**План на часот**

Лекција 1.1.4 Идентификување на осомничени на интернет

|  |  |  |
| --- | --- | --- |
| Лекција 1.1.4 Идентификување на осомничени на интернет | | Траење: 1 час |
| **Потребни ресурси:**   * Лаптоп или персонален компјутер со инсталиран Windows 7, 8 или 10 и со Microsoft Office 2010 или понов * Проектор и платно за проектирање * Бела табла, флип-чарт табла или други техники за евидентирање на инпутите на учесниците * Овие ресурси се потребни само ако инструкторот користи презентација PowerPoint | | |
| **Цел на сесијата:**  Да се информираат делегатите за односот меѓу онлајн-активноста на поединецот и неговиот идентитет во реалниот свет и некои предизвици поврзани со создавањето на таа врска. | | |
| **Потесни цели:**  На крајот на оваа сесија учесниците ќе бидат во можност да:   * Ја објаснат значајната интернет-терминологија * Опишат што е IP-адреса * Опишат како може да се најде сомнителна IP-адреса. * Опишат како може да се поврзе сомнителна IP-адреса со вистинско лице * Наведат три технички предизвици за идентификација на осомничени лица на интернет. | | |
| **Насоки за инструкторот**  Оваа сесија нуди информации за идентификација на сомнителните лицеа онлајн и поврзувањето на онлајн-активноста на лице со неговиот идентитет во реалниот свет, како и опишување на некои предизвици при создавањето на таа врска.  Сите информации за оваа сесија се вклучени во презентацијата PowerPoint насловена „Сесија 1.1.4 – Идентификување на осомничени на интернет“ во пакетот со ресурси. Инструкторот е одговорен да обезбеди материјалите да бидат ажурирани. Измени може да се прават; меѓутоа, треба да се постигнат целите. | | |
| **Содржина на часот** | | |
| **Броеви на слајдови** | **Содржина** | |
| Слајдови од 2 до 4 | Инструкторот треба да го повтори концептот IP-адреса. На овие слајдови се особено дадени истакнатите точки што се релевантни за оваа лекција. | |
| Слајд 6 | Во овој дел од курсот се објаснува како може да се поврзе IP-адреса со одредена сомнителна онлајн-активност. Тоа е неопходна компонента на истрага заснована на интернетот. | |
| Слајд 7 | Инструкторот треба да објасни дека веб-серверите обично водат евиденција за сите дојдовни барања.  Меѓутоа, инструкторот треба да објасни и дека ова претставува опција за конфигурација во веб-серверот и лицето што управува со веб-серверот може да го исклучи логингот, а особено може тоа да го направи ако се обидува да скрие активност на лицата што го користат веб-серверот. Тоа ќе значи дека нема да бидат зачувани дневници/записници од активноста на пребарувањето низ мрежата. | |
| Слајд 8 | Инструкторот треба да објасни дека ова претставува пример на дневник на веб-сервер. Инструкторот треба да упати да нагласените податоци во дневникот и да укаже:   1. IP-адреса на изворот – 216.128.130.126 2. Време/датум на HTTP-барањето – 23/Sep/2006:21:30:02 -0400 – Инструкторот треба да укаже на временската зона, во овој случај GMT-4. 3. Работата што била побарана “/pgp/” – ова е познато како ресурс и ќе има значење во контекст на серверот што го обработува барањето. Тоа може да биде документ на серверот, папка на серверот или слика, на пример. 4. Страница на која што бил корисникот кога кликнал на линкот што довел до барањето. Ова е познато како реферер. Во овој случај долгиот стринг што почнува со dir.yahoo.com. Од ова може да кажеме дека корисникот ја разгледувал оваа страница, кликнал на линк што го одвел на овој сервер примајќи барање за ресурс по име “/pgp/”.   Стринг за идентификација на пребарувачот (старување на Mozilla/4.0), кој е обезбеден од пребарувачкиот софтвер на персоналниот компјутер на клиентот, иако ова може да се лажира/смени. | |
| Слајд 9 | Инструкторот треба да објасни дека за разлика од веб-пребарувањето, праќачот и примателот на е-пошта немаат директна интеракција. | |
| Слајд 11 | Инструкторот треба да објасни дека SMTP (Едноставен протокол за пренос на пошта - Simple Mail Transfer Protocol) е процес со кој е-пошта се праќа и проследува, а POP (Post Office Protocol) или алтернативно IMAP е процес со кој се прегледува/прима е-пошта.  Инструкторот треба да зборува во текот на процесот на испорака на е-пошта преку излезен меил-сервер и дојдовен меил-сервер.  Инструкторот треба да објасни дека во случај на е-пошта заснована на веб (g-mail) наместо да користи POP3 за да оствари интеракција со дојдовниот меил-сервер, корисникот се пријавува на веб-серверот и ја чита е-поштата директно на дојдовниот меил-сервер. | |
| Слајд 13 | Инструкторот треба да објасни дека, иако учесниците можеби не ја препознаваат е-поштата во овој формат, секоја е-порака што некогаш е прочитана има хедери (заглавија) како овие.  Инструкторот треба особено да нагласи   1. Примените заглавија, кои ги покажуваат IP-адресите што ја обработиле оваа е-порака 2. Адреси на е-пошта од и до 3. Предмет 4. Датум   Инструкторот треба да укаже дека е можно некои од овие информации да бидат лажни ако некој се обидува да го скрие изворот на е-пошта и според тоа, за анализа на заглавието на е-пошта ќе биде потребна вештина за правилно толкување. | |
| Слајд 14 | Инструкторот треба да побара од учесниците да размислат за други услуги што може да имаат IP-адреси.  Инструкторот треба да поттикне дискусија со примери, како што се Skype, Pokemon Go, DropBox, Facebook, Google, Microsoft. Итн. | |
| Слајд 15 | Во овој дел од курсот се објаснува како може да се поврзе IP-адреса со одредена сомнителна онлајн-активност. Тоа е неопходна компонента на истрага заснована на интернетот. | |
| Слајд 16 | Инструкторот треба да ги потсети учесниците дека интернетот е многу посложен отколку што ние може да се надеваме да опфатиме со краток вовед како овој. Инструкторот треба да ги предупреди учесниците дека не постои едноставно мапирање „еден на еден“ меѓу кое било лице во светот и IP-адреси на интернет. Има многу приочини зошто една IP-адреса задолжително не идентификува едно лице (тоа е неопходна но не доволна информација)  Треба да се дискутира за два специфични примера:   1. Статички наспроти динамички IP-адреси – инструкторот треба да побара од учесниците да размислат за нивната интерна поврзаност дома. Најверојатно тие користат кабелски интернет-провајдер или DSL-провајдер. Во двата случаја, инструкторот треба да објасни дека провајдерот на интернет-услуги би можел да ја смени, и најверојатно периодично ќе ја менува, својата IP-адреса. Ова значи дека е важно не само да се знае која IP-адреса била употребена, туку и КОГА таа била употребена за да може да се идентификува определен претплатник. Слично може да се случи во рамките на организациите – секогаш кога повторно ќе се активира персонален компјутер, тој може да добие различна IP-адреса. 2. Преведување на мрежна адреса (Network address translation) – Инструкторот треба да објасни дека наспроти фактот дека има 4 милиони достапни IP-адресм тие не се алоцраат една по една, туку се алоцирани во групи. Една група е алоцирана на организација, и ниедна друга организација не може да користи која било IP-адреса во таа група. Инструкторот треба да објасни дека ова води до неефикасна алокација на IP-адреси и според тоа, постои проблем дека достапните IP-адреси може да се исцрпат. Инструкторот треба да објасни дека ова, меѓу другите причини, довело до потребата за ревидирана верзија на IP со вклучување подолги адреси (IP version 6). Инструкторот треба да објасни дека има одредени групи IP-адреси за кои не е дозволено да се користат на интернет. Со други зборови, тие нема да бидат проследени од споделената мрежна инфраструктура. Инструкторот може да даде примери на IP-адреса што почнува со 10, или на која било IP-адреса што почнува со „192.168“. Инструкторот треба да објасни дека овие IP-адреси може да се користат совршено добро на локална мрежа, но не и на интернет. Инструкторот треба да објасни дека овие IP-адреси се користат за поефикасно да се искорисат достапните IP-адреси на следниов начин:    1. Во рамките на организацијата, на секој персонален компјутер му се дава IP-адреса што не може да се користи на интернет.    2. Организацијата има мал број, можеби само една вистинска IP-адреса што и е доделена.    3. Секогаш кога персонален компјутер сака да комуницира со друг компјутер на интернет, инфраструктурата на организацијата (интернет порт-рутер особено) ја заменува вистинската интернет IP-адреса за интерна IP-адреса по што го проследува сообраќајот надвор од интернет.    4. Ова овозможува голем број персонални компјутери да споделат една IP-адреса за комуницирање на интернет а оваа техника е позната како преведување на мрежна адреса Network Address Translation (NAT).   Меѓутоа, суштината на користењето на оваа техника е дека сите персонални компјутери во рамките на организацијата на преостанатиот дел од интернетот му изгледаат како да се еден компјутер со една IP-адреса. Ако IP-адресата се идентификува како дел од истрагата, тоа е самата организација, која е во позиција да утврди кој интерен персонален компјутер го генерирал предметниот сообраќај. | |
| Слајд 17 | Инструкторот треба да објасни дека IP е еден од клучните извори на информации за идентитетот на претплатникот. Процесот за барање такви информации од провајдерот на интернет-услуги ќе зависи од националното законодавство, иако обично се бара определена форма на налог од обвинителството или од судот. Временскиот период во кој се бара од ISP да ја зачува евиденцијата, исто така, претставува прашање на националното законодавство, Период од две години е вообичаен во времето на пишувањето.  Кој ISP ја поседува предметната ISP-адреса: https://www.whoismyisp.org/ е корисен ресурс во однос на ова.  Инструкторот треба да укаже дека ISP не мора да биде национален ISP во вашата земја и според тоа може да биде потребна меѓусебна помош за да се добие пристап до овие информации. | |
| Слајд 18 | Инструкторот треба да укаже дека мултинационалните провајдери на услуги, обично, водат евиденција, на пример, за IP-адресата од која некој се најавил на определен налог. Инструкторот треба да објасни дека во случаи кога вие сте свесни за сомнителен, на пример, Facebook налог, може да биде можно да се најде адреса поврзана со актвноста на овој налог од Facebook.  Меѓународната соработка, вклучувајќи и соработка со мултинационални ISP подетално е опфатена на друго место на овој курс. | |
| Слајд 19 | Инструкторот треба да опише сценарио каде истрагата укажува на IP-адреса во сопственост на една компанија. Инструкторот треба да укаже дека во голем борј случаи компаниите користат NAT за споделување на една IP-адреса меѓу сите интерни компјутери. Во овие случаи само компанијата е во позиција да го поврзе користењето на определена IP-адреса со посебен интерен персонален компјутер. Според тоа, ќе биде потребен ангажман со компанијата за да помогне во истрагата.  Како се одвива оваа активност со компанијата ќе зависи од националното законодавство.  Инструкторот треба да објасни дека оваа ситуација може да се искомплицира со фактот дека, дури иако можеби постои евиденција, таа можеби не постои во вашата земја. Ако, на пример, компанијата е дел од мултинационална организација, таа можеби нема да ја контролира или да управува со сопствената инфраструктура. Во таков случај, ако постои евиденција, таа може да биде во друга јурисдикција. Дали компанијата во вашата земја е во позиција да ја обезбеди документацијата ќе зависи од организациската и од техничката структура. | |
| Слајд 21 | Инструкторот треба да објасни дека криминалците може да се обидат на меѓународно ниво да ја скријат својата IP-адреса, правејќи речиси невозможно да се идентификува нејзината IP адреса/.  Инструкторот, исто така, треба да објасни дека одредени технологии низ нивната нормална употреба и работа, исто така, би можеле речиси да оневозможат да се идентификува сомнителна IP-адреса. | |
| Слајд 22 | Инструкторот треба да објасни дека услугите постојат онлајн посебно за да се скрие изворот на пребаривањето и интернет-активноста. Инструкторот треба да покаже пример на веб-страницата на следниот слајд.  Инструкторот треба да укаже дека слични услуги се достапни за да се анонимизира изворот на е-пошта.  Инструкторот треба да објасни дека другите услуги, како што се TOR, onion router, може да се користат за да се скрие изворот на IP-податоци. | |
| Слајд 24 | Инструкторот треба да објасни дека NAT од класа Carrier претставува сериозен проблем за идентификување на оснмничен поврзан со определена IP-адреса. Проблемот е во тоа дека е потребна втора информација, позната како број на порт, за да може недвосмислено да се поврзе определен корисник со IP-адресата. Во многу случаи, бројот на порт не е складиран во евиденцијата за услугите. Инструкторот треба да се наврати на заглавијата на е-пошта и на дневницте на веб-серверот и да укаже дека во ниеден од овие извори не се присутни информации за бројот на порт.  Забелешка за инструкторот: Видете https://en.wikipedia.org/wiki/Carrier-grade\_NAT for useful background information. | |
| **Практични вежби**  За оваа лекција не се предвидени практични вежби. | | |
| **Оценување/Проверка на знаењето**  За оваа лекција не се подготвени никакви проверки на знаење или оценување. | | |