Primjena odabranog pristupa penetracijskom testiranju računalnih sustava

Application of the Selected Penetration Testing Approach for Computer System

Ivona Zakarija
Odjel za elektrotehniku i računarstvo
Sveučilište u Dubrovniku
e-mail: ivona.zakarija@unidu.hr

Tomislav Domić
Odjel za elektrotehniku i računarstvo
Sveučilište u Dubrovniku
e-mail: tomislav.domic@hi.t-com.hr

Vedran Batoš
Odjel za elektrotehniku i računarstvo
Sveučilište u Dubrovniku
e-mail: vedran.batos@unidu.hr

UDK 004:656.61
Prethodno priopćenje / *Preliminary communication*
Rukopis primljen / *Paper accepted*: 21. 3. 2013.

Sažetak

Nove računalne tehnologije primjenjuju se u suvremenim sustavima za nadzor i upravljanje brodovima, počevši od navigacijskog sustava, komunikacijske opreme, propulzijskog sustava, sustava za rukovanje teretom pa sve do pomoćnih sustava poput sustava klimatizacije i ventilacije, sustava goriva, pomoćnog rashladnog sustava. Uz sva tehnička poboljšanja i tehnološki sofisticirane brodske sustave, sigurnost na suvremenom brodu nije zadovoljavajuća jer su pomorske nezgode i dalje vrlo česte. Sigurnost plovidbe broda uz ostale čimbenike ovisi i o sigurnosti brodskog računalnog sustava, zato se sa sigurnošću računalnih sustava u kontekstu pomorske sigurnosti ne smije olako postupati.

Ovaj rad obrađuje postupak penetracijskog testiranja Black box metodom. Kratka obrada računalne sigurnosti daje uvod u izvođenje cjelokupnog postupka testiranja kroz četiri faze. Uporabom raspoloživih nekomercijalnih alata i programskih okruženja za penetracijsko testiranje ostvaruju se jednostavna i dostupna sredstva za provjeru, ali uz istaknutu mogućnost proboja sigurnosti. Uz prikazane postupke djelovanja, rad analizira potencijalne nedostatke i daje praktična rješenja za njihovo odstranjivanje. Osim toga, pri realizaciji ovakvog pristupa svi procesi su provedeni u stvarnom radnom okruženju, s ciljem da se čitatelju što jasnije prikaže sam postupak.

KLJUČNE RIJEČI

penetracijsko testiranje
black box metoda
računalna sigurnost
programska oprema
ranjivost
sigurnost u pomorstvu

Summary

In modern ship monitoring and control systems new computer technologies are applied, starting from the navigation system, communication equipment, propulsion system, cargo handling system to the auxiliary systems such as air conditioning and ventilation, fuel system, auxiliary cooling system. In spite of all the technical advances and sophisticated marine systems, the safety on a modern ship is still disputable having in mind that marine accidents occur quite frequently. Safety of navigation, among other things, depends on the safety of the ship computer system. Consequently, security of the computer systems in the context of safety at sea requires some serious consideration.

This paper examines procedure of conducting penetration testing using Black box method. Short analisys of computer security gives introduction to conducting testing procedure throught 4 phases. Using free tools and software solution enviroments for pentesting, content points on easy-to-get applications and possible security breaches. Implementing processing methods, the paper analyses potential vulnerabilities and gives a practical explanation for their removal. In addition, all processes are implemented in real enviroment aiming to give clear presentation to the reader.

KEY WORDS

Penetration Testing
Black Box
Computer Security
Software
System Vulnerabilities
Maritime Safety

UVOD / *Introduction*

U moderno doba čovjek sve više aktivnosti prepušta strojevima i oslanja se na njihovu pomoć pri izvršenju brojnih zadaća. Iako strojevi nisu skloni greškama u radu, njihovo je ponašanje često predvidivo i time sklono manipulacijama.

Nove računalne tehnologije primjenjuju su u suvremenim sustavima za nadzor i upravljanje brodovima, počevši od navigacijskog sustava, komunikacijske opreme, propulzijskog sustava, sustava za rukovanje teretom pa sve do pomoćnih sustava poput sustava klimatizacije i ventilacije, sustava goriva, pomoćnog rashladnog sustava. Zadnjih desetljeća komunikacija i automatizacija su toliko uznapredovale da se gotove sve brodske funkcije mogu neprestano daljinski nadzirati i upravljati s kopna [1,2,3]. Razvojem satelitskih komunikacija [4] usavršavaju se i sustavi pozicioniranja [5], a

uporaba računalne tehnologije sve je veća. Konačna procjena sigurnosti i djelovanje u skladu s tom procjenom obaveza je zapovjednika, a mora biti u skladu s propisanim normama. Pri donošenju odluka i procjeni rizika zapovjednik se sve više oslanja na računalne sustave [6]. U slučaju proboja sigurnosti potencijalni zlonamjerni napadač može preuzeti kontrolu nad brodom i upravljati skoro svim vitalnim brodskim sustavima. Ovakav događaj ugrožava sigurnost pomorskog sustava, a moguće posljedice su nesreće na moru, gubitak flote i ljudskih života, onečišćavanje okoliša, piratske otmice, financijski gubici brodske kompanije.

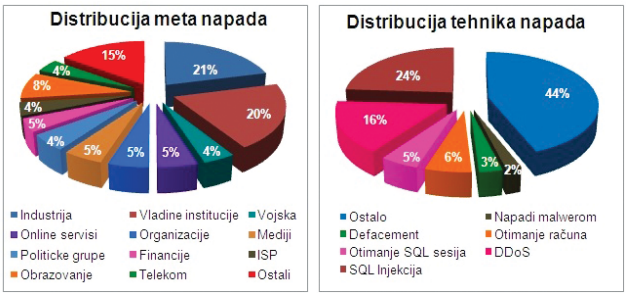
S obzirom da je pomorski promet izrazito internacionaliziran i globaliziran dio gospodarstva, normiran je međunarodnim konvencijama, pravilima klasifikacijskih društava i nacionalnom pravnom regulativom [7,8]. Međunarodna pomorska organizacija (*International Maritime Organization* - IMO) propisuje međunarodnu konvenciju o sigurnosti života na moru (SOLAS) u kojoj stoji da su svi putnički i transportni brodovi teži od 300 tona bruto obavezni primjenjivati GMDSS (*Global Maritime Distress and Safety System*) [9]. Ovaj sustav podrazumijeva opremu, propise i procedure za poboljšanje razine sigurnosti na moru [10].

Uz sva tehnička poboljšanja i tehnološki sofisticirane brodske sustave, sigurnost na suvremenom brodu nije zadovoljavajuća jer su pomorske nezgode i dalje vrlo česte. Sigurnost plovidbe broda uz ostale čimbenike ovisi i o sigurnosti brodskog računalnog sustava, zato se sa sigurnošću računalnih sustava u kontekstu pomorske sigurnosti ne smije olako postupati [11,12].

Znajući da niti jedan sustav nije 100% siguran, napadač odabirom vektora napada pokušava na suptilan način izazvati proboj sigurnosti. To obično dovodi do krađe podataka, izmjene sigurnosnih i konfiguracijskih postavki te u najgorem slučaju do onemogućavanja poslovanja i potpunog gubitka podataka. Zato se u svrhu sprečavanja takvih i sličnih incidenata pojavila potreba za provođenjem standardizirane provjere sigurnosti. Uvidjevši ovu činjenicu u praksi, razvila se nova grana u računalnoj sigurnosti koja se naziva penetracijsko testiranje. Ovim radom se uz opisane pristupe i metodologije testiranja prikazuju najučinkovitiji načini za provjeru sigurnosti računalnih sustava.

SIGURNOSNI ZAHTJEVI / *Security demands*

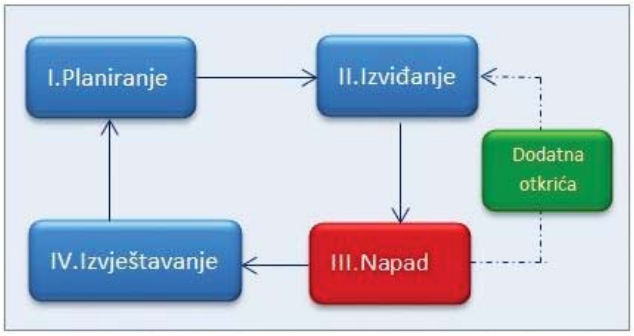
Sustav se smatra sigurnim ako zadovoljava kriterije koji jamče tajnost, dostupnost i integritet podataka [13]. Tajnost podataka je stavka definirana korištenjem i pristupom informacija za to ovlaštenim korisnicima. Dostupnost osigurava kontrolu i mogućnost korištenja podataka, dok integritet podataka jamči konzistentnost procesa i valjanost podataka unutar sustava. Integritet je osiguran tako da kontrolne procese mogu pokretati samo korisnici koji za to imaju privilegije. Neophodno je da sva tri kriterija budu osigurana kako bi njihovo djelovanje bilo u sprezi. Općenito, napadači iskorištavaju ranjivosti u računalnim sustavima koje im omogućavaju uspješan proboj sigurnosti. Ranjivosti se dijele na one u programskom kodu, konfiguraciji, mrežnim protokolima i fizičke ranjivosti [14]. Najzastupljenije su ranjivosti u programskom kodu dok se najuspješniji napadi izvode koristeći fizičke ranjivosti. To je vidljivo iz statistika mrežnih sigurnosnih računalnih (engl. *cyber*) napada [15] prikazanih grafikonima na slici (Slika 1).



Slika 1. Statistika cyber napada u kolovozu 2012. [16]
Figure 1 Cyber attacks statistics for August 2012 [16]

PENETRACIJSKO TESTIRANJE / *Penetration testing*

Penetracijsko testiranje (engl. *pentest*) je standardizirani postupak kojim se provjerava sigurnost računalnog sustava. Idealno provođenje *pentesta* simulira pothvate koje bi napravio pravi napadač tijekom izvođenja napada. Na ovaj se način kontroliranim postupkom utvrđuju potencijalni sigurnosni propusti u sustavu i pružaju smjernice za njihovo ispravljanje. Načelno se *pentest* izvodi slijedeći jednu od tri glavne metodologije; *white, black* ili *grey box* [17]. *Black box* uzima za pretpostavku da napadač ne zna ništa o meti koju napada, što predstavlja veliki utrošak vremena i napora u prikupljanu podataka kojima se određuje potencijalni vektor napada. Cjelokupni proces testiranja izvodi se kroz četiri faze, vodopadnim slijedom uz mogućnost iteracije, što je prikazano na slici (Slika 2).



Slika 2. Slijed izvođenja penetracijskog testiranja
Figure 2 Penetration testing sequence of execution

U fazi planiranja (engl. *planning phase*) određuje se opseg i metoda izvođenja *pentesta* u dogovoru s naručiteljem. Time izvršitelj može pripremiti strategiju djelovanja, a naručitelj se osigurava od mogućih negativnih posljedica testiranja. Sljedeća je faza najopsežnija po broju postupaka koje treba provesti jer se radi o sakupljanju informacija. Faza izviđanja (engl. *discovery phase*) dijeli se na uzimanje otisaka, skeniranje i enumeraciju te analizu ranjivosti [18]. Nakon pažljivo obrađenih informacija slijedi odabiranje vektora napada, kojim se pokušava iskoristiti pronađena ili ciljana ranjivost. Faza napada (engl. *attack phase*) sačinjava jezgru svakog penetracijskog testiranja, koja ne mora uvijek polučiti uspjehom pa penetracijski tester odabire nove vektore napada u slučaju neuspjeha. Nakon uspješno izvedenog napada, cijeli postupak se dokumentira i utvrđuju se ranjivosti koje je potrebno sanirati. Fazom izvještavanja (engl. *reporting phase*) treba kategorizirano prikazati utvrđeno stanje računalnog sustava i ponuditi smjernice za njegovo poboljšanje, ako za tim

ima potrebe. Nakon izvršenog testiranja sustav je potrebno vratiti u početno stanje da organizacija može nesmetano nastaviti sa svojim radom.

PRAKTIČNA UPORABA ALATA U PENETRACIJSKOM TESTIRANJU / *Practical use of tools in penetration testing*

Za potrebe testiranja koriste se programskim okruženjima, koja su u velikoj mjeri utemeljena uglavnom na Linux platformi, iz razloga što je ova platforma jedna od bržih platformi s visokom učinkovitošću procesiranja podataka. *Backtrack* je takva vrsta distribucija koja sadrži niz preinstaliranih alata potrebnih za provođenje sigurnosnih ispitivanja.

Faza izviđanja / *Footprinting phase*

Osnovna metoda za prikupljanje informacija o logičkoj infrastrukturi računalne mreže je postavljanje *Whols* upita (engl. *query*) Internet registrima. U tu svrhu koristimo *DMitry* alat koji nudi informacije o korištenom IP bloku adresa, nazivu organizacije, kontakte elektroničke pošte, ASN (engl. *Autonomous system number*) broju, ISP-u, DNS poslužiteljima te tehničkom i administrativnom osoblju. Dobiveni rezultati prikazani su na slici (Slika 3).

```
root@bt:~# dmitry -i jadrolinija.hr
Inet-whois information for 194.1.255.75
---------------------------------
HostIP:194.1.255.75
HostName:jadrolinija.hr
inetnum:     194.1.255.0 - 194.1.255.255
netname:     JADROLINIJA-HR
country:     HR
org:         ORG-JA139-RIPE
status:      ASSIGNED PI
mnt-by:      RIPE-NCC-END-MNT
----------------------------
route:       194.1.255.0/24
descr:       JADROLINIJA over METRONET
origin:      AS35549
mnt-by:      METRONET
source:      RIPE # Filtered
```

Slika 3. Isječak rezultata *DMitry* alata
Figure 3 Screen excerpt from DMitry results

Kao dodatna metoda prikupljanja podataka koristi se *python* skripta *Metagoofil* za pretraživanje relevantnog sadržaja povezanog s metom. Koristeći API-je web tražilica, skripta dohvaća datoteke s putanjama na mreži, imena autora, nazive instaliranih aplikacija i mapa za dijeljenje podataka.

Ove vrste informacija mogu se iskoristiti kod *socijalnog inženjeringa*, odnosno zavaravanja službenog osoblja. S ciljem dobivanja potpune liste dostupnih računala na mrežnoj domeni, koristimo skriptu *Reverseraider*. Ova skripta uzima gotove datoteke s listama mogućih DNS imena i u kombinaciji s nazivom mrežne domene provjerava aktivna računala PING metodom.

```
root@bt:/pentest/enumeration/reverseraider#
./reverseraider -d msccruises.com -w w*/fast.list
intranet.msccruises.com   92.242.144.50
www.msccruises.com        193.138.73.230
pop.msccruises.com        fe80:1::225:90ff:fe19:4b12
http.msccruises.com       92.242.144.50
intranet.msccruises.com   fe80:1::225:90ff:fe19:4b12
ftb.msccruises.com        92.242.144.50
backup.msccruises.com     92.242.144.50
smtp.msccruises.com       fe80:1::225:90ff:fe19:4b12
ns.msccruises.com         92.242.144.50
db.msccruises.com         fe80:1::225:90ff:fe19:4b12
test.msccruises.com       fe80:1::225:90ff:fe19:4b12
```

Slika 4. Isječak rezultata *Reverseraider* alata
Figure 4 Screen excerpt from Reverseraider tool

Prikupljene informacije služe za skeniranje svih dostupnih resursa mete i njihovu analizu s ciljem pronalaženja potencijalnih sigurnosnih ranjivosti. Dobiveni rezultati prikazani su na slici (Slika 4). Za potrebe skeniranja na mreži koristi se *nmap* koji je ujedno nezaobilazan alat za mnoge penetracijske testere. Njegovo djelovanje je usmjereno na individualna računala kojima se tako može doznati verzija OS-a, broj i vrste otvorenih portova, njihove specifikacije, postavke mrežnih protokola, metode enkripcije i sl. Na slici (Slika 5) prikazano je *nmap* skeniranje otvorenih portova. Komunikacija s metom temelji se na slanju različitih vrsta IP paketa (TCP Null, SYN, ACK, FIN, UDP) [19] pri čemu je napadaču u interesu da ovaj postupak izvede neprimjetno kako ne bi pokrenuo automatske alarme u uređajima koji blokiraju ovakve aktivnosti (vatrozid, IPS, IDS i sl.)

```
root@bt:~# nmap -F
www.flightlesstravel.com
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  open   pop3
443/tcp  open   https
465/tcp  open   smtps
993/tcp  open   imaps
995/tcp  open   pop3s
```

Slika 5. *Nmap* skeniranje otvorenih portova
Figure 5 Nmap open ports scanning

Kako bi smanjili izlaganje mrežnih i ljudskih resursa na mreži, potrebno je ustanoviti koje informacije zaista trebaju biti dostupne javnosti. S tim ciljem treba napraviti slijedeće korake: ugasiti mrežne servise i portove koji se ne koriste, osigurati detaljnu inspekciju paketa na vatrozidu, ograničiti

aktivnosti zaposlenika na društvenim mrežama i implementirati sigurnosne police unutar organizacije za pristup podacima i pokretanje procesa.

Analiza ranjivosti / *Vulnerability analysis*

Nakon što su identificirani osnovni računalni resursi te njihove pristupne točke i metode komunikacije može se početi s ispitivanjem ranjivosti. Ovaj postupak uključuje pretraživanje poznatih baza ranjivosti (engl. *exploit database*) po zadanim specifikacijama, ali i pisanje vlastitih skripti koje su u mogućnosti iskoristiti ranjivosti.

novi sken2 Vulnerability Summary | Host Summary
Completed: Jul 5, 2012 13:12 (1 Error)

Plugin	Count	Severity	Name	Family
53895	1	Critical	Adobe Flash Media	Misc.
57537	1	High	PHP < 5.3.9 Multipl	CGI abuses
46803	2	Medium	PHP expose_php Ir	Web Servers
12217	1	Medium	DNS Server Cache	Information Dis

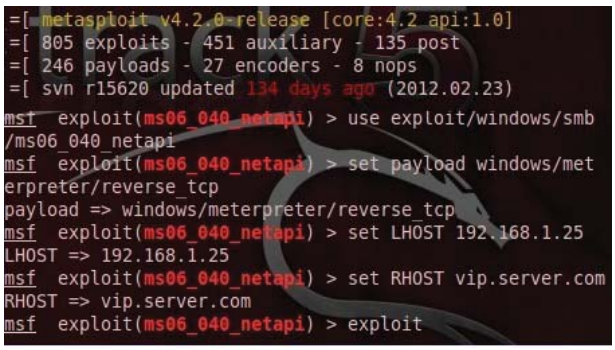
Slika 6. Nessus skeniranje ranjivosti
Figure 6 Nessus vulnerability scanning

Skripte koje su u mogućnosti iskoristiti još neotkrivene ranjivosti (engl. *0day exploits)* izrazito su tražene na crnom tržištu. Jedan od ponajboljih skenera ranjivosti je *Nessus*. Svoju učinkovitost pokazuje na mogućnostima skeniranja aktivnih aplikacija, DNS poslužitelja, nezaštićenih dijeljenih resursa, tvorničkih računalnih postavki i sl. Koristi ICMP, ali i TCP ping metode slanja paketa koje su naslijeđene od nmap-a. Sposoban je generirati detaljne izvještaje o pronađenim ranjivostima za koje nudi i praktična rješenja. Dobiveni rezultati skeniranja ranjivosti prikazani su na slici (Slika 6.). Dobar primjer web orijentiranog skenera je *Nikto* koji, uz poznate ranjivosti, daje i opise nepodešenih stavki koje se mogu uspješno iskoristiti u napadu.

Korisne mjere koje se mogu poduzeti za prevenciju ranjivosti su nadogradnja ili instalacija aplikacija sa zadnjom inačicom, uklanjanje informativnih zaglavlja s aktivnih uređaja i servisa te osiguravanje enkripcije prometa SSH i VPN metodama.

Faza napada / *Attack Phase*

Ova faza je jezgra bilo kojeg penetracijskog testa te time svako najzanimljivija i najizazovnija jer ne mora uvijek biti uspješna te zahtijeva puno znanja i preciznosti za uspješno izvođenje. U inicijalnoj fazi izrabljivanja (engl. *exploitation phase*) penetracijski tester izvodi pokušaje proboja sigurnosti koristeći za to posebno sastavljene dijelove programskog koda (engl. *exploits*). Oni su u većini slučajeva korisni ako sustav nije nadograđen, ima inicijalne postavke ili je pogrešno konfiguriran. Nakon uspješnog izvođenja napada u fazi izrabljivanja, napadač će steći određene privilegije nad sustavom koje potom koristi u fazi zauzimanja položaja (engl. *privilege escalation phase*) kako bi prisvojio što je moguće više



```
=[ metasploit v4.2.0-release [core:4.2 api:1.0]
=[ 805 exploits - 451 auxiliary - 135 post
=[ 246 payloads - 27 encoders - 8 nops
=[ svn r15620 updated 134 days ago (2012.02.23)
msf  exploit(ms06_040_netapi) > use exploit/windows/smb
/ms06_040_netapi
msf  exploit(ms06_040_netapi) > set payload windows/met
erpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms06_040_netapi) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf  exploit(ms06_040_netapi) > set RHOST vip.server.com
RHOST => vip.server.com
msf  exploit(ms06_040_netapi) > exploit
```

Slika 7. Podešavanje exploit parametara za *Metasploit*
Figure 7 Exploit parameters configuration for Metasploit

kontrole nad računalnim resursima i u konačnici ispunio svoj cilj. Najpoznatija programska platforma za izvođenje napada je *Metasploit* koja je svoju popularnost stekla zbog mogućnosti korištenja goleme biblioteke *exploita* za više operativnih platformi i mrežnih protokola. Program također nudi mogućnost enkodiranja podataka (engl. *payloada*) tako da mogu neprimjetno proći kroz vatrozid i IDS uređaje [20]. Na slici (Slika 7.) je prikazano podešavanje *exploit* parametara. Nadalje, baze podataka također predstavljaju važno strateško uporište svake organizacije. Za njihovo testiranje koristimo *DarkMySQLi* program koji koristeći loše strukturirane podatke u bazama može omogućiti njihovo čitanje, mijenjanje i izvršavanje. Prije njegovog korištenja, moramo provjeriti parsira li web sučelje kvalitetno ulazne znakove, što možemo napraviti dodavajući znakove na prvotnu URL adresu (označeno crveno).

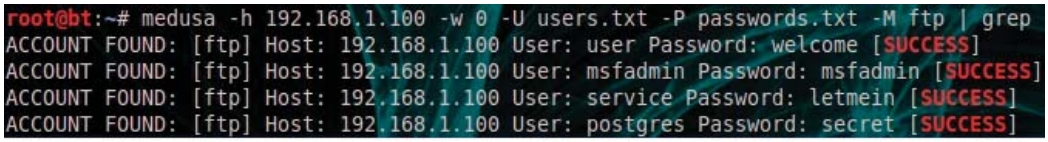
URL: http://www.newscoorporation/popup_news.php?id="22

Ako poslužitelj javi grešku slijedećeg oblika, znači da je ranjiv na *SQL Inject* tehniku.

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result

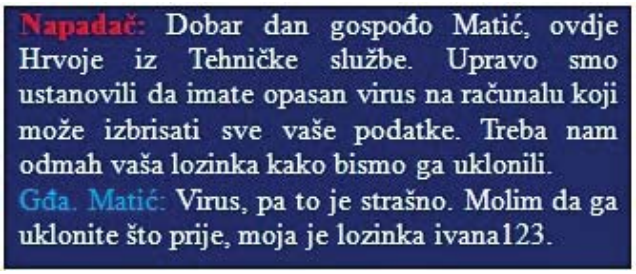
U fazi napada koriste i *brute force* alate za pogađanje lozinki. *Medusa* je primjer takvog alata koja je namijenjena brzom i paralelnom ispitivanju podataka za prijavu na servise. Korištenje paralelnih procesa omogućuje ispitivanja na više različitih host računala odjednom.

Moguće je korištenje više različitih datoteka za ispitivanje vrijednosti nasuprot brojnih servisa koji su definirani po modulima (FTP, HTTP, IMAP, RSH i dr.). Slika (Slika 8.) prikazuje *brute force* provjeru lozinki *Medusa* alatom. Unatoč svim tehnološkim dostignućima prikazanih alata za napad, kao najučinkovitija metoda pokazao se *socijalni inženjering* koji se bavi predviđanjem ljudskog ponašanja na osnovi informacija u njihovom okruženju [21]. Primjer socijalnog inženjeringa prikazan je na slici (Slika 9.)



```
root@bt:~# medusa -h 192.168.1.100 -w 0 -U users.txt -P passwords.txt -M ftp | grep
ACCOUNT FOUND: [ftp] Host: 192.168.1.100 User: user Password: welcome [SUCCESS]
ACCOUNT FOUND: [ftp] Host: 192.168.1.100 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT FOUND: [ftp] Host: 192.168.1.100 User: service Password: letmein [SUCCESS]
ACCOUNT FOUND: [ftp] Host: 192.168.1.100 User: postgres Password: secret [SUCCESS]
```

Slika 8. Brute force provjera lozinki *Medusa* alatom
Figure 8 Brute force passwords lookup with Medusa tool



Slika 9. Klasični primjer socijalnog inženjeringa
Figure 9 Social engineering example

Tako napadač dezinformiranjem zaposlenika ili partnera može doći do vrijednih podataka koji mu omogućuju pristup inače zaštićenim resursima. Kako bi osigurali sustav protiv napada potrebno je postaviti kvalitetne police osiguranja. Kod prijave na servis ili računalo, preporučljivo je korištenje složenih zaporki s nasumičnim nizom znakova. Dalje, korisniku se treba ograničiti broj prijava na servis a kao dodatno osiguranje koristiti se logičkim upitom (engl. *captcha*) kojim se potvrđuje da čovjek izvršava prijavu. Nemoguće je predvidjeti sve vektore napada, ali u većini slučajeva napadači koriste činjenicu da administratori ne mijenjaju inicijalne postavke aktiviranih servisa [22,23,24].

ZAKLJUČAK / *Conclusion*

Iz dana u dan sve je veći broj *cyber* prijetnji i učestalih napada na računalne sustave. Korištenjem *black box* metode, napadač i ne mora imati fizički pristup mreži što mu olakšava njegovo djelovanje i osigurava veliku dozu anonimnosti. Vidjeli smo koliko je jednostavno napadaču, jednom kad skupi potrebne podatke o meti, izvesti precizan i brz napad. Uzimajući u obzir da se većina napada događa zbog krađe podataka, brodske kompanije trebale bi posebno biti na oprezu kako se većina transakcija odvija *online* kartičnim plaćanjem. Kako bi izbjegle poslovne gubitke, organizacije moraju osigurati proaktivno nadgledanje sustava uz njegovu nadogradnju i omogućiti edukaciju zaposlenika koja jamči čvrst integritet i kvalitetno poslovanje.

LITERATURA / *References*

[1] S. Krile, Udžbenik Sveučilišta u Dubrovniku: Pomorski komunikacijski sustavi - Mobilne radiomreže, Dubrovnik, 2011.
[2] P. Ristov, S. Krile, „Programski paketi za rukovanje kontejnerima“, Naše More, 2010, Vol 57, No 1-2,pp. 18-31
[3] T. Hirner, P. Farkaš, S.Krile, „One Unequal Error Control Method for Telemetric Data Transmission“, Journal of Electrical Engineering, 2011, Vol. 62, No. 3, pp 158-162
[4] S. Krile , „The Satellite Link Resource Management for Mobile Network“, Proc. of 23rd ICSSC' 05 (International Communications Satellite Systems Conference), Rim, Italia, 2005.
[5] Z. Lušić, S. Kos, S. Krile, „Strukturna analiza metoda pozicioniranja na moru“, Naše more, 2008., Vol. 55, No 1-2, pp. 3-17.
[6] Z. Lušić, S. Kos, „Utjecaj brodara na odluke zapovjednika broda“, Naše More, 2011, Vol 58, No 3-4, pp. 95-102
[7] J. Šundrica, D. Roje, N. Vulić, „Utjecaj sustava upravljanja kvalitetom i sigurnošću na onečišćenje mora i gubitke u pomorstvu“, Naše More, 2010., Vol 57, No 3-4, pp. 113-120.
[8] I. Šošić, „Somalski pirati – rastući međunarodni problem koji treba hitno riješiti“, Naše More, 2011., Vol 58, No 1-2,pp. 82-89
[9] IMO, *International SOLAS Convention,* http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-%28SOLAS%29,-1974.aspx, (14.3.2013)
[10] S. Krile., Udžbenik Sveučilišta u Dubrovniku: Elektroničke komunikacije u pomorstvu - mobilne satelitske veze, Dubrovnik, 2004.
[11] M. Bilić,“Organizacija rada na brodu i brodara kao preduvjet za sigurnost plovidbe“, 2011, Vol 58, No 3-4, pp. 107-111
[12] R. V. Pomeroy,B.M. Sherwood, Managing The Human Element In Modern Ship Design And Operation, Proc. of. Royal Institution of Naval Architects (RINA) International Conference: Human Factors in Ship Design and Operation Conference,London,UK,2002
[13] Andress, J. The Basics of Information Security, Elsevier, 2011
[14] Ericson, J. The Art of Exploitation, 2nd Edition, No Starch Press, 2008.
[15] A.Munitić, A.Jeličić, „Hipotetične uzročno-posljedične veze i krugovi povratnog djelovanja razvoja virtualnog svijeta, interneta i tehnologije“, Naše More, 2008., Vol 55, No 1-2,pp. 47-58
[16] [P. Passeri, August 2012 Cyber Attacks Statistics, http://hackmageddon.com/2012/09/07/august-2012-cyber-attack-statistics, (10.9.2012)
[17] Ec-Council, Ethical Hacking and Countermeasures, CEnglage Learning, 2009.
[18] J. Faircloth, Penetration Tester's Open Source Toolkit, Elsevier, 2011.
[19] C. Hurley, Penetration Tester's Open Source Toolkit, Syngress, 2007.
[20] A. Singh, Metasploit Penetration Testing Cookbook, Packt Publishing Ltd, 2012.
[21] C. Hadnagy, The Art of Human Hacking, John Wiley & Sons, 2010.
[22] W. Pritchett, DE SMET D. BackTrack 5 Cookbook, PACKT Publications 2012.
[23] A. Gupta, LALIBERTE S. Defend I.T.: Security by Example, Addison-Wesley Professional, 2004.
[24] D. Stuttard, M. Pinto,The Web Application Hacker's Handbook, Wiley, 2011.