CARNET

Capture The Flag (CTF) natjecanja u području informacijske sigurnosti

CERT.hr-PUBDOC-2019-12-395

CERT.hr

Sadržaj

1 Uvod

Sigurnost je bitan faktor svih segmenata informacijske tehnologije. Pogreška u programskom kôdu, postavkama ili primjeni komponenti računalnog sustava može omogućiti napadačima zloupotrebu takve ranjivosti i napad na sustav, što može rezultirati neovlaštenim pristupom, neovlaštenim dohvaćanjem podataka, izvršavanjem proizvoljnog računalnog kôda na sustavu ili prekidom rada određene usluge.

Kako bi se među djelatnicima u području informacijskih tehnologija, ali i široj javnosti, proširila svijest o važnosti primjene sigurnosnih mjera te izbjegavanju i ispravljanju mogućih sigurnosnih propusta u programskom kôdu, postavkama ili nekoj drugoj komponenti računalnog sustava, osmišljena su razna CTF natjecanja u kojima se na zabavan način i uz natjecateljsku atmosferu mogu steći praktična znanja iz područja računalne sigurnosti. Sudjelovanjem na takvim natjecanjima programeri, sigurnosni stručnjaci, ali i zainteresirani pojedinci, obično se okušavaju u suprotnoj ulozi – ulozi napadača, i pokušavaju izvesti razne „hakerske“ napade na unaprijed pripremljene sustave.

Na taj način upoznaje se s načinima na koje se sustavi mogu napasti, kako se točno može iskoristiti određena ranjivost, stječe se bolji uvid u rizike i opasnosti koje sa sobom donosi određena ranjivost i može se prioritizirati njihovo ispravljanje. Učenje ofenzivnih vještina (napadanje sustava) najbolji je način da se uistinu nauči zaštititi sustav i poboljšaju defenzivne (obrambene) vještine.

Postoje razna događanja i *web* stranice za vježbanje primjene znanja o području računalne sigurnosti, neki su u obliku natjecanja, a neki sadrže kolekciju zadataka kojima se može pristupiti bilo kad. Ovaj dokument opisat će nekoliko takvih stranica i događanja.

2 Vrste CTF natjecanja

Capture the Flag (CTF) poseban je oblik natjecanja među sudionicima u području informacijske sigurnosti. Naziv proizlazi iz toga što natjecatelji moraju pronaći rješenje zadatka, tzv. „zastavu“ (engl. *flag*). Od tuda dolazi i ime tih natjecanja – natjecatelji moraju „osvojiti/uhvatiti zastavu” (engl. *Capture the Flag*). Rješenje (zastava) je obično tekstualni niz oblikovan na jedinstven, prepoznatljiv način kako bi natjecatelji bili sigurni da su pronašli rješenje. Primjerice, natjecanje PicoCTF svoja rješenja (zastave) formatira u obliku „PicoCTF{___}”, gdje između vitičastih zagrada piše neki nasumični tekst.

Uobičajena je podjela na dvije vrste CTF natjecanja:

- *Jeopardy-style* CTF natjecanja i
- *Attack-defense* CTF natjecanja

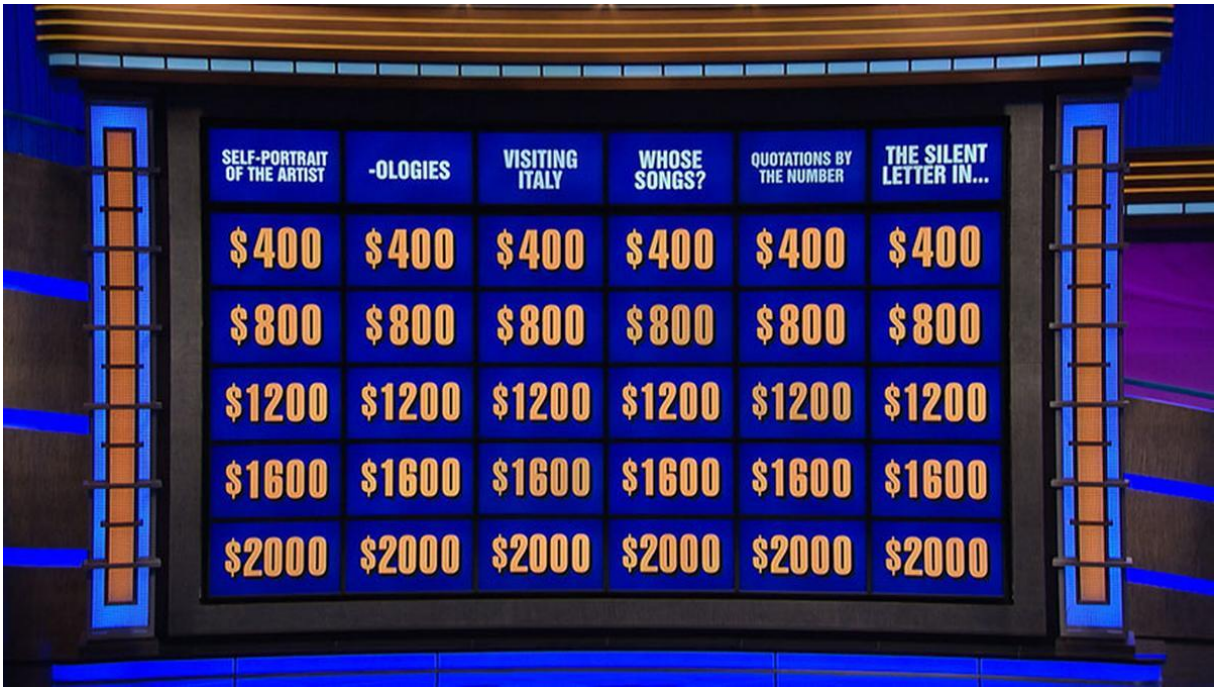
No, osim njih, postoje i:

- specijalizirani CTF-ovi koji se fokusiraju na određene teme i područja (npr. socijalno inženjerstvo, prikupljanje informacija iz otvorenih izvora, izrada *botneta* i sl.),
- izolirane virtualne mreže koje simuliraju stvarno okruženje (npr. infrastrukturu neke tvrtke s ranjivim računalima),
- razne kibernetičke vježbe (obično u vojnom kontekstu)…

Također, postoje i razne stranice sa zadacima na kojima se korisnik može pripremati za natjecanja ili vježbati i unaprjeđivati svoje vještine.

2.1 *Jeopardy-style* CTF natjecanja

Jeopardy-style CTF natjecanja organizirana su na način da postoji više zadataka koji su grupirani u kategorije. Ova vrsta CTF natjecanja dobila je ime po američkom TV kvizu „Jeopardy!“ koji se sastoji od pitanja različite težine grupiranih u kategorije, kao što je prikazano na slici 1.

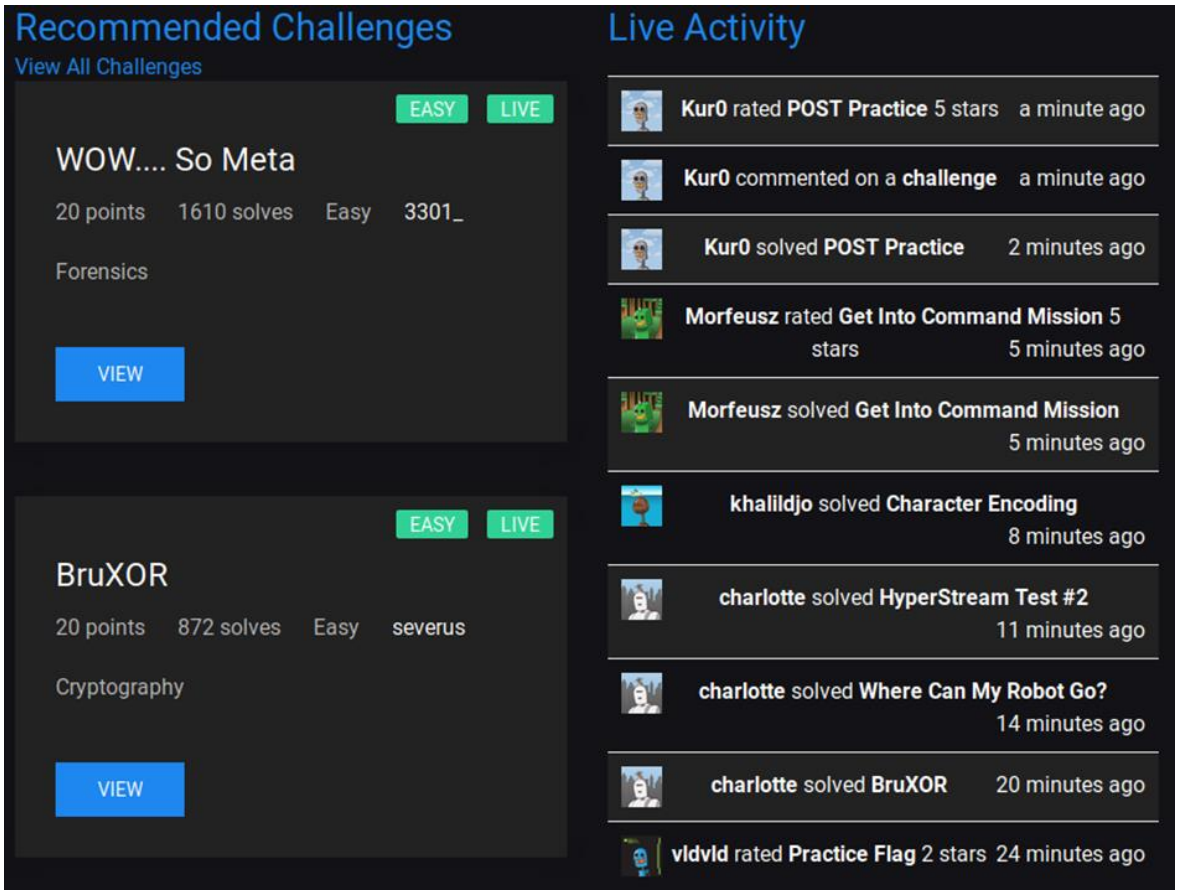


Slika 1 ***Ploča s pitanjima podijeljenim po kategorijama i težinama u američkom TV kvizu „Jeopardy!“*** **(1)**

Neke od uobičajenih kategorija u *Jeopardy-style* CTF natjecanjima su *web* sigurnost, digitalna forenzika, kriptografija, reverzni inženjering, razvoj *exploita* i steganografija. Timovi ili pojedinci dobivaju bodove za svaki uspješno riješen zadatak, pri čemu teži zadaci nose više bodova. Pobjednik je onaj tko do isteka vremena natjecanja skupi najviše bodova. Postoji velik broj ovakvih natjecanja koja su konceptualno vrlo slična. Neki primjeri su *Jeopardy-style* CTF-ova su:

- PicoCTF
- PlaidCTF
- Insomni'hack
- SECCON CTF
- C3CTF
- ...

Na *web* stranici ctftime.org dostupan je veliki popis svih vrsta CTF natjecanja (prošlih i nadolazećih). Na slici 2 prikazana je početna stranica natjecanja *CTFlearn*.



Slika 2 ***CTFlearn početna stranica***

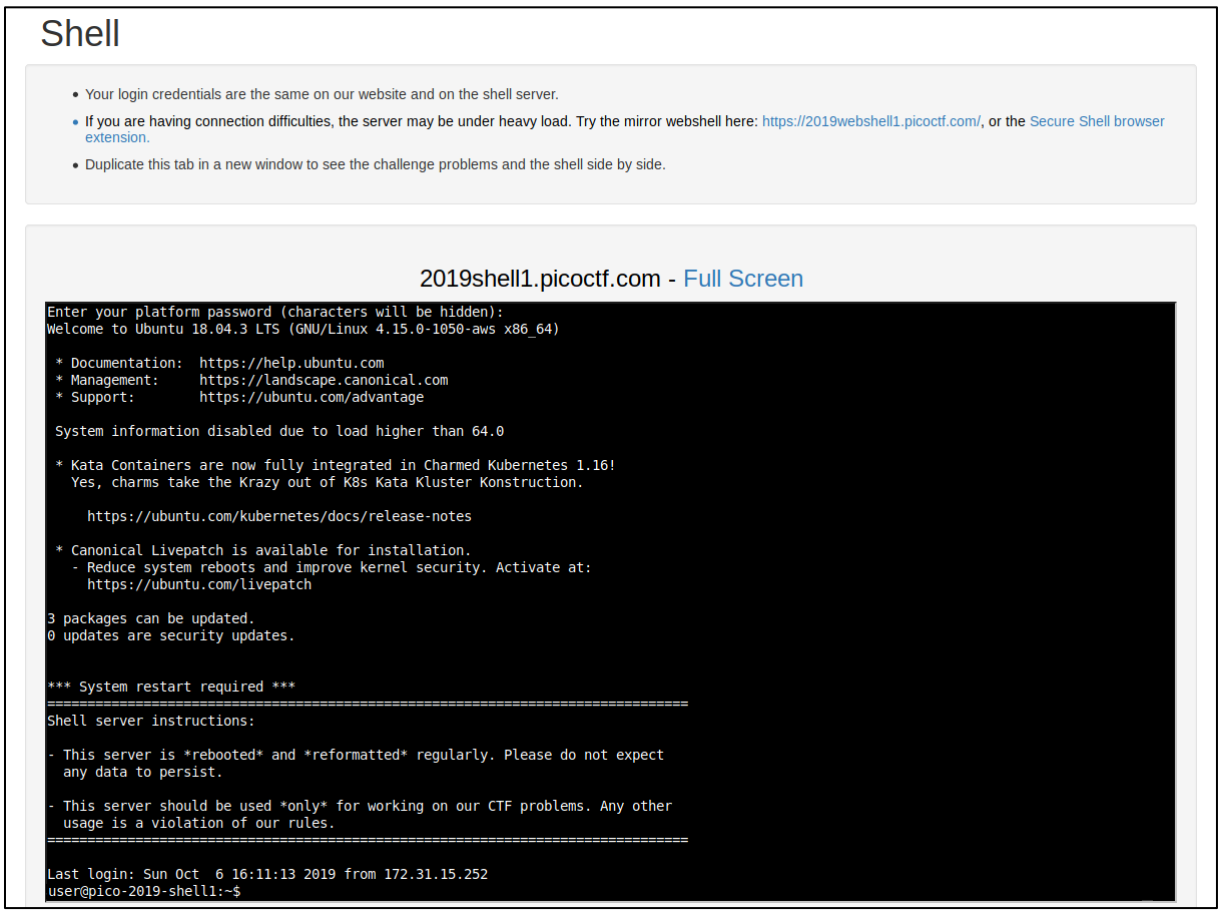
U ovom poglavlju će koncept i uobičajena pravila ove vrste CTF-ova biti objašnjeni na primjeru *PicoCTF*-a, ali koncepti su vrlo slični i na drugim *Jeopardy-style* CTF natjecanjima.

PicoCTF je besplatno *Jeopardy-style* CTF natjecanje u području računalne sigurnosti, koje su izradili sigurnosni stručnjaci sveučilišta Carnegie Mellon u SAD-u (2). Natjecanje je namijenjeno učenicima srednjih škola sa svrhom širenja interesa za područje informatike i informacijske sigurnosti. Zadaci su ofenzivno orijentirani jer tvorci ovog natjecanja smatraju da je to najbolji način poticanja radoznalosti. Sudjelovanje ne zahtijeva nikakva posebna predznanja, već je minimalni uvjet kritičko razmišljanje. Određena znanja programiranja itekako pomažu, no kako je svrha ovog natjecanja stjecanje novih znanja, važnija je želja za učenjem i istraživanjem.

U natjecanju se može sudjelovati individualno ili timski do najviše pet sudionika po timu. Svi članovi jednog tima rješavaju iste zadatke i dijele postignute bodove. Također, postoji i funkcionalnost učionica gdje profesori mogu stvoriti svoje učionice i pratiti napredak svojih učenika.

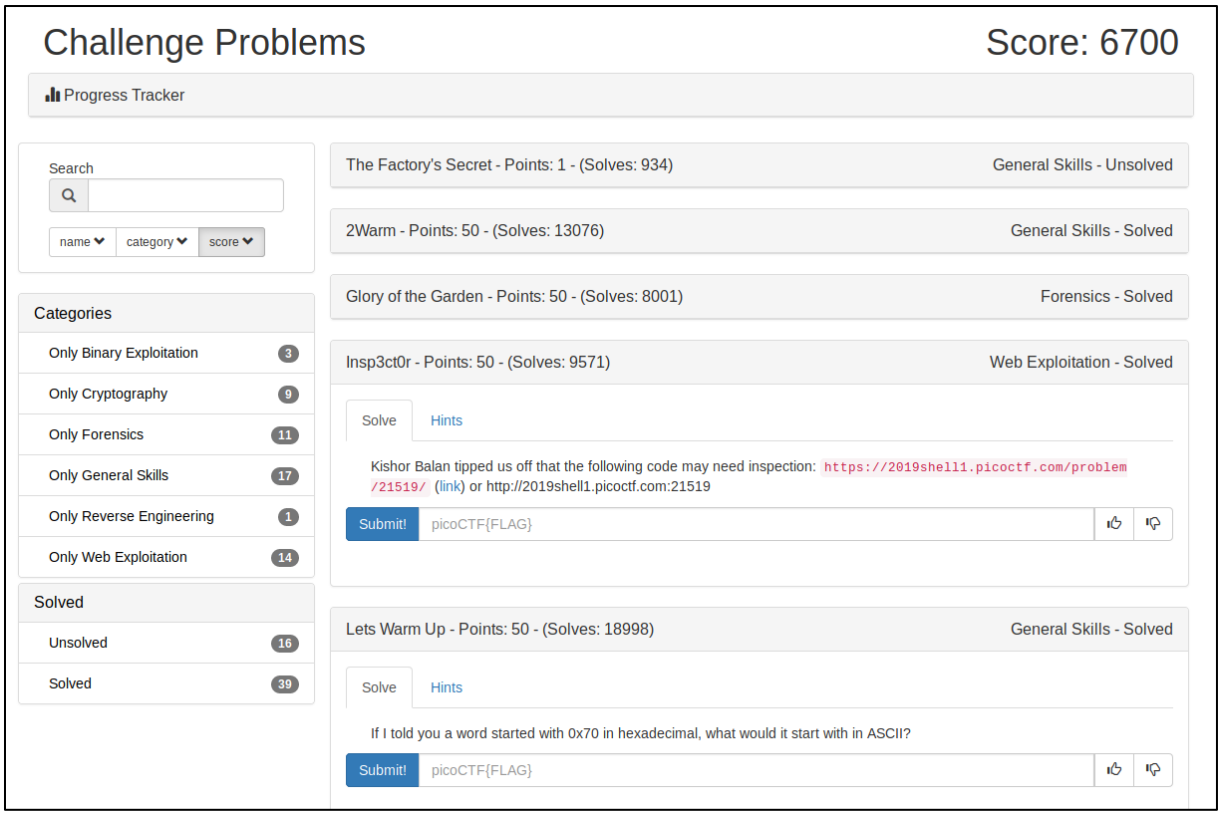
PicoCTF natjecanje traje dva tjedna, a na kraju natjecanja tim koji je skupio najviše bodova (ili koji je prvi skupio maksimalan broj bodova) osvaja prvo mjesto i novčanu nagradu. Nešto manju nagradu osvajaju i ostali visoko pozicionirani timovi. Iako je ovo natjecanje namijenjeno učenicima srednjih škola, bilo tko može sudjelovati, uz napomenu da nagradu mogu osvojiti isključivo učenici.

Zadacima se može pristupiti i nakon završetka natjecanja i po njima budući natjecatelji ili bilo tko tko se zanima za ovakav oblik natjecanja može vidjeti o kakvim je zadacima riječ, kako stoji sa znanjem iz određenih područja, pokušati ih riješiti i naučiti nešto novo. Za pristup zadacima prošlog natjecanja potrebna je samo registracija putem valjane adrese e-pošte. Jedini alat koji je nužno potreban za rješavanje zadataka je *web* preglednik, no preporučeno je korištenje i SSH klijenta (npr. *Putty*) za pristup ljuski (engl. *shell*) na poslužiteljima natjecanja. U slučaju da natjecatelji iz bilo kojeg razloga ne mogu koristiti vlastiti SSH klijent, *PicoCTF* im nudi *web* ljusku (engl. *webshell*) za pristup koja je prikazana na slici 3. Ne koriste se privatne ni izolirane mreže pa nije potrebno koristiti nikakav VPN alat.



Slika 3 *Prikaz picoCTF web ljuske*

Zadacima i statusima njihovog rješavanja pristupa se preko *web* preglednika. Natjecatelju su prikazani zadaci koje je riješio i koje tek treba riješiti kao što je prikazano na slici 4, koliko koji zadatak nosi bodova te poveznice prema materijalima sa sadržajima obuhvaćenim u zadacima. Zadaci često uz sebe imaju i savjete koji služe za usmjeravanje natjecatelja prema rješenju problema, no na težim zadacima ti su savjeti sve rjeđi.



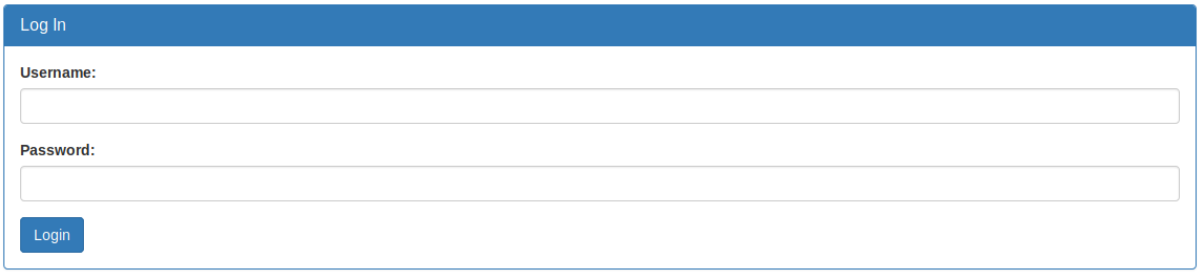
Slika 4 ***Popis zadataka***

Kada natjecatelj tek krene s natjecanjem, dostupno mu je samo nekoliko zadataka za rješavanje. Novi zadaci postat će mu vidljivi tek kad riješi nekoliko prethodnih. Isto vrijedi i za kategorije - u početku natjecatelj vidi samo opću kategoriju, no uz dovoljno riješenih zadataka otvorit će mu se i nove kategorije s novim zadacima.

Kategorije koje se pojavljuju su:

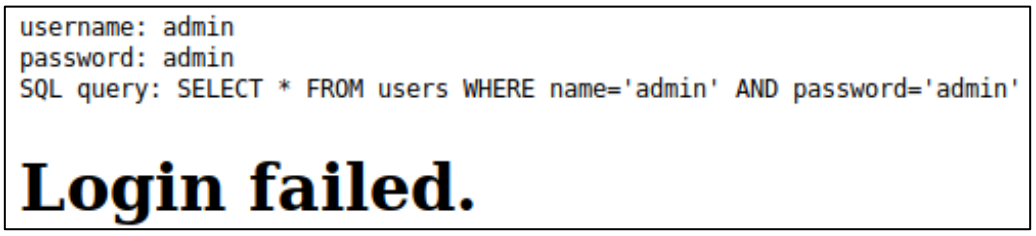
- opće vještine,
- kriptografija,
- računalna forenzika,
- iskorištavanje *web* ranjivosti,
- reverzno inženjerstvo i
- binarno iskorištavanje ranjivosti.

Prvi zadaci su vrlo jednostavni i traže od natjecatelja osnovna računalna znanja poput pretvaranja heksadekadskih brojeva u tekst na temelju ASCII kôda ili samo spajanje na udaljeni poslužitelj pomoću protokola SSH. Kasniji zadaci su već nešto specifičniji i traže određena specifična znanja. Npr. jedan zadatak u kategoriji *web* ranjivosti prikazuje korisniku jednostavnu *web* formu za prijavu koja je prikazana na slici 5.



Slika 5 ***PicoCTF zadatak s web formom***

Savjet (engl. *hint*) za ovaj zadatak natjecatelju govori da postoji baza podataka koja sadrži pristupne podatke o svojim korisnicima te usmjeruje natjecatelja na razmišljanje o tome na koji su način ova *web* forma i baza podataka međusobno povezani. Time se natjecatelj navodi na pokušaj izvođenja *SQL injection* napada. Uz malo istraživanja natjecatelj može otkriti dodatni parametar u kojemu je pohranjen SQL upit koji će se pokrenuti u bazi. Taj upit prikazan je na slici 6.



Slika 6 ***Prikaz SQL upita s podatcima unesenim u web formu***

Sad kad vidi SQL upit koji će se proslijediti bazi, natjecatelj zna što će točno baza podataka izvršiti. Ova informacija natjecatelju govori gdje griješi i što bi trebao promijeniti i pomaže mu da precizira napad kako bi došao do željenog rezultata i riješio zadatak.

Zadaci u kategoriji reverznog inženjerstva u pravilu traže od natjecatelja da iz programa izvuku skrivenu šifru, bilo iz njegovog izvornog kôda (engl. *source code*) kao što je prikazano na slici 7 ili pomoću *debugger/disassembler* alata (npr. x64dbg, IDA, Ghidra…) ako izvorni kôd nije dostupan.

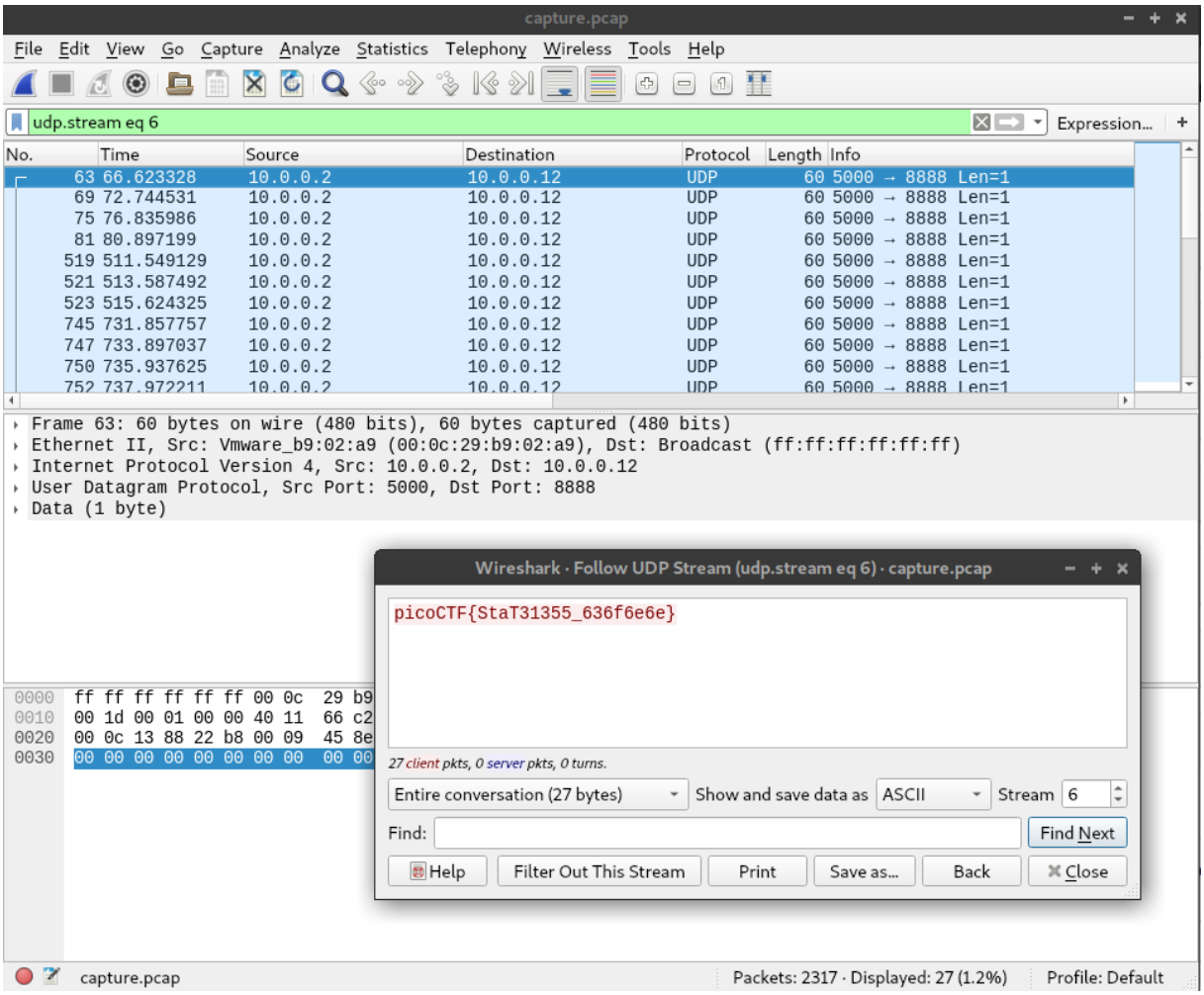
Na slici 7 prikazan je dio izvornog kôda programskog jezika Java koji sadrži skrivenu šifru. Uputa ovog zadatka usmjeruje natjecatelja da istraži što točno radi *charAt()* funkcija u programskom jeziku Java i na taj način otkrije traženu šifru iz kôda i riješi zadatak.

```
// I came up with a more secure way to check the password without putting
// the password itself in the source code. I think this is going to be
// UNHACKABLE!! I hope Dr. Evil agrees...
//
// -Minion #8728
public boolean checkPassword(String password) {
    return password.length() == 32 &&
           password.charAt(0)  == 'd' &&
           password.charAt(29) == '4' &&
           password.charAt(4)  == 'r' &&
           password.charAt(2)  == '5' &&
           password.charAt(23) == 'r' &&
           password.charAt(3)  == 'c' &&
           password.charAt(17) == '4' &&
           password.charAt(1)  == '3' &&
           password.charAt(7)  == 'b' &&
           password.charAt(10) == '_' &&
           password.charAt(5)  == '4' &&
           password.charAt(9)  == '3' &&
           password.charAt(11) == 't' &&
           password.charAt(15) == 'c' &&
           password.charAt(8)  == 'l' &&
           password.charAt(12) == 'H' &&
           password.charAt(20) == 'c' &&
           password.charAt(14) == '_' &&
           password.charAt(6)  == 'm' &&
           password.charAt(24) == '5' &&
           password.charAt(18) == 'r' &&
           password.charAt(13) == '3' &&
           password.charAt(19) == '4' &&
           password.charAt(21) == 'T' &&
           password.charAt(16) == 'H' &&
           password.charAt(27) == 'b' &&
           password.charAt(30) == '8' &&
           password.charAt(25) == '_' &&
           password.charAt(22) == '3' &&
           password.charAt(28) == '7' &&
           password.charAt(26) == '8' &&
           password.charAt(31) == 'e';
}
```

Slika 7 ***Izvorni kôd iz kojeg je potrebno pronaći lozinku***

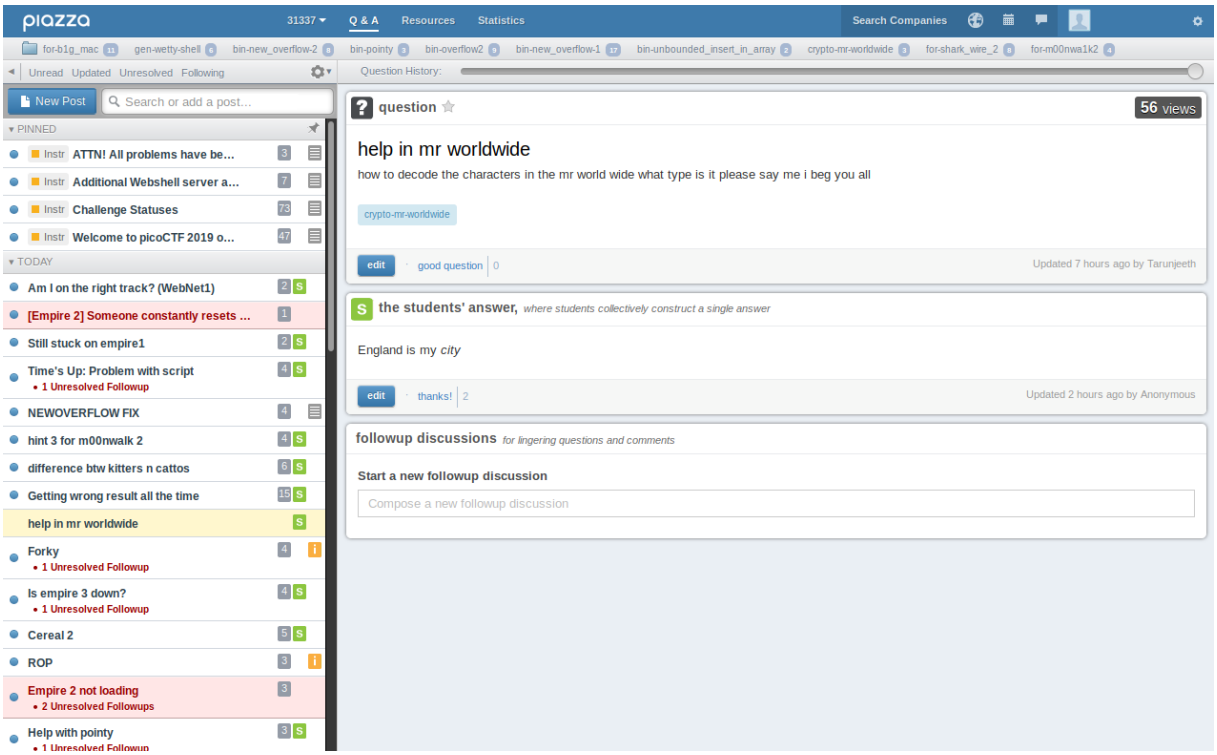
Kad je riječ o zadacima iz računalne forenzike, javlja se više tipova zadataka. Neki zadaci traže od natjecatelja da npr. otkrije informacije skrivene u *.pcap* datoteci sa snimljenim mrežnim prometom za što se najčešće koristi alat *Wireshark* i analiza mrežnih tokova (engl. *network stream*).

Na slici 8 prikazano je pronađeno rješenje jednog takvog zadatka analizom UDP mrežnog toka. Više o praćenju mrežnih tokova i općenito *Wireshark* alatu može se pronaći u dokumentu Nacionalnog CERT-a Wireshark.



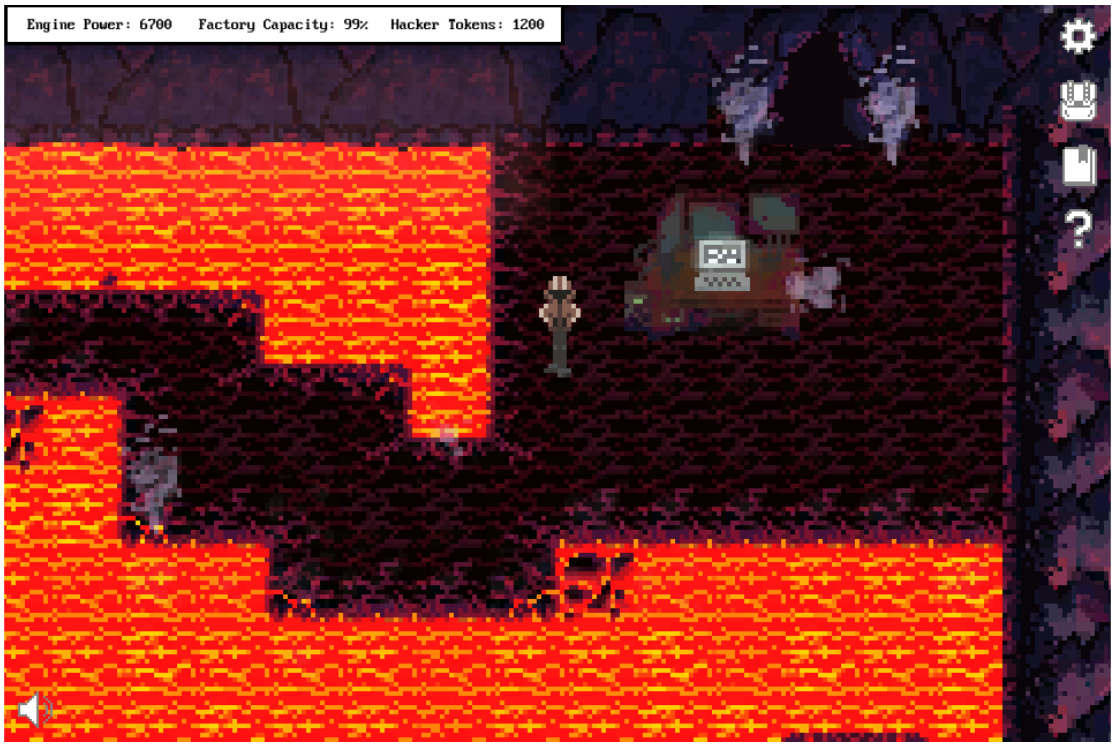
Slika 8 ***Korištenje Wiresharka kako bi se pronašlo rješenje zadatka***

Većina zadataka može se riješiti bez prethodnog predznanja, no ključno je istraživati pretraživanjem na *webu* i upoznati se s tematikom obuhvaćenom u zadatku. Ako zapnete na nekom od zadataka, *PicoCTF* ima forum na stranicama naziva *piazzae* (prikazan na slici 9) gdje si natjecatelji mogu međusobno pomagati i davati savjete. Uz to, postoje i kratki edukacijski dokumenti koji objašnjavaju osnove određenih kategorija za one koji se nikada nisu susreli s tim i kratki video materijali koji objašnjavaju određene zadatke iz prethodnih natjecanja.



Slika 9 ***Piazza stranice gdje natjecatelji mogu tražiti pomoć***

Natjecanje sadrži i igru sa zadacima koja se pokreće u *web* pregledniku koja je prikazana na slici 10. Natjecatelj se nalazi u napuštenoj tvornici gdje mora tražiti računala na kojima rješava zadatke. Ti zadaci su isti oni koji se rješavaju izvan igre. Igra je potpuno izborni, manji dio natjecanja, srž natjecanja je ipak u zadacima koje je moguće rješavati i izvan *web* igre.



Slika 10 ***PicoCTF igra u web pregledniku***

PicoCTF natjecanje je izvrsna početna točka za radoznale ljude koji tek ulaze u svijet informatike i računalne sigurnosti. Zadaci su pažljivo dizajnirani kako bi na zabavan način uveli natjecatelje u razna područja informatike i šire, no natjecanje nije samo za početnike. Čak i oni koji već imaju iskustva u spomenutim područjima mogu pronaći izazovne zadatke kroz koje će nešto naučiti.

2.2 *Attack-defense* CTF natjecanja

Attack-defense CTF natjecanja razlikuju se od prethodno opisanih *Jeopardy-style* CTF natjecanja po tome što se više natjecateljskih timova aktivno „bore“ jedan protiv drugoga. Svaki tim brani jednu ili više svojih aplikacija ili poslužitelja od drugih timova koji ih aktivno napadaju, te istovremeno pokušavaju napasti poslužitelje/aplikacije protivničkih timova.

Boduju se uspješni napadi i obrane te je tim s najviše bodova na kraju natjecanja pobjednik. Očuvanje funkcionalnosti svoje aplikacije/poslužitelja je obično preduvjet za stjecanje bilo kakvih bodova, kako natjecatelji ne bi samo isključili svoje aplikacije/poslužitelje i tako ih „zaštitili“. Primjerice, ako natjecatelji brane svoje *web* stranice, i napadaju tuđe, preduvjet za stjecanje bilo kakvih bodova (i za obranu i za napad) bio bi da njihova *web* stranica funkcionira za „obične korisnike“, tj. da i dalje izvršava svoju funkciju. To se često automatizirano provjerava tako da organizatori natjecanja izrade posebne programe koji simuliraju korisnike („*botovi*“) i bilježe izvršava li pojedina aplikacija i dalje svoju funkciju.

Dok su *Jeopardy-style* CTF natjecanja često u potpunosti *online*, tj. timovi rješavaju zadatke i natječu se udaljeno, iz svih dijelova svijeta, za *attack-defense* natjecanja je uobičajeno da se održavaju lokalno, tj. timovi se skupe na jedno mjesto gdje je postavljena sva infrastruktura za natjecanje (lokalna, izolirana mreža). Često je moguće vidjeti da se prije neke sigurnosne konferencije održi *online Jeopardy-style* CTF natjecanje kao početna, kvalifikacijska runda, pa da onda timovi koji se kvalificiraju otputuju na konferenciju i uživo se natječu u finalima u obliku *attack-defense* CTF natjecanja.

Jedno od najstarijih CTF natjecanja je DEF CON CTF koji se prvi puta održao 1996. godine (3). DEF CON je inače jedna od najpopularnijih konvencija kibernetičke sigurnosti koju posjećuju sigurnosni stručnjaci diljem svijeta. Upravo iz tog razloga je i CTF natjecanje koje organizira i dalje svjetski poznato te privlači velik broj vrhunskih svjetskih hakera i sigurnosnih stručnjaka.

Na stranici ctftime.org je moguće naći i popis *attack-defense* CTF natjecanja. Uz DEF CON CTF, neka druga *attack-defense* CTF natjecanja su:

- UCSB iCTF
- RuCTFE
- Nuit du Hack CTF
- VolgaCTF
- ...

Slika 11 ***Natjecateljski timovi na DEF CON CTF natjecanju 2019. godine*** **(4)**

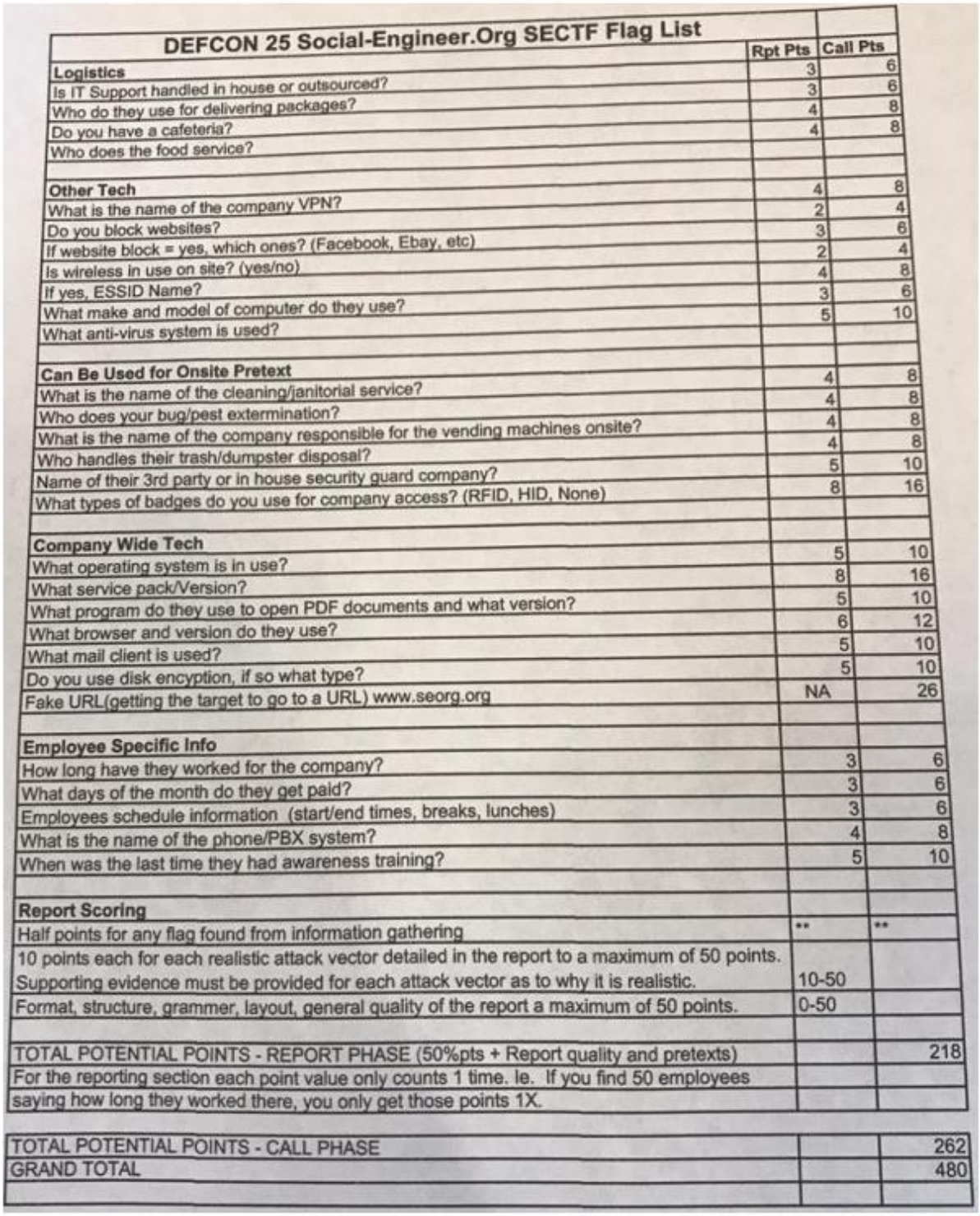
2.3 Specijalizirana CTF natjecanja

Postoje i brojna specijalizirana CTF natjecanja koja se fokusiraju na specifičnu temu ili područje. Jedan takav primjer su CTF natjecanja u socijalnom inženjerstvu. Postoji više natjecanja iz ovog područja, no kao primjer bit će opisano vjerojatno najpoznatije natjecanje ovog tipa, natjecanje SECTF koje se između ostaloga održava i na konferenciji DEF CON.

SECTF se sastoji od dva dijela – početna faza prikupljanja informacija, pa zatim faza primjene socijalnog inženjerstva putem telefonskog poziva. Natjecatelji prije natjecanja dobiju popis tvrtki koje predstavljaju mete i imaju tri tjedna za prikupljanje što je više moguće korisnih informacija koje će im pomoći da socijalnim inženjerstvom obmane, tj. prevare osobu s druge strane telefonske linije. Mete nisu informirane o održavanju samog natjecanja. Za vrijeme natjecanja natjecatelji se zatvore u zvučno izoliranu prostoriju iz koje zovu telefonske brojeve djelatnika ciljanih tvrtki.

Slika 12 ***Natjecatelj u zvučno izoliranoj prostoriji na SE CTF natjecanju na konferenciji DEF CON*** **(5)**

Cilj natjecanja SECTF je prikupiti određene informacije od ciljanih tvrtki. Natjecatelj koji prikupi najviše informacija pobjeđuje, bilo to u fazi prikupljanja informacija prije ili telefonski tijekom natjecanja. Na slici 13 pokazan je popis zadataka, tj. *flagova*, na natjecanju SECTF koje je bilo održano uz DEF CON 25.



DEFCON 25 Social-Engineer.Org SECTF Flag List	Rpt Pts	Call Pts
Logistics	3	6
Is IT Support handled in house or outsourced?	3	6
Who do they use for delivering packages?	4	8
Do you have a cafeteria?	4	8
Who does the food service?		
Other Tech	4	8
What is the name of the company VPN?	2	4
Do you block websites?	3	6
If website block = yes, which ones? (Facebook, Ebay, etc)	2	4
Is wireless in use on site? (yes/no)	4	8
If yes, ESSID Name?	3	6
What make and model of computer do they use?	5	10
What anti-virus system is used?		
Can Be Used for Onsite Pretext	4	8
What is the name of the cleaning/janitorial service?	4	8
Who does your bug/pest extermination?	4	8
What is the name of the company responsible for the vending machines onsite?	4	8
Who handles their trash/dumpster disposal?	5	10
Name of their 3rd party or in house security guard company?	8	16
What types of badges do you use for company access? (RFID, HID, None)		
Company Wide Tech	5	10
What operating system is in use?	8	16
What service pack/Version?	5	10
What program do they use to open PDF documents and what version?	6	12
What browser and version do they use?	5	10
What mail client is used?	5	10
Do you use disk encyption, if so what type?	NA	26
Fake URL(getting the target to go to a URL) www.seorg.org		
Employee Specific Info	3	6
How long have they worked for the company?	3	6
What days of the month do they get paid?	3	6
Employees schedule information (start/end times, breaks, lunches)	4	8
What is the name of the phone/PBX system?	5	10
When was the last time they had awareness training?		
Report Scoring	**	**
Half points for any flag found from information gathering		
10 points each for each realistic attack vector detailed in the report to a maximum of 50 points. Supporting evidence must be provided for each attack vector as to why it is realistic.	10-50	
Format, structure, grammer, layout, general quality of the report a maximum of 50 points.	0-50	
TOTAL POTENTIAL POINTS - REPORT PHASE (50%pts + Report quality and pretexts)		218
For the reporting section each point value only counts 1 time. Ie. If you find 50 employees saying how long they worked there, you only get those points 1X.		
TOTAL POTENTIAL POINTS - CALL PHASE		262
GRAND TOTAL		480

Slika 13 ***Popis zadanih informacija koje su natjecatelji SECTF-a pokušavali prikupiti*** **(6)**

Svrha ovakvih natjecanja je demonstrirati koliko se zapravo informacija može prikupiti iz javnih izvora ili iz samih razgovora sa zaposlenicima tvrtki, bez napada na tehničku infrastrukturu.

Zanimljivo je spomenuti i iCTF natjecanje održano 2010. godine koje je bilo povezano s temom kibernetičkog ratovanja (7). Natjecateljima je prikazan scenarij u kojem izmišljena država „Litya" kontrolira *botnet* koji izvodi ilegalne aktivnosti diljem svijeta. Cilj

natjecanja bio je rastaviti spomenutu *botnet* infrastrukturu. Uz klasično bodovanje, natjecatelji su rješavanjem zadataka skupljali i novac kojim su mogli podmititi Lityine administratore kako bi ostvarili privremeni pristup Lityinoj infrastrukturi. Prije početka natjecanja svakom timu dodijeljen je jedan *bot* kojeg su morali instalirati u infrastrukturu kako bi imali alternativni pristup mreži. Uz spomenuti *bot*, natjecateljima su prije natjecanja prikazane Lityine „misije" koje je bilo potrebno zaustaviti. Bitno je napomenuti i da se ciljana infrastruktura nadzirala pa su natjecatelji trebali paziti što rade i kada izvode napade kako bi izbjegli detekciju.

Sigurnosna tvrtka SANS održava takozvani CTF nestalih osoba (eng. *Missing Persons CTF*) (8). Cilj ovog natjecanja je pomaganje policiji u stvarnoj potrazi za nestalim osobama. Natjecanje nije strogo tehničkog oblika i natjecatelji ne moraju imati prethodna iskustva sa CTF natjecanjima. *Flagovi* su informacije o nestalim osobama koje natjecatelji moraju prikupiti i kojima ostvaruju bodove. Potrebne informacije su kategorizirane u razne skupine, od osnovnih (npr. ime, nadimak, adresa e-pošte osobe) do naprednih (npr. model mobitela, registarska oznaka vozila).

SANS također svake godine za vrijeme božićnih praznika organizira i *Holiday Hack Challenge* (9). *Holiday Hack Challenge* je natjecanje donekle slično prethodno opisanom *PicoCTF*-u – sudionici dobiju pristup igri koja ima neku svoju priču (obično s božićnom tematikom), a za napredovanje u igri moraju rješavati zadatke vezane uz računalnu sigurnost.

Primjerice, na slici 14 je prikazano kako je izgledala *Holiday Hack Challenge* igra 2016. godine. Kada je sudionik natjecanja unutar igre došao do zaključanih vrata, dobio je priliku riješiti zadatak kako bi se vrata otključala. Rješavanje zadatka se odvijalo u posebnom sučelju prikazanom na slici 15 – sudionik je dobio lokalni pristup jednom *Linux* računalu gdje je morao pomoću vještina računalne sigurnosti doći do rješenja.

Slika 14 ***Sučelje igre Holiday Hack Challenge iz 2016. godine*** **(9)**

```
**************************************************************************
*                                                                        *
*To open the door, find both parts of the passphrase inside the /out.pcap file*
*                                                                        *
**************************************************************************
scratchy@1056203eb485:/$ ls -la /out.pcap
-r-------- 1 itchy itchy 1087929 Dec  2 15:05 /out.pcap
scratchy@1056203eb485:/$ sudo su
sudo: unable to resolve host 1056203eb485

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for scratchy:
scratchy@1056203eb485:/$ sudo -l
sudo: unable to resolve host 1056203eb485
Matching Defaults entries for scratchy on 1056203eb485:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User scratchy may run the following commands on 1056203eb485:
    (itchy) NOPASSWD: /usr/sbin/tcpdump
    (itchy) NOPASSWD: /usr/bin/strings
scratchy@1056203eb485:/$
```

Slika 15 ***Sučelje za rješavanje jednog zadatka iz Holiday Hack Challengea 2016. godine*** **(9)**

2.4 Izolirane virtualne mreže koje simuliraju stvarna okruženja

Neka CTF natjecanja/stranice za vježbu omogućuju korisnicima pristup izoliranoj mreži u kojoj se nalaze ranjiva virtualna računala i aplikacije. Svrha toga je korisniku omogućiti izravan pristup cijeloj ranjivoj infrastrukturi, a ne samo jednoj aplikaciji za vježbu. Primjer stranice za vježbu koja koristi izolirane virtualne mreže je *Hack The Box*, i na njenom primjeru će biti objašnjena ova vrsta zadataka/natjecanja.

Hack The Box je stranica na kojoj korisnici mogu vježbati penetracijsko testiranje. Stranica je besplatna i bitno je napomenuti da se virtualna računala dijele i s ostalim korisnicima. Postoji i mogućnost plaćanja kojima se ostvaruju neke pogodnosti kao što su privatna virtualna računala za vježbu, pristup starijim, „umirovljenim" virtualnim računalima i vježbama i sl.

Registracija na *Hack The Box* naočigled djeluje kao da je potrebno imati pozivni kôd (engl. *invite code*), no zapravo je stvar u tome da korisnici koji se žele registrirati moraju „hakirati" stranicu za registraciju i sami sebi generirati traženi kôd. Ovaj proces je neka vrsta ulaznog ispita, i korisnici koji ne znaju riješiti taj zadatak se vjerojatno neće ni snaći s ostalim zadacima unutar *Hack The Boxa*.

Nakon uspješne registracije korisniku se prikažu uputstva za spajanje na izoliranu virtualnu mrežu putem VPN-a. Nakon što se uspješno spoji, korisnik može početi s vježbanjem. *Hack The Box* preporuča korisnicima da se na izoliranu mrežu spajaju kroz posebno virtualno računalo (engl. *virtual machine*), jer kako se ta mreža dijeli s ostalim korisnicima, poneki korisnik može odlučiti napasti drugog korisnika u mreži. Tada je za žrtvu napada sigurnije da nastrada virtualno računalo koje je ipak donekle izolirano od ostatka fizičkog računala. Na *Hack The Boxu* se mogu pronaći i razni zadaci nalik zadacima *Jeopardy-style* CTF natjecanja, no glavni sadržaj su ipak ranjiva virtualna računala.

Slika 16 je primjer stranice s informacijama o jednom takvom računalu koje ima IP adresu u virtualnoj mreži preko koje ga korisnici mogu napasti.

Slika 16 ***Ranjivo virtualno računalo za vježbu na stranici Hack The Box***

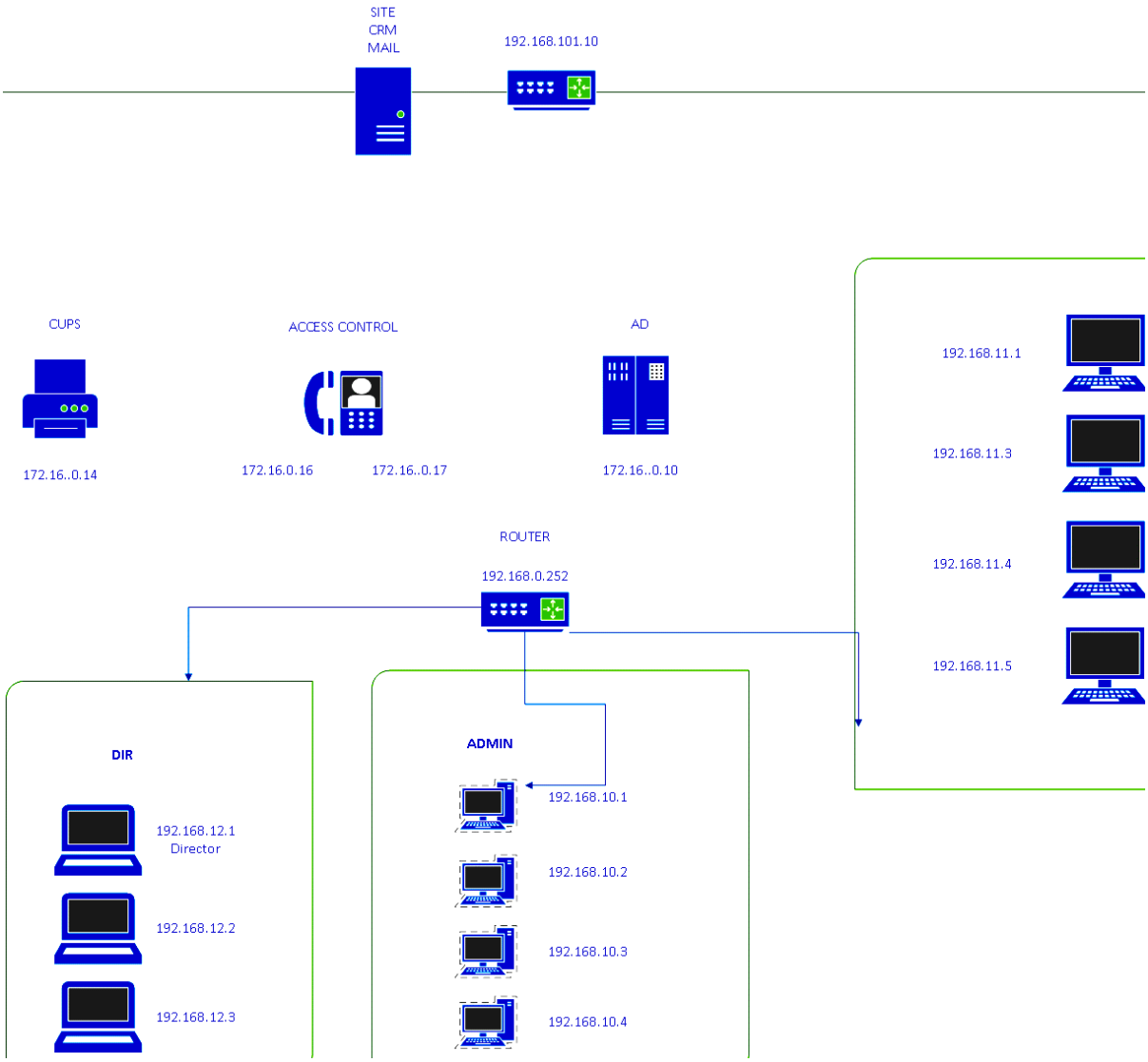
Kod ovakvih zadataka uobičajeno je prvo mrežno skenirati računalo kako bi se otkrilo što više informacija o dostupnim mrežnim servisima pa onda nekako ostvariti kontrolu nad tim računalom (npr. iskorištavanjem ranjivog mrežnog servisa, pogađanjem lozinke i sl.). Za svako računalo postoje dva cilja, tj. rješenja (*flag)* koja je potrebno pronaći iz tekstualnih datoteka na računalima: korisničko rješenje (engl. *user flag*) do kojega je obično moguće doći preuzimanjem neke osnovne kontrole nad računalom, i administratorsko rješenje (engl. *root flag*) za koje je potrebno u potpunosti preuzeti kontrolu nad računalom.

Računala ne dolaze s opisom zadatka, već korisnici trebaju sami otkriti kako napasti računala. Računala mogu imati različite operacijske sustave (*Windows*, *Linux*, BSD...), a na njima se može pronaći i širok spektar raznih servisa i aplikacija. Konačni cilj napada na bilo koje virtualno računalo unaprijed se zna – doći do korisničkog i administratorskog rješenja (*user*/*root flag*), no način na koji će korisnici doći do cilja se razlikuje od zadatka do zadatka.

Osim individualnih ranjivih računala, u nekim plaćenim paketima članstva na *Hack The Boxu* dostupne su i cijele ranjive mreže koje se sastoje od više računala.

Još jedna slična stranica koja koristi izolirane virtualne mreže je lab.pentestit.ru. Ova stranica sličnog je koncepta kao Hack The Box, no razlika je u tome glavni sadržaj na stranici nisu individualna ranjiva računala, već cijela ranjiva mreža. Pristup ranjivoj mreži

se također ostvaruje putem VPN-a. Kada se korisnik spoji, može pristupiti ranjivoj mreži u kojoj se mogu naći razna računala i aplikacije. Ranjiva mreža je napravljena tako da bude što sličnija uobičajenim mrežama stvarnih tvrtki. Arhitektura jedne takve mreže prikazana je na slici 17.



Slika 17 ***Prikaz arhitekture jedne ranjive mreže na stranici lab.pentestit.ru*** **(10)**

Obično je dostupna samo jedna mreža, no, kao što se vidi na prethodnoj slici, u toj mreži ima veći broj računala. U ovoj mreži korisnici moraju iskoristiti ranjivosti na razini operacijskih sustava, aplikacija i njihovog kôda, mrežne opreme i kriptografskih mehanizma. Uz to, ljudski faktor također igra ulogu u rješavanju. Organizatori se trude da svaka mreža bude jedinstvena i da sadržava najnovije poznate ranjivosti.

Za razliku od stranice *Hack The Box*, rješenja zadataka (*flagovi*) nisu na razini individualnih računala, već na razini cijele mreže, tj. fiktivne tvrtke. Nema striktno definiranih *user* i *root flagova*, već korisnici trebaju naći određene tokene koji su raspoređeni diljem virtualne infrastrukture. Neki od tih tokena se mogu pronaći u porukama e-pošte (nakon što korisnik dobije pristup sustavu e-pošte), u servisima za upravljanje izvornim kôdom, u bazi podataka, na usmjerivaču (engl. *router*) i sl. Sve u

svemu, stranica *lab.pentestit.ru* svojim korisnicima nudi velik izolirani prostor za vježbanje kibernetičkih napada koji je dizajniran tako da što više sliči pravim IT infrastrukturama, te je za razliku od *Hack The Boxa* na kojemu se pristup takvoj vrsti zadataka (cijela ranjiva mreža) plaća, na stranici *lab.pentestit.ru* je pristup tome besplatan.

Za ovo poglavlje je korisno napomenuti još jednu stranicu – *VulnHub*. Ova stranica nudi mogućnost preuzimanja datoteka virtualnih računala koje korisnici onda mogu lokalno pokrenuti u svojoj okolini. Princip rješavanja je sličan kao kod stranica *Hack The Box* i *lab.pentestit.ru*, a glavna razlika je upravo u tome što se korisnik ne spaja na neku vanjski ranjivu mrežu, već takvu mrežu postavlja lokalno, na svojem računalu, pomoću programa za virtualizaciju (npr. *VirtualBox* ili *VMware player*). Uz svako virtualno računalo postoji i kratak opis tematike koju pokriva i što je potrebno napraviti. *VulnHub* je kroz godine rada prikupio velik broj ranjivih računala, te je vjerojatno i inspirirao neke od sličnih stranica kao što su *Hack The Box* i *lab.pentestit.ru*.

2.5 Defenzivne kibernetičke vježbe

Uz CTF natjecanja, postoje i općenitije kibernetičke vježbe koje pokušavaju što realnije simulirati stvarne situacije kibernetičke sabotaže ili kibernetičkog ratovanja. Takve vježbe se često organiziraju na razini državnih ili svjetskih organizacija, a jedna od takvih vježbi je i *Cyber Europe* koju organizira Agencija Europske unije za kibernetičku sigurnost (ENISA, engl. *European Union Agency for Cybersecurity*, prethodno *European Network and Information Security Agency*).

Slika 18 *Neki od sudionika na vježbi Cyber Europe* (11)

Vježba *Cyber Europe* održana 2018. godine bavila se incidentom u zrakoplovnoj industriji koji je eskalirao u krizu na europskoj razini (11). Sudionici su se bavili forenzikom, analizom zlonamjernog kôda i prikupljanjem informacija, no uz to je bilo potrebno i održavati kontinuitet poslovanja i upravljati rizicima.

NATO savez također održava svoje kibernetičke vježbe od kojih je jedna od najvećih zvana *Cyber Coalition*. Svrha ovih vježbi je jačanje međunarodne suradnje u obrani od kibernetičkih prijetnji. Na vježbama održanima 2019. godine prisustvovalo je otprilike 900 sudionika iz članica NATO saveza (12).

Američka agencija za nacionalnu sigurnost (NSA) također održava svoje kibernetičke vježbe pod nazivom *Cyber Defense Exercise* (CDX) (13). Sudionici ovih vježbi su studenti vojnih snaga Kanade i Sjedinjenih Američkih Država, a održavaju se sa svrhom treniranja obrane od kibernetičkih napada. Studenti u ovim vježbama igraju obrambenu ulogu gdje im je cilj zaštititi određenu infrastrukturu od kibernetičkih napada koje izvode NSA-ini sigurnosni stručnjaci.

2.6 Stranice sa zadacima za vježbu

Osim CTF natjecanja, postoje i razne druge stranice na kojima korisnici zainteresirani za informacijsku sigurnost mogu vježbati, učiti nove vještine, upoznavati se s novim tipovima zadataka ili se pripremati za CTF natjecanja. Takve stranice su brojne i sadrže široki spektar vrsta zadataka, često se nazivaju i „*wargame*“ stranice, a neke od najpoznatijih su *HackThisSite, OverTheWire i SmashTheStack*.

HackThisSite je besplatna *web* stranica namijenjena za provjeru i poboljšanje ofenzivnih vještina. Korisnici *HackThisSitea* mogu rješavati zadatke usko vezane za područje računalne sigurnosti koji su prikazani u obliku sličnom *Jeopardy-style* CTF natjecanjima. Rješavanje zadataka nije vremenski ograničeno, naglasak ne leži na natjecanju, već na samim zadacima i na stjecanju znanja za njihovo rješavanje (14).

Zadaci su na *HackThisSiteu* podijeljeni u nekoliko kategorija, od osnovnih zadatka, do realističnih zadataka, programiranja, reverznog inženjerstva, forenzike itd.

Prilikom rješavanja zadataka korisniku se predstavljaju kratki opisi zadatka uz vrlo malo smjernica. Zadaci nekih kategorija (npr. kod realističnih i programerskih kategorija) kratkim tekstom objašnjavaju korisniku što treba postići na određenoj *web* stranici ili kakav program je potrebno razviti da bi se dobio željeni rezultat, no daljnjih savjeta nema ili su rijetki.

Zadaci osnovne kategorije su najjednostavniji te zahtijevaju osnovno znanje HTML-a i PHP-a. Od korisnika se očekuje da iz HTML stranice pročita skrivene informacije ili izmjeni dijelove stranice kako bi riješio zadatak. Kasniji zadaci obuhvaćaju i osnovnu razinu razumijevanja implementacije aplikacija napisanih u programskom jeziku PHP na *web* poslužitelju.

JavaScript zadaci slični su onima osnovne kategorije, no fokus je na samom *JavaScript* kôdu. Korisniku se kod ovih zadataka najčešće predstavi obrazac u koji je potrebno unijeti rezultat, a na stranici gdje se taj obrazac nalazi je ukomponirana i kratka *JavaScript* skripta koju je potrebno pronaći i analizirati.

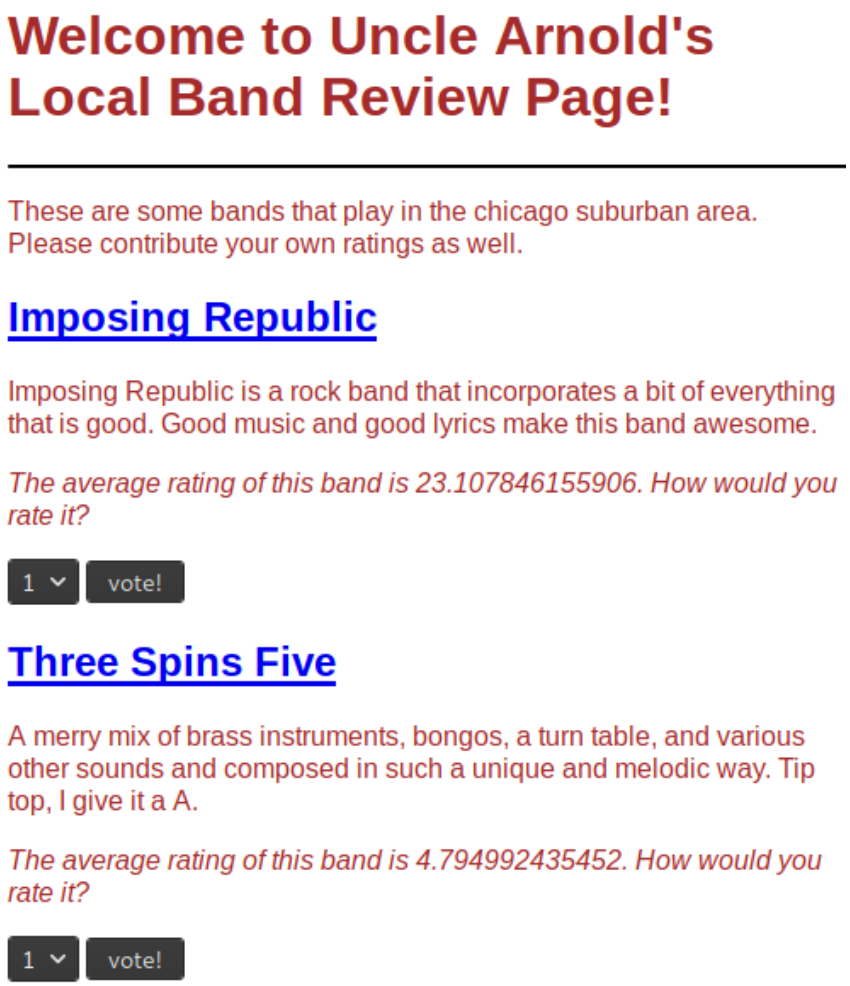
```
 5 function checkpass(pass)
 6 {
 7 if(pass == rawr+" "+moo)
 8 {
 9 alert("How did you do that??? Good job!");
10 window.location = "../../../missions/javascript/6/?lvl_password="+pass;
11 } else {
12 alert("Nope, try again");
```

Slika 19 ***JavaScript datoteka iz koje je potrebno iščitati šifru***

Kategorija proširenih osnova zahtijeva razumijevanje programiranja. Neki od programskih jezika obuhvaćenih ovom kategorijom su C, PHP, *Perl*, *Java* i *Batch*. Korisnik ne mora biti iskusni programer u nekom od spomenutih jezika, no potrebno je opće znanje programiranja i razumijevanje slijeda izvršavanja kôda. U ovim zadacima se korisniku prikazuje kratki kôd kojeg mora analizirati i napraviti izmjenu kako bi izveo napad ili ispravio ranjivost. Ponekad se od korisnika traži da unese točan URL preko kojeg će se ranjivost u kôdu iskoristiti.

Slika 20 ***Zadatak kategorije proširenih osnova gdje korisnik mora iskoristi ranjivost u PHP kôdu***

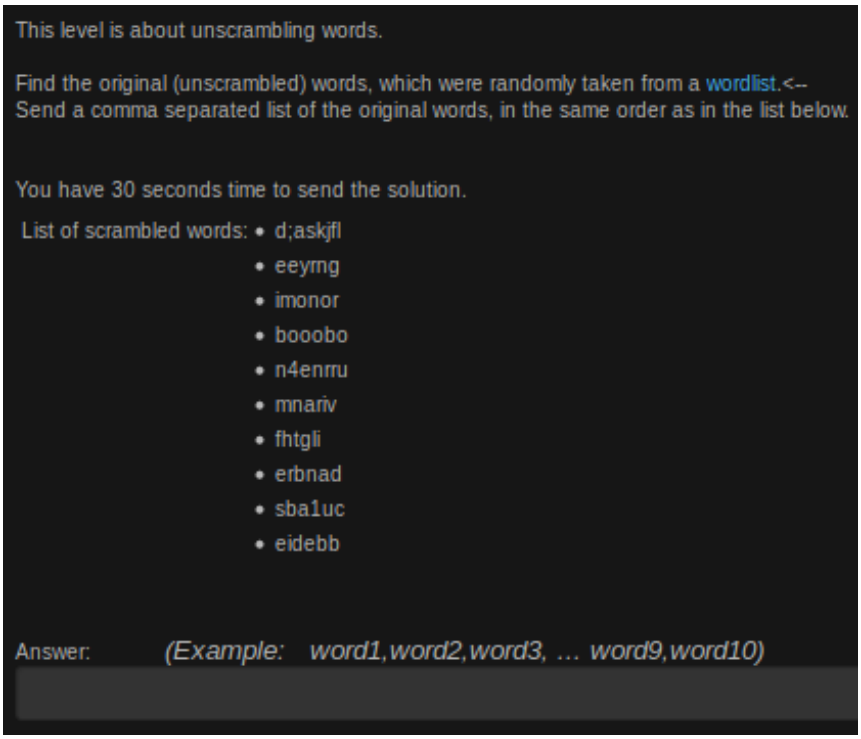
Kategorija realističnih zadataka sadrži niz *web* stranica koje korisnik mora napasti na razne načine. Ciljevi nisu samo postati administrator stranica, već uključuju i upravljanje podacima na samoj stranici ili dohvat informacija iz njih.



Slika 21 ***Zadatak realistične kategorije gdje je cilj svrstati određenu glazbenu grupu na vrh popisa***

Kod aplikacijskih zadataka korisniku se daje određena aplikacijska datoteka koju mora preuzeti lokalno i upravljati njome kako bi dobio željeni rezultat. Potrebno znanje za rješavanje ovih zadataka uključuje reverzni inženjering same aplikacije. Kategorija se uglavnom fokusira na *Microsoft Windows* aplikacije, no određeni zadaci dolaze i u *MacOS* i *Unix* inačicama.

Zadaci kategorije programiranja zahtijevaju veće znanje programiranja od ostalih kategorija. U ovim zadacima se korisniku predstavi dinamično generiran niz vrijednosti iz kojeg korisnik mora generirati traženi rezultat u zadanom vremenskom periodu. Vrijeme rješavanja ovih zadataka je ograničeno na svega nekoliko sekundi (ovisno o zadatku), a nakon isteka vremena generira se novi niz čime se mijenja i traženi rezultat. S obzirom na vremensko ograničenje, korisnik je prisiljen napisati svoj program kojim će automatizirati rješavanje zadatka i tako ga riješiti dovoljno brzo. Zanimljivo je spomenuti da jedan od zadataka ove kategorije uključuje i pisanje vlastitog IRC *bota*.

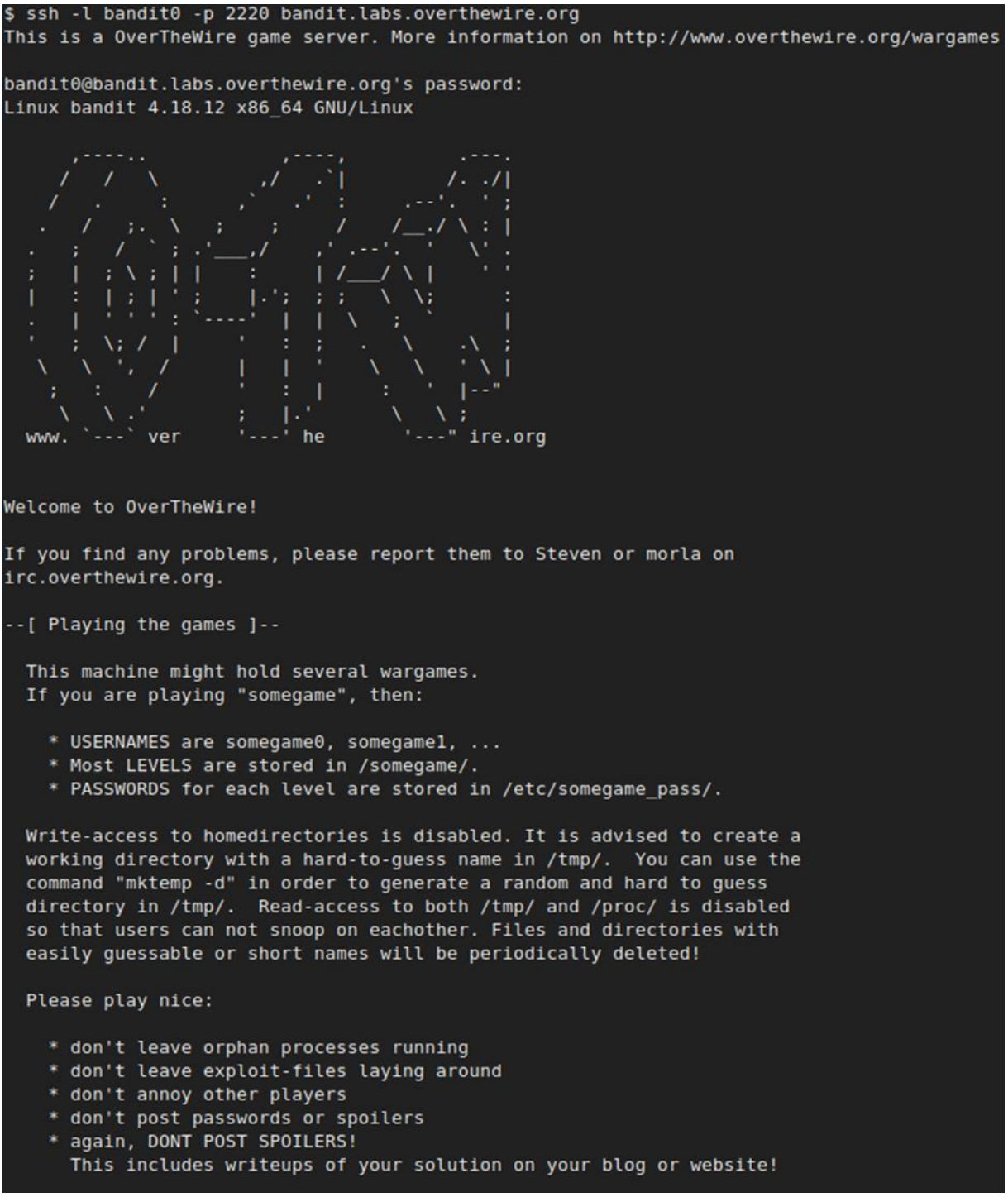


Slika 22 ***Zadatak programske kategorije gdje je cilj dešifrirati riječi unutar trideset sekundi***

Za vrijeme pisanja ovog dokumenta (kraj 2019. godine) postoje samo tri zadataka u kategoriji forenzike. Dva od tri zadataka obuhvaćaju traženje podataka u kopijama USB diska, a jedan zadatak obuhvaća traženje digitalnih manipulacija na slici. U kategoriji steganografije su zadaci fokusirani na traženje skrivenih podataka u slikama ili audio zapisima. IRC (end. *Internet Relay Chat*) kategorija je posebna po tome što se od korisnika traži napad na *botove* na službenom *HackThisSite* IRC poslužitelju.

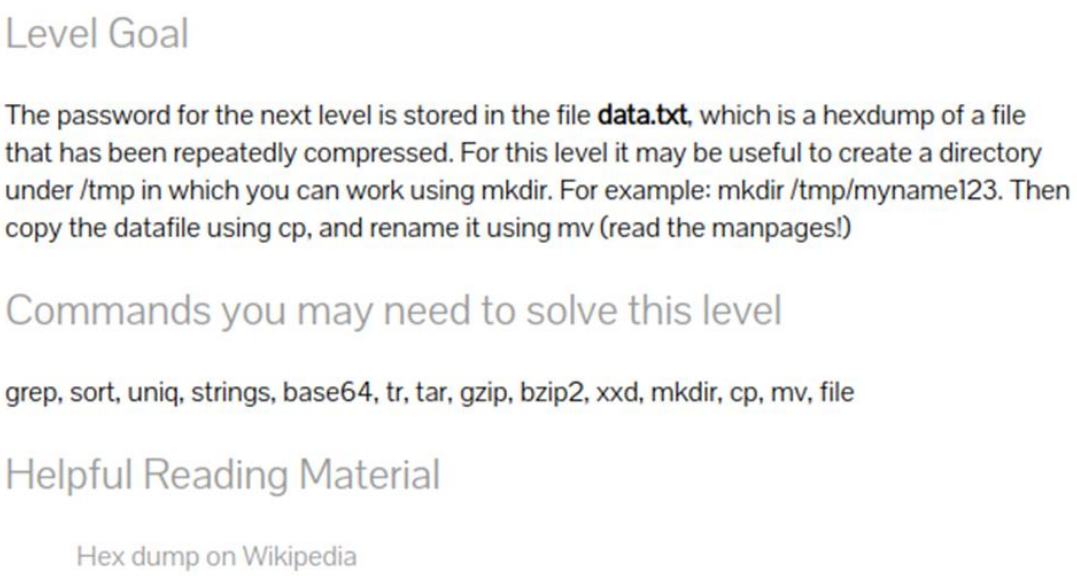
Zadaci na *HackThisSiteu* variraju od vrlo jednostavnih do izrazito složenih. Sami zadaci i njihovi opisi malo usmjeravaju korisnika prema cilju, no pomoć se može naći na službenim forumima stranice i IRC-u.

Još jedna popularna stranica sa zadacima je *OverTheWire*. Ova stranica nudi nekoliko „igri" raznih težina koje se igraju na udaljenim poslužiteljima, gdje svaka igra ima nekoliko razina. Pristup samim igrama se uglavnom ostvaruje putem protokola SSH (eng. *Secure Shell*), no to nije slučaj za sve igre. Slika 23 prikazuje tekst koji korisnik vidi kada se spoji na prvu razinu najjednostavnije igre.



Slika 23 ***Početni tekst prve razine jedne od igara na stranici OverTheWire***

Svaka razina koristi zasebno SSH korisničko ime, a cilj razina je pronaći šifru za iduću razinu. Npr. prvi zadatak najjednostavnije igre koristi korisničko ime „*bandit0*“ s istom šifrom. Kada korisnik riješi zadatak, otkrije šifru za iduću razinu te se ponovo spaja na udaljeni poslužitelj s korisničkim imenom „*bandit1*“ koristeći šifru koju je otkrio u prethodnoj razini. Zadaci se rješavaju putem SSH veze na udaljenom poslužitelju, no detalji samih razina nalaze se na *web* stranicama *overthewire.org*. Primjer jednog zadatka se može vidjeti na slici 24.



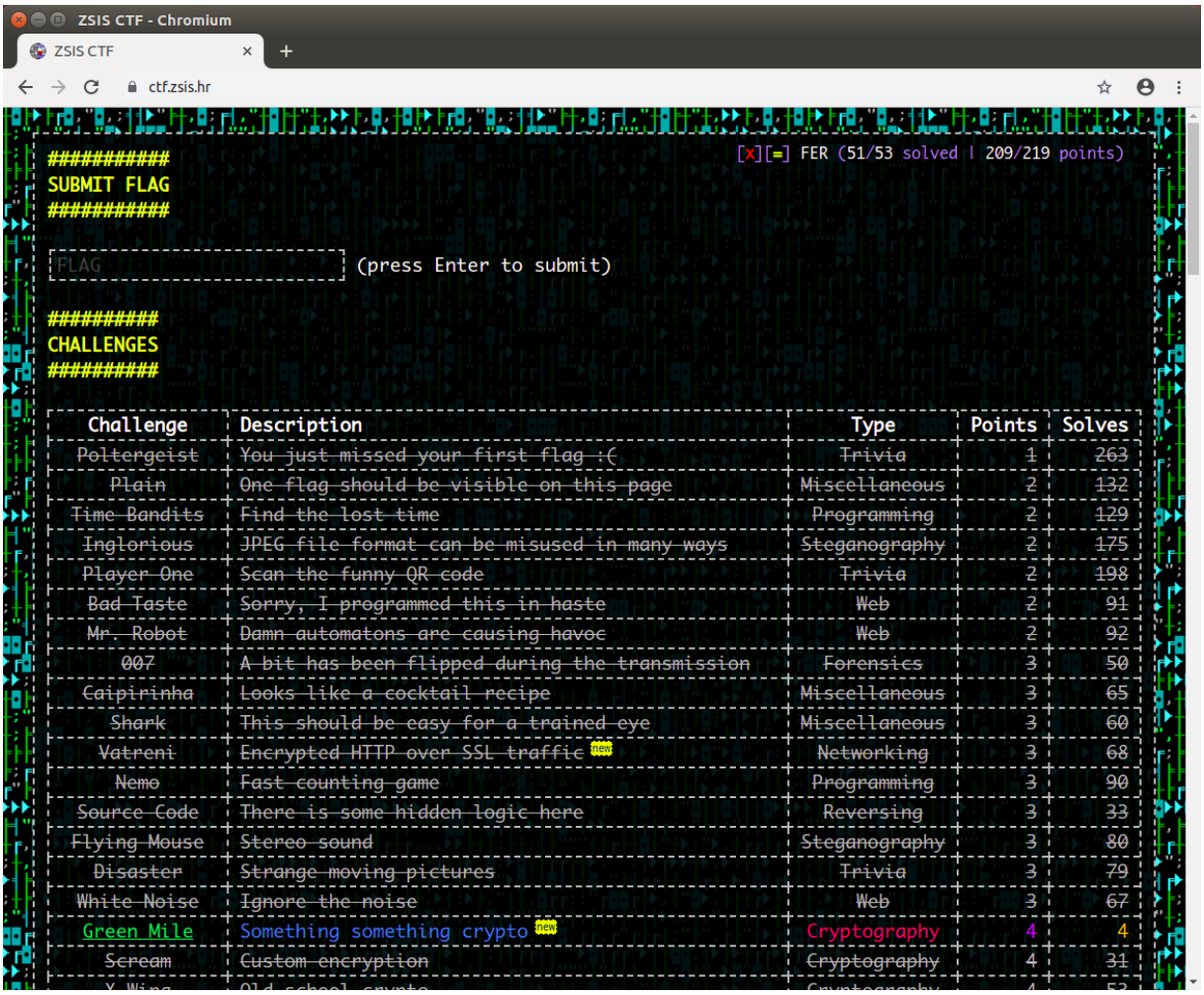
Slika 24 ***Opis jednog zadatka jedne razine na overthewire.org stranici***

Same igre međusobno podosta variraju, od pristupa do tematike. Prva igra se rješava putem SSH klijenta, dok je npr. druga igra fokusirana na *web* ranjivosti i rješava se u *web* pregledniku. Opisi zadataka također variraju od detaljnih uputstava sa smjernicama do praktički nikakvih informacija.

3 Zaključak

Na CTF natjecanjima je na zabavan način i uz natjecateljsku atmosferu moguće naučiti puno praktičnih znanja iz područja računalne sigurnosti. Postoje i brojne stranice nalik CTF natjecanjima čiji je fokus više na učenju i vježbanju, a manje na natjecanju između timova.

Koncept CTF natjecanja postao je toliko popularan da se sada gotovo svaki vikend održava neko *online* natjecanje otvoreno svima koji žele sudjelovati. Popis nekih nadolazećih (i prošlih) CTF natjecanja dostupan je na *web* stranici ctftime.org. Postoje i CTF natjecanja organizirana u Hrvatskoj, od kojih je jedno ZSIS CTF – *Jeopardy-style* CTF natjecanje otvoreno za sve zainteresirane, a organizira ga Zavod za sigurnost informacijskih sustava (ZSIS).



Slika *25 Početna stranica ZSIS CTF-a (nakon prijave)*

4 Literatura

1. **THE J!EFFECT.** Ever made your own Jeopardy! Board? *Jeopardy!* [Mrežno] 11. siječnja 2017. [Citirano: 16. prosinca 2019.] https://www.jeopardy.com/jbuzz/jeffect/ever-made-your-own-jeopardy-board.
2. **Carnegie Mellon University.** About picoCTF. *Carnegie Mellon University.* [Mrežno] [Citirano: 11. prosinca 2019.] https://picoctf.com/about.
3. **DDTek, vulc@n of.** A history of Capture the Flag at DEF CON. *DEF CON Communications.* [Mrežno] [Citirano: 11. prosinca 2019.] https://www.defcon.org/html/links/dc-ctf-history.html.
4. **Rhysider, Jack.** EP 43: PPP. *Darknet Diaries.* [Mrežno] 23. srpnja 2019. [Citirano: 17. prosinca 2019.] https://darknetdiaries.com/episode/43/.
5. **Mitchell, Blake.** Locked in a soundproof booth: My experience at DefCon's SE-CTF competition. *Medium.* [Mrežno] 14. kolovoza 2018. [Citirano: 11. prosinca 2019.] https://medium.com/cmd-security/locked-in-a-soundproof-booth-my-experience-at-defcons-se-ctf-competition-2282a0c55caf.
6. **Ensign, Melanie.** Melanie Ensign. *Twitter.* [Mrežno] 13. srpnja 2017. [Citirano: 11. prosinca 2019.] https://twitter.com/imeluny/status/885678335644254208.
7. *Hit 'em Where it Hurts: A Live Security Exercise on Cyber Situational Awareness.* **Adam Doupé, Manuel Egele, Benjamin Caillat, Gianluca Stringhini, Gorkem Yakin, Ali Zand, Ludovico Cavedon, Giovanni Vigna.** s.l. : University of California, Santa Barbara, 2011.
8. **SANS.** Cyber Defense Initiative® 2019. *SANS.* [Mrežno] 10. prosinca 2019. [Citirano: 13. prosinca 2019.] https://www.sans.org/event/cyber-defense-initiative-2019/bonus-sessions/19390.
9. —. The 2019 SANS Holiday Hack Challenge. [Mrežno] 2019. [Citirano: 16. prosinca 2019.] https://holidayhackchallenge.com/.
10. **Halon, Jack.** Pentestit Lab v11 - Introduction & Network. *Jack Hacks.* [Mrežno] 27. srpnja 2017. [Citirano: 13. prosinca 2019.] https://jhalon.github.io/pentestit-lab-11-intro/.
11. **Cyber Europe.** Cyber Europe 2018: Preparing Aviation to respond to cyber crises. *Cyber Europe.* [Mrežno] [Citirano: 13. prosinca 2019.] https://www.cyber-europe.eu/.
12. **Second Line of Defense.** Finland Participates in NATO Cyber Coalition 2019 Exercise. *Second Line of Defense.* [Mrežno] 12. srpnja 2019. [Citirano: 13. prosinca 2019.] https://sldinfo.com/2019/12/finland-participates-in-nato-cyber-coalition-2019-exercise/.
13. **NSA | CSS.** Cyber Defense Exercise (CDX). *National Security Agency | Central Security Service.* [Mrežno] 4. veljače 2016. [Citirano: 13. prosinca 2019.] https://apps.nsa.gov/iaarchive/programs/cyber-defense-exercise/index.cfm.
14. **Hammond, Jeremy.** About the Project. *Hack This Site.* [Mrežno] 13. listopada 2004. [Citirano: 13. prosinca 2019.] https://www.hackthissite.org/info/about.
15. **UC Santa Barbara.** iCTF. *The UC Santa Barbara iCTF Competition.* [Mrežno] [Citirano: 11. prosinca 2019.] https://ictf.cs.ucsb.edu/.
16. **CARNET.** CARNET sudjelovao u NATO vježbi "Cyber Coalition 2019". *CARNET.* [Mrežno] 9. prosinca 2019. [Citirano: 13. prosinca 2019.] https://www.carnet.hr/carnet-sudjelovao-u-nato-vjezbi-cyber-coalition-2019/.