UBT-CERT Internship

Java e parë dhe e dytë

Simulimi dhe testimi në rrjetë, aplikacione dhe sisteme

Maj 2017

Përgatitur nga studentët e SHKI/UBT:
Rrustem Shehu

Veton Bejtullahu

Ardit Krasniqi

Ndihmës: Blent Kurtalani UBT-CERT trajner

Përmbajtja

Hyrje

Ky dokument është një përmbledhje e informacioneve të cilat kontribojnë në vetëdijsimin e sulmeve eventuale që mund të ndodhin , si dhe parandalimi i tyre me anë të disa veglave të cilat do të shqyrtohen përgjat këtij dokumentimi.

Të gjitha këto mekanizma të sigurise do të ndikojnë direkt në përmirësimin e sigurise dhe parandalimin e sulmeve të sistemeve kompjuterike të kompanive , në mënyrë që klientet të jenë sa më të sigurt gjatë përdorimit të shërbimeve të ndryshme nga kompanitë.

Koncepti etik (Defense cyber security)

Etika e sigurise kibernetike ka kuptimin e gjetjeve të mangësive të sistemeve kompjuterike , web aplikacioneve etj., në mënyrë që të rregullojmë ato mangësi , kështu parandalohen sulmet eventuale që mund të ndodhin.

Duke bërë hulumtim me anë të veglave të sigurisë dhe gjetjen e sa më shum mangesive në ndonjë sistem, pastaj rregullimi i mangesive të gjetura përbën etiken e sigurisë.

Çka është “footprinting”

Footprinting është një vegel e cila na ofron informacione të shumta për një target të caktuar në rrjetë p.sh. institucion publik, privat, akademik ose kompani. Duke bërë një analizë tv informatave në mund të parashikojmë se qfarë infrastrukture përdorë kompania e caktuar , gjithashtu mund të zbulojm se si përmes atyre informacioneve mund të kryhet një sulm kibernetik. Pastaj duhet sygjeruar targetin përkates se si tv mbuloj të dhenat e ndjeshme , në mënyrv që të jetv sa me i sigurt.

Analiza e parë “I”

Përdorimi I veglës “**ping**” të sistemit operativ e bazuar në Command-line, shërben për testimin e host-ve dhe IP-ve se a janë në funksionim normal.

Përmes veglës “**ping**” gjatë ekzekutimit në mund të marrim informata se sa paketa janë dërguar me sukses, sa pranuar dhe humbur. Gjithashtu tregon edhe kohën e dërgimit dhe pranimit të paketës.

Skenari I përdorur:

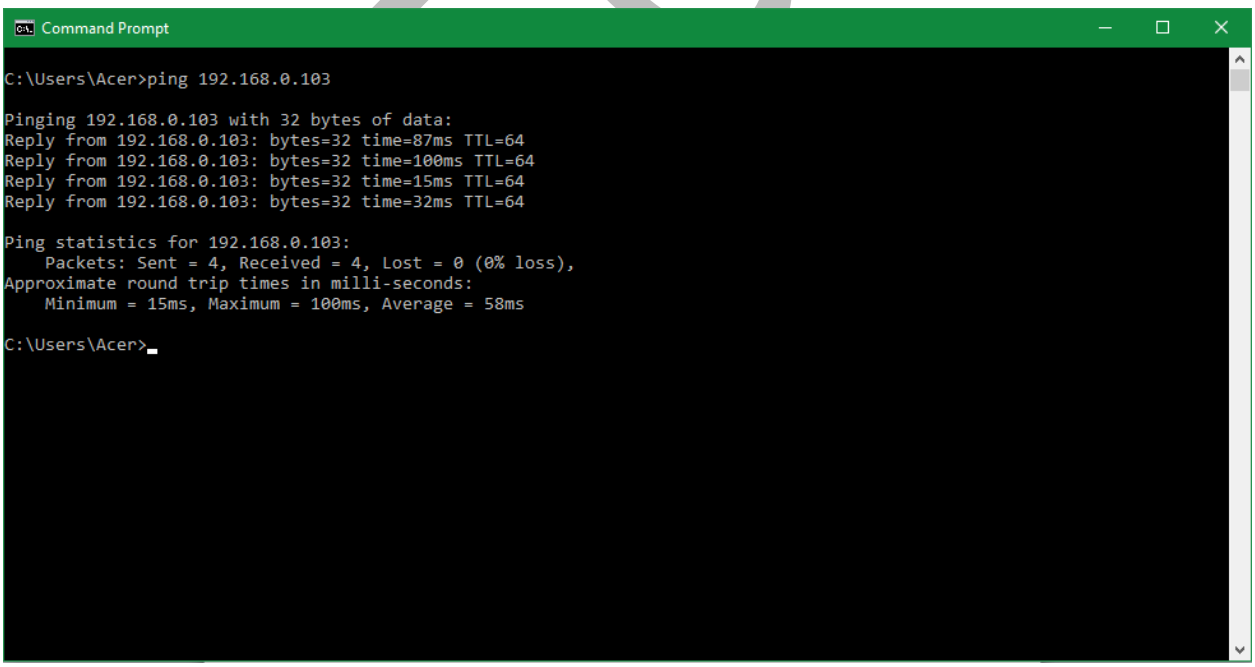


Figura 1

Rekomandim

- Rekomandohet që në rrjetë të maskohen informacionet që I mbledh vegla “ping”, kjo eliminon mundësinë e zbulimit dhe mbledhjes së informatave për host-et dhe IP e caktuar në infrastrukturën tonë.

Analiza e dytë “II”

Aplikacioni “**SmartWhois**” vegel e cila pranon një emer të domenit dhe pastaj na jep informacione të shumta si në vijim:

- Lokacioni
- Emri I ISP[1]-së
- Pronari I domain-t dhe IP adresës
- Informata për pronarin e domain-t
- Data regjistrimit dhe skadimit domain-t

Skenari I përdorur:

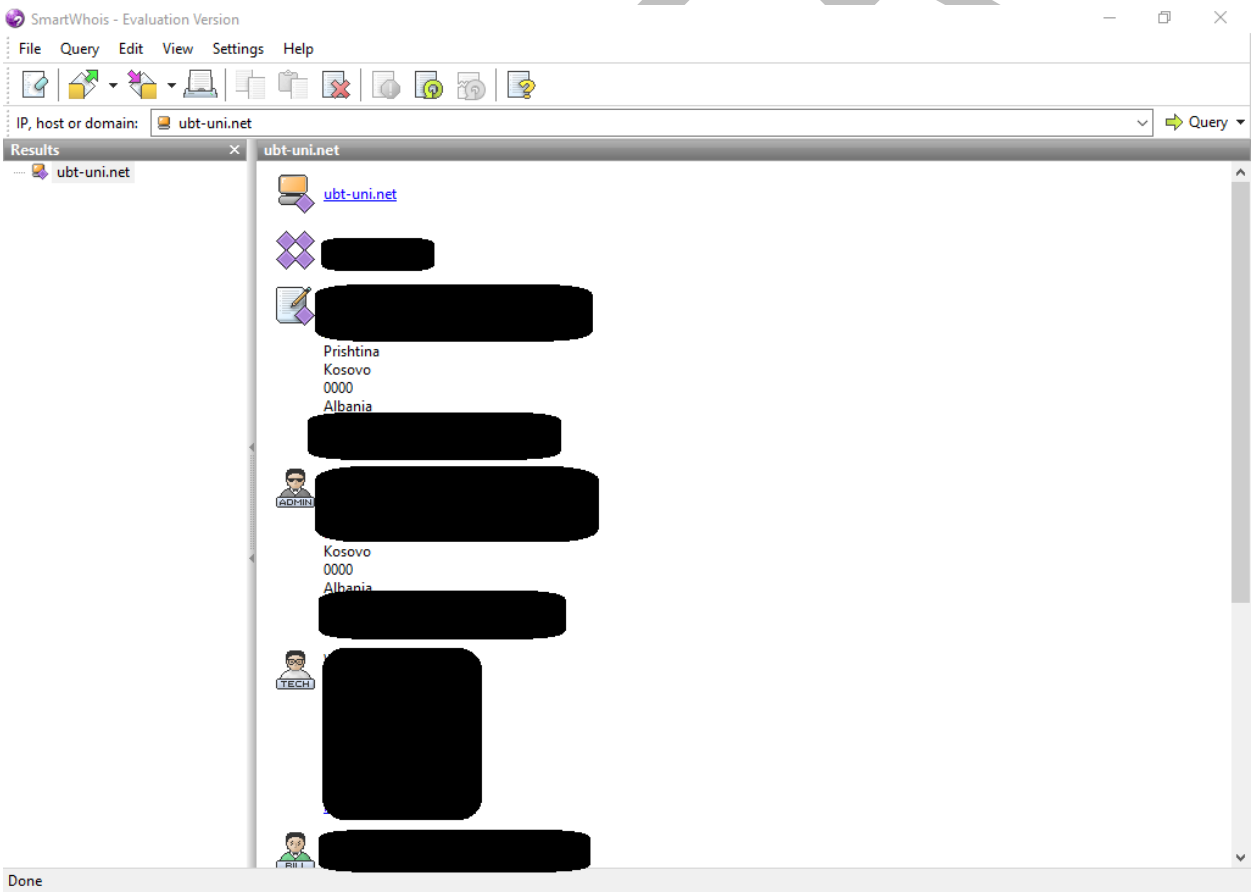


Figura 2

[1] ISP Internet Service Provider, ata që na furnizojnë me internet

Aplikacioni “**EmailTracker**” përdoret për zbulimin se nga ka ardhur nje email , të cilin ne dyshojm se mund të permbaje spam apo diqka tjeter. Por dhe na jep informacione të tjera të rëndësishme, si në vijim:

- Paraqitjen gjeografike të lokacionit dërguesit
- Mbledhja e informatave për ISP dhe domain.

Skenari I përdorur:

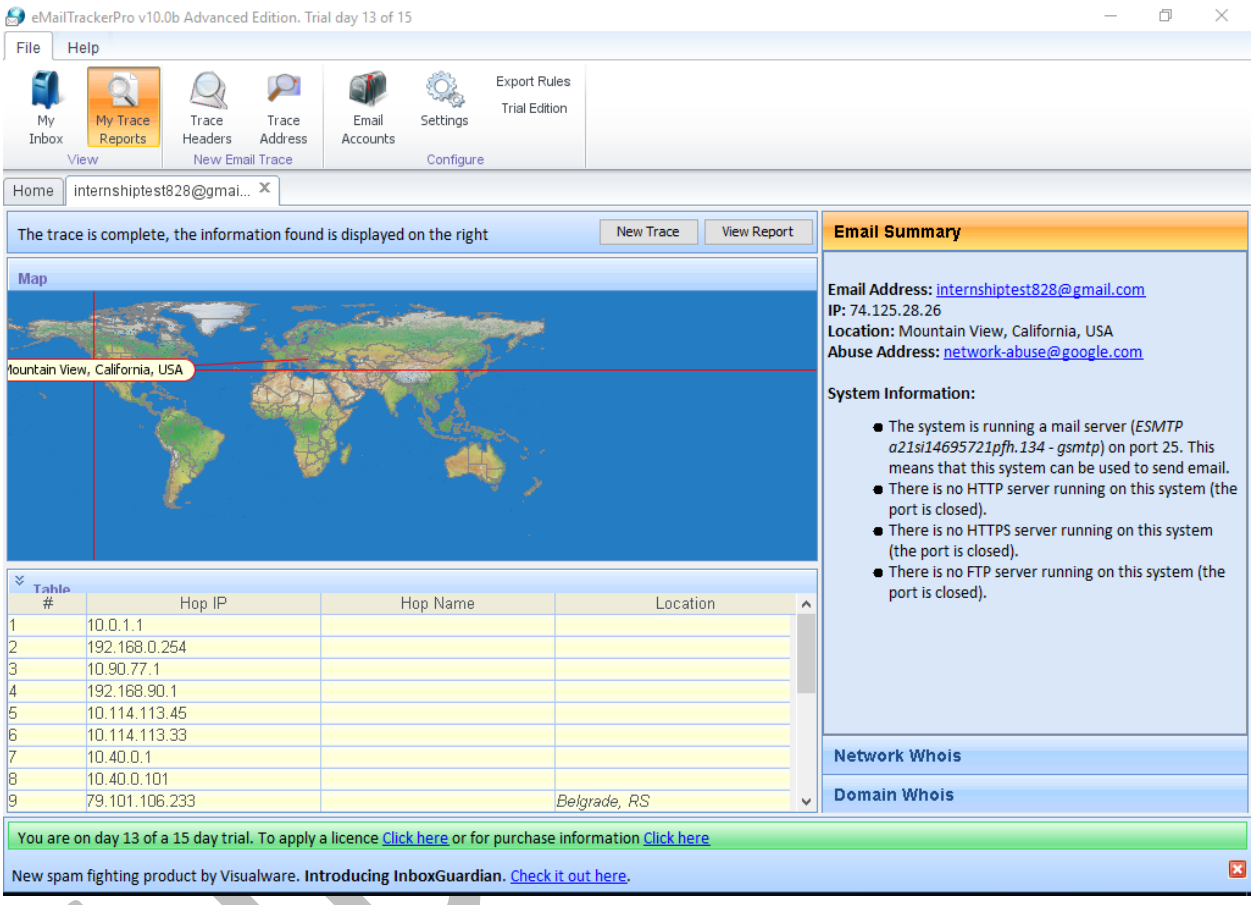


Figura 3

Rekomandim

- Nese deshirojm që të mos shfaqet asnjë informacion rreth emrit tv pronarit apo informacion tjeter të rendesishme preferohet të bëhët një pagese në kompanin e cila ofron domain në mënyrë që të fshihen këto informacione.

Çka është Scanning Network

"**Scanning Network**" shërben për identifikimin në host , me cilat porta bëhët komunikimi, e disa sherbime të tjera.Me ane të kësaj vegle ne mund të gjejm portet e hapura , qfar sistemi operativ përdor dhe disa dobesi te tjera ne rrjete.

Analiza e pare "I"

"**IP scanner**" shërben për të marr lloje të ndryshme të informacioneve në lidhje me kompjuterët në rrjetën lokale.

Skenari I përdorur:

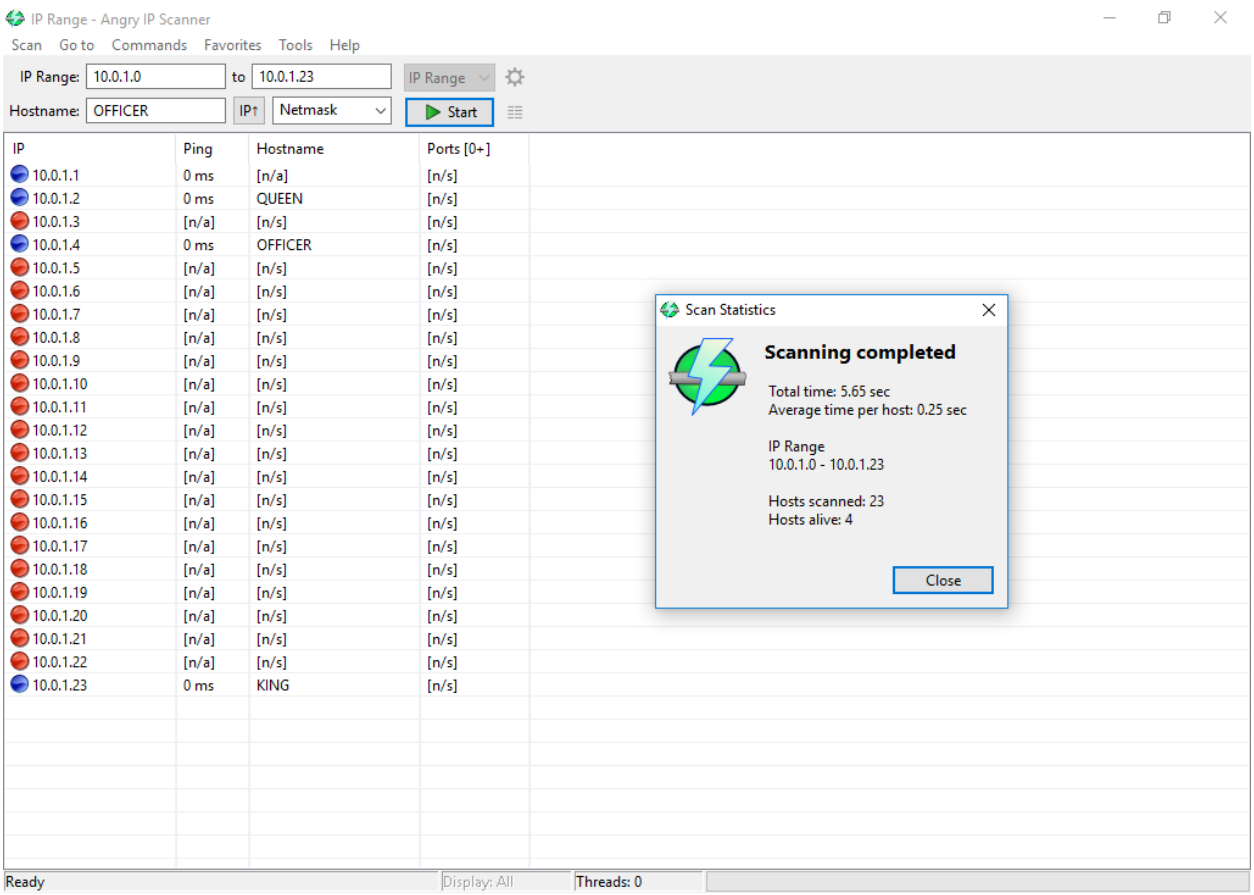


Figura 4

Analiza e dytë “II”

“**Friendly pinger**” aplikacion i cili na mundëson administrimin dhe monitorimin e të gjitha paisjeve që janë të lidhur në një rrjet të caktuar.

Skenari I përdorur:

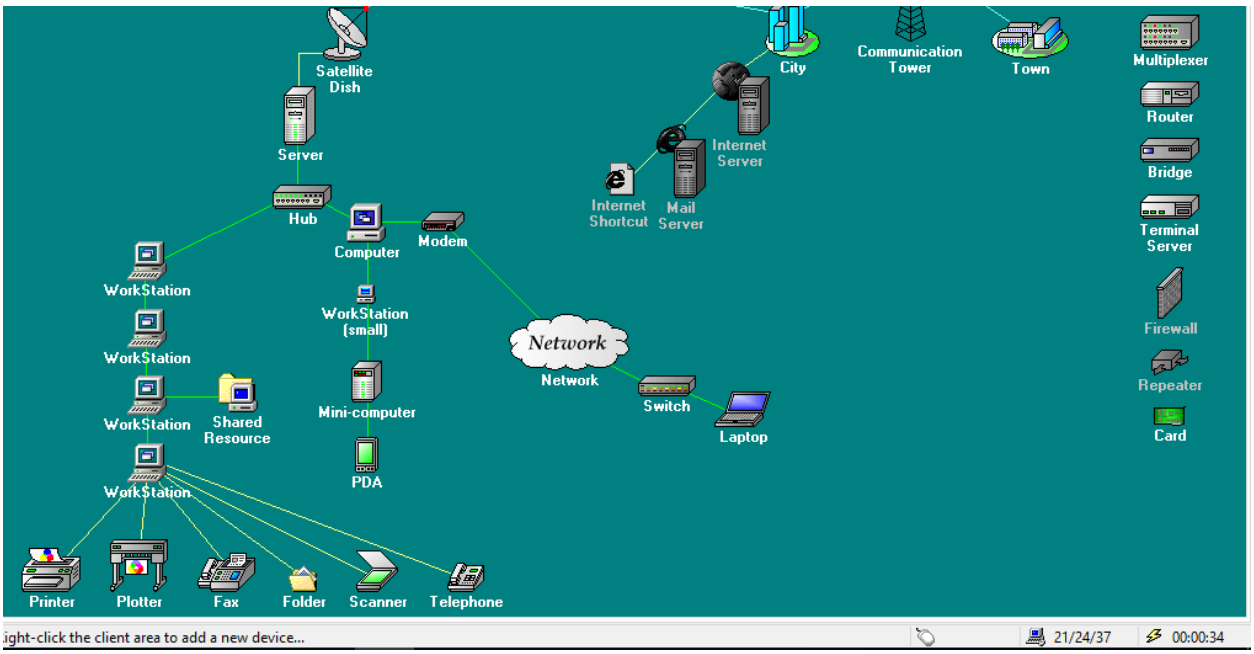


Figura 5

Analiza e trete “III”

“Nessus” është platforma më e besueshme e skanimit të dobësive për auditorët dhe analistët e sigurisë. Përdoruesit mund të planifikojnë skanime nëpër skanerë të shumëfishtë, të përdorin wizards për të krijuar linja veprimi të thjeshta dhe të shpejta, të planifikojnë skanimet dhe dërgojnë rezultatet përmes emailit. Nessus mbështet më shumë teknologji se çdo program tjetër, duke përfshirë sistemet operative, pajisjet e rrjetit, hypervisors, databazat, tableta / telefonat, serverat web dhe infrastrukturat kritike.

Skenari i përdorur:

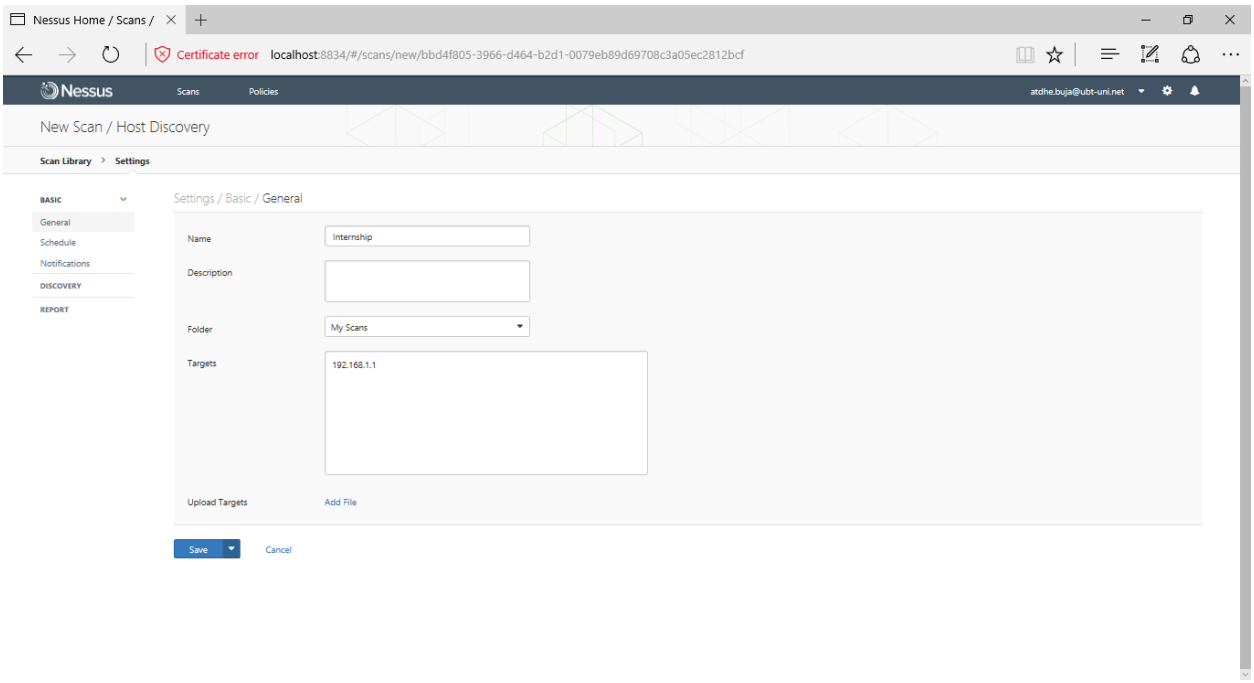


Figura 6

Rekomandim

- Pasi ka mundesi qe te ri-konfigurohen portet dhe mos te lihen default sipas programit, rekomandohet qe te behet gjithmone ky veprim, para se te nisim te bejme administrimin e pajisjeve, sistemeve kompjuterike dhe rrjetës.

Çka është Enumeration

Dy proceset meparshme “**Footprinting**” dhe “**Scanning Network**” kishin te benin me shume me mbledhjen e informatave per infrastrukturen dhe sistemet kompjuterike. **Enumeration** eshte procesi I trete dhe me i rendesishëm, permes te cilit provohet te merren te dhena per perdoruesit, emrat e makinave, informata te infrastruktures se rrjetes dhe sherbimeve (ang. services) nga sistemi kompjuterik.

Analiza e pare“I”

“**SuperScan**” mundëson skanimin, marrjen e të dhënave nga e gjithë rrjeta dhe paisjeve që gjenden në të, varësisht nga lloji që ne zgjedhin (Enumeration type).

Çka është System Hacking

“System Hacking” eshte nje shkence e testimit te sistemeve kompjuterike rrjetes dhe vete paisjeve kompjuterike per dobesit (ang.Vulnerabilities) qe mund te I kene si dhe perfshine mbledhjen e informacioneve per ate sistem.

Analiza e pare“I”

“**LCP-Link Control Protocol**” Duke perdorur kete vegel, mund te gjejme detajet per perdoruesit si: Emri përdoruesit, fjalëkalimi, gjatësia e fjalëkalimit dhe poashtu në vazhdimësi të procesit të kësaj vegle provon që përmes teknikave të ndryshme si Dictionary, Brute-force & hybrid sulmet të gjej fjalëkalimet në makinat e targetuara.Skenari i përdorur:

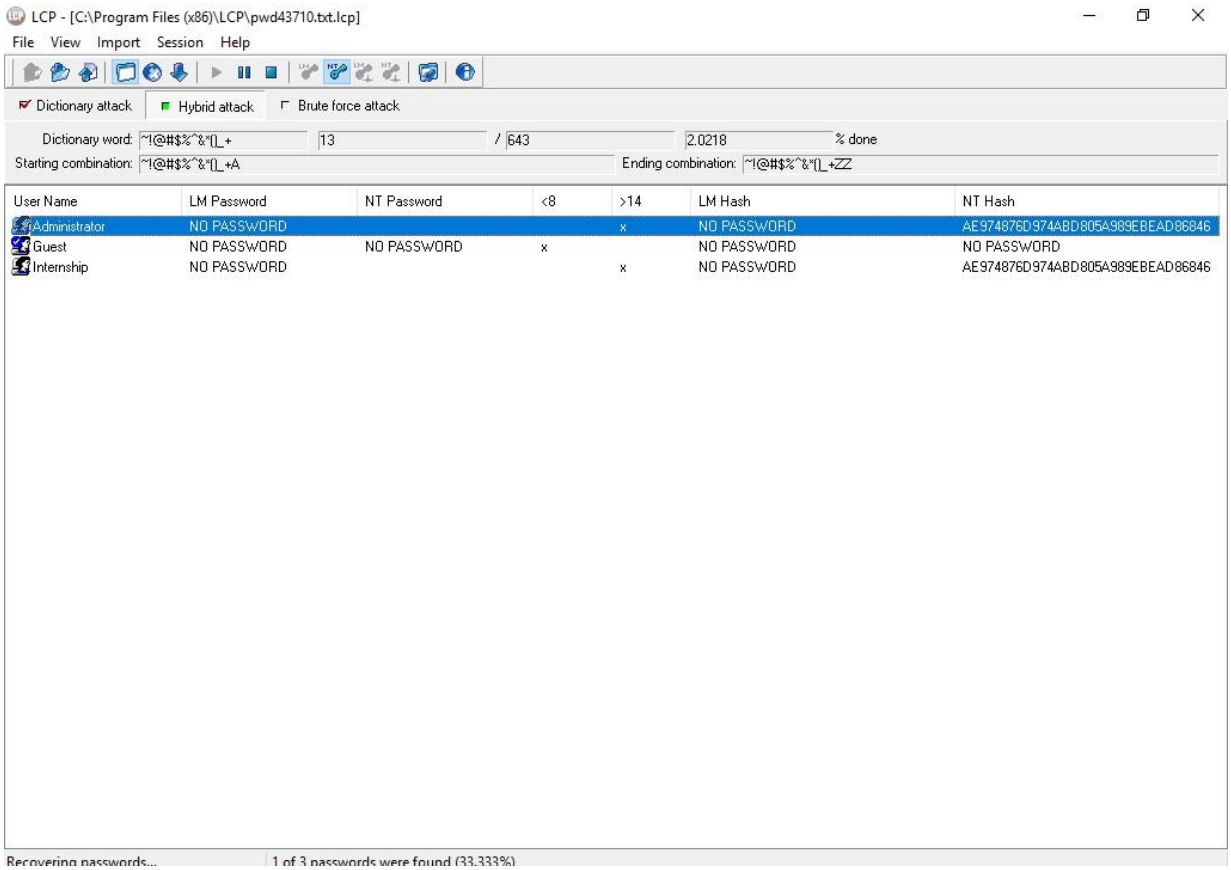


Figura 7

Analiza e dyte“II”

“**ADS Spy**” është një mjet që mund të përdoret për të kërkuar dhe hequr Rrjetat Alternative të të Dhënave (ADS) nga sistemet e skedarëve NTFS. Rrjedhjet alternative të të dhënave janë një mënyrë për të ruajtur meta-informacionin për skedarët pa ruajtur informacionin në skedarin që i përket, të bartur nga pajtueshmëria e hershme me MacOS nga Windows NT4. Kohët e fundit, rrëmbyesit dhe shfletuesit filluan të përdorin këtë teknikë për të ruajtur informacione të fshehura në sistem dhe madje edhe të ruajnë skedarët e ekzekutueshëm trojanë në rrjedhat ADS të skedarëve të rastësishëm në sistem. Përdorni me kujdes.

Skenari I perdorur:

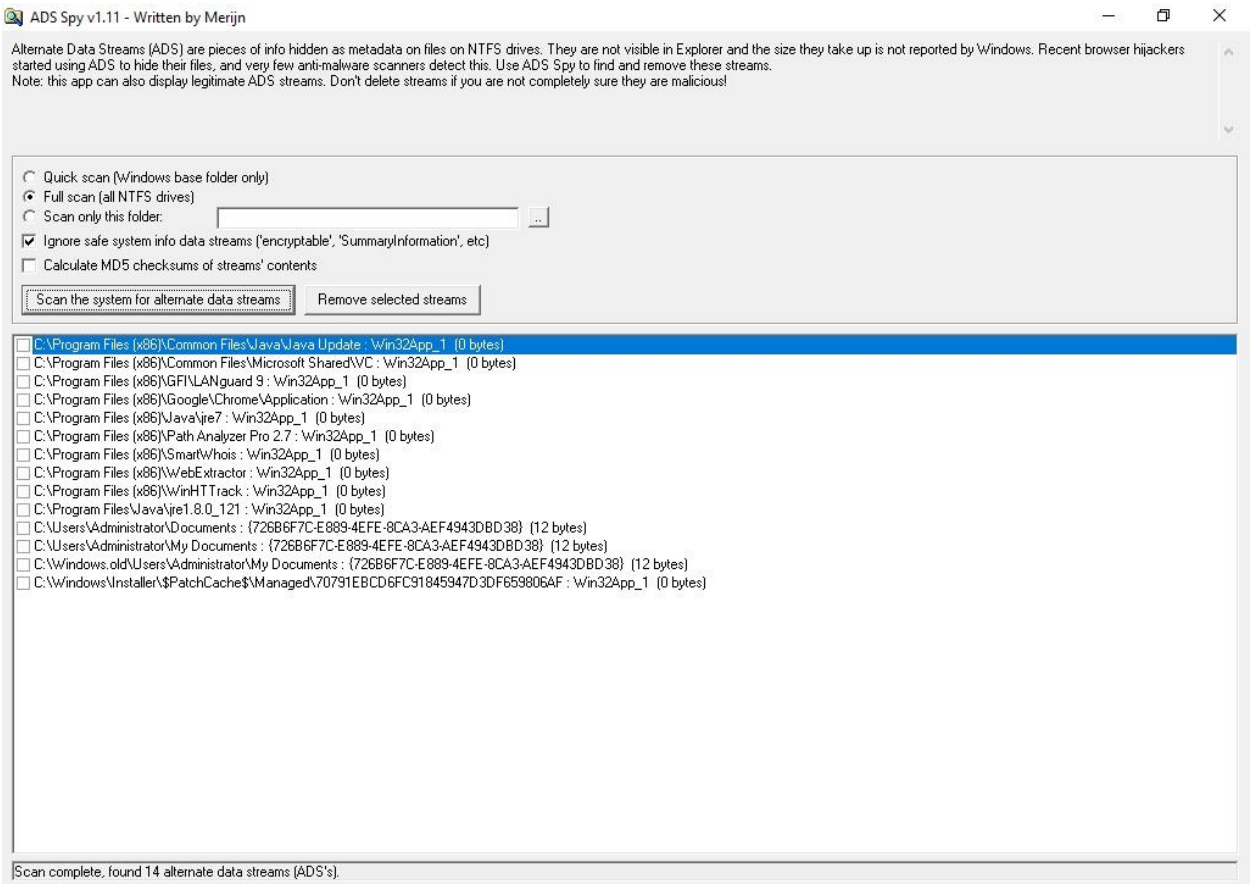


Figura 8

Analiza e trete“III”

“**Stealth**” vegla përdor procesin e njëjtë të Steganografisë që çdo skedar që maskohet brenda një skedari. Aplikacioni, i quajtur Stealth, ndihmon kontrollin e atyre që shohin atë në një rrjet, duke u lejuar menaxherëve të autorizojnë një grup njerëzish për qasje në informacione, aplikacione ose pjesë të një rrjeti të caktuar, që ata që veprojnë jashtë një grupi pune të caktuar nuk janë në gjendje të shohin.

Skenari i perdorur:

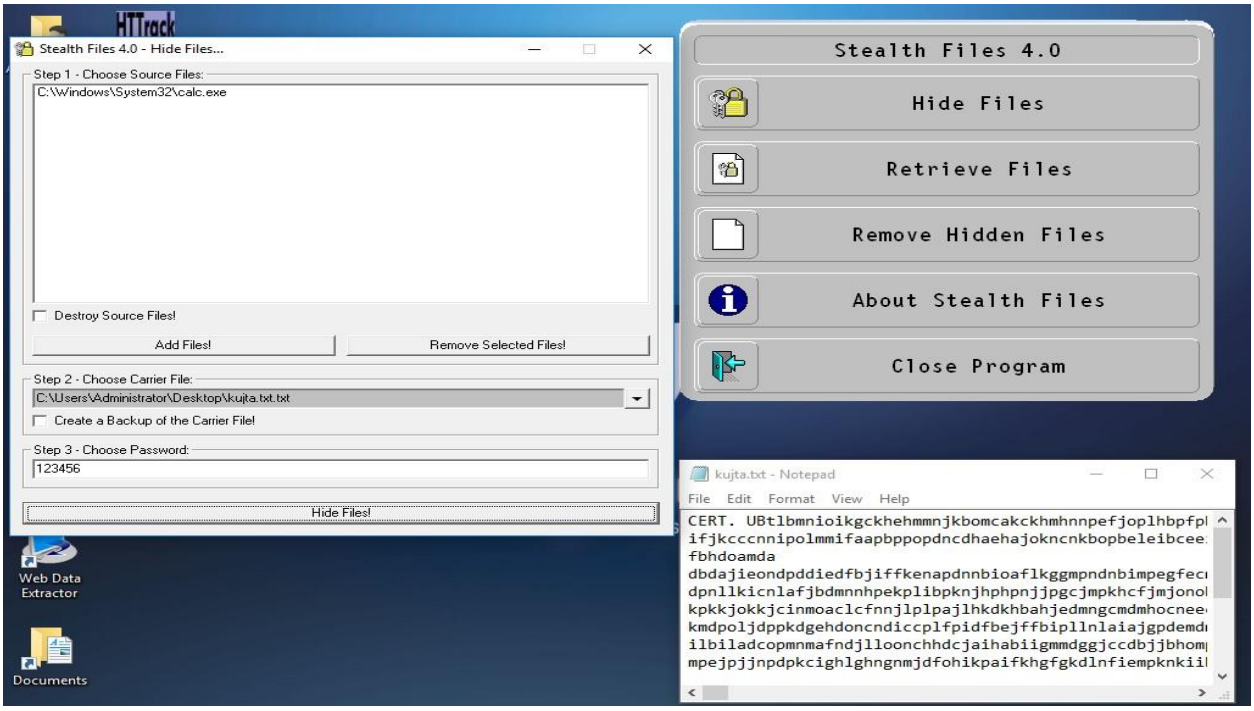


Figura 9

Stealth Retrieve procesi, në figurën mëposhtme:

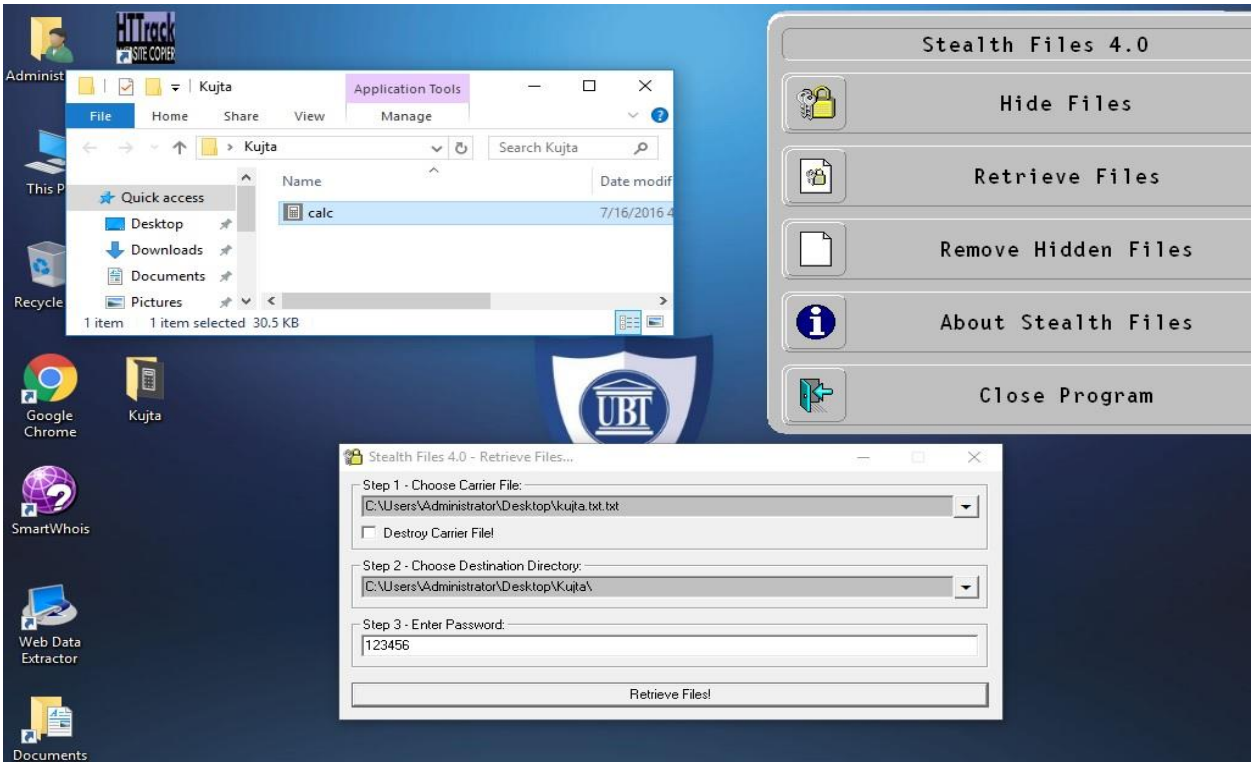


Figura 10

Rekomandim

- Gjithmonë duhet pasur kujdes kur të pranojmë apo hapim skedar në kompjuter, për shkak që përdorimi i sulmeve bazuar në konceptin e Steganografisë mund të rrezikoj gjithë sistemin kompjuterik. Rekomandohet verifikimi i llojit, madhësisë, përmbajtjet së skedarit.

Analiza e katert“IV”

“**AuditPol**” paraqet komandën në sistemin operativ Windows Server që lejon ndryshimin ose ri-konfigurimin e politikave të auditimit të kompjuterit (deaktivizimi i ruajtjes së gjurmëve).

Çka është Trojans and Backdoors

Kali trojan, apo **Trojan**, është çdo program me qëllim të keq për kompjuter që është përdoret për të hyrë në një kompjuter duke mashtruar përdoruesit për qëllimin të saj të vërtetë. Trojanë janë përgjithësisht të përhapur nga ndonjë formë e inxhinierisë sociale, për shembull kur një përdorues është mashtruar në ekzekutimin e një shtojce të e-mail-it të maskuar për të qenë jo i dyshimtë.

Backdoor.Trojan është një emër zbulimi i përdorur nga Symantec për të identifikuar programe softuerësh keqdashës që ndajnë funksionin primar të mundësimit të një sulmuesi të largët që të ketë qasje në ose të dërgojë komanda në një kompjuter të kompromet uar.

Analiza e pare “I”

“**TCPview**” program që në mënyrë detaje tregon gjitha informacionet për proceset, protokolet, adresat lokale dhe ato nga largësia, gjendja e koneksionit TCP deri te pajisja e fundme.

Kur të filloni TCPView ajo do të rendisë të gjitha pikat e drejtpërdrejta TCP dhe UDP, duke zgjidhur të gjitha adresat IP në versionet e emrave të tyre të domain.

Skenari I perdorur:

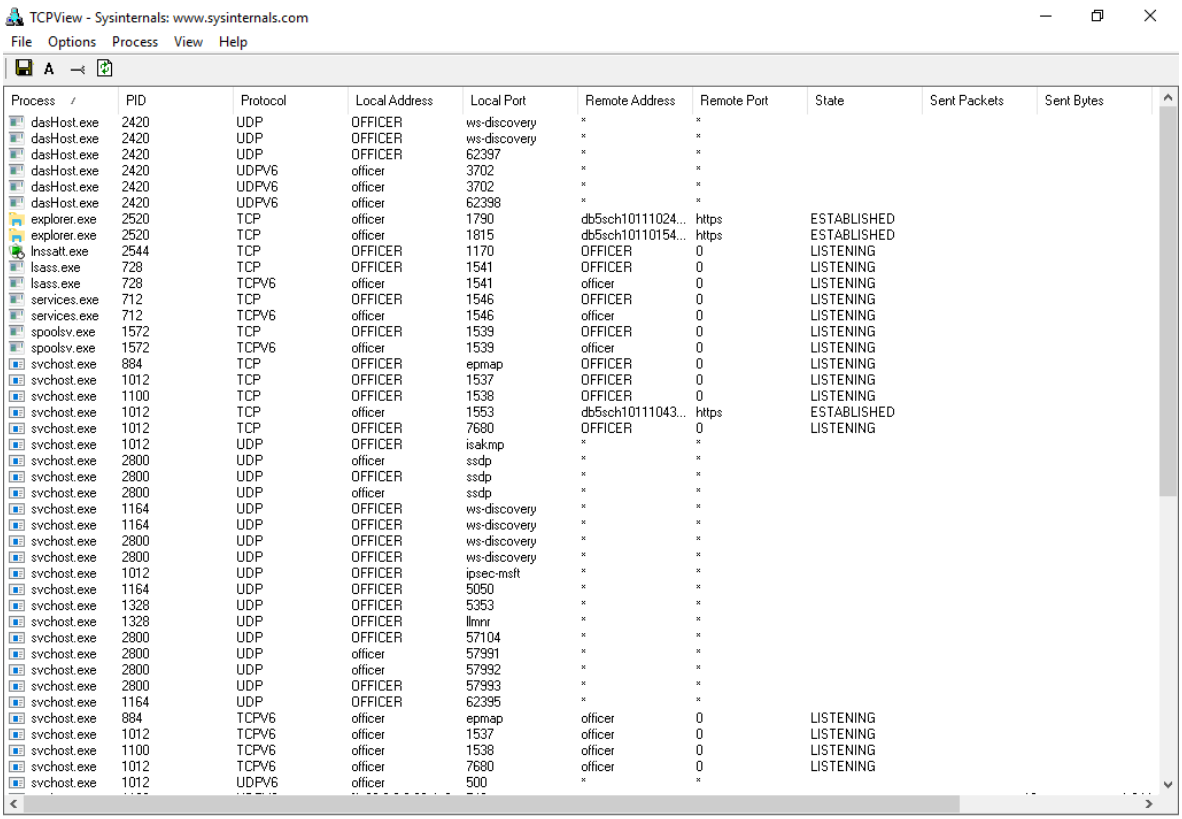


Figura 11

Analiza e dyte “II”

“**Autoruns**” njëjtë sikurse TCPView edhe kjo vegël përdor logjikën e identifikimit të informacioneve por për makinat lokale dmth nuk jep mundësi të zbulimit të informacioneve nga largësia.
Ky program, i cili ka njohuritë më të hollësishme për vendndodhjet e nisjes automatike të çdo monitori të nisjes, ju tregon se cilat janë programet e konfiguruara për tu hapur gjatë ndezjes së sistemit ose login, dhe kur nisni aplikacione të ndryshme të Windows-it. Pasqyra përmbledhëse tregon qartë si nga pjesa hardware poashtu edhe software me detajet për proceset që zhvillohen brenda një kompjuteri.

Skenari i perdorur:

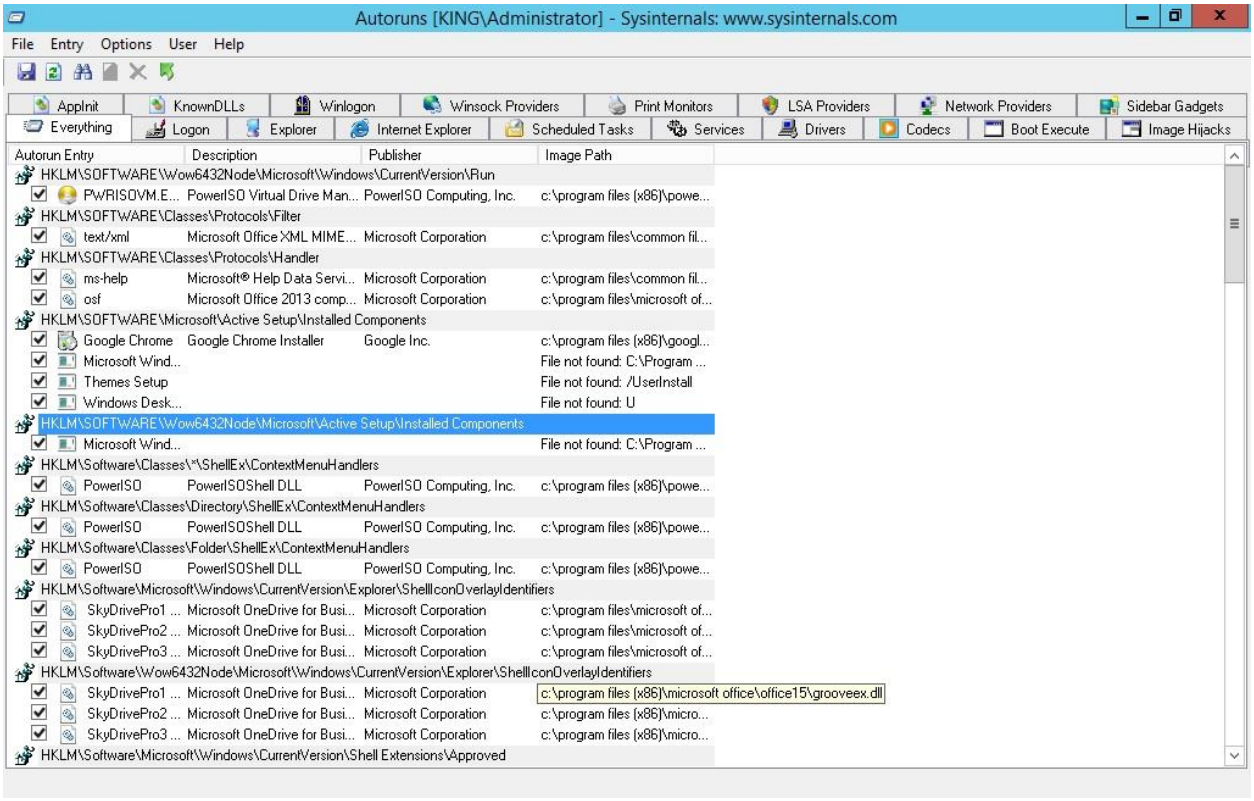


Figura 12

Analiza e trete “III”

JV 16

Skenari I perdorur:

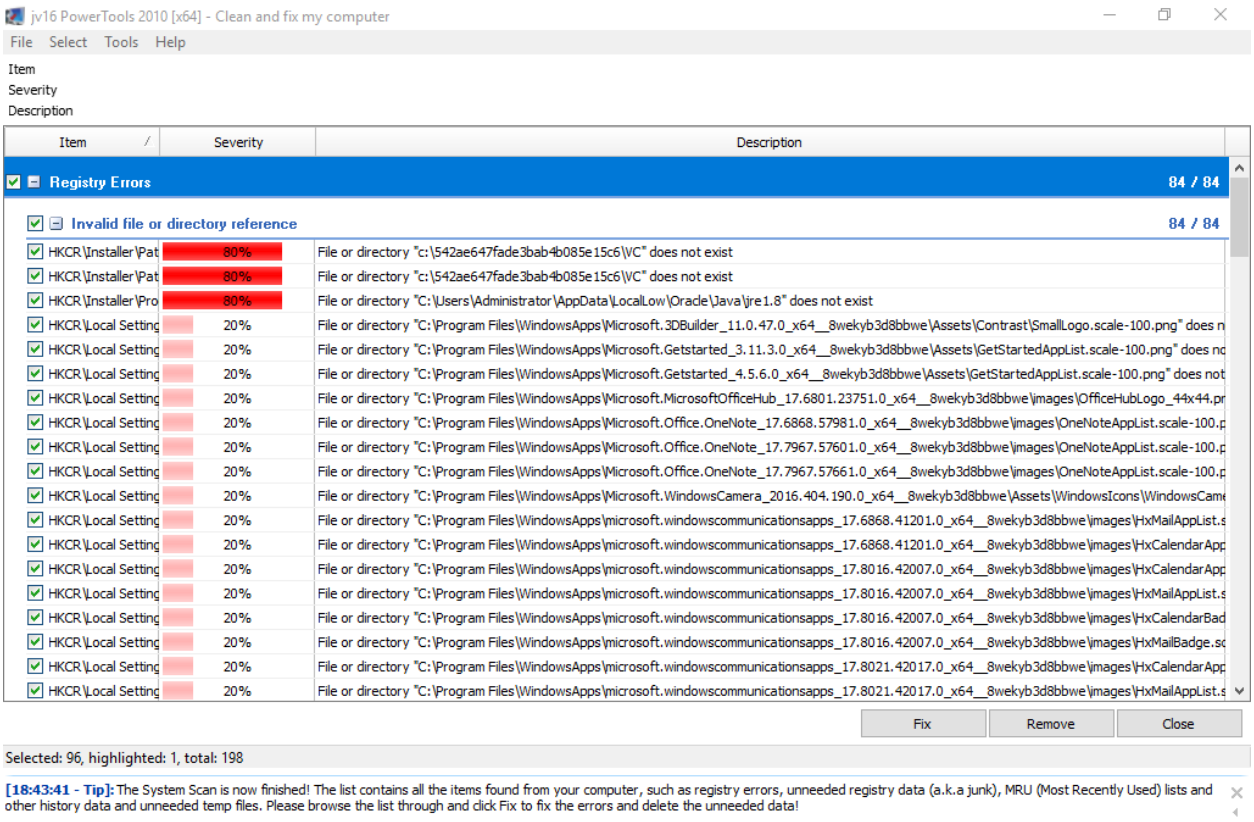


Figura 13

Rekomandim

- Rekomandohet që të planifikohet dhe realizohet një monitorim i mirëfilltë i të gjitha proceseve që ndodhin në rrjetë dhe pajisje kompjuterike, vetëm në këtë mënyrë mund të ndalojmë një Trojan që zhvillohet brenda një procesi të dyshimtë.

Çka është Viruses and Worms

Virusi eshte program I vet-replikueshem qe prodhon kodin e vet duke u kopjuar ne kode te tjera te ekzekutueshme dhe eshte I demshem per sistemin kompjuterik, ndersa ekzekutimi I kodit te Worms-it ka mundesi te infektimit te shume paisjeve te tjera d.m.th shpërndahet.

Analiza e pare “I”

“**Virus Maker**” në një ambient testues dhe të mbyllur është përdorur kjo vegël me qëllim të krijimit të kodit të virusit, i cili të jep mundësi të ndryshme dhe të avancuara të infektimit, ndryshimit të konfigurimeve të kompjuterit dhe sistemit kompjuterik.

Skenari I perdorur:

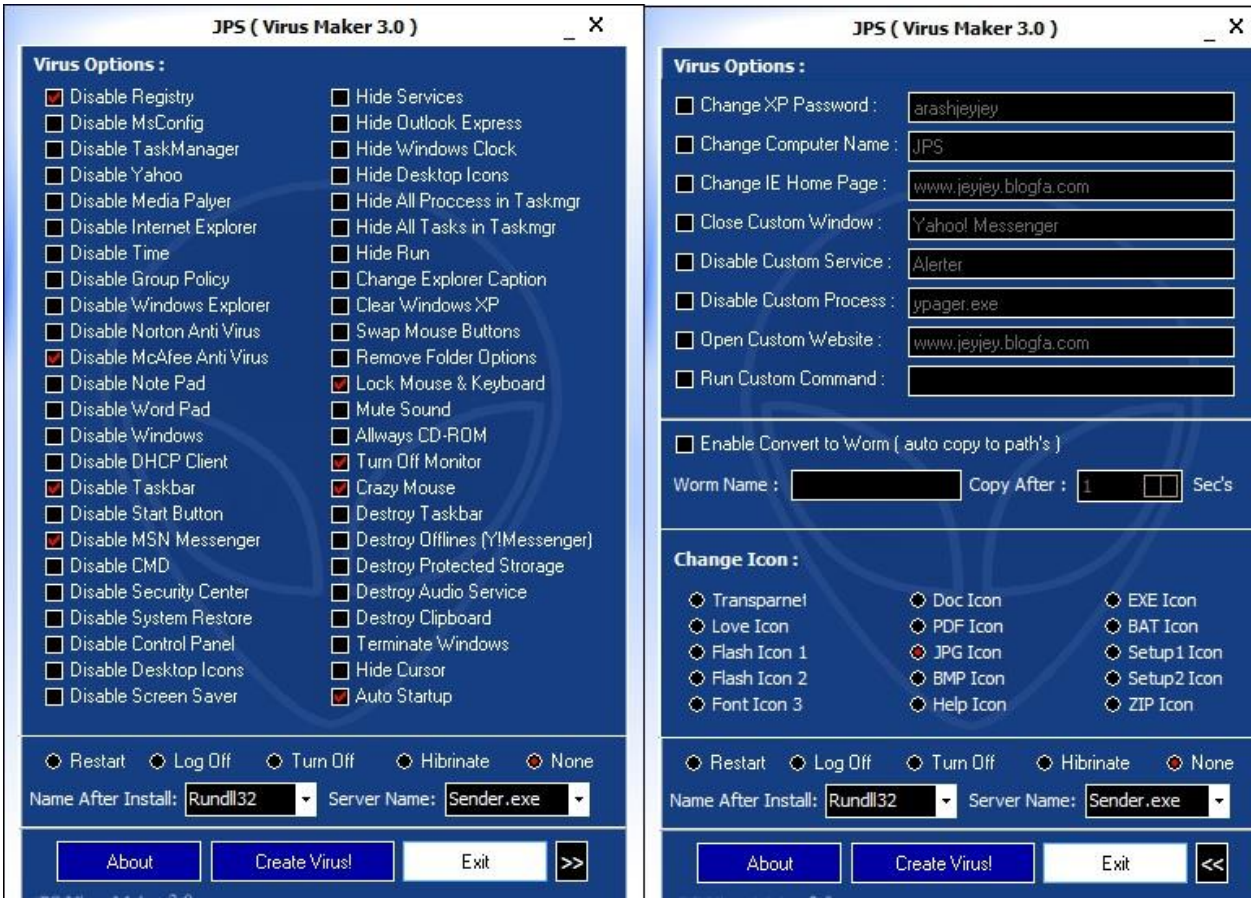


Figura 14

Rekomandim

- Përdorimi i Antivirusit dhe të jemi të sigurtë që gjithmonë është funksional dhe i pajisur me verzionin e fundit (up-to-date).

Çka është Sniffers

"**Sniffers**" apo pergjuesit jane lloje te programeve apo pajisje harduer-ke qe monitorojne cdo bit te informates, qe hyn ose del nga rrjeti kompjuterik.

Analiza e pare "I"

"TheDude"

Skenari I perdorur:

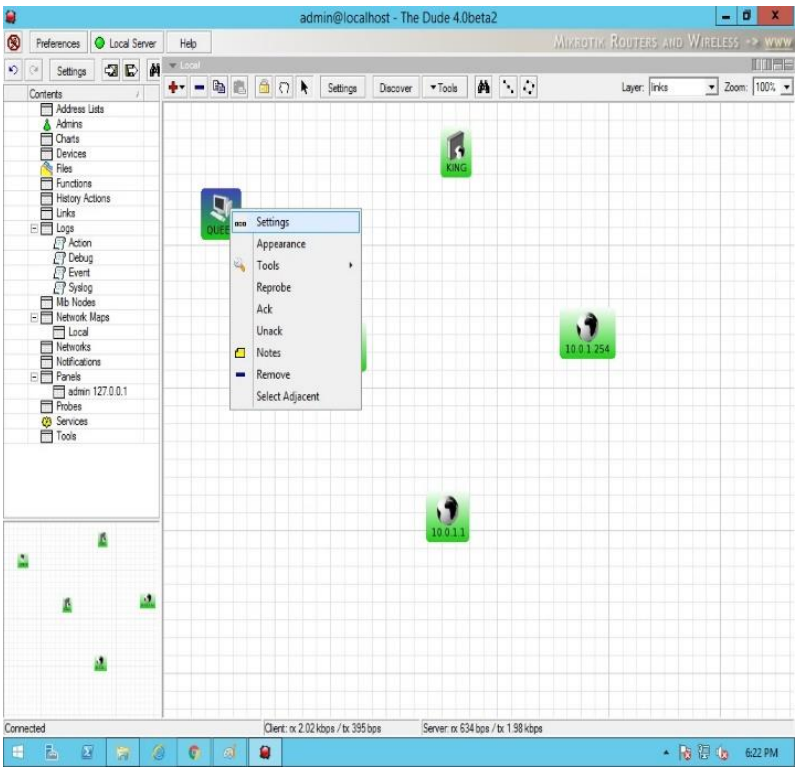


Figura 15

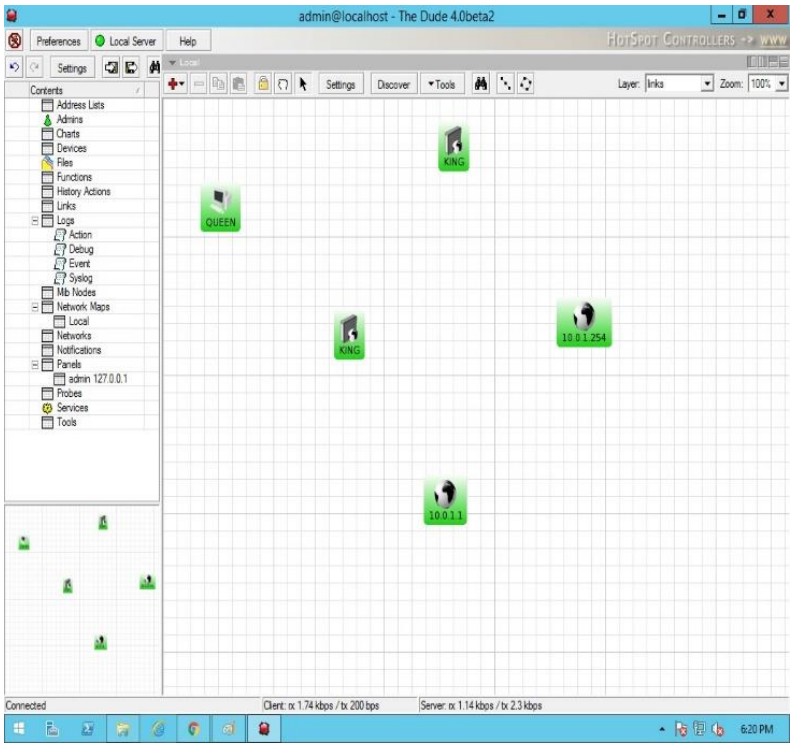


Figura 16

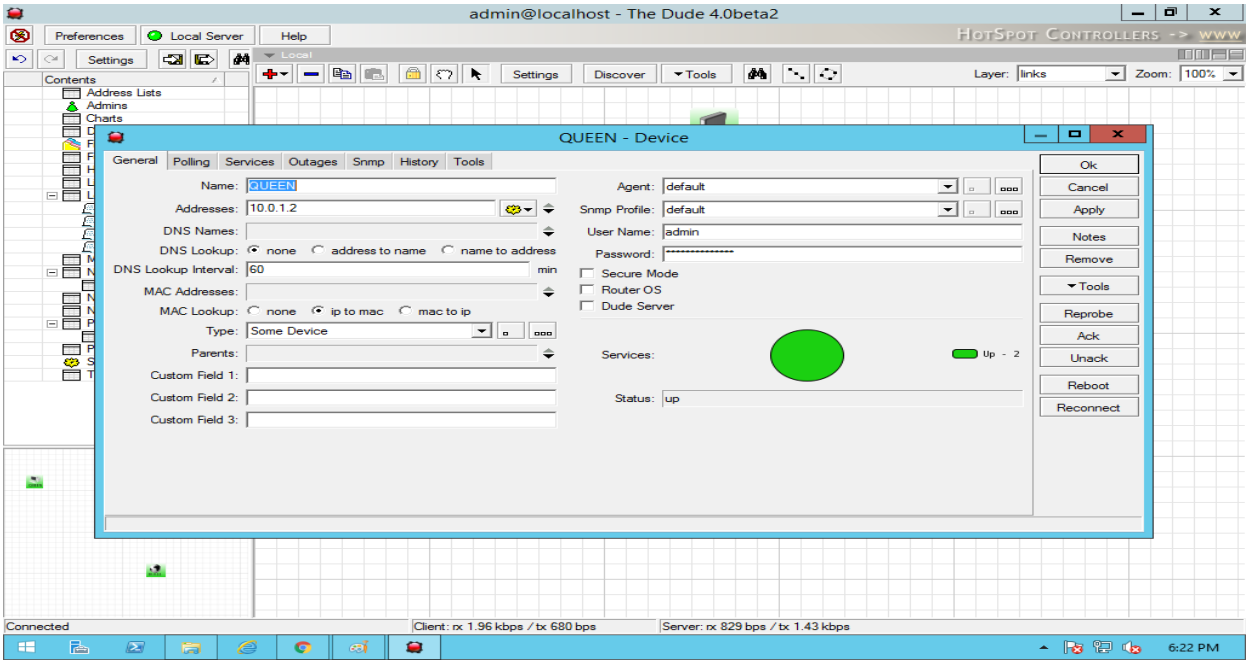

admin@localhost - The Dude 4.0beta2
Preferences
Local Server
Help
HotSpot Controllers -> www
Settings
Discover
Tools
Layer: links
Zoom: 100%
Contents
Address Lists
Admins
Charts
QUEEN - Device
General
Polling
Services
Outages
Snmp
History
Tools
Name: QUEEN
Addresses: 10.0.1.2
DNS Names:
DNS Lookup: none address to name name to address
DNS Lookup Interval: 60 min
MAC Addresses:
MAC Lookup: none ip to mac mac to ip
Type: Some Device
Parents:
Custom Field 1:
Custom Field 2:
Custom Field 3:
Agent: default
Snmp Profile: default
User Name: admin
Password:
Secure Mode
Router OS
Dude Server
Services:
Up - 2
Status: up
Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
Reconnect
Connected
Client: rx 1.96 kbps / tx 680 bps
Server: rx 829 bps / tx 1.43 kbps
6:22 PM

Figura 17

Analiza e dyte “II”

“**WireShark**”

Skenari I perdorur:

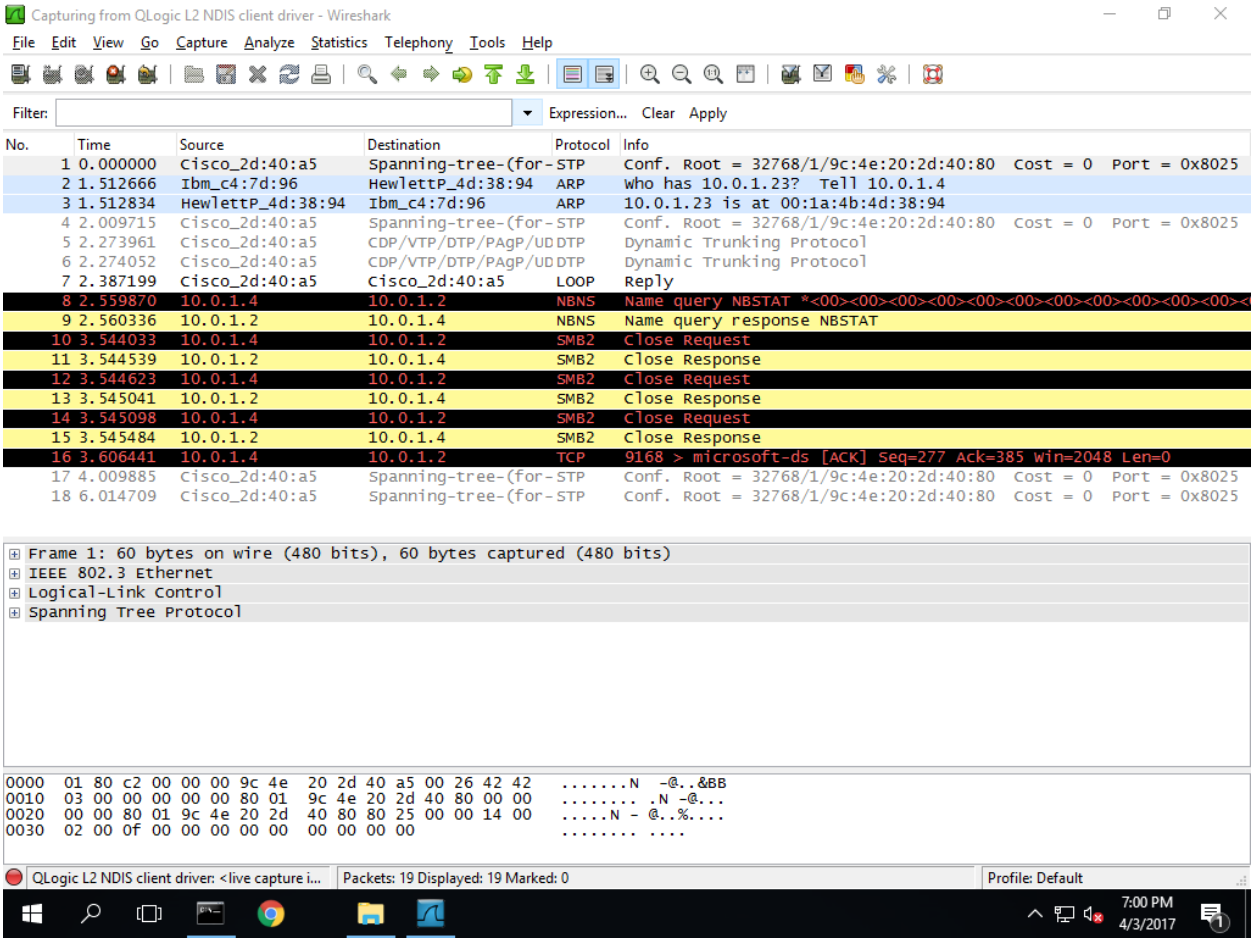


Figura 18

Çka është Social Engineering

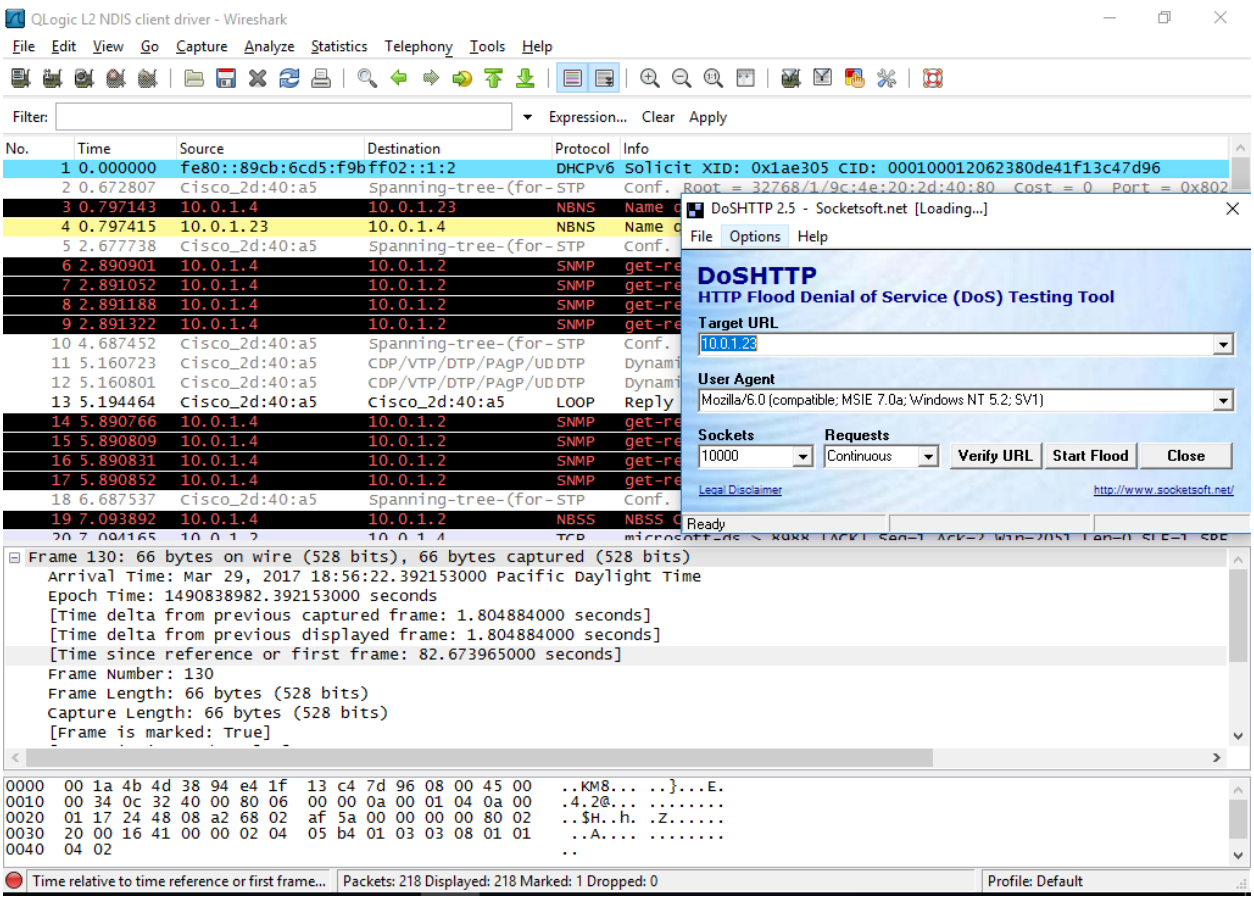
Social Engineering apo Arti I te Bindurit te Njerzeve per te zbuluar informata konfidenciale. Eshte nje metode me ane te se ciles nje haker mund te mbledhe te dhena rreth objektivit te tij per te realizuar sulmin. Ketu kemi te bejme me mashtrime nga hakeret, vjedhjen e identitetit, spiunazhi etj.

Rekomandim

- Trajnime te stafit per vetedijesim te politikave te sigurise, por dhe individualisht duhet të kemi kujdes gjatë bisedave më të tjerët për çështjet e ndieshme të infrastrukturës që menaxhojmë ose jemi vetëm përdorues të saj.

Çka është DoS, DDoS

DoS (Denial of service) dhe **DDoS** (Distribute DOS) jane lloje te sulmeve, qe kane per qellim largimin nga funksioni të sistemeve, pajisjeve dhe rrjetat kompjuterike. Logjika e këtyre sulmeve funksionin duke



bërë dërgimin e numrit të madhë të paketave në rrjetë gjë që të cilën disa sisteme apo pajisje nuk mund të i përballojnë dhe dalin nga funksioni.

Skenari I perdorur:

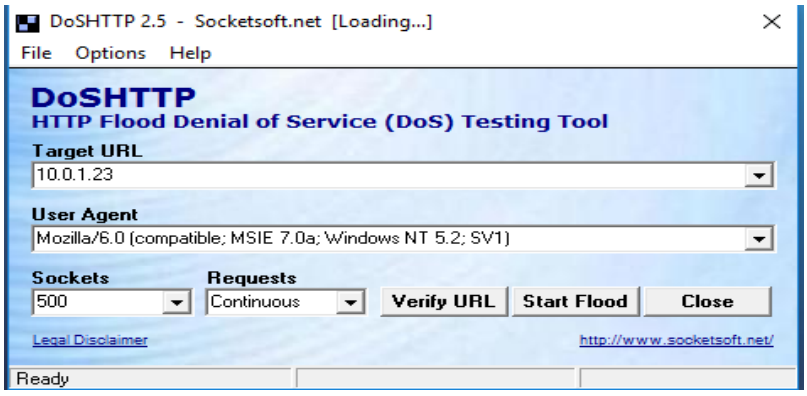


Figura 19