA

Detekcija ranjivosti predstavlja računalnu metodu kojom se detektiraju kibernetičke ranjivosti. Navedenim su kibernetičkim ranjivostima upoznati proizvođači softvera/operacijskog sustava, kao i računalni napadači. Na slici 7 prikazana je provedba testiranja radara na Kraljici mora.

*Slika 7 Testiranje radara na Kraljici mora*

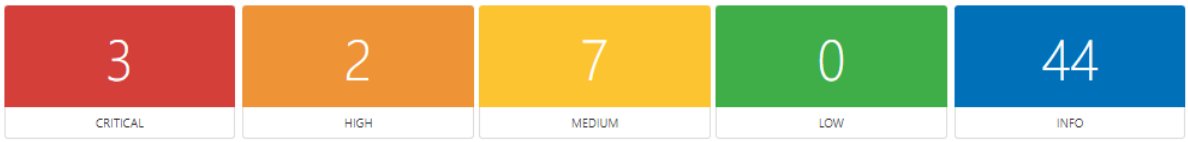
Izvor: autor

Testiranja provedena prijašnjih godina ukazuju da su upravo operacijski sustavi najslabije karike na području pomorske kibernetičke sigurnosti. Bitno je napomenuti da se veliki dio pomorskih sustava, kao što je Navi Sailor Radar 4000, sastoji od operacijskih sustava koji su potpuno neovisni o okruženju u kojega se implementiraju.

Stoga se koristi engleski termin: „*third-party component*“. Treća strana predstavlja kompaniju koja je zadužena za proizvodnju ili prodaju opreme za korištenje unutar računala ili periferije veće kompanije, gdje ta ista veća kompanija ne sudjeluje u razvoju navedene opreme. Iako korištenje neovisnih (vanjskih) aplikacija umanjuje novčana ulaganja u razvojnom procesu, navedene aplikacije kritična su prijetnja kibernetičkoj sigurnosti sustava [7].

## 4.1. REZULTATI ISPITIVANJA

Slika 8 prikazuje rezultate provedenog testiranja kibernetičke sigurnosti radara. Nessus Professional detektirao je 12 ranjivih točaka, od kojih su tri kategorizirane kao kritične. Dvije su prijetnje kategorizirane kao visoka razina prijetnje, dok je njih sedam kategorizirano pod srednju razinu prijetnje.

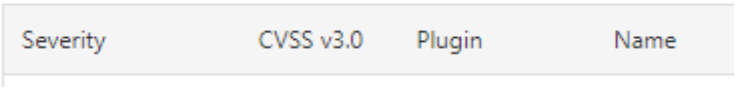



*Slika 8 Rezultati provedenog testiranja*

Izvor: autor

## 4.2. LISTA PRONAĐENIH RANJIVOSTI

Nessus Professional rezultate ispitivanja prikazuje strukturirano, po stupcima (slika 9). Prvi je stupac pokazatelj ozbiljnosti sigurnosnih propusta te dodjeljuje atribute: kritična, visoka, srednja te niska opasnost. Nadalje, stupac CVSS (engl. *Common Vulnerability Scoring System*) prikazuje sustav rangiranja karakteristika sigurnosnih ranjivosti. Brojčana vrijednost karakterizira ozbiljnost ranjivosti. CVSS je korisna vrijednost kod procjene i određivanja prioritetnih sigurnosnih prijetnji. Navedena vrijednost pomaže kompanijama kod donošenja ispravnih odluka, odnosno kod određivanja načina rješavanja sigurnosnih prijetnji. Kompanija Tenable Research koristi CVSS vrijednosti koje su prikupljene od strane Nacionalne baze podataka ranjivosti (engl. *National Vulnerability Database*) [8]. Preostali su stupci „Plugin“ i „Name“, koji predstavljaju broj *plugin-a*, odnosno naziv istoga.




*Slika 9 Atributi rezultata ispitivanja*

Izvor: autor

### 4.3. RANJIVOSTI KRITIČNE RAZINE

U potpoglavlju 4.3. objašnjene su tri kibernetička prijetnje, koje su klasificirane kao kritične. Tri kritične kibernetičke prijetnje otkrivene su pomoću *plugin-ova* pod brojevima 153952, 1148367 te 108797. Slika 10 prikazuje tri kritične ranjivosti, koje su detektirane pomoću Nessus Professional-a.

| Severity | CVSS v3.0 | Plugin | Name |
|---|---|---|---|
| CRITICAL | 7.5 | 153952 | Apache 2.4.49 < 2.4.51 Path Traversal Vulnerability |
| CRITICAL | 10.0 | 148367 | Python Unsupported Version Detection |
| CRITICAL | 10.0 | 108797 | Unsupported Windows OS (remote) |

*Slika 10 Ranjivosti kritične razine*

Izvor: autor

**153952** – „*Apache 2.4.49 < 2.4.51 Path Traversal Vulnerability*“ - udaljeni web poslužitelj posjeduje ranjivost. Apache verzija 2.4.49 nije aktualna verzija web poslužitelja. Verzija 2.4.49 posjeduje sljedeće ranjivosti:

- Računalni napadač može steći mogućnost pristupa datotekama koje su pohranjene na web poslužitelju
- Računalni napadač može manipulirati i kontrolirati URL zahtjeve koji stignu na web poslužitelj

„*Path Traversal Vulnerability*“ predstavlja ranjivost gdje računalni napadači mogu pristupiti datotekama na serveru na kojemu je pokrenuta određena aplikacija. Time se dovodi u opasnost sigurnost aplikacijskog programskog koda, kao i sigurnost povjerljivih informacija o samome sustavu.

Kao primjer navedene ranjivosti poslužit će određena internetska trgovina, te slike proizvoda koje se nalaze na internetskoj stranici trgovine. Slike su na internetskoj trgovini prikazane pomoću HTML protokola: „<img src="/loadImage?filename=218.png">“. Navedeni loadImage URL (engl. Uniform Resource Locator, adresa određene internetske stranice ili datoteke na internetu.) koristi filename parametar kako bi prikazao specifičnu datoteku. Specifična datoteka pohranjena jest na lokaciji „/var/www/images/218.png“. Ukoliko aplikacija ne posjeduje kvalitetne sigurnosne protokole, računalni napadač može promijeniti spomenuti URL u: „https://insecure-website.com/loadImage?filename=../../../etc/passwd“, kako bi osigurao pristup osjetljivoj informaciji (u ovome slučaju to je korisnička lozinka).

Naredba ../ koristi se u svrhu pristupa direktoriju koji se, hijerarhijski gledano, nalazi „stepenicu“ iznad određenog direktorija. Naredba ../../../ omogućuje prelazak iz direktorija „/var/www/images/218.png“ u korijenski direktorij (engl. root directory), gdje se omogućuje pristup datoteci: „/etc/passwd“ [21][22].

Rješenje: nadogradnja Apache poslužitelja na verziju 2.4.51 ili jednu od viših [9].

**148367** – „*Python Unsupported Version Detection*“ – zastarjela/ne podržana verzija Pythona. Verzija Pythona instalirana na testiranom sustavu je zastarjela te ju proizvođač više ne podržava. Time se ukazuje da proizvođač više neće objaviti nove sigurnosne zakrpe.

Rješenje: nadogradnja Pythona na verziju koja posjeduje podršku [10].

**108797** – „*Unsupported Windows OS*“ – zastarjeli/ne podržani operacijski sustav. Testirani radar na Kraljici mora koristi Microsoft Windows 7 Professional. Navedeni je sustav nadograđen posljednjom verzijom servisnog paketa (engl. *Service Pack 1*), podrška za operacijski sustav Microsoft Windows 7 Professional jest ukinuta 2019.

Rješenje: nadogradnja operacijskog sustava na inačicu koja posjeduje podršku [11].

### 4.4. RANJIVOSTI VISOKE RAZINE

U potpoglavlju 4.4. objašnjene su dvije kibernetička prijetnje, koje su klasificirane kao ranjivosti visoke razine. Dvije kibernetičke prijetnje visoke razine otkrivene su pomoću *plugin-*

*ova* pod brojevima 42873 te 153884. Slika 11 prikazuje dvije ranjivosti visoke razine, koje su detektirane pomoću Nessus Professional-a.

| | | | |
|---|---|---|---|
| HIGH | 5.0 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 4.3 | 153884 | Apache 2.4.49 < 2.4.50 Multiple Vulnerabilities |

*Slika 11 Ranjivosti visoke razine*

Izvor: autor

**42873** – „*SSL Medium Strength Cipher Suites Supported (SWEET32)*“ – koristi se set algoritama koji pružaju enkripciju podataka srednje razine. Pod enkripciju srednje razine Nessus Professional smatra svaku enkripciju gdje duljina enkripcijskih ključeva iznosi najmanje 64 bita, dok najviše iznosi 112 bitova.

SSL (engl. *Secure Sockets Layer*) jest protokol koji pruža mogućnost enkripcije podataka. SSL se koristi za sigurnost komunikacije između web poslužitelja i klijenta (web preglednik). SSL omogućuje prijenos podataka između klijenta i web poslužitelja na način da ih nije moguće presresti i pročitati. Upravo zato, koristi se set algoritama za enkripciju podataka, kako računalni napadači ne bi presreli razmjenu podataka između klijenta i web poslužitelja.

U ovome slučaju, SSL koristi algoritme za enkripciju podataka koji „sjeckaju“ podatke u takozvane „blokove podataka“. Algoritmi poput Triple DES-a (engl. *Data Encryption Standard*) te Blowfish-a jesu enkripcijski algoritmi čiji blokovi podataka iznose 64 bita. S druge strane, AES (engl. *Advanced Encryption Standard*) jest enkripcijski algoritam čiji blokovi podataka iznose 128 bita. Čime je duljina bloka podataka manja, veća je mogućnost da računalni napadač presretne podatke [23].

Rješenje: preporučuje se izbjegavanje seta algoritama koji pružaju enkripciju srednje razine [12].

**153884** – „*Apache 2.4.49 < 2.4.50 Multiple Vulnerabilities*“ - udaljeni web poslužitelj posjeduje ranjivosti. Apache verzija 2.4.49 nije aktualna verzija web poslužitelja. Verzija 2.4.49 posjeduje sljedeće ranjivosti:

- De – referencija null pokazivača tijekom HTTP/2 zahtjeva. Time se napadaču omogućuje izvršenje napada na raspoloživost resursa.
- Računalni napadač može steći mogućnost pristupa datotekama koje su pohranjene na web poslužitelju
- Računalni napadač može manipulirati i kontrolirati URL zahtjeve koji stignu na web poslužitelj

Kada server zaprimi HTTP (engl. Hypertext Transfer Protocol) zahtjev, server ga obrađuje. HTTP protokol „handler" provjerava veličinu zaglavlja prema postavljenim konfiguracijama na serveru. U HTTP protokolu jesu definirani zaglavlje i tijelo. Cilj je provjeriti je li zaglavlje manje od određene veličine. Ukoliko je ograničenje prekršeno, tada se na HTTP zahtjev šalje odgovarajući HTTP odgovor (engl. *response code*). HTTP odgovor poručuje zašto određeni zahtjev nije validan.

Međutim, kod verzije Apache HTTP servera 2.4.49, HTTP odgovor nije bio u potpunosti inicijaliziran za HTTP/2 protokol „handler". Ukoliko bi zaglavlje prekršilo ograničenje, tada je dolazilo do dereferencije null pokazivača.

Kada serveri zaprimaju HTTP zahtjeve, oni moraju stvoriti dretve, koje upravljaju zaprimljenim zahtjevima. U slučaju dereferencije null pokazivača, dretve jednostavno prestaju djelovati. Dakle, null pokazivač pokazuje na memoriju koja zapravo ne postoji. Shodno tome, od trenutka otkrića navedenog propusta, računalni napadači su mogli izrađivati HTTP zahtjeve, koji bi kasnije izazvali dereferenciju null pokazivača. U tome slučaju, dereferencija dovodi do rušenja servera (sustava) [24].

Rješenje: nadogradnja Apache poslužitelja na verziju 2.4.50 ili jednu od viših [13].

### 4.5. RANJIVOSTI SREDNJE RAZINE

U potpoglavlju 4.5. objašnjeno jest sedam kibernetičkih prijetnji, koje su klasificirane kao ranjivosti srednje razine. Sedam kibernetičkih prijetnji srednje razine otkrivene su pomoću *plugin-ova* pod brojevima 51192, 57582, 104743, 11213, 57608, 45411 te 65821. Slika 12 prikazuje sedam ranjivosti visoke razine, koje su detektirane pomoću Nessus Professional-a.

| | | | |
|---|---|---|---|
| MEDIUM | 6.4 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.4 | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.1 | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.0 | 11213 | HTTP TRACE / TRACK Methods Allowed |
| MEDIUM | 5.0 | 57608 | SMB Signing not required |
| MEDIUM | 5.0 | 45411 | SSL Certificate with Wrong Hostname |
| MEDIUM | 4.3 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |

*Slika 12 Ranjivosti srednje razine*

Izvor: autor

**51192** – „*SSL Certificate Cannot Be Trusted*“ – SSL certifikat nije valjan. Budući da SSL certifikat u ovome slučaju nije pouzdan, razlozi ove detekcije ranjivosti mogu biti:

- SSL certifikat nije potpisan (izdan) od strane pouzdanih izdavača SSL certifikata.
- SSL certifikat nije bio valjan tijekom provedenog skeniranja sustava.

SSL (engl. Secure Sockets Layer) jest protokol koji pruža mogućnost enkripcije podataka. SSL se koristi za sigurnost komunikacije između web poslužitelja i klijenta (web preglednik). U tome je slučaju potreban određeni certifikat, koji dokazuje da se na određenoj web stranici koristi enkripcija podataka. Zato se koristi SSL certifikat.

„*SSL Certificate Cannot Be Trusted*“ upućuje da je SSL certifikat potpisan od strane SSL izdavača koji nije na listi pouzdanih izdavača korisničkog web preglednika (npr. Google Chrome) [25].

Rješenje: Upotreba valjanog SSL certifikata [14].

**57582** – „*SSL Self-Signed Certificate*“ – legitimnost navedenog potpisa nije potvrđena od strane pouzdanih izdavača SSL certifikata.

„*SSL Self-Signed Certificate*“ upućuje da je SSL certifikat potpisan od strane samog servera. Navedena vrsta certifikata jest besplatna te se često koristi u svrhu testiranja web stranica. Takvi certifikati nisu izdani od strane pouzdanih izdavača SSL certifikata [26].

Navedeni problem može dovesti do kibernetičkog napada koji se naziva „Man in the middle“ napad. Isti predstavlja napad gdje napadač presreće poruke (informacije) te manipulira

razgovorom između dvije strane (klijenta i servera). Tada napadač može saznati osjetljive informacije poput zaporki korisničkih računa, detalje korisničkog računa ili bankovnog računa, brojeve kreditnih kartica i slično.

Rješenje: Upotreba valjanog SSL certifikata [15].

**104743** – „*TLS Version 1.0 Protocol Detection*“ – koristi se zastarjela verzija TLS (engl. *Transport Layer Security*). TLS protokol jest unaprijeđena verzija SSL protokola, stoga se TLS također koristi za sigurnost komunikacije između web poslužitelja i klijenta (web preglednik). Početkom 2020. godine, TLS protokoli 1.0 i 1.1 su napušteni od strane web preglednika.

Rješenje: korištenje TLS protokola verzija 1.2 i 1.3 te njihove podrške. Također, preporučen je prekid korištenja TLS protokola 1.0 i njegove podrške [16].

**11213** – „*HTTP TRACE / TRACK Methods Allowed*“ – opcija „debugging “ je omogućena na web poslužitelju. Web poslužitelj omogućuje korištenje „TRACE“ i „TRACK“ metoda. Navedene su metode HTTP protokoli koji su korišteni u svrhu otklanjanja grešaka kod konekcija web poslužitelja.

Opcija *trace* predstavlja metodu koja „reflektira“ zahtjev koji je poslan web poslužitelju, od strane klijenta (korisnika). Time je omogućeno korisniku vidjeti zahtjev koji je poslao web poslužitelju.

Ukoliko je opcija *trace* omogućena na web poslužitelju, isti je doveden u opasnost od izvršenja računalnih napada uz pomoć skripti (engl. *Cross-site scripting*). Računalni napadač u mogućnosti je izraditi skriptu, koja se sama pokreće onoga trenutka kada dospije na korisničko računalo. Takve skripte najčešće dospijevaju na korisničko računalo putem elektroničke pošte, odnosno putem internetskog linka koji je poslan od strane računalnog napadača. Unutar skripte implementirana jest naredba *trace* te ukoliko je omogućeno korištenje opcije *trace* na web poslužitelju, napadač može saznati korisničke kolačiće (engl. *user's cookies*) [27].

Rješenje: preporučeno je onemogućiti korištenje iznad navedenih metoda [17].

**57608** – „*SMB Signing not required*“ – izostanak potrebe potpisa na SMB (engl. *Server Message Block*) poslužitelju.

Navedeni problem može dovesti do kibernetičkog napada koji se naziva „Man in the middle“ napad. Isti predstavlja napad gdje napadač presreće poruke (informacije ) te manipulira razgovorom između dvije strane (klijenta i servera). Tada napadač može saznati osjetljive informacije poput zaporki korisničkih računa, detalje korisničkog računa ili bankovnog računa, brojeve kreditnih kartica i slično.

SMB jest protokol koji se koristi u svrhu klijent-server komunikacije gdje se omogućuje pristup datotekama, printerima ili serijskim priključcima putem interneta. SMB koristi metodu *request-response*, gdje klijent šalje SMB zahtjev na server radi uspostave komunikacije. Kada server dohvati zahtjev, isti šalje SMB odgovor klijentu te dolazi do uspostave komunikacije.

SMB potpisivanje, poznato i kao sigurnosno potpisivanje jest sigurnosni mehanizam SMB protokola. SMB potpisivanje omogućuje digitalni potpis poslanih podataka. Kada je SMB potpisivanje uključeno, svaka poruka koja se šalje pomoću SMB protokola posjeduje potpis koji se sastoji od sadržaja poruke, koja je šifrirana pomoću AES algoritma. Time je omogućena provjera sadržaja poruke od strane primatelja. Nadalje, SMB potpis potvrđuje identitet pošiljatelja/primatelja. Ukoliko sadržaj poruke ne odgovara potpisu, primatelj zna da je poruka oštećena [28].

Rješenje: opcija potpisivanja poruka mora biti uključena [18].

**45411** – „*SSL Certificate with Wrong Hostname*“ – SSL certifikat namijenjen je drugome poslužitelju.

Rješenje: Upotreba valjanog SSL certifikata [19].

**65821** – „*SSL RC4 Cipher Suites Supported (Bar Mitzvah)*“ – koristi se enkripcija podataka koja je popularna bila tijekom 80-ih godina prošlog stoljeća. RC4 (Rivest Chiper) jest vrsta enkripcije koja enkriptira datoteku bit po bit. Problem navedene enkripcije jest ta da ista nije dovoljno nasumična. Tada je računalni napadač u mogućnosti otkriti dijelove izvorne (kodirane) poruke.

Rješenje: onemogućiti korištenje RC4 enkripcije podataka. Preporučuje se korištenje TLS 1.2 protokola te njegove podrške [20].

Nakon obrađenih prijetnji srednje razine, opisane su sve prijetnje detektirane od strane Nessus Professional-a. Preostale 44 detekcije su zapravo informativnog karaktera te se neće pojasniti u ovome radu. Takve informacije nisu prijetnja sustavu, već prikazuju stanje skeniranog sustava te pomažu u donošenju odluka na području sigurnosne politike.

### 4.6. ANALIZA RANJIVOSTI

Nakon obrade dobivenih rezultata skeniranja Nessus Professional-a, analizirat će se tri kritične kibernetičke ranjivosti te njihov utjecaj na sustav. Budući da se testiranje sigurnosti radara provelo u trenutku dok je brod bio na vezu te dok Wärtsilä Transas Navi Sailor radar 4000 nije bio priključen na internet, detektirane ranjivosti zapravo ne predstavljaju kibernetičke rizike visokog nivoa. S druge strane, iako internetska konekcija u trenutku skeniranja sustava nije bila uspostavljena, to ne znači da ne bi trebala postojati briga i potreba za unaprjeđenje sigurnosti radarskog sustava.

Tri su detektirane kritične ranjivosti radarskog sustava: „*Apache 2.4.49 < 2.4.51 Path Traversal Vulnerability*“, „*Python Unsupported Version Detection*“ i „*Unsupported Windows OS*“.

Prva detektirana kritična ranjivost odnosi se na besplatni web poslužitelj, Apache HTTP poslužitelj. Isti predstavlja jedan od najkorištenijih web poslužitelja današnjice. Iako Nessus Professional preporučuje nadogradnju na najnoviju inačicu Apache HTTP poslužitelja, potrebno je napomenuti činjenicu vezanu za spomenuti web poslužitelj. Korisnička podrška Apache poslužitelja bazirana jest na zajednici svih korisnika, gdje korisnici postavljaju pitanja i navode svoje probleme s Apache poslužiteljem, kao i moguća rješenja. Posebno je navedeno da je na odgovor i rješenje često potrebno čekati nekoliko sati, moguće i do nekoliko dana.

Druga kritična detektirana ranjivost odnosi se na verzija Pythona koja je instalirana na testiranom radarskom sustavu. Instalirana verzija Pythona je zastarjela te ju proizvođač više ne podržava. Time je ukazano da proizvođač više nema namjeru objavljivati nove sigurnosne zakrpe. Preporučuje se ažuriranje Pythona na najnoviju inačicu, upravo zbog pružanja korisničke podrške te zbog objavljenih sigurnosnih zakrpa za novije verzije Pythona. Kao i

Apache poslužitelj, Python također posjeduje korisničku podršku koja jest bazirana na zajednici svih korisnika, gdje korisnici postavljaju pitanja i navode svoje probleme s Pythonom, kao i moguća rješenja.

Treća kritična detektirana ranjivost odnosi operacijski sustav koji testirani radar koristi. Riječ je o Microsoft Windows 7 Professional operacijskom sustavu. Podrška za operacijski sustav Microsoft Windows 7 Professional jest ukinuta 2019. Bitno je napomenuti da, iako je ukinuta podrška za navedeni sustav, to ne znači na računalo (u ovome slučaju radar) ne može funkcionirati. Radar je i dalje u mogućnosti izvršavati svoju funkciju, ali je sustav značajno podložniji računalnim napadima.

# 5. ZAKLJUČAK

Predstavljeno je testiranje kibernetičke sigurnosti radara Navi Sailor 4000 na Kraljici mora te su analizirane sigurnosne prijetnje, detektirane od strane Nessus Professional-a. Testiranje ukazuje da je zastarjelim verzijama operacijskog sustava Microsoft Windows 7 te Apache poslužitelja potrebna nadogradnja na novije, odnosno trenutačne verzije. S druge strane, rezultati skreću pozornost na ranjivosti sustava koje se odnose nužno na operacijski sustav ili web poslužitelj. Veliki problem predstavlja korištenje zastarjelih verzija operacijskih sustava i web poslužitelja. Koriste se verzije koje su napuštene od strane proizvođača, više ne postoji podrška za iste te proizvođači nemaju namjeru objavljivati sigurnosne zakrpe za buduće sigurnosne prijetnje. Testiranje ukazuje i na probleme s konfiguracijom sigurnosnih protokola, odnosno korištenja ne pouzdanih načina enkripcije podataka.

Provedeno testiranje upućuje na moguće opasnosti koje pridonosi implementacija komponenata trećih strana, u ovome slučaju proizvodi kompanija Microsoft te Apache Software Foundation-a. Iako korištenje neovisnih (vanjskih) aplikacija umanjuje novčana ulaganja u razvojnom procesu, navedene aplikacije kritična su prijetnja kibernetičkoj sigurnosti sustava. Budući da su novčana ulaganja uvelike bitan faktor u pomorskoj industriji, korištenje besplatnog Apache web poslužitelja izvrstan je primjer spomenute situacije. Gledajući na financijsku dobit te financijsku ravnotežu, nedostaci takvih proizvoda često su zanemareni. Potrebno je proučiti svaki dio sustava, kritične točke potrebno je prepoznati i sanirati, dok se sustav kontinuirano mora održavati i nadograđivati.

Kibernetičke prijetnje u pomorskoj industriji nova su realnost i učestalost. Iako nesvjesne, brodske kompanije moraju unaprijediti zaštitu od kibernetičkih prijetnji te informatički osvijestiti svoje zaposlenike. Budući da se svakoga dana sve više pomorskih kompanija okreće korištenju računalnih tehnologija, potrebno je izraz „kibernetička sigurnost“ učiniti prioritetnim.

# LITERATURA


1. http://www.bom.gov.au/australia/radar/about/what_is_radar.shtml (30.6.2022.)
2. https://www.wartsila.com/voyage/integrated-vessel-control-systems/navi-radar (1.7.2022.)
3. Sviličić B., Bacasdoon J., Tawfik A.K., Pecota S., *Towards a Cyber Secure Shipboard ECDIS*, Rijeka, 2022.
4. Doričić, M., *Ispitivanje kibernetičke sigurnosti brodskog ECDIS-a*, Rijeka, 2020.
5. https://docs.tenable.com/releasenotes/Content/nessus/nessus1020.htm (25.6.2022.)
6. https://www.tenable.com/plugins (26.6.2022.)
7. https://www.lawinsider.com/dictionary/third-party-components (30.5.2022.)
8. https://docs.tenable.com/nessus/Content/RiskMetrics.htm (26.6.2022.)
9. https://www.tenable.com/plugins/nessus/153952 (1.7.2022.)
10. https://www.tenable.com/plugins/nessus/148367 (1.7.2022.)
11. https://www.tenable.com/plugins/nessus/108797 (1.7.2022.)
12. https://www.tenable.com/plugins/nessus/42873 (2.7.2022.)
13. https://www.tenable.com/plugins/nessus/153884 (2.7.2022.)
14. https://www.tenable.com/plugins/nessus/51192 (2.7.2022.)
15. https://www.tenable.com/plugins/nessus/57582 (3.7.2022.)
16. https://www.tenable.com/plugins/nessus/104743 (3.7.2022.)
17. https://www.tenable.com/plugins/nessus/11213 (3.7.2022.)
18. https://www.tenable.com/plugins/nessus/57608 (4.7.2022.)
19. https://www.tenable.com/plugins/nessus/45411 (4.7.2022.)
20. https://www.tenable.com/plugins/nessus/65821 (5.7.2022.)
21. https://portswigger.net/web-security/file-path-traversal (10.9.2022.)
22. https://tech-lib.xyz/definition/url.html (10.9.2022.)
23. https://crashtest-security.com/prevent-ssl-sweet32/ (11.9.2022.)
24. https://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2021-31618/ (11.9.2022.)
25. https://blog.hubspot.com/website/fix-ssl-certificate-error (11.9.2022.)
26. https://www.keyfactor.com/blog/self-signed-certificate-risks/ (12.9.2022.)
27. https://www.youtube.com/watch?v=_zjMrdQoK8g (12.9.2022.)
28. https://www.blumira.com/integration/how-to-configure-smb-signing/ (12.9.2022.)
29. CERT, *CVSS – Common Vulnerability Scoring System*, Zagreb, 2010.
30. https://nvd.nist.gov/general (18.9.2022.)

31. CERT, *Skeniranje računalnih mreža*, Zagreb, 2007.

# POPIS ILUSTRACIJA