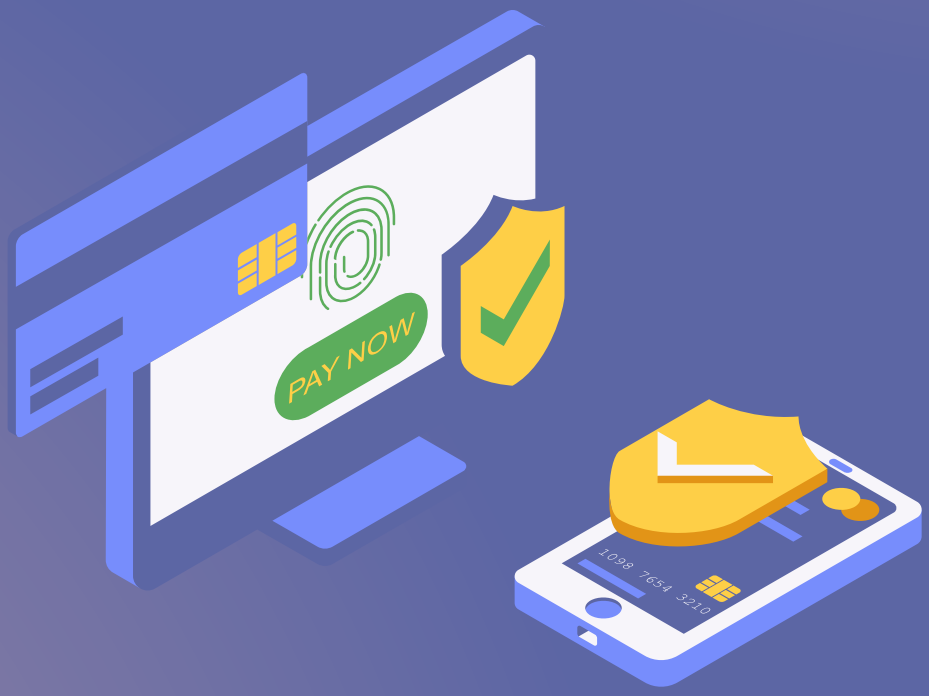
Ulysseus
EUROPEAN UNIVERSITY

UCG
University of Montenegro
1974

Sajber bezbjednost

Besplatni resursi za studente

ULYSSEUS INOVACIONI HAB ZA SAJBER BEZBJEDNOST



https://www.ucg.ac.me/rektorat/ucsh

Sadržaj:

Uvod

Ulysseus Inovacioni Hab za sajber bezbjednost

(Univerzitet Crne Gore)

U okviru programa Evropskog univerziteta Ulysseus Univerzitet Crne Gore je preuzeo zadatak formiranja Inovacionog haba sa tematskim fokusom na sajber bezbjednosti i planiranom funkcionalnošću do kraja 4. godine projekta (2027) ali sa pripremnim aktivnostima koje počinju odmah. Naučni direktor haba je prof. dr Igor Đurović, profesor Elektrotehničkog fakulteta.

Jedan je od osam tematskih habova Ulysseusa i njegovog kampusa. Hab će biti mjesto saradnje (ko-kreacije) obrazovanja, nauke i inovacija; univerziteta i preduzetništva - usmjeravanih potrebama društva tj. društvenim izazovima i na uslugu društvu. Ovdje će se održavati otvoreni časovi, programi Living Laba, Science Shopa, Inkubatora i druge metode interaktivnosti između univerziteta i društva, posebno mladih.

Zajednički i dualni obrazovni programi partnera biće takođe tematski povezani sa izazovima definisanim u okviru habova kao i međunarodni Ulysseus program studentskih obuka za nauku i inovacije. Hab će organizovati i takmičenja u cilju usmjeravanja studenata i istraživača ka ovoj važnoj oblasti za digitalno društvo.
Ulysseus takođe predviđa podršku za aktivnosti transfera inovacija i znanja u okviru alijanse partnera, gdje će Inovacioni hab imati ulogu u jačanju održivog procesa transfera znanja, kreiranja startapova u saradnji sa pridruženim partnerima a u cilju jačanja privrede i održivog razvoja teritorija.

Putem Haba, jačaće se kapaciteti studenata i profesionalaca iz oblasti sajber bezbjednosti, uz oslanjanje na zajedničke snage Ulysseus univerziteta – njegovih univerzitetskih članica kao i mreže pridruženih partnera iz privrede.

Kontakt: ulysseus@ucg.ac.me

Obični korisnici

U oblasti sajber bezbjednosti, obični korisnici (ili krajnji korisnici) su sve osobe koje koriste računarske sisteme, mreže i internet za svakodnevne aktivnosti, ali nisu nužno stručnjaci za sajber bezbjednost. Oni su često meta sajber napada jer mogu biti slabija karika u sigurnosnom lancu.

Kao takvi, moraju biti upoznati sa osnovnim vještinama i mjerama zaštite u svakodnevnom korišćenju interneta.

1 "CRDF Global: OSNOVNA PRAVILA INFORMACIONE BEZBJEDNOSTI"

Kurs je namijenjen svim korisnicima koji žele da nauče više o osnovnim prijetnjama u informacionom okruženju, zaštitu ličnih podataka, bezbjedno korišćenje elektronskih uređaja i sredstava informisanja. Projekat je realizovao CRDF Global u saradnji sa Državnim sekretarijatom SAD-a.

Link: https://cybereducation.org/mc/index.php/usr/login/login?lang=mis

2 "ALISON: Digital and Cyber Security Awareness"

Kurs pruža znanja kako da identifikujete rizike sajber bezbjednosti, naučite dobre prakse u cilju sajber zaštite, kako da spriječite sajber napade i koristite pravilan digitalni bonton.

Link:https://alison.com/course/digital-and-cyber-security-awareness

Zašto je važno znati elementarnu sajber higijenu?

Lična bezbjednost: Razumijevanje osnovnih koncepata sajber bezbjednosti može pomoći pojedincima da zaštite svoje lične podatke, kao što su lozinke, finansije i drugi osjetljivi podaci, od sajber pretnji i napada poput krađe identiteta i prevara.

Profesionalna bezbednost: Na radnom mestu, poznavanje osnova sajber bezbjednosti može spriječiti kršenje zaštite podataka, zaštititi informacije kompanije i održati integritet sistema i mreža.

Početni nivo

Početni nivo u sajber bezbjednosti obuhvata osnovne vještine i znanja potrebne za razumijevanje i primjenu osnovnih principa zaštite informacionih sistema i podataka. Ovo je često prva stepenica za one koji žele da započnu karijeru u sajber bezbjednosti ili da unaprijede svoje razumijevanje bezbjednosnih praksi. U nastavku možete naći nekoliko ključnih kurseva za savladavanje početnog nivoa u sajber bezbjednosti:

1 "Preduzmi ideju"

Platforma "Preduzmi ideju" nudi veliku količinu edukativnog materija iz oblasti inovacija i tehnološkog preduzetništva. Ova platforma sadrži razne kurseve, mentorske programe, radionice namjenjene studentima, mladim profesionalcima ali i univerzitetskim profesorima sa ciljem pružanja snažne podrške osnivanju startap programa i komercijalizacije inovacija.

Link: https://www.preduzmi.rs/

2 "Simplilearn: An Ultimate Guide to Cyber Security for Beginners"

Kurs pruža elementarna znanja i detaljan pregled oblasti sajber bezbjednosti. Pruža osnovni nivo znanja koji je odlična prva stepenica ka izgradnji karijere u ovoj oblasti. Naučićete i kako sami da usmjerite svoj karijerni put kroz ovu oblast.

Link: https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-for-beginners

3 "Cybrary IT: Introduction to IT & Cybersecurity"

Kurs daje osnovna znanja iz informacionih tehnologija i sajber bezbjednosti. Kompetence koje nudi kurs služe kao osnova za buduće profesionalce: administratora mreže, Incident Responder-a, administratora sistema, testera penetracije, inženjera u oblaku, menadžera za sajber bezbjednost i analitičara privatnosti.

Link: https://www.cybrary.it/course/introduction-to-it-and-cybersecurity

4 "UWashingtonX: Introduction to Cybersecurity"

Ovaj kurs prolazi kroz ključne termine i koncepte u oblasti sajber bezbjednosti, identifikaciju prijetnji, povezivanje odgovarajućih vrsta kontrola sa prijetnjama, interakcije među međunarodnim sajber-bezbjednosnih agencija i pravnim izazovima.

Link: https://www.preduzmi.rshttps://www.edx.org/learn/cybersecurity/university-of-washington-introduction-to-cybersecurity

5 "Heimdal Sigurnost: Cyber Security for Beginners"

Kurs za početnike u oblasti gdje ćete naučiti kako da podesite svoj bezbednosni sistem i steći uvid u osnovni rječnik sajber bezbednosti. Naučićete i da birate alate i akcije kako biste se zaštitili od virusa i prijetećih sadržaja, identifikujete ranjivosti Vašeg sistema. Stećićete vještine za bezbjedno pretraživanje web-a, zaštitu onlajn naloga i svih ličnih podataka.

Link: https://cybersecuritycourse.co/

6 "Great Learning: Introduction to Cyber Security"

Ovaj sveobuhvatni kurs pokriva teme od osnova sajber bezbjednosti, uključujući ključne koncepte i popularne napade, do naprednih tema kao što su kriptografija, bezbjednosni ciljevi i njihova implementacija, i projektovanje bezbjednosnih sistema. Takođe ćete naučiti o ranjivostima kao što je prelivanje bafera i učestvovati u studiji slučaja o napadu na WhatsApp u stvarnom svetu.

Link: https://www.mygreatlearning.com/academy/learn-for-free/courses/introduction-to-cyber-security

7 "RITx: Cybersecurity Fundamentals"

Kurs prolazi kroz osnove mrežne i sistemske administracije, osnove osiguranja informacija kao što su povjerljivost, integritet i dostupnost, kao i osnovne koncepte kriptografije.

Link: https://www.edx.org/learn/cybersecurity/rochester-institute-of-technology-cybersecurity-fundamentals

8 “IBM: Cybersecurity Basics”

Na kursu ćete naučiti osnovne pojmove iz sajber bezbjednosti, kako se testiranje penetracije koristi u sajber bezbjednosti, ulogu kriptografije u sajber bezbjednosti i kako se ona koristi. Pored toga kurs pokriva i teme kao što je svrha, funkcija i tipovi zaštitnih zidova, trijada CIA-e i šta se podrazumijeva pod poverljivošću, integritetom i dostupnošću, društveni inženjering i kako se koristi u phishing napadima i još mnogo toga.

Link: https://www.edx.org/learn/cybersecurity/ibm-cybersecurity-basics?index=product&queryID=a81d65dea384bf0322c7a19de7cb3c3a&position=1

Srednji nivo

Srednji nivo vještine u sajber bezbjednosti se odnosi na nivo stručnosti i znanja koji prevazilazi osnovne koncepte, ali još uvek ne dostiže napredne ili stručne nivoe. Obično uključuje vještine kao što su analiza mreže, otkrivanje prijetnji, razumijevanje uobičajenih sajber prijetnji, sprovođenje bezbjednosnih mjera i korišćenje alata za zaštitu sistema i podataka. Stručnjaci za sajber bezbjednost srednjeg nivoa su sposobni da otkriju, analiziraju i saniraju osnovne prijetnje u sajber bezbjednosti koristeći uobičajene alate otvorenog koda.

1 "REWIRE: CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE"

PKursevi u ponudi su: Cyber Incident Responder, Cyber Threat Intelligence Specialist, Penetration Tester i CISO.

Kursevi su obezbijeđeni u okviru REWIRE projekta, podržanog od strane evropske komisije, koji kao glavni cilj ima osmišljavanje predloga i održivih rješenja koja će dovesti do smanjenja razlike između potreba industrije i ponude obrazovnog sektora u pogledu kompetencija iz domena sajber bezbjednosti.

Link: https://vle.rewireproject.eu/

U okviru projekta razvijena je i CyberABILITY platforma, koja nudi pregled trenutnog tržišta rada, pregled karijernog puta u oblasti sajber bezbjednosti, vještina i kompetencija koje su potrebne profesionalcima zainteresovanim da grade karijeru u ovoj oblasti. Na ovoj platformi može se naći i lista dostupnih treninga i sertifikacija.

Link: https://cyberability-platform.informacni-bezpecnost.cz/

2 „OpenCourseWare: Computer Systems Security"

Kurs se tiče dizajna i implementacije sigurnih računarskih sistema. Tokom kursa biće obrađeni modeli prijetnji, napadi koji ugrožavaju bezbjednost i tehnike za postizanje bezbjednosti. Pored ovih tema biće riječi i o bezbjednosti operativnog sistema (OS), mogućnosti, kontroli toka informacija, jezičkoj bezbjednosti, mrežnim protokolima, bezbjednosti hardvera i bezbjednosti u web aplikacijama.

Link: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/

3 "OPEN SECURITY TRAINING.INFO"

Nudi otvoren repozitorijum prepun edukativnog sadržaja koji pokriva teme iz sajber bezbjednosti od početnog do naprednog nivoa. Teme koje su obrađene uključuju:

Početni nivo:

Android forenzika i bezbednosno testiranje, Tehnike hakovanja i otkrivanje upada, Analiza toka i traženje mreže, Uvod u celularnu bezbjednost, Uvod u mrežnu forenziku, Uvod u bezbjedno kodiranje, Uvod u procijenu ranjivosti, Ofanzivne, odbrambene i forenzičke tehnike za određivanje identiteta korisnika na web-u, Razumijevanje kriptologije: osnovni koncepti, Razumevanje kriptologije: kriptoanaliza…

Srednji nivo:

Uvod u softverske zloupotrebe (eksploatacije 1), Eksploatacija 2: Eksploatacija u Windows okruženju, Srednji Intel k86: arhitektura, sklapanje, aplikacije i aliteracija...

Napredni nivo:

Napredni k86: Virtuelizacija sa Intel VT-k, Napredni k86: Uvod u BIOS i SMM, Uvod u softwer obrnutog inženjeringa, Zlonamjerni softwer obrnutog inženjeringa...

Na kursu ćete naučiti osnovne pojmove iz sajber bezbjednosti, kako se testiranje penetracije koristi u sajber bezbjednosti, ulogu kriptografije u sajber bezbjednosti i kako se ona koristi, svrhu, funkciju i tipove zaštitnih zidova, trijadu CIA-e i šta se podrazumijeva pod poverljivošću, integritetom i dostupnošću, društveni inženjering i kako se koristi u phishing napadima i još mnogo toga.

Link: https://opensecuritytraining.info/Training.html

4 "Simplilearn: Introduction to CISSP (Certified information systems security professional)"

Kurs obuhvata osnove CISSP-a, od bezbjednosti informacija, upravljanja rizikom, zaštitu imovine itd. Ovaj kurs otvara puteve ka karijerama kao što su bezbjednosni analitičar, konsultant za bezbjednost, menadžer bezbjednosti ili glavni službenik za bezbjednost informacija (CISO).

Link: https://www.simplilearn.com/free-cissp-training-skillup

5 "Simplilearn: Introduction to Cloud Security"

Kurs o osnovama, najboljim praksama i dostupnim rješenjima za izazove računarstva u oblaku kako biste mogli da zaštitite važne informacije i resurse. Pokriveni su svi osnovni koncepti prijetnje i napada, rizika, privatnosti i rješenja kao i o kriptografskim primitivima (kriptografiju javnog ključa; digitalni potpisi; šeme šifriranja kao što su blok šifre i stream šifre; hash funkcije; i protokole za autentifikaciju kao što su Kerberos ili TLS/SSL).

Link: https://www.simplilearn.com/learn-cloud-security-basics-skillup

6 "Simplilearn: Introduction to Cybercrime"

Kurs o sajber kriminalu daje uvid u različite sajber napade sa kojima se organizacije suočavaju, od pretnji sajber bezbednosti do toga kako se ovi napadi sprečavaju.

Link: https://www.simplilearn.com/free-cybercrime-course-for-beginners-skillup

7 "UWashingtonX: Building a Cybersecurity Toolkit"

Kurs vas uči da identifikujte alate i vještine neophodne za formiranje današnjeg kompleta alata za profesionalnu sajber bezbjednost i uskladite odgovarajuće alate sa različitim svrhama u procesu upravljanja sajber bezbjednošću.

Link: https://www.edx.org/learn/cybersecurity/university-of-washington-building-a-cybersecurity-toolkit

8 "RITx: Cybersecurity Fundamentals"

CISA preko svoje virtuelne platforme za učenje (https://ics-training.inl.gov/learn) nudi više od 20 potpuno besplatnih kurseva koji se tiču industrijskih kontrolnih sistema i sajberbezbjednosnih praksi. Kursevi su različiti po formatu u zavisnosti od ličnih preferenci, da li želite sami da prelazite kroz gradivo ili uz instruktora. Teme koje su obuhvaćene a obrađuju se samostalno, uključuju: Operativna bezbjednost (OPSEC) za kontrolne sisteme, Razlike u primeni ICS-a, Uticaj uobičajenih IT komponenti na ICS, Uobičajene ICS komponente, Sajber bezbjednost unutar IT & ICS domena, Rizici u sajber bezbjednosti, Trenutni trendovi i pretnje, Trenutni trendovi i ranjivosti, Utvrđivanje uticaja incidenta u vezi sa sajber-bezbjednošću.

Link: https://www.cisa.gov/ics-training-available-through-cisa

9 "ALISON: Certified Information Systems Security Professional (CISSP 2019)"

Na kursu ćete savladati analizu sigurnosti sistema, upravljanje identitetom i pristupom, arhitekturu bezbjednosnog sistema, uticaj životnog ciklusa razvoja softvera na bezbjednost, kršenje bezbjednosti pomoću oporavka od katastrofe, bezbjednosnu reviziju kako interno tako i eksterno.

Link: https://alison.com/course/certified-information-systems-security-professional-cissp-2019

10 "ALISON: Computer Networking - Local Area Networks and the OSI Model"

Kurs je fokusiran na edukaciju- kako izgraditi LAN, kako konfigurisati različite uređaje, kako dizajnirati mrežu i kako riješiti probleme s mrežama. Teme koje se obrađuju su: Kako radi OSI model; Kako funkcionišu slojevi; Šta su mrežni protokoli; Koje su različite vrste mrežnih topologija; Koji se protokol koristi za komunikaciju između dva čvora; i Različite vrste mrežnih uređaja.

Link: https://alison.com/course/computer-networking-local-area-networks-and-the-osi-model-revised

11 "ALISON: Network Troubleshooting, Standards and Best Practices"

Na kursu ćete naučiti da sumirate kritične korake u procesu rješavanja problema, naučiti više o alatima za rješavanje problema, najčešće probleme sa mrežom sa kojima se suočava mrežni profesionalac, prepoznati glavne bezbjednosne prijetnje, naučiti da identifikujte moguće komplikacije pri rješavanju problema sa VAN-om, steči uvid u politike i procedure kritične za računarski sistem/mrežu organizacije

Link: https://alison.com/course/network-troubleshooting-standards-and-best-practices

12 "ALISON: CompTIA Security+ (Exam SYO-501)"

Tokom kursa ćete naučiti da opišite proces analize rizika, o identifikovanju bezbjednosnih pretnji, implementaciju bezbjednosti hosta i softvera, upravljanje identitetom i pristupom, napredne koncepte kriptografije, proces oporavka od katastrofe, izgradite plan kontinuiteta poslovanja.

Link: https://alison.com/course/comptia-security-exam-syo-501

13 "ALISON: Basics of Computer Networking"

Tokom kursa naučićete više o prednostima i komponentama računarske mreže, različitim konfiguracijama lokalne mreže, razliku između različitih topologija mreže, svojstva različitih slojeva OSI modela, različite alate koji se koriste u računarskom umrežavanju, internet protokole koji se koriste u umrežavanju, funkcije operativnih sistema, procedure uključene u konfigurisanje protokola za dinamičku konfiguraciju hosta (DCHP).

Link: https://alison.com/course/basics-of-computer-networking

14 "ALISON: Guide to Security for Linux Systems"

Kurs pokriva teme: Funkcije Oracle VirtualBox-a; Različite sistemske kartice u Linux CentOS 8; Proces stvaranja virtuelne mašine; Ulogu instalacionog programa anaconda u CentOS-u; Elemente koji čine Linux bezbjednost; Različite vrste narušavanja bezbjednosti; Koncept vlasništva nad Linux datotekama i dozvolama

Link: https://alison.com/course/guide-to-security-for-linux-systems

15 "ALISON: Ethical Hacking; Network Analysis and Vulnerability Scanning"

Na kursu ćete naučiti da kako se web aplikacije hakuju kroz testiranje penetracije, proces mrežnog skeniranja pomoću Nmap alata, koncept ranjivosti skriptovanja na više lokacija (KSSS), ulogu Network Mapper-a (Nmap) u etičkom hakovanju, osnovne karakteristike Nmap-a, najčešće korišćene Nmap komande, tehnike skeniranja portova u Nmap-u, značenje Nmap skripti i kako se koriste.

Link: https://alison.com/course/ethical-hacking-network-analysis-and-vulnerability-scanning

WEB 3.0

Web 3.0 ili Web3 je treća generacija World Wide Web-a (WWW), koja uključuje direktno uranjanje u digitalni svijet. Obuhvata individualnu kontrolu ličnih podataka i korišćenje kriptovaluta i blokčejna. Trenutno je u toku, razvijanje decentralizovanog i otvorenog veba sa većom korisnošću za svoje korisnike.

1 "Alchemy univerzitet"

Kurs: Osnove JavaScript-a

Kurs se sastoji od preko 50 lekcija formulisanih kroz 3 modula: Osnove kodiranja u JavaScript-u; Pravljenje, pretraga i manipulisanje strukturama podataka; Mreže i pisanje koda za komunikaciju unutar mreže. Kurs traje tri nedelje i pruža temelje za sticanje vještina neophodnih za razvoj blockchaina.

Link: https://www.alchemy.com/university/courses/js

Kurs: Ethereum Developer Bootcamp

Kurs se sastoji od preko 90 lekcija a nastavni plan i program uključuje interaktivne izazove kodiranja, video zapise, pisane vodiče i nedeljne projekte - kao i završni projekat koji se može podnijeti za zvaničnu sertifikaciju iz Alhemije. Kurs obrađuje teme: Učenje osnovne blokchain kriptografije; Blockchain bilansi i strukture podataka; Ethereum; Uvod u Solidity sintaksu i tipove podataka, itd.

Link: https://www.alchemy.com/university/courses/ethereum

Kurs: Learn Solidity

Naučićete Solidity sintaksu kao i najbolje prakse koristeći v0.8.20 i okruženje za kodiranje u pretraživaču. Tokom kursa ćete izgraditi pametne ugovore u stvarnom svijetu kao što su Voting Dapp ili Escrow ugovor.

Link: https://www.alchemy.com/university/courses/solidity

2 “CryptoZombies”

Svi kursevi na ovoj platformi su potpuno besplatni a nudi sve neophodne materijale za učenje o razvoju blockchaina. Kursevi su u najvećoj mjeri vezani za Ethereum i učenje Solydity od temelja. Iskustvo učenja je interaktivno, krećete od osnovnih znanja pa do naprednih nivoa.

Link: https://cryptozombies.io/

Dodatni edukativni resursi

1 "RITx: Computer Forensics"

Kurs obuhvata teme poput: Sudske prihvatljivosti dokaza za sajber napade tokom istražnih postupaka; forenzičke alate za sticanje, očuvanje i analizu slike Sistema; pregledanje forenzičkih izvještaja, karakteristike različitih Windows i Unix/Linux sistema datoteka i procesa oporavka datoteka.

Link: https://www.edx.org/learn/computer-forensics/rochester-institute-of-technology-computer-forensics?index=product&queryID=51787be79abc40fcdf6a4ec25112e541&position=7

2 "UWashingtonX: Building a Cybersecurity Toolkit"

Kurs se tiče identifikacije koji alati i vještine su neophodni za formiranje današnjeg kompleta alata za profesionalnu sajber bezbednost;

Uskladite odgovarajuće alate sa različitim svrhama u procesu upravljanja sajber bezbjednošću;

Sintetizujte uvide stečene tokom istraživanja skupova vještina, radeći na samovrednovanju talenata i interesovanja usklađenih sa nizom uloga u sajber bezbjednosti

Link: https://www.edx.org/learn/cybersecurity/university-of-washington-building-a-cybersecurity-toolkit?index=product&queryID=af9ecdff7e0f04fe259d15ead61a13ec&position=6

3 "GIT Hub: Cybersecurity Educational Resources"

Ova lista zbog svoje temeljnosti naziva se i Univerzitet sajber bezbjednosti a sastavljena je od besplatnih obrazovnih resursa koji se fokusiraju na učenje kroz rad.

Podijeljena je u 6 dijelova, raspoređenih od osnovnih do naprednih nivoa: Introduction and Pre-security, Free Beginner Red Team Path, Free Beginner Blue Team Path, Bonus practices/latest CVEs and Extremely Hard rooms.

Linkovi: https://github.com/CSIRT-MU/edu-resources; https://github.com/brootware/awesome-cyber-security-university

5 "TryHackMe: edukativna platforma"

TryHackMe sadrži i besplatan i plaćen sadržaj za sve nivoe profesionalaca u sajber bezbjednosti i pokriva širok spektar tema, od obuka za ofanzivnu i defanzivnu bezbjednost pa do vježbi Capture the Flag. Platforma, takođe, ima module o Linuxu, bezbjednosti mreže, web hakovanju i osnovama Windowsa, kao i kurseve o kriptografiji i osnovnoj eksploataciji računara.

Link: https://tryhackme.com/r/hacktivities

6 "Hack The Box"

Hack The Box je proctor koji nudi uživo obuku za hakere, a usmjeren je ka ofanzivnoj bezbednosti. Sajt uključuje i plaćene i besplatne nivoe koji uključuju namjerno ranjive platforme koje naglašavaju i ilustruju ranjivosti, eksploatacije i obrasce napada.

Link: https://academy.hackthebox.com/#pills-skill-paths-tab

7 "Bugcrowd University"

Univerzitet Bugcrowd je edukativni resurs koji sadrži materijale za poboljšanje vještina istraživača sajber bezbjednosti. Uključuje sadržaj koji se odnosi na najkritičnije i najrašireniје greške i njihovo tretiranje. Svaki modul ima slajdove, video zapise i laboratorije za istraživače da ovladaju vještinom lova na greške sa ciljem stvaranja novog standarda za obuku za testiranje bezbjednosti.

Link: https://bugcrowd.com/engagements

8 "Federal Virtual Training Environment"

Federalno virtuelno okruženje za obuku (FedVTE) nudi više od 800 sati obuke iz raznih oblasti sajber bezbednosti. FedVTE, pokriva teme od etičkog hakovanje i nadzora, upravljanje rizikom do analize malvera. Nivelacija kursa se kreće od početnih do naprednih nivoa. Nekoliko kurseva je usklađeno sa različitim IT sertifikatima, kao što su CompTIA Network+ i Security+ i Certified Information Sistems Security Professional.

Link: https://fedvte.usalearning.gov/public_fedvte.php

ULYSSEUS INNOVATION ECOSYSTEM

Ulysseus
EUROPEAN UNIVERSITY

Universidad de Sevilla
Université Côte d'Azur
Università di Genova
Technical University of Košice
MCI The Entrepreneurial School
Haaga-Helia University of Applied Sciences
Universität Münster
UCG Univerzitet Crne Gore

https://ulysseus.eu/;
https://www.ucg.ac.me/rektorat/ulysseus;
https://www.ucg.ac.me/rektorat/ucsh

ulysseus@ucg.ac.me