**Plani i leksionit**

**Leksioni** 1.1.4 Identifikimi i të dyshuarve në Internet

|  |  |  |
| --- | --- | --- |
| Leksioni 1.1.4 Identifikimi i të dyshuarve në Internet | | Kohëzgjatja: 1 orë |
| **Burimet që kërkohen:**   * Laptop apo PC me program Windows 7, 8 apo 10 dhe me Microsoft Office 2010 apo më të ri. * Projektor dhe ekran. * Dërrasë e bardhë, tabakë letre apo teknika të tjera për regjistrimin e kontributeve të pjesëmarrësve. * Këto burime nevojiten vetëm nëse trajneri përdor prezantim në PowerPoint. | | |
| **Qëllimet e sesionit:**  T’u japë pjesëmarrësve informacion për marrëdhënien midis aktivitetit online të një individi dhe identitetit të tij të vërtetë në botën reale dhe disa nga sfidat e lidhura me krijimin e kësaj lidhjeje. | | |
| **Objektivat:**  Në fund të leksionit**,** pjesëmarrësit do të jenë në gjendje të:   * Shpjegojnë terminologjinë e rëndësishme të Internetit. * Përshkruajnë se çfarë është një adresë IP. * Përshkruajnë se si mund të gjejnë një adresë IP të një të dyshuari. * Përshkruajnë se si mund të lidhin një adresë IP të një të dyshuari me një person real. * Listojnë tre sfida teknike për identifikimin e një të dyshuari në Internet. | | |
| **Udhëzime për trajnerin**  Ky sesion ofron informacion për identifikimin e të dyshuarve online dhe lidhjen e aktivitetit të një individi online me identitetin e tij në botën reale, si edhe përshkruan disa nga sfidat e krijimit të asaj lidhjeje.  I gjithë informacioni për këtë sesion përfshihet në prezantimin në PowerPoint titulluar “Sesioni 1.1.4 – Identifikimi i të dyshuarve në Internet” të paketës me burime. Trajneri është përgjegjës për të siguruar që materialet të jenë të përditësuara. Ndryshime mund bëhen, megjithatë, objektivat duhen realizuar. | | |
| **Përmbajtja e leksionit** | | |
| **Numrat e diapozitivave** | **Përmbajtja** | |
| Diapozitivat 2-4 | Trajneri duhet të rifreskojë konceptin e adresës IP. Pikat e spikatura që lidhen sidomos me këtë leksion përmblidhen në këto diapozitiva. | |
| Diapozitivi 6 | Kjo pjesë e kursit shpjegon se si mund të jetë e mundur të lidhet një adresë IP me aktivitete të dyshimta online. Ky është një komponent i nevojshëm i një hetimi me bazë internetin. | |
| Diapozitivi 7 | Trajneri duhet të shpjegojë se serverët e uebit zakonisht mbajnë të dhëna për të gjitha kërkesat hyrëse.  Trajneri gjithashtu duhet të shpjegojë se ky është një opsion konfigurimi në një server të uebit dhe një njeri që administron një server të tillë mund ta mbyllë hyrjen në të me qëllim për të fshehur aktivitetin e njerëzve që përdorin serverin e uebit. Kjo mund të bëjë që asnjë hyrje në internet për aktivitete kërkimi në të të mos ruhet. | |
| Diapozitivi 8 | Trajneri duhet të shpjegojë se ky është një shembull i një regjistri të serverit të uebit. Trajneri duhet t’i referohet regjistrimit të theksuar në regjistër dhe të vërë në dukje:   1. Adresën IP të burimit – 216.128.130.126 2. Kohën/datën e kërkesës HTTP – 23/shtator/2006:21:30:02 -0400 – Trajneri duhet të vërë në dukje zonën kohore, në këtë rast GMT-4. 3. Gjënë që kërkohet “/pgp/” – kjo njihet si burimi dhe ka kuptim në kontekstin e serverit që trajton kërkesën. Mund të jetë për shembull, një dokument i serverit, një dosje në server apo një imazh. 4. Faqja ku ka qenë përdoruesi kur ka klikuar në linkun që çoi në këtë kërkesë. Kjo njihet si referuesi. Në këtë rast, është një varg i gjatë që fillon me dir.yahoo.com. Nga kjo mund të mësojmë se përdoruesi ka qenë duke parë këtë faqe, ka klikuar në një link që e ka çuar në këtë server, i cili mori kërkesën për një burim të quajtur “/pgp/”.   Vargu identifikues i kërkuesit (që fillon me Mozilla/4.0), jepet nga programi kërkues i kompjuterit të klientit, ndonëse ai mund të falsifikohet/ndryshohet. | |
| Diapozitivi 9 | Trajneri duhet të shpjegojë se ndryshe nga kërkimi në ueb, dërguesi dhe marrësi i një emaili nuk ndërveprojnë drejtpërdrejt. | |
| Diapozitivi 11 | Trajneri duhet të shpjegojë se SMTP-ja (protokolli i thjeshtë i transferimit të postës elektronike – email) është procesi me anë të të cilit një email dërgohet dhe i përcillet një tjetri, POP-i (Protokolli i Zyrës Postare) apo ndryshe IMAP, që është procesi me anë të të cilit emaili kontrollohet/merret.  Trajneri duhet të flasë përmes procesit të dërgimit të një emaili me anë të një serveri të postës dalëse dhe një serveri të postës hyrëse.  Trajneri duhet të shpjegojë që në rastin e një emaili me bazë uebin (për shembull, gmail) përdoruesi, në vend të përdorimit të POP3 për t’u ndërfaqur me serverin e postës hyrëse, hyn në një server në ueb dhe e lexon emailin drejtpërdrejt në serverin e postës hyrëse. | |
| Diapozitivi 13 | Trajneri duhet të shpjegojë se, edhe pse pjesëmarrësit mund të mos e njohin emailin në këtë format, çdo email që ata kanë lexuar, ka tituj të tillë.  Trajneri duhet të nënvizojë në veçanti:   1. Titujt e marrë, të cilët tregojnë adresat e IP-së që kanë përpunuar këtë email. 2. Adresat e dërguesit dhe të marrësit (to dhe from). 3. Subjektin. 4. Datën.   Trajneri duhet të vërë në dukje se është e mundur që një pjesë e këtij informacioni të falsifikohet nëse dikush orvatet të fshehë burimin e emailit dhe si rrjedhojë analiza e titullit kërkon një farë aftësie teknike për ta interpretuar me korrektesë. | |
| Diapozitivi 14 | Trajneri duhet t’u kërkojë pjesëmarrësve të mendojnë për shërbimet e tjera që mund të kenë adresa IP.  Trajneri duhet të simulojë diskutime me shembuj të tillë si Skype, Pokemon Go, DropBox, Facebook, Google, Microsoft dhe të tjerë. | |
| Diapozitivi 15 | Kjo pjesë e kursit shpjegon se si mund të jetë e mundur të lidhet një adresë IP me një aktivitet të dyshimtë online. Ky është një komponent i nevojshëm i një hetimi me bazë internetin. | |
| Diapozitivi 16 | Trajneri duhet t’ u kujtojë pjesëmarrësve se Interneti është shumë më kompleks se sa mund të na shkojë ndërmend të mësojmë në një kurs të tillë të shkurtër prezantues si ky. Trajneri duhet t’i paralajmërojë të pranishmit se nuk ka një përkim të thjeshtë një me një, midis çdo personi në botë dhe një adrese IP në Internet. Ka shumë arsye përse një adresë IP nuk identifikon pa tjetër një individ të caktuar (është një informacion i nevojshëm por jo i mjaftueshëm).  Duhen diskutuar dy shembuj konkretë:   1. Adresa IP Statike përkundrejt asaj Dinamike – Trajneri duhet t’u kërkojë pjesëmarrësve të shqyrtojnë rastin e lidhjes së tyre të internetit në shtëpi. Ka shumë të ngjarë se ata përdorin ose një ofrues interneti kabllor ose një ofrues DSL. Në të dy rastet, trajneri duhet t’u shpjegojë se ofruesi i shërbimit të internetit mund ta ndërrojë, dhe me shumë gjasa, do ta ndërrojë, periodikisht adresën e tij IP. Kjo do të thotë se është me rëndësi jo vetëm të dihet adresa IP që përdoret, por edhe KUR është përdorur kjo adresë IP, për të qenë në gjendje të identifikohet një abonent i caktuar. Një gjë e ngjashme mund të ndodhë brenda organizatave – çdo herë që ristartohet një kompjuter ai mund të japë një adresë të ndryshme IP. 2. Përkthimi i adresës së rrjetit – Trajneri duhet të shpjegojë se pavarësisht faktit që ka 4 miliardë adresa të disponueshme IP, ato nuk i caktohen njerëzve një nga një, por ato caktohen në grupe. Kur një grup i caktohet një organizate, asnjë organizatë tjetër nuk mund të përdorë ndonjë nga adresat IP të atij grupi. Trajneri duhet të shpjegojë se kjo shpie në caktime jo shumë efikase të adresave IP dhe si rrjedhojë, ka një problem me mbarimin e adresave të disponueshme IP. Trajneri duhet të shpjegojë se kjo, ndër arsye të tjera, ka çuar në nevojën e versionit të rishikuar të IP-së, duke përfshirë adresa më të gjata (versioni 6 i IP-së). Trajneri duhet të shpjegojë se ka disa grupe të caktuara të adresave IP që nuk lejohen të përdoren në Internet. Me fjalë të tjera, ato nuk do të përcillen nga infrastruktura e përbashkët e rrjetit. Trajneri mund të japë shembuj të një adrese IP që fillon me 10, ose një adresë IP që fillon me “192.168”. Trajneri duhet të shpjegojë se këto adresa IP mund të përdoren më së miri në një rrjet lokal, por jo në Internet. Trajneri duhet të shpjegojë se këto adresa IP përdoren me qëllim për të përdorur në mënyrë më efikase adresat e disponueshme IP, në mënyrën e mëposhtme:    1. Brenda një organizate, ku çdo kompjuteri i jepet një adresë IP që nuk mund të përdoret në Internet.    2. Organizatës i caktohet një numër i vogël adresash IP, mbase vetëm një.    3. Sa herë që një PC do të komunikojë me një kompjuter tjetër në Internet, infrastruktura e organizatës (në veçanti rauteri i hyrjes në Internet (gateway router)) zëvendëson IP-në e vërtetë të internetit, me adresën e brendshme IP përpara se ta përcjellë trafikun në Internet.    4. Kjo bën të mundur që një numër i madh kompjuterësh të kenë një adresë të vetme IP për të komunikuar me internetin, dhe kjo teknikë njihet me emrin Përkthimi i Adresës së Rrjetit (NAT).   Si rezultat i përdorimit të kësaj teknike, të gjithë kompjuterët PC në një organizatë duken për pjesën tjetër të Internetit sikur janë një kompjuter i vetëm me një adresë të vetme IP. Nëse kjo adresë IP identifikohet si pjesë e një hetimi, vetëm organizata mund të jetë në gjendje të përcaktojë se cili nga kompjuterët e brendshëm e ka shkaktuar trafikun në fjalë. | |
| Diapozitivi 17 | Trajneri duhet të shpjegojë se IP-ja është një nga burimet kyç për të marrë informacion rreth identitetit të abonentit. Procesi për kërkimin e një informacioni të tillë nga një Ofrues i Shërbimit të Internetit do të varet nga legjislacioni i brendshëm, ndonëse zakonisht kërkohet një formë e caktuar urdhri nga prokuroria apo gjykata. Periudha kohore për të cilën ISP-të kërkohet të ruajnë informacionin është gjithashtu një çështje që varet nga legjislacioni i vendit. Një periudhë prej 2 vitesh është e zakonshme në kohën e shkrimit.  Në këtë drejtim pronësia nga ISP-ja e adresës IP në fjalë është një burim i rëndësishëm: https://www.whoismyisp.org/.  Trajneri duhet të vërë në dukje se ISP-ja mund të mos jetë një ISP kombëtare në vendin tuaj dhe si rrjedhojë mund të ketë nevojë për ndihmë të ndërsjellë ligjore për të pasur qasje në një informacion të tillë. | |
| Diapozitivi 18 | Trajneri duhet të vërë në dukje se ofruesit e shërbimeve shumëkombëshe zakonisht i mbajnë të dhënat e adresave IP, për shembull nga ku është futur në internet një llogari e caktuar. Trajneri duhet të shpjegojë se në rastet kur keni dijeni për një të dyshuar, për shembull, një llogari në Facebook, mund të jetë e mundur që një adresë IP të lidhet me aktivitetin e kësaj llogarie nga Facebook.  Bashkëpunimi ndërkombëtar, përfshirë bashkëpunimin me ISP shumëkombëshe, mbulohet diku tjetër në këtë kurs me më shumë hollësi. | |
| Diapozitivi 19 | Trajneri duhet të përshkruajë skenarin kur një hetim vë në dukje në adresë IP në pronësi të një shoqërie. Trajneri duhet të tregojë se në shumë raste shoqëritë tregtare përdorin NAT-in për të ndarë një adresë të vetme IP midis të gjithë kompjuterëve të brendshëm. Në këto raste, vetëm shoqëria është në gjendje të lidhë përdorimin e adresës konkrete IP me një kompjuter të caktuar të brendshëm. Prandaj kërkohet bashkëpunimi me kompaninë për të ndihmuar me hetimin.  Mënyra se si do të zhvillohet një bashkëpunim i tillë varet nga legjislacioni i vendit.  Trajneri duhet të shpjegojë se një situatë e tillë mund të ndërlikohet nga fakti se, edhe pse të dhënat mund të ekzistojnë, ato nuk gjenden brenda vendit. Nëse për shembull, një kompani është pjesë e një organizate shumëkombëshe, ajo mund të mos kontrollojë apo operojë infrastrukturën e saj. Në një rast si ky, nëse ekzistojnë të dhëna, ato mund të ndodhen në një juridiksion tjetër. Fakti nëse një kompani në vendin tuaj është në gjendje të japë të dhëna varet nga struktura organizative dhe teknike e saj. | |
| Diapozitivi 21 | Trajneri duhet të shpjegojë që kriminelët mund të përpiqen t’i bëjnë të palexueshme qëllimisht adresat e tyre IP, duke e bërë praktikisht të pamundur identifikimin e këtyre adresave IP.  Trajneri duhet gjithashtu të shpjegojë se disa teknologji të caktuara, përmes përdorimit dhe shfrytëzimit normal, mund ta bëjnë praktikisht të pamundur identifikimin e adresës IP të një të dyshuari. | |
| Diapozitivi 22 | Trajneri duhet të shpjegojë se ekzistojnë shërbimet specifike online për të fshehur burimin e kërkimit dhe aktivitetin e Internetit. Trajneri duhet të tregojë shembuj faqesh në ueb në diapozitivin tjetër.  Trajneri duhet të vërë në dukje se ka shërbime të ngjashme për t’i bërë anonime burimet e emaileve.  Trajneri duhet të shpjegojë se shërbime të tjera të tilla si TOR, rauteri qepë (onion router),mund të përdoren për të fshehur të dhënat për burimin e IP-së. | |
| Diapozitivi 24 | Trajneri duhet të shpjegojë se Carrier grade NAT është një problem serioz për identifikimin e një të dyshuari të lidhur me një adresë të caktuar IP. Problemi është se një informacion i dytë, i njohur si numri i portës (port number), kërkohet për të lidhur në mënyrë të qartë një përdorues të caktuar me adresën IP. Në shumë raste, numri i portës nuk ruhet në të dhënat e pajisjes. Trajneri duhet t’i kthehet përsëri regjistrave të serverit të uebit dhe titujve të emailave dhe të vërë në dukje se asnjë informacion për numrin e portës nuk gjendet në asnjërin prej këtyre dy burimeve  Shënim i trajnerit: Shih https://en.wikipedia.org/wiki/Carrier-grade\_NAT, për informacion të mëtejshëm formues. | |
| **Ushtrime praktike**  Nuk janë parashikuar ushtrime praktike për këtë leksion. | | |
| **Vlerësimi/kontrolli i njohurive**  Nuk është kërkuar ndonjë kontroll apo vlerësim për njohuritë e marra në këtë sesion. | | |