Ekaia, 2021, 39, 313-326
https://doi.org/10.1387/ekaia.21939

ekaia
ZIENTZIA eta TEKNOLOGIA ALDIZKARIA

ISSN 0214-9001 – eISSN 2444-3255

Zibererasoetatik babesteko, *hacking* etikoaren balioa

(The importance of ethical hacking to protect ourselves from cyber-attacks)

Ainhoa Etxeberria, Iñaki Goirizelaia, Juan Jose Unzilla, Jasone Astorga, Maider Huarte*

Bilboko Ingeniaritza Eskola (Universidad del País Vasco/ Euskal Herriko Unibertsitatea)

LABURPENA: 2020an, teknologiak bultzatutako gizarte batean bizi gara, eta datuak komunikatzeko sistemak funtsezkoak bihurtu dira gure eguneroko bizitzaren alderdi guztietan. Covid19-k erakutsi digu ezagutzen ez dugunak eszenatoki eta bizimodu berrietara eraman gaitzakeela, duela hilabete batzuk imajinatu ere ezin genituen lekuetara. Gaur egun, pertsonen, enpresen eta erakundeen arteko harremanak inoiz baino gehiago oinarritzen dira telekomunikazio-sareetan, eta, beraz, zibersegurtasun sofistikatuaren beharra oso garrantzitsua bihurtzen ari da gero eta handiagoak diren zibererasoetatik babesteko. Enpresak eta erakundeak diru kopuru handiak inbertitzen ari dira beren segurtasun zibernetikoan. Egoera horretan, *hacking* etikoa ohiko tresna bihurtu da behar den segurtasun-maila zehazteko. *Hacking* etikoaren helburua da sare informatikoetan ahuleziak eta kalteberatasunak aurkitzea, hackerrek sareetan sartzeko eta softwarearen ahuleziak azaltzeko erabiltzen dituzten ezagutza eta tresna berberak erabiliz. Dibulgazio-artikulu honek *hacking* etikoa zer den, zer onura dituen eta zergatik den beharrezkoa azaltzen du. *Hacking* etikoari buruzko artearen egoera bat aurkezten du, eta erakusten du enpresek eta erakundeek nola inplementa lezaketen *hacking* etikoa, sarbide-testetan (Penetration Testing Execution Standard, PTES) oinarritutako metodologia erabiliz.

HITZ GAKOAK: *hacking* etikoa, *pentesting*, sarbide-testa, zibersegurtasuna.

ABSTRACT: *In 2020, we are living in a technology driven society where data communication systems have become essential in all aspects of our daily life. Covid19 has shown us that the unknown can take us to new scenarios and ways of life that we could not even imagine months ago. Nowadays, relationships between people, companies, and institutions are based more than ever, on telecommunication networks and thus the need for sophisticated cybersecurity is becoming extremely important to protect us from ever-increasing cyber-attacks. Companies and institutions are investing substantial amounts of money in their own cybersecurity. In this scenario, ethical hacking has become a frequent tool to determine the needed security-level. Ethical hacking aims to find weaknesses and vulnerabilities in computer networks, using the same knowledge and tools that hackers use to penetrate networks and expose software vulnerabilities. This disclosure article describes what ethical hacking is, its benefits and why it is needed. It presents a state of the art about ethical hacking and shows how companies and institutions could implement ethical hacking using a methodology based on Penetration Tests (Penetration Testing Execution Standard, PTES).*

KEYWORDS: ethical hacking, pentesting, penetration test, cybersecurity.

**** Harremanetan jartzeko / Corresponding author:*** Iñaki Goirizelaia. Bilboko Ingeniaritza Eskola (UPV/EHU), Ing. Torres Quevedo Plaza, 1 (48013 Bilbo). – inaki.goirizelaia@ehu.eus –

Nola aipatu / How to cite: Etxeberria, Ainhoa; Goirizelaia, Iñaki; Unzilla, Juan Jose; Astorga, Jasone; Huarte, Maider (2021). «Zibererasoetatik babesteko, *hacking* etikoaren balioa»; *Ekaia*, 39, 2021, 313-326. (https://doi.org/10.1387/ekaia.21939).

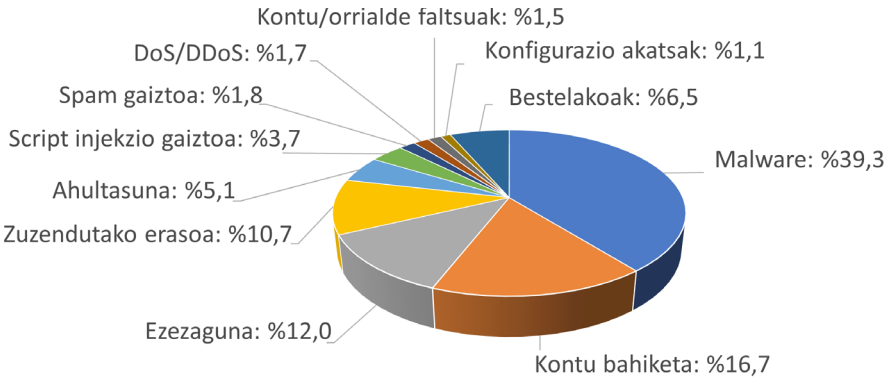
Jasoa: 2020, abuztuak 5; Onartua: 2020, urriak 10.

ISSN 0214-9001 - eISSN 2444-3255 /

1. SARRERA

Duela urte batzuk, zibersegurtasuna gutxi batzuek baino ez zuten kontuan hartzen. Teknologiaren aurrerapenak, mundu osoa uneoro konektatuta egotera ekartzearekin batera, zenbait arrisku ere ekarri ditu. Hainbestekoa da teknologiaren erabilera gaur egun, non edozein momentutan erasotuak izan baikaitezke; gailu kopuruaren igoerarekin zibererasoen arriskua ere handiagoa izango da. Hala ere, komunikazio-sareen segurtasuna hasieratik existitzen den kontzeptua den arren, IoT delakoaren (Internet of Things, Gauzen Internet) izugarrizko bilakaerarekin ezinbesteko tresna bihurtu da.

Azkeneko 25 urteetan, zibererasoek jasandako aldaketa teknologikoak direla eta, suebakiak edo antibirusak instalatzea jada ez da nahikoa. Gero eta sofistikatuagoak bihurtu dira gizakien zein zerbitzarien ahultasunak bilatzen dituzten erasoak. Ohikoak dira *Phishing*[1], DDoS[2] edo *malware*[3] teknikak aplikatuz aurrera eramaten diren erasoak. Horien adibide izan daitezke duela gutxi gertatu diren erasoak, hala nola, WannaCry, NotPetya eta British Airwaysen aurkako zibererasoa [1].



1. irudia. 2019ko erasorik ohikoenak, http://hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics webgunetik eskuratuak.

Azken urteetan zibererasoen hazkunde esponentzialak eraginda, eta, ondorioz, segurtasunak hartutako garrantzia dela eta, komunikazio- eta datu-sareen funtzionamendua bermatzeko, ekipamenduaren segurtasunak be-

[1] Biktimaren konfiantza irabazi eta horrela informazio konfidentziala lortzeko asmoz iruzur egiteko teknika multzoa.

[2] Zerbitzu-ukapen banatuak, hau da, zerbitzu bat bertan behera uzteko erasoak.

[3] Kode kaltegarri mota bat da. Haren helburua da jabearen baimen gabe sistema hondatu eta han sartzea.

rebiziko garrantzia hartu du ia-ia arlo guztietan. Informazioaren eta Komunikazioaren Teknologien garapenak bizitzeko eta lan egiteko aro berriak ekarri ditu eta, horrekin batera, erasotuak izateko bide berriak ere bai (ikusi lehen irudia). Kasurako, nortasun-lapurreta, edo fitxategi sekretuak edo datu pribatuak argitaratzea mundu-mailan oihartzun handia izan duten adibideak dira.

Segurtasuna ez da bakarrik gizabanakoen ardura bihurtu, baizik arlo guztietan bereganatu du garrantzia. Erakundeak eta tamaina guztietako enpresak ez dira salbuespen, eta gero eta gehiago dira segurtasunari garrantzia ematen diotenak, eta erasotuak izateko beldurrak beren komunikaziosarearen segurtasunean gero eta diru gehiago inbertitzera eraman ditu.

Ondorioz, gero eta gehiago dira *hacking* etikoan inbertitzen dutenak. Horrek, sarbide-testak egiteko («penetration testing» edo «pentesting») azterketak sortzera eraman du, segurtasunaren ahultasunak erasotzaileek baino lehenago aurkitu eta konpondu ahal izateko.

2. **ZER DA *HACKING* ETIKOA?**

Hacking kontzeptuari buruz asko eztabaidatu da. Ez da erraza denen gustuko definizioa aurkitzea. Batzuen ustez, jokabide maltzur batekin lotuta dago. Beste batzuentzat, ordea, portaera adimentsua eta dibertigarria da. Kontzeptu hau argitzeko Richard Stallmanen iritzia nabarmendu behar da[4]: «Zaila da hacking-a bezain askotarikoa den zerbaiten definizio soila ematea, baina uste dut jarduera horiek guztiek izaera dibertigarria eta adimentsua eta esploratzeko gogoa dutela. Beraz, hacking-ak posible denaren mugak aztertzea esan nahi du, espiritu dibertigarri eta adimentsu batekin».

Hacking-a komunikazio-sistema batean baimenik gabeko sarbidea lortzean oinarritzen den prozesua da, eta *hackerra*, berriz, ekintza hori aurrera eramaten duen pertsona. Sisteman aurkitutako ahultasunez baliatzen da sarbide hori eskuratzeko. Askotan helburua ondo pasatzea da, erronka gainditzea, eta ez dago asmo txarrik.

Sisteman asmo maltzurrekin sartzen denean, *cracker* kontzeptuari buruz hitz egiten ari gara. Sistemako fitxategiak ezabatzetik informazio sentikorra lapurtzeraino joan daitezke burutzen diren ekintzak. *Cracking*-a, bere horretan, guztiz legez kontrakoa da. Hala ere, komunikazio-sisteman asmo onarekin eta baimenarekin sartzen garenean *hacking* etikoari buruz hitz egiten ari gara.

---

[4] https://stallman.org/articles/on-hacking.html

Hacking etikoa erasotzaile batek topa eta exekuta ditzakeen erasoek sor ditzaketen galera ekonomikoak edo beste kalte handiagoak gertatu baino gehiago, sare edo sistema baten mehatxuak, hau da, ahultasunak bilatzeko ekintza bat da. Artikulu honetan *hacking* etikoa burutzeko sarbide-test (pentest) izeneko tresna aurkeztuko da.

Hacking etikoaren helburua sare edo sistemetako segurtasuna hobetzea da, horretarako azterketan zehar agertzen diren ahultasunak konponduz. Gainera, azterketa hauek gauzatzen dituztenek benetako erasotzaileek erabiltzen dituzten metodo eta erreminta berak erabiltzen dituzte. Lehen aipatu bezala, *hacking* etikoa *hacking* arruntetik edo *cracking*-etik urruntzen duen ezaugarri nagusia, lehenengoak sarearen segurtasuna hobetu eta erasoetatik babestu nahi duen jabearen baimena izatea da.

2.1. *Hacking* etikoaren garrantzia

Datuen elkartrukatzeak eta ekipamenduen interkonexioak sekulako garrantzia hartu dute edozein motatako enpresetan eta erakundeetan. Gero eta gehiago dira egunerokotasunean datu sentikor eta baliotsuak maneiatzen dituzten enpresa pribatuak zein erakunde publikoak. Ondorioz, gero eta erakargarriagoak dira eraso maltzurrak gauzatzen dituzten hackerrentzat.

Lehen aipatu bezala, eraso horiek ekiditeko, ez da nahikoa suebakiak edo antibirusak instalatzea, erasoak gero eta sofistikatuagoak baitira. *Cracker*rek egunero aurkitzen dituzte suebakiak zeharkatzeko modu berriak, erakundeak eguneratuta egotera behartuz.

Hacker etikoek segurtasun berri bat eskaintzen dute. Erakundearen segurtasun-babesak behatu beharrean, beste proba batzuen artean, sarbide-testak egiten dituzte. Beste era batera esanda, erakundearen sarea hackeatzen dute haren ahultasunak bilatzeko. Behin sarearen gabeziak ezagutzen direnean ezarri ahal baitira babesik onenak.

2.2. *Hacking* etikoaren onurak

Hacking etikoak begi bistakoa den babesa ekartzeaz gain, hainbat dira ekar ditzakeen onurak; besteak beste, onura teknikoak, ekonomikoak eta sozialak.

Onura teknikoak

Hacking etikoak sistema batean izan daitezkeen ahultasunak aurkitzea ahalbidetzen du. Gainera, eguneratu gabeko software-bertsioen ondorioz ahulak izan daitezkeen software-bertsioak identifikatzen ditu, kontu oso erabilgarria prebentzio neurriak hartzeko orduan. Izan ere, erasotua

izan aurretik ezagutzen da nondik erasotu ahal zaion enpresa bati, eta hori saihesteko neurriak har daitezke.

Onura ekonomikoak

Erasotua izan aurretik ahultasunak bilatzen dituenez, neurri batean erasotuak izatetik babesten du. Bestetik, erasotuak izatekotan honek sor ditzakeen kostuak murrizten dira. Gainera, eraso baten ondorioz honek sor ditzakeen inaktibitateei loturiko kostuak murrizten laguntzen du, eta neurri batean behintzat, aktibitatearen jarraipena ziurtatzen du.

Onura sozialak

Azkenik, bezeroengan eragin positiboa duten onura sozialak daude. *Hacking* etikoari esker, jendearen baliabide digitalak babestuago daude, eta norberaren pribatutasuna hobeto zaindu daiteke. Horrek ekarriko du segurtasun altua beharko luketen aplikazio telematiko gehiago sortzea. Ondorioz, gizartearen konfiantza baliabide telematikoetan handitu egingo litzateke eta aplikazio oso sentikorrak, bozka telematikoa adibidez, erabiltzeko aukera gehiago egongo lirateke.

3. **ARTEAREN EGOERA**

Hacking etikoa zer den azaltzeko hainbat artikulu azpimarratzea gustatuko litzaiguke, esaterako Sahare, Naik eta Khandey-en artikulua [2]. Artikulu horretan, *hacking* etikoari buruzko informazio orokorra ematen dute: definizioa, hacker mota hauek zeintzuk diren eta zein den haien eginbeharra, eta hori gauzatu ahal izateko jarraitu beharreko pausuak zeintzuk diren. Ildo berean, Ushmani [3] ikertzaileak gauza bera lantzen du, eta *hacking* etikoak negozioan sor dezakeen inpaktua gehitzen du.

Ondoren aipatzen dugun artikuluan (Patil *et al*.) [4], egungo gizartearen egunerokotasunean informatika- eta komunikazio-sistemek duten garrantzia kontuan hartuta, egileek defendatzen dute erabiltzaileek *hacking* etikoa ezagutu behar dutela, babestuta egon ahal izateko. Horretarako, artikulu honetan *hacking* etikoaren kontzeptua sartzen dute, eta hackerrek erasoak egiteko gehien erabiltzen dituzten teknika eta mekanismo batzuk berrikusten dituzte.

Bestalde, oso interesgarriak dira egindako inplementazioak. Kontuan hartuta IoT gailuak gero eta ohikoagoak direla eta askotan informazio sentikorra biltzen eta erabiltzen dutela, beharrezkoa da haien segurtasuna bermatzea. IoT gailuetan segurtasun-ahuleziak detektatzeko eta zuzentzeko tresna gisa, artikulu horretan [5] egileek Pentos izeneko tresna bat aurkeztu

dute. Tresna horrek GUI bat du Kali Linuxen [6]. Pentos tresnak WiFi edo Bluetooth erabiltzen du IoT gailu kalteberei buruzko informazioa lortzeko eta hainbat sarbide-test egitea ahalbidetzen du. Testen ondorioz, tresnak gailuen segurtasuna hobetzeko gomendioak ematen ditu.

IoTren azterketa egiten jarraituz, Papp eta kideen artikuluan [7], egileek egungo IoT gailuen segurtasun-kalteberatasunak berrikusten dituzte, eta haiek hackeatzeko hainbat teknika eta tresna aurkezten dituzte. Hardwarearen hackeoan eta firmwarearen erauzketan zentratzen dira, ondoren aztertzeko, adibidez, pasahitz hardkodeatuak (programaren kodean txertatutako pasahitz finkoak, programa bera aldatu gabe ezin direnak aldatu), scriptetako bug-ak, eta abar. lortzen ahalegintzen dira. Sarbide-testa (penetration testing) aurkezten dute IoT gailuen ahultasunak detektatzeko eta zuzentzeko mekanismo gisa, eta, horrela, haien segurtasun-maila hobetzen dute.

Amaitzeko, ezin da ahaztu *hacking* etikoan lege-inplikazio izan daitezkeela, etikaren garrantzia agerian utziz. Thomas-en artikuluan [8] ikusten denez, sarbide-testak egiteaz arduratzen direnek etikoki zuzen jokatzearen garrantziaz hausnartzen da. Datu pertsonalak edo sentikorrak baimenik gabe lortzearen ondorioz *hacking* etikoari eta pribatutasun-erregulazioei dagokienez AEBetan eta Australian hartutako hurbilketak alderatzen ditu artikuluak.

Ildo berean, Danish-en artikulua [9] dago, etikaz aritzen dena eta nola *hacker* mota hauen lana benetako asmoaren arabera legezkoa izan daitekeen ala ez.

Gainera, legearen balizko urraketei dagokienez, DeMarcoren artikuluak [10] *hacking* etikoko testak edo sarbide-testak egitean, legearen ikuspuntutik segurtasun-ahuleziak detektatzeko eta babesteko dauden arriskuak aztertzen ditu; legearen balizko urraketak edo ekintzak erakundearen ospea arriskuan jar dezaketenak. Batez ere «capture the flag (bandera lortu)» motako ariketetan zentratzen da, non zibersegurtasunaren ezagutza aurreratua duen talde bat baimenik ez duen baliabide batera sartzen saiatzen den.

4. *HACKING* ETIKOA AURRERA ERAMATEKO TEKNIKAK

Hacking etikoa aurrera eramateko ohikoen diren teknikak ahultasunen analisia eta sarbide-testa edo pentestinga dira.

4.1 Ahultasunen analisia

Sistemaren, softwarearen edo sarearen analisia da; helburua da ahultasunak eta akatsak bilatzea. Honen bitartez, enpresaren edo erakundearen

aktibitatearen segurtasuna zehazten da, baita eraso posibleen mailak ere. Horretarako, zenbait metodologia eta erreminta erabiltzen dira [11].

Analisia aurrera eramateko, hiru metodo erabiltzen dira: kaxa zuria, grisa eta beltza. Lehenengoan, enpresa barneko erabiltzaile edo rol batekin lotuta dago, zeinek enpresa barruko datu kritikoetara sarbide osoa edo partziala duen. Sarea guztiz ondo ezagutzen du. Kutxa grisaren kasuan, probatzaileak badu zenbait informazio baina ez osoa. Hirugarrenean, berriz, erasotzailearen rola hartzea ahalbidetzen du, enpresa edo erakundearen sistema barruko ezaugarririk ezagutu gabe.

Aipatutako metodoetako edozein erabiliz gero ahultasunak bilatzeko, aplikazio-software ugari daude, «eskaner» izenez ezagutzen direnak. Horietako asko ordaindu beharrekoak dira, hala nola Acunetix [12], Netsparker [13], ProxyStrike [14] edo Burp [15]. Beste batzuk doan dira: adibidez, Nmap [16], Metasploit [17], Nessus-en [18] bertsio mugatua, ordaindu behar den tresna indartsuago bat ere eskaintzen duena, edo Kali Linux suitea, erreminta multzo oso bat eskaintzen duena (besteak beste, informazioa biltzea, ahuleziak aztertzea, haririk gabeko sareen aurkako erasoak, web-aplikazioen segurtasun-analisiak, estres-testak edo pasahitzei egindako erasoak).

4.2. **Sarbide-testa (pentest)**

Sarbide-testa sistemaren ahultasunak bilatzeko tresna erabilgarrienetariko bat bilakatu da. Test honetan, sistemaren aurkako erasoak egiten dira, sistemaren ahultasunak aurkitzeko. Teknika honek segurtasun-erroreak eta hutsuneak konpontzeko balio du. Gainera, erasoetatik babesteko eta sistemaren ahalmena balioztatzeko ere balio du. Sisteman ahultasunak izatearen arrazoiak honako hauek izan daitezke, esate baterako: diseinu erroreak, sarearen konektibitatea, gizakiak sortutako erroreak eta abar.

Sarearen segurtasun fisikoa zein logikoa balioztatzeko eta ebaluatzeko balio du. Analisia hiru mota desberdinetan burutu daiteke, aztertzaileak aldez aurretik ezagutzen duen sarearen informazioaren arabera: kutxa zuria, grisa eta beltza.

Kutxa Zuriko proba sarbide-test modurik osoena da. Sarbide-test modu hori egiteko, *hacker* etikoak enpresaren funtsezko informazio guztia du: topografia, pasahitzak, IPak, loginak eta gainerako datu garrantzitsu guztiak, sareari, zerbitzariei, balizko segurtasun-neurriei, *firewall*ei eta abarri buruzkoak. Hau da, sareko azpiegitura guztia ebaluatzen duen azterketa integral batetik abiatzen da.

Kutxa beltza erabiliz, sarbide-test hau ia itsuan egindako proba da, helburuko sareari buruzko informazio askorik eduki gabe. Sarbide-test hauek kanpoko eraso baten ezaugarrietatik hurbilen daudenak dira. Ezaugarri ho-

riek direla eta, horrelako pentesta egiten duen probatzaileak sarearen mapaketa handirik egin gabe, ziberkriminalen oso antzera jardungo du, sareko egituran ahuleziak antzemateko.

Kutxa grisa aurreko bi moduen nahasketa bezala definitzen da. Kutxa Grisa moduan probatzaileak badu nolabaiteko informazio zehatza sarbide-testa egiteko. Informazio hori urria da, eta ez da alderagarria Kutxa Zuriaren sarbide-test batean eskuragarri dagoenarekin, ez kopuruan ez eta garrantzian ere.

Eraso metodologiek praktikak hobetzeko prozesu, fase, erreminta eta teknikak zehazten dituzte. Fase bidezko azterketa batek gutxienez plangintza, exekuzioa eta exekuzioaren ondorengoak izan behar ditu. Horietaz gain, fase kopuruaren arabera hainbat dira erabil daitezken metodologiak, hala nola, PTES (Penetration Testing Execution Standard) [19], OWASP (Open Web Application Security Project) [20] edota OSSTMM (Open Source Security Testing Methodology Manual) [21].

Kasu honetan ere erreminta desberdin batzuk erabil daitezke; esate baterako, Nmap [16], Nessus [18] eta Metasploit [17].

Nahiz eta azterturiko kontzeptuak, sarbide-testak eta ahultasun analisiak oso antzekoak iruditu, ezberdinak dira; izan ere, kasu bakoitzean finkatutako helburua lortzeko jarraitzen den prozedura ezberdina da. Sarbide-testen kasuan, sare batean ahuleziak bilatzeko helburuarekin, estres testak egiten dira eta ahulezia horietarako irtenbideak proposatzen dira. Estres-testak, erresistentzia-test izenez ere ezagutuak, sistema, software edo hardware baten haustura-puntua aurkitzeko balio du. Gainera, sistemaren hutsegite baten ondoren horren jarrera aztertzea dute helburutzat. Ahultasun-analisiaren kasuan, aldiz, sistemaren ahultasunak eskuz edo automatikoki, software bidez, bilatzen dira. Ohiko ahultasunen artean, honako hauek aurkitzen dira: pasahitzen ahultasunak (segurtasun-maila baxua), behar ez diren atakak zabalik egotea (adibidez, sistema eragile batzuetan jatorriz zabalik dagoen SMB —Service Message Block— protokoloaren ataka WannaCry erasoa aurrera eramateko erabili zen), suebakien gabeziak eta abar. Sarbide-testak lehenbizi aipatutako horiek aurkitzen ditu, eta gero horientzako soluzioak ematen ditu.

5. ENPRESETAN ETA ERAKUNDEETAN *HACKING* ETIKOA GAUZATZEKO METODOLOGIA

Sarbide-testak ez dira fase bakar batean oinarritzen, baizik eta fase desberdinez osatuta daude, erabiltzen den metodologiaren arabera. Lehenago aurreratu bezala, metodologia ezberdinak daude *hacking* etikoa burutzeko. Horietako bat sarbide-testarekin erlazionaturiko guztia aztertzen

duen PTES metodologia da. Zazpi atal bereizten ditu, edozein ingurunetan garatu daiteke, eta emaitza eraginkorrak lortzen ditu. Metodologia hau erabiltzen denean, azterketa zazpi fasetan banatzen da:

— Beharrezko erreminten aurkezpena.
— Informazio-bilketa.
— Eraso-modelizazioa.
— Ahultasunen analisia.
— Ahultasunen ustiapena.
— Ustiapenaren ondorengo fasea.
— Dokumentazioa.

Hasteko, sarbide-testa burutzeko erabiliko diren erremintak eta teknikak azaltzen zaizkio azterketa eskatzen duenari. Gainera, garrantzitsua da sarbide-testaren mugak finkatzea gaizki-ulertuak ekiditeko, bai eta zein motari, hau da, kutxa zuriari, grisari edo beltzari, jarraituz egingo den azterketa ere.

Bigarren pausoa informazio-bilketa da, eta horretarako sarearen analisia egiten da. Hau da, sarean dauden gailuen informazioa eskuratzeko balio du, sarera konektaturik dauden gailuen kopurua, bakoitzean zabalik dauden atakak eta bakoitzean dagoen zerbitzua eta bertsioa. Ohikoa da informazio hori eskuratzeko Nmap gisako erremintak erabiltzea. 2. irudian aipatutako erremintaz baliatuz, sarera konektaturiko gailu batean zabalik dauden atakak eta horietan dauden zerbitzuak ikus daiteke:

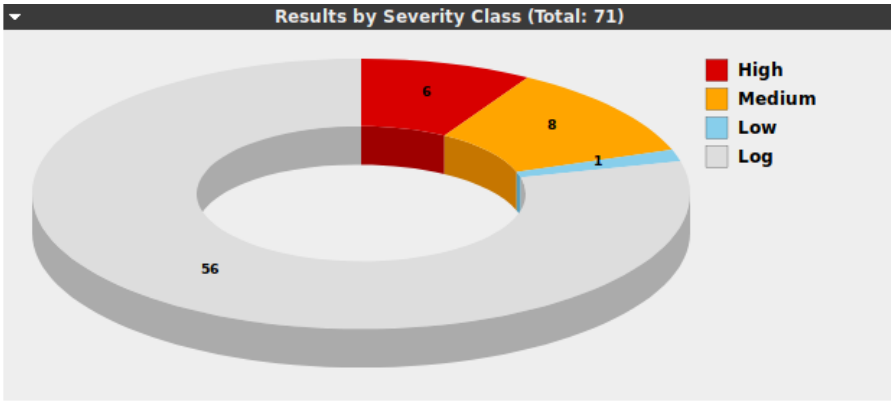
```
Nmap scan report for 192.168.1.2
Host is up (0.090s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:AD:BC:33 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.4
Host is up (0.0025s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE      VERSION
25/tcp   open  smtp         Microsoft ESMTP 6.0.2600.5512
80/tcp   open  http         Microsoft IIS httpd 5.1
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:C2:C0:BA (Oracle VirtualBox virtual NIC)
Service Info: Host: ehu; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 192.168.1.100
Host is up (0.00078s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2002/tcp open  rpcapd        WinPcap remote packet capture daemon
MAC Address: 0A:00:27:00:00:15 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

2. irudia. Informazio-bilketa Nmap erreminta erabiliz.

https://doi.org/10.1387/ekaia.21939



3. irudia. OpenVas erreminta bidez gailu batean egindako ahultasun analisiaren emaitzak, ahultasunek izan dezaketen arriskuen arabera bilduta.

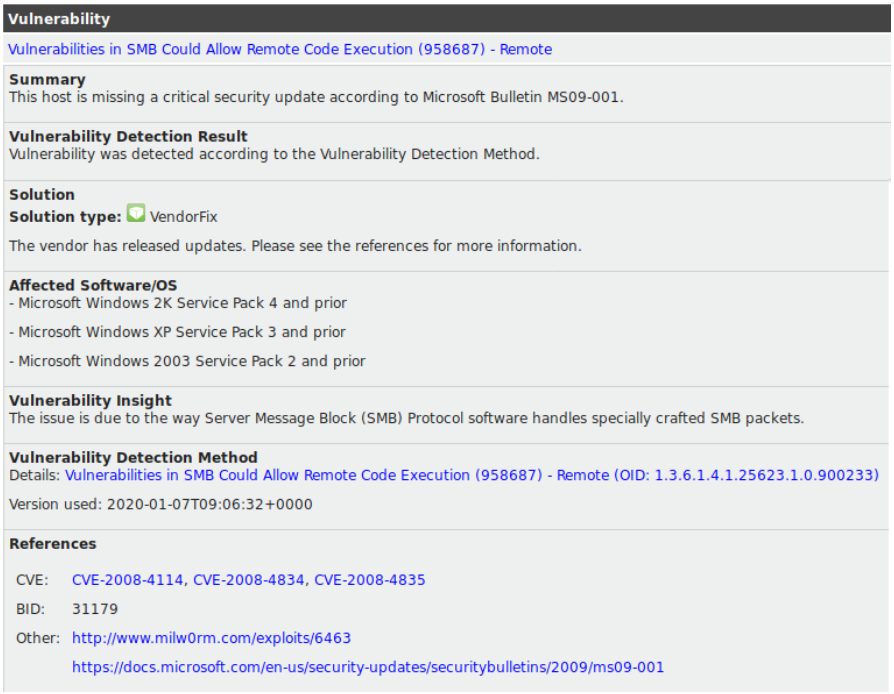
Hirugarren pausoan, **eraso-modelizazioan**, sarbide-testa arrakastatsua izateko jarraitu beharreko urratsak finkatzean dira, hots, zer-nolako proba eramango diren aurrera. Adibidez, zer gailuk osatzen duten sarea zehazteko probak edota erasotuak izateko aukera gehien duten gailuak zeintzuk diren jakiteko. Ondoren, **ahultasunen analisiaren** bidez sarearen edo sistemaren ahultasunak bilatzeko prozesua dator. Prozesu horrek segurtasuna arriskuan jar dezake. Hasieran zehazturiko irismenak analisiaren sakonera eta zabalera mugatzen ditu. Hau da, zer-nolako informazioa bilatu nahi den edota zer gailutan exekutatu nahi den analisia. Erreminta ugari daude ahultasunak bilatzeko, hala nola, Nessus ordainpekoa edo OpenVas [22] doakoa.

Adibidez, OpenVas erremintak analisia sare osoan edo gailu bakar batean zehazteko aukera ematen du. 3. eta 4. irudietan ikus daitekeen bezala, analisia sare osoan egiten bada, gailu bakoitzaren IP helbidea eskuratzearekin batera, bakoitzean dauden ahultasunak bilatzen ditu, eta horiek gailu bakoitzari zer-nolako arriskua ekar diezaiokeen.

Vulnerability	Severity	QoD	Host	Location
Microsoft IIS Web Server End Of Life Detection	10.0 (High)	80%	192.168.1.4	80/tcp
OS End Of Life Detection	10.0 (High)	80%	192.168.1.4	general/tcp
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	192.168.1.4	445/tcp
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (High)	98%	192.168.1.4	445/tcp
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.4	445/tcp
Microsoft IIS WebDAV Remote Authentication Bypass Vulnerability	7.6 (High)	99%	192.168.1.4	80/tcp
Microsoft Windows SMTP Server DNS spoofing vulnerability	6.4 (Medium)	80%	192.168.1.4	25/tcp
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99%	192.168.1.4	80/tcp
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	5.0 (Medium)	70%	192.168.1.4	80/tcp
Missing `httpOnly` Cookie Attribute	5.0 (Medium)	80%	192.168.1.4	80/tcp

4. irudia. OpenVas bidez aurkitutako arrisku gehien ekartzen duten ahultasunen informazioa.

5. irudiak erakusten duenez, erreminta hau erabiliz lor daitekeen informazioa ez da hor geratzen: aurkitutako ahultasun bakoitzaren inguruan informazio gehigarria ematen du, hots, izan dezakeen eragina, konponbidea, zer sistema eragileri eragiten dion ahultasun horrek edota informazio gehigarria lortzeko loturak.



Vulnerability

Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote

Summary
This host is missing a critical security update according to Microsoft Bulletin MS09-001.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2K Service Pack 4 and prior

- Microsoft Windows XP Service Pack 3 and prior

- Microsoft Windows 2003 Service Pack 2 and prior

Vulnerability Insight
The issue is due to the way Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Vulnerability Detection Method
Details: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote (OID: 1.3.6.1.4.1.25623.1.0.900233)

Version used: 2020-01-07T09:06:32+0000

References

CVE: CVE-2008-4114, CVE-2008-4834, CVE-2008-4835

BID: 31179

Other: http://www.milw0rm.com/exploits/6463

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-001

5. irudia. «Vulnerabilities in SMB Could Allow Remote Code Execution» ahultasunaren informazio gehigarria.

Fase honen bukaeran, sistemaren segurtasun-kontrola zeharkatzeko eraso bektoreak lortzen dira. Hau da, bildutako informazioaren arabera helburuko sistema edo gailura sarbidea lortzeko erabiltzen den metodoa da, sarean aurkitutako ahultasunetan oinarritzen dena eta erakundearen gaitasuna arriskuan jar dezaketena.

Sisteman aurkitzen diren ahultasunak eta eraso bektoreak identifikaturik daudenean, haien ustiapena egin behar da. Fase honek segurtasuna hautsiz sisteman sarbidea lortzea du helburutzat. Aurreko fasean aurkitutako ahultasun kritikoak, inpaktu handiena eragiten dutenak, aztertzen dira lehendabizi.

Aurkitutako ahultasunek sarean izan dezaketen eraginaz gain, ohikoa izaten da erabiltzaileek aukeratu dituzten pasahitzak aztertzea, bai ahul-

tasun baten ondorioz bistaratu ahal direnak, bai eraso zehatzen bidez bistaratzen direnak. Azken adibide bat hiztegi-erasoa izango litzateke, hots, erabiltzailearen izena eta pasahitzak eskuratzeko identitate-lapurreta erako metodo bat. Eraso honek erabiltzailearen izena eta pasahitza ezagutu gabe gailu edo sistemara sarbidea lortzeko aukera ematen du, hitz, esaldi edo letrekin eta horien konbinazioekin saiatuz. Erasoa burutzeko, besteak beste, hiztegietako hitzez, animalien izenez eta ohikoak diren pasahitzez osaturiko zerrendak erabiltzen dira [23]. 6. irudian, metasploit tresna erabiliz egindako hiztegi-eraso baten adibidea ikus daiteke, non «admin» erabiltzaile-izenarentzat pasahitz ezberdin asko erabiltzen diren. Hala ere, kasu honetan, saiakera desberdinetan ez da lortu erabiltzaile-izen eta pasahitz konbinazio zuzenik, eta ondorioz ez da sarbidea eskuratu.

6. irudia. Hiztegi-eraso baten exekuzioa

Seigarren fasea **ustiapenaren ostekoa** da, eta arriskuan dagoen gailuaren balioa zehaztea du helburutzat. Gailuaren balioa sarean duen eraginaren eta gordetzen duen informazio sentikorraren arabera neurtzen da. Fase honek datu sentikorra identifikatzen eta dokumentatzen laguntzen du.

Azkenik, dokumentu batean biltzen dira arestian azaldutako atal guztiak. Hau da, azterketaren helburua eta aurkitzen diren ahultasun guztiak batzen dira, bai eta haiek ekiditeko hartu beharreko neurriak zein gomendioak ere.

6. **ONDORIOAK**

Azken urteetako teknologiaren garapenak eta horren eskutik etorri diren zibererasoen hazkuntza esponentzialak segurtasunaren garrantzia area-

gotu du, *hacking* etikoa moduko ekintzak sortuz segurtasuna eta konfiantza bermatzeko. Izan ere, *hacking* etikoa crackerrengandik babesteko erreminta bezala sortu zen, erasoak gero eta sofistikatuagoak baitira.

Sarean gure datuen erabilpenak garrantzi handiagoa bereganatu duenez, horren babesa ezinbestekoa bilakatu da, eta horretarako ez da nahikoa suebakiak izatea. Datuen segurtasuna lortu ahal izateko, beharrezkoa da erasotzaileek erabiltzen dituzten metodo berberak erabiltzea sarearen babesa bermatzeko. Hori dela eta, gero eta erakunde gehiagok kontratatzen dituzte *hacking* etikoaren jakitun diren pertsonak, beren segurtasuna ziurtatzeko. Hacker etikoak, sarbide-testak gauzatzen dituzten sare horretako ahultasunak bilatzeko, horien lana guztiz beharrezkoa bihurtu da sareak seguruak izan daitezen. Sarbide-testen azkeneko txostenean aurkitutako ahultasun guztiak biltzen dira, eta horietako bakoitza konpontzeko irizpideak zehazten dira.

Hacking etikoak jendea prestatzera, ikastera, eramaten du, eta ez du inork ziurtatzen erakutsitakoa era egokian edo ekintza legez kontrakoak gauzatzeko erabiliko duten. Izan ere, pertsona bakoitza ezberdina da, eta ezin daiteke aldez aurretik jakin zer egingo duen. *Hacking* etikoa behar bezala gauzatzen bada, gizarteari onura ugari ekar diezazkioke, nahiz eta arriskuak izan. *Hacking* etikoa, cracking-a bezala, une oro hobetuz eta garatuz doa, eta sor daitezkeen arazoak aldez aurretik identifikatzea ezinbestekoa da erantzun egokiak eman ahal izateko.

Beraz, *hacking* etikoari esker, enpresek eta erakundeek gure datu pertsonalak modu seguruagoan kudeatzeko aukera dute, eta, horrela, beren jardueraren etorkizuna bermatzeko behar-beharrezkoa den konfiantza irabazten dute. Gainera, beren eguneroko aktibitatea geldiaraz dezaketen zibererasoetatik babesten dira, horrek dakarren mota guztietako kostu handia saihestuz.

BIBLIOGRAFIA

[1] «Sapphire,» [Online]. Eskuragarri: https://www.sapphire.net/news-views/british-airways-sufferfrom-latest-attack-technique/. [Atzitze-data: 2020 10 02].

[2] SAHARE, B., NAIK, A. eta KHANDEY, S. 2014. «Study of Ethical Hacking». *International Journal of Computer Science Trends and Technology (IJCDT)*, **2**, 6-10.

[3] USHMANI, A. 2018. «Ethical Hacking». *Internation Journal of Information Technology (IJIT)*, **4**, 1-4.

[4] PATIL, S., JANGRA, A., BHALE, M., RAINA, A. eta KULKARNI, P. 2017. «Ethical hacking: The need for cyber security». *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 1602-1606.

[5] VISOOTTIVISETH, V., AKARASIRIWONG, P., CHAIYASART, S. eta CHOTIVATUNYU, S. 2017. «PENTOS: Penetration Testing Tool for Inter-

net of Things Devices». *TENCON 2017-2017 IEEE Region 10 Conference*, 2279-2284.

[6] «Kali Linux» [Online]. Eskuragarri: https://www.kali.org. [Atzitze-data: 2020 10 02].

[7] PAPP, D., TAMAS, K. eta BUTTYAN, L. 2019. «IoT Hacking – A Premier». *Infocommunications Journal*, 1-12.

[8] THOMAS, G., BURMEISTER, O. eta LOW, G. 2019. «The Importance of Ethical Conduct by Pentration Testers in the Age of Breach Disclosure Laws». *Australasian Journal of Information Systems*, **23**, 1-14.

[9] DANISH, J., MUHAMMAD, N. eta KHAN, A. 2011. «Is ethical hacking ethical?». *Internation Journal of Engineering Science and Technology (IJEST)*, **3**, 3758-3763.

[10] DEMARCO, J.V. 2018. «An approach to minimizing legal and reputational risk in Read Team hacking exercises». *Computer law & security review*, **34**, 908-911.

[11] ROMERO, M.I., FIGUEROA, G.L., VERA, D.S., ALAVA, J.E., PARRALES, G.R., ALAVA, C.J., MURILLO, A.L., CASTILLO, M.A. 2018. *Introducción a la seguridad informática y el análisis de vulnerabilidades*, 3ciencias, Alcoy (Alicante).

[12] «Acunetix» [Online]. Eskuragarri: https://www.acunetix.com/. [Atzitze-data: 2020 10 02].

[13] «Netsparker» [Online]. Eskuragarri: https://www.netsparker.com/. [Atzitze-data: 2020 10 02].

[14] «Kali tools, ProxyStrike Package Description» [Online]. Eskuragarri: https://tools.kali.org/webapplications/proxystrike. [Atzitze-data: 2020 10 02].

[15] «Burp Suite» [Online]. Eskuragarri: https://portswigger.net/burp. [Atzitze-data: 2020 10 02].

[16] «Nmap» [Online]. Eskuragarri: https://nmap.org/. [Atzitze-data: 2020 10 02].

[17] «Metasploit» [Online]. Eskuragarri: https://www.metasploit.com/. [Atzitze-data: 2020 10 02].

[18] «Nessus» [Online]. Eskuragarri: https://es-la.tenable.com/products/nessus. [Atzitze-data: 2020 10 02].

[19] «PTES» [Online]. Eskuragarri: http://www.penteststandard.org/index.php/PTES_Technical_Guidelines#Intelligence_Gathering. [Atzitze-data: 2020 10 02].

[20] «OWASP» [Online]. Eskuragarri: https://www.owasp.org/images/1/19/OTGv4.pdf. [Atzitzedata: 2020 10 02].

[21] «OSSTMM» [Online]. Eskuragarri: https://www.isecom.org/OSSTMM.3.pdf. [Atzitze-data: 2020 10 02].

[22] «OpenVas» [Online]. Eskuragarri: https://www.openvas.org/. [Atzitze-data: 2020 10 02].

[23] «SPECOPS» [Online]. Eskuragarri: https://specopssoft.com/blog/what-is-password-dictionaryattack/. [Atzitze-data: 2020 10 02].