UBT-CERT Internship

Java e parë dhe e dytë

Simulimi dhe testimi në rrjetë, aplikacione dhe sisteme

18 Prill 2017

Përgatitur nga studentët e SHKI/UBT: Sherif Maliqi student I vitit të II

Kujtim Morina student I vitit të I

Blerona Cakolli studente e vitit të III

Edi Bushati student i vitit të II

Ndihmës: Atdhe Buja CERT manager

Përmbajtja

Hyrje

Ky dokument është përgatitur me qëllim që të vetëdijsoj të gjithë ata qe jane te angazhuar ne fushen e TIK-ut dhe I dedikohet komunitetit te TIK-ut.

Përmirëson nivelin e sigurise te sistemeve kompjuterike te nje kompanie ose organizate, ndihmon perdoruesit e ketyre sistemeve per shfrytezim sa me te sigurt te tyre.

Koncepti etik (Defense cyber security)

Ky dokument pasqyron aspektin etik apo mbrojtës, duke identifikuar dobësit (ang. Vulnerabilities), verifikimin e funksionimit normal të mekanizmave të sigurisë dhe testimin e sistemeve kompjuterike dhe rrjetës, përmes përdorimit të veglave apo programeve të ndryshme.

Çka është "footprinting"

Ky proces "footprinting" i referohet funksioneve të zbulimit dhe mbledhjes të sa më shumë informatave për një target të caktuar në rrjetë p.sh. institucion publik, privat, akademik ose kompani. Si rezultat I këtij procesi "footprinting" ne krijojmë në mendjen tonë një skemë vizuale të arkitekturës së sistemeve të informacionit, përdoruesve dhe grupeve, sistemit mbrojtës (ang.Firewall) dhe aseteve të tjera të Teknologjisë së Informacionit (TI-së).

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 ne 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:

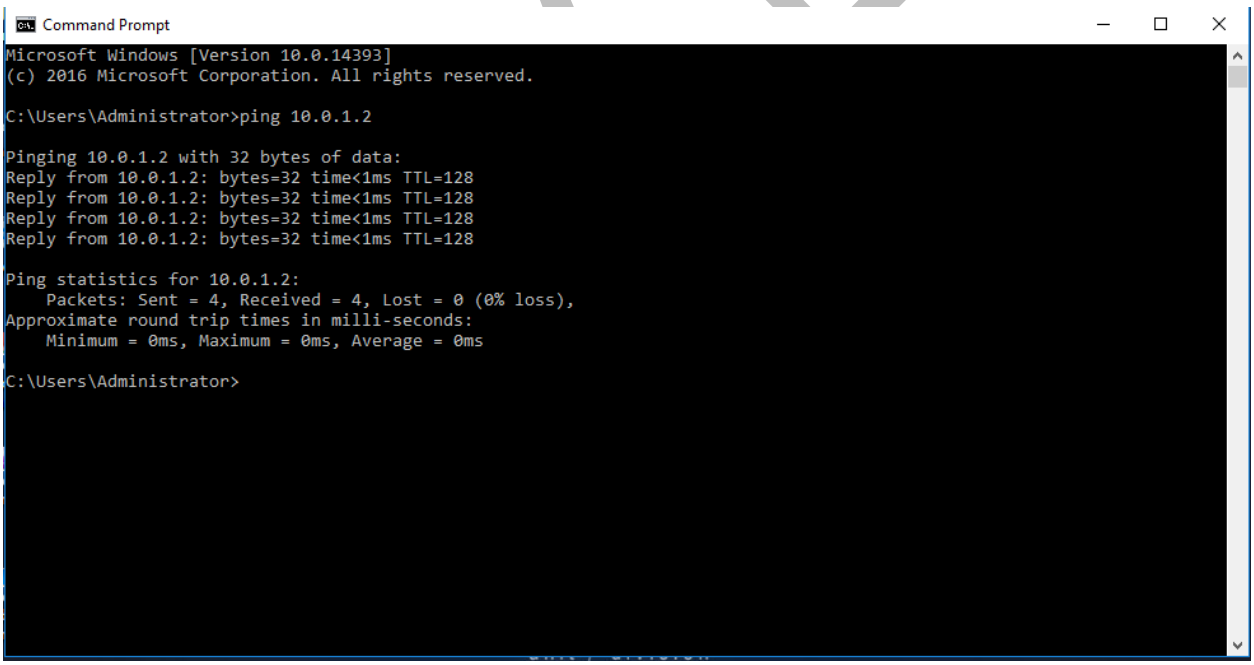


Figura 1

Rekomandim

- Është mirë që çdo herë në infrastrukturë d.m.th 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**” është shumë I përdorshëm na lejon të lexojmë të gjitha informatat e mundshme për një IP adresë, hostname ose domain. Duke përfshirë informacionet 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:

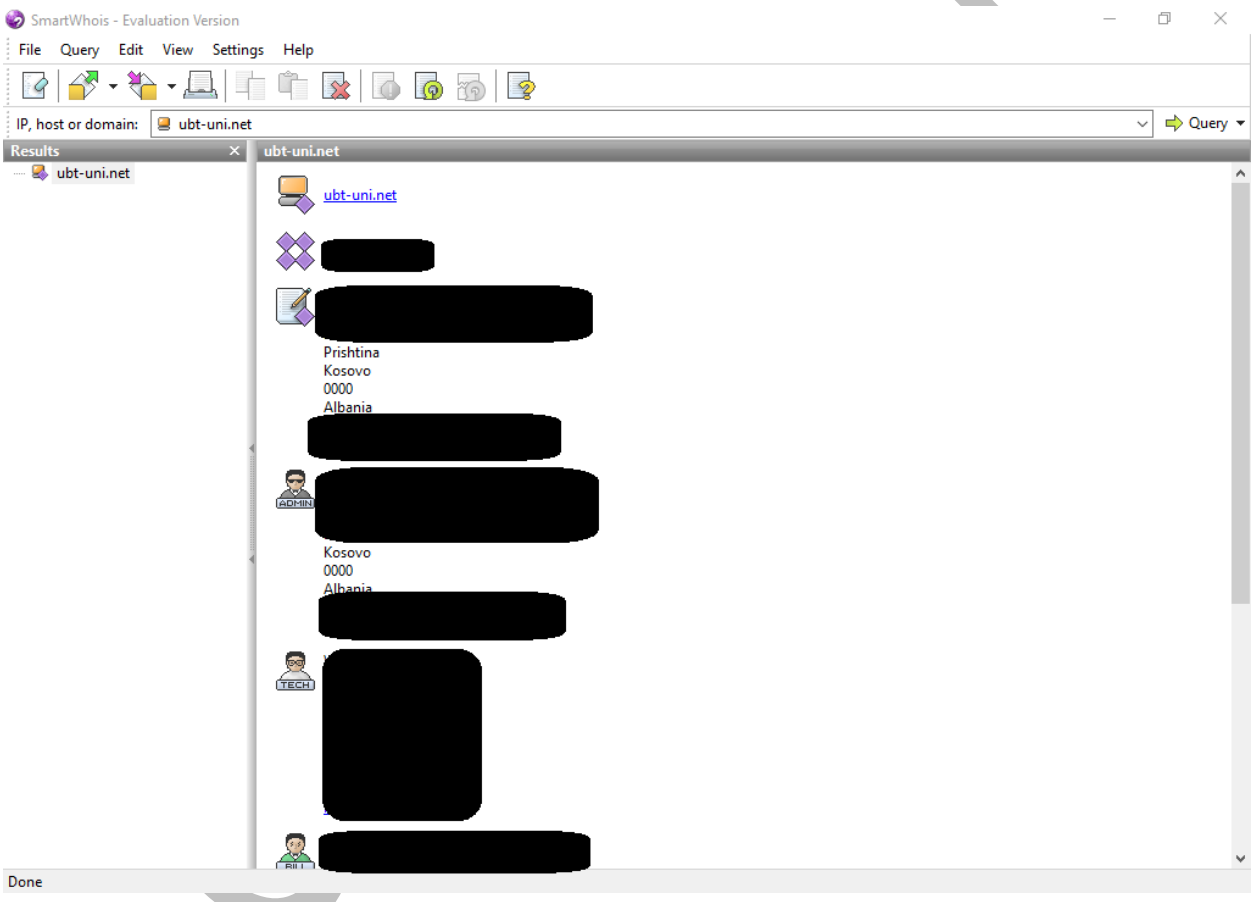


Figura 2

Aplikacioni “**EmailTracker**” përdoret për qëllim të analizës së email header-it që të bëhet I ditur lokacioni I vërtetë I dërguesit. Por dhe na jep informacione të tjera të rëndësishme, si në vijim:

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

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

Skenari I përdorur:

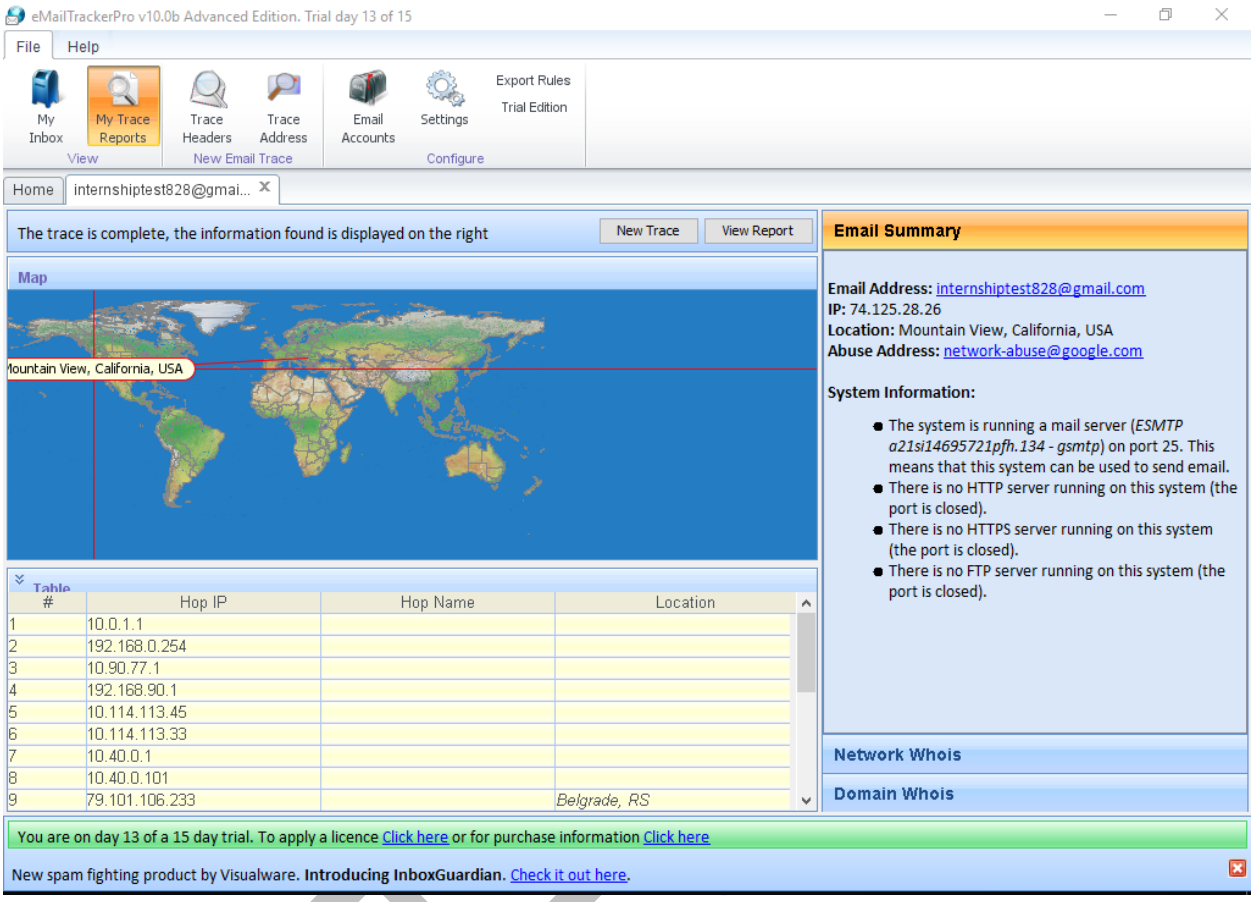


Figura 3

Rekomandim

- Në momentin që planifikoni blerjen e ndonjë domain për përdorim rekomandohet që të jemi të sigurtë që informacionet e ndieshme të mos bëhen publike nga Provider i domain që bleni. Në shumicën e provider ofrohet një pagesë ekstra për ruajtjen e fshehtësisë së të dhënave të ndieshme për domain-in tuaj ose pronarin e saj.

Çka është Scanning Network

"**Scanning Network**" eshte process qe I referohet nje grupi te procedurave per identifikimin e hosts, porteve dhe sherbimeve qe funksionojne ne rrjete. Skanimi I rrjetes ka per qellim kontrollin e sistemeve kompjuterike qe perdoren, porteve te hapura dhe mbledhjen e informatave me detaje per sistemin operativ, dobesive ne infrastrukturen e rrjetes etj.

Analiza e pare "I"

"**IP scanner**" mundësohet nga shumë vegëla që gjenden në internet pa pagesë, me qëllim që të marrim lloje të ndryshme të informacioneve në lidhje me kompjuterët në rrjetën lokale.

Skenari I përdorur:

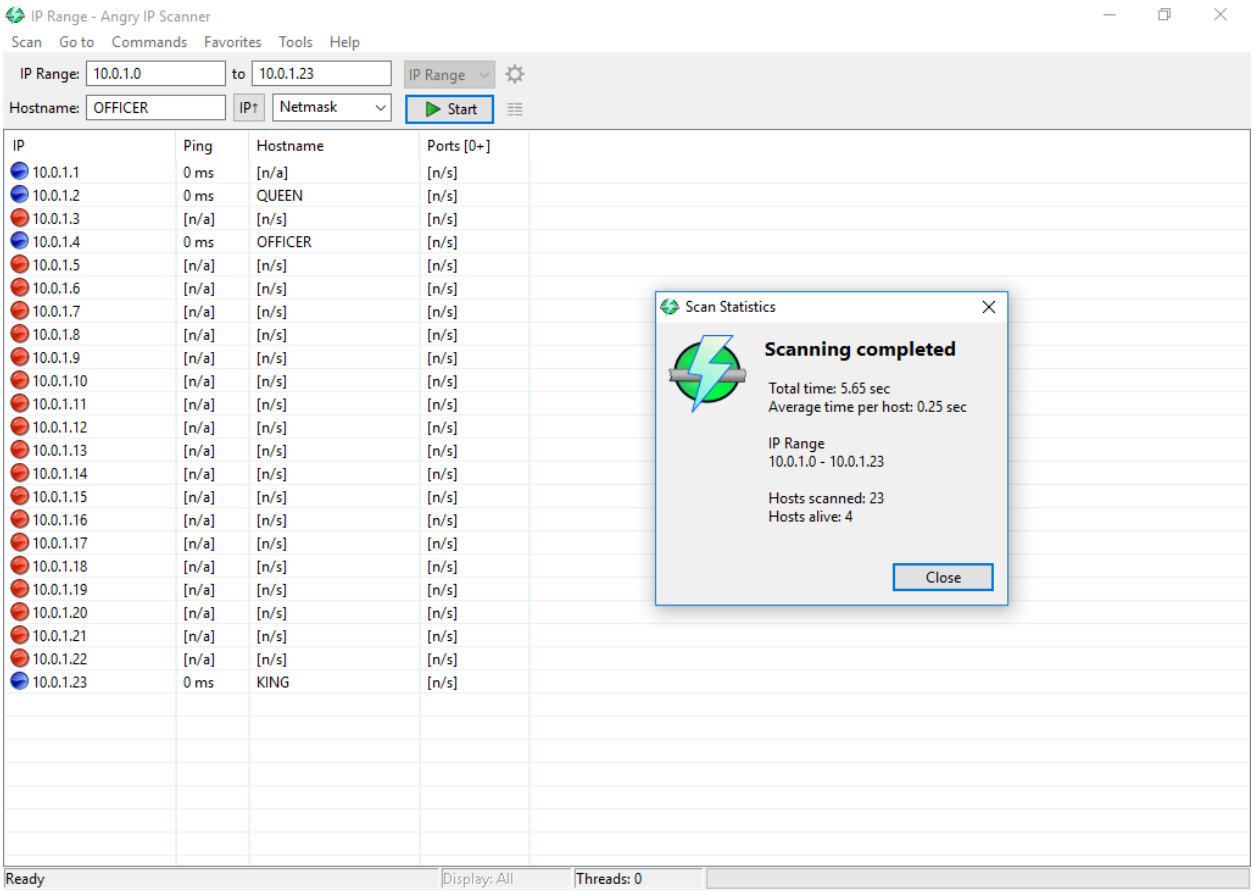


Figura 4

Analiza e dytë “II”

“**Friendly pinger**” është një aplikacion lehtë i përdorshëm për administrimin, monitorimin dhe inventarizimin e rrjetës dhe paijisjeve të tjera të TI-së.

Skenari I përdorur:

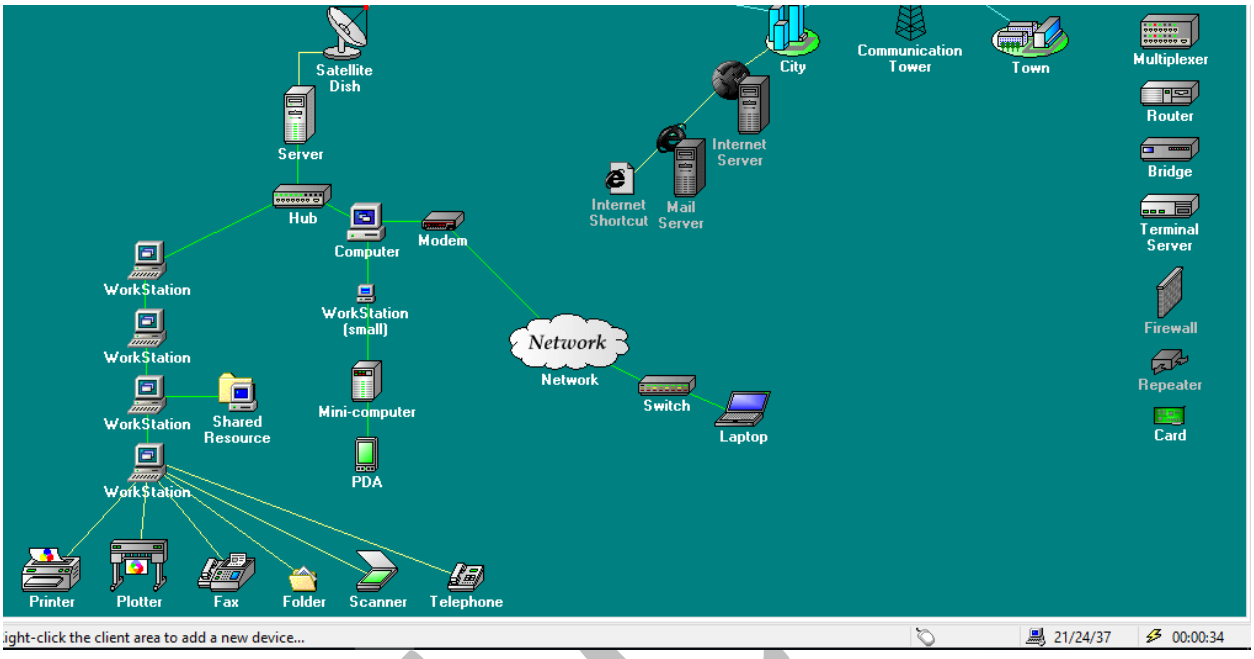


Figura 5

Analiza e trete “III”

“**Nessus**” paraqet një platformë të tërë dhe shumë të avancuar që ju lejon auditim të rrjetës nga largësia për që kuptuar nëse është prishur apo keqpërdor. Ka mundësi për auditim lokal në makina specifike për identifikimin e dobësive (ang. Vulnerabilities).

Skenari I përdorur:

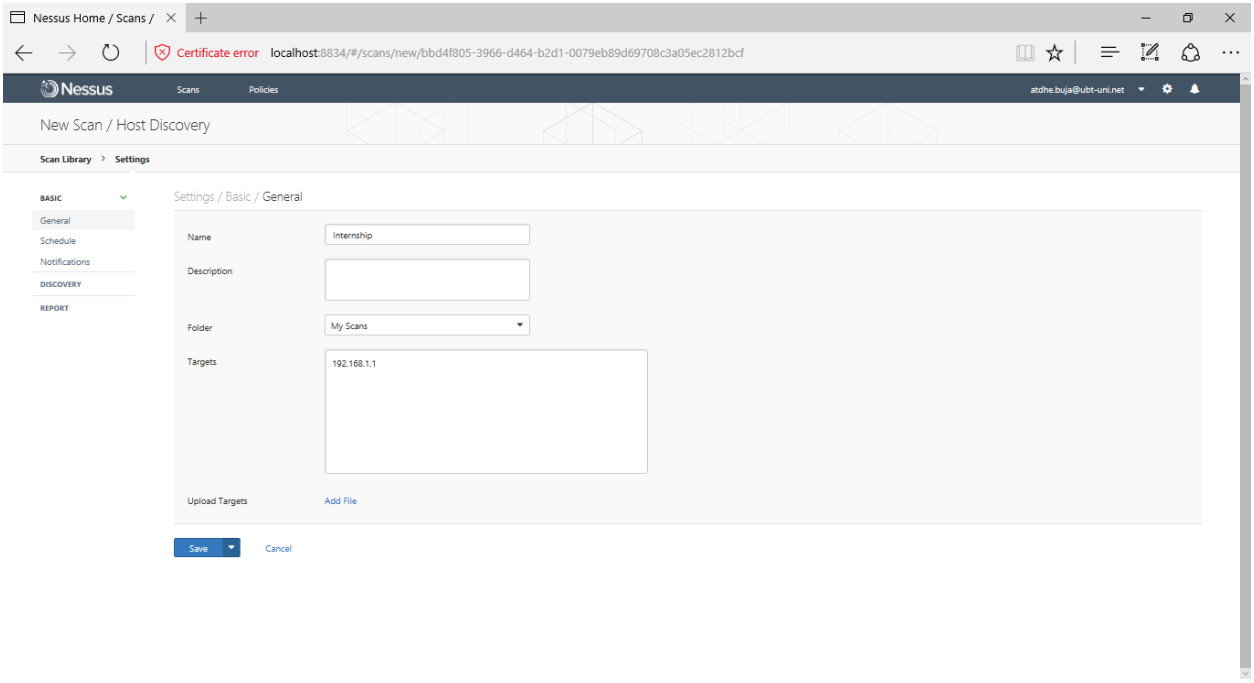


Figura 6

Rekomandim

- Duhet pasur kujdes kur jemi tek administrimi i pajisjeve, sistemeve kompjuterike dhe rrjetës që sa më pak të përdorim portet by default që vijnë të konfiguruara nga prodhuesit. Ka mundësi teknike që kjo të ri-konfigurohet nga vetë ne dhe rekomandohet që të bëhet gjithmonë.

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). Për më shumë shihni figurën në vazhdim.

Skenari I përdorur:

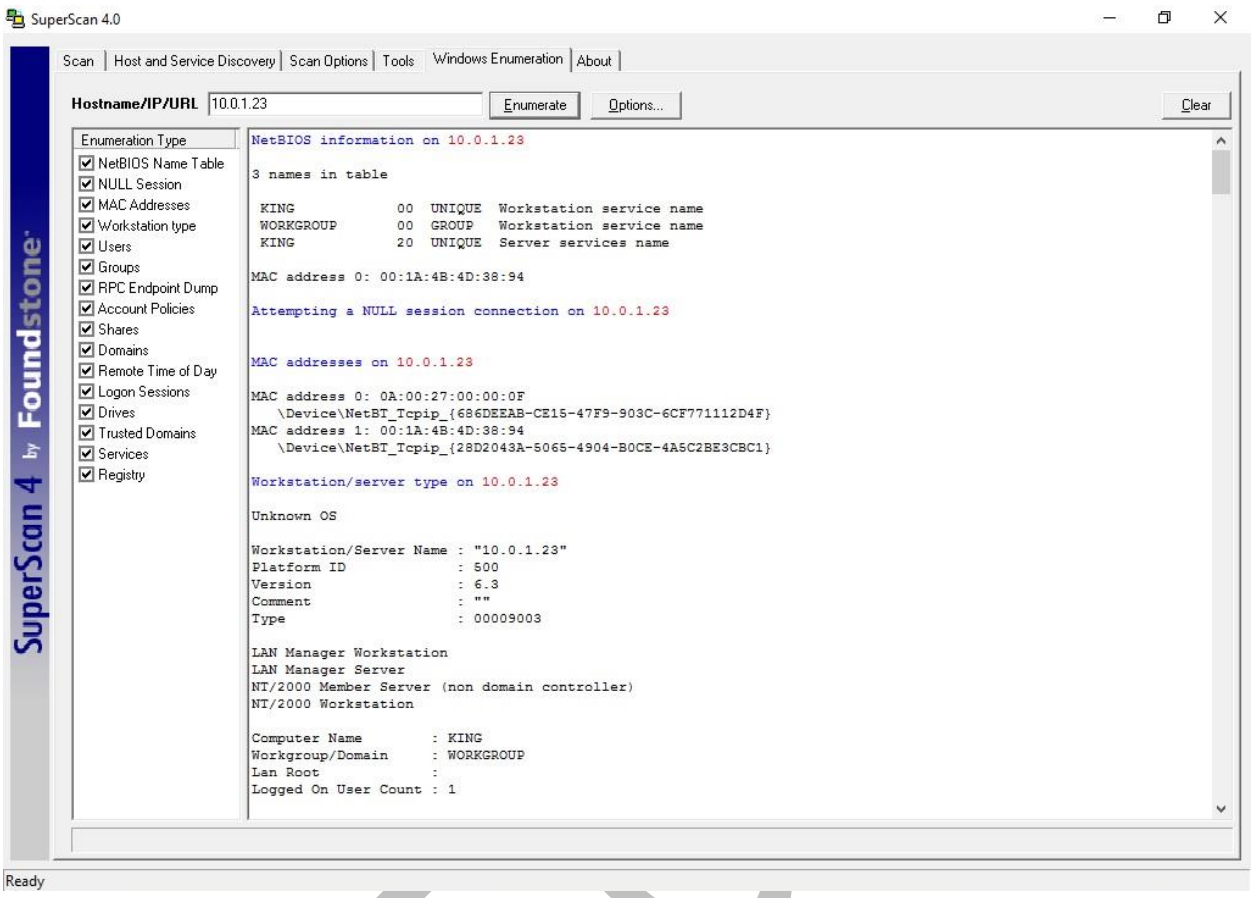


Figura 7

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.

Analiza e pare"I"

"**LCP- Link Control Protocol**" përdorimi i kësaj vegle ka dhënë rezultate interesante për përdoruesit dhe detajet për ta si psh. 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:

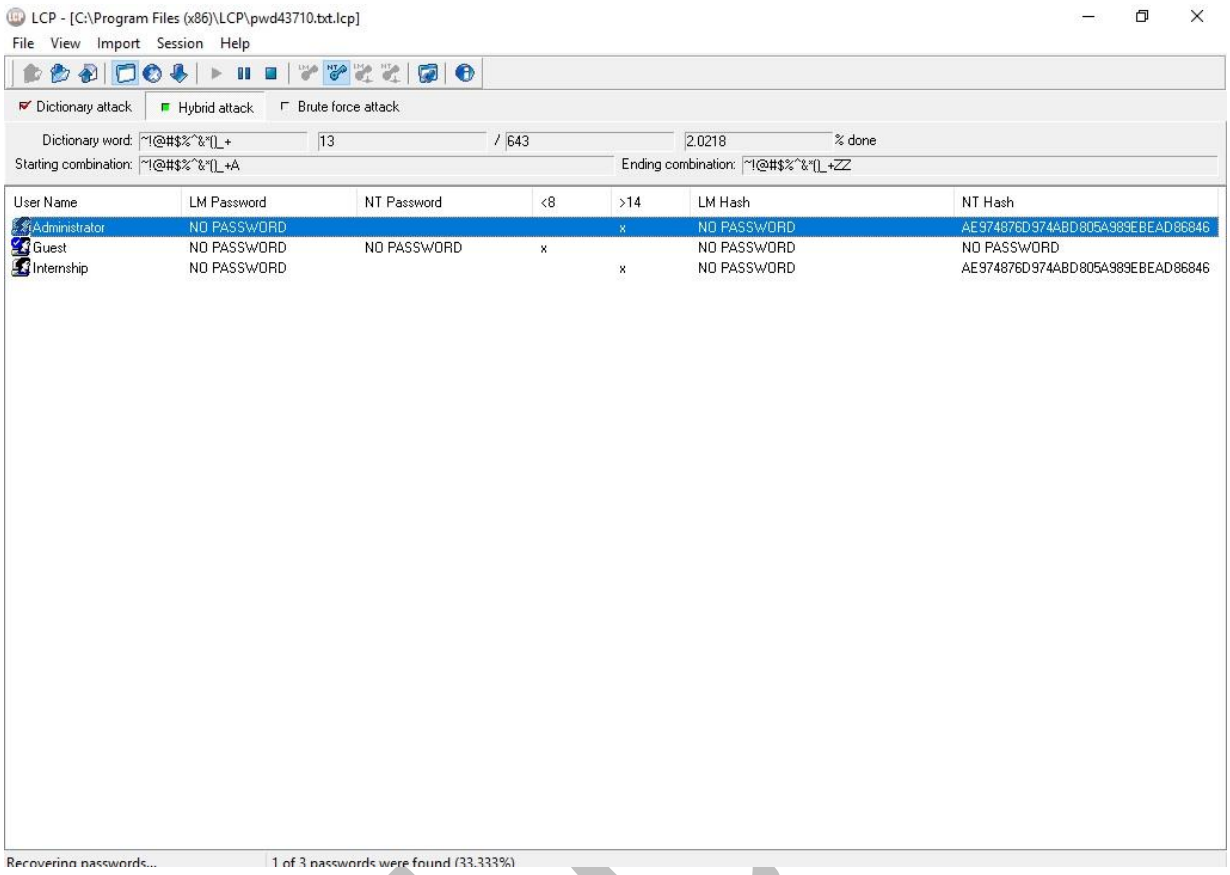


Figura 8

Analiza e dyte“II”

“**ADS Spy**” kjo vegël përmes Alternate Data Stream tregon disa pjesë të vogëla të fshehura si metadata në skedar më saktë disqet NTFS. Përmes gjenerimit të pasqyrës përmbledhëse të këtyre informacioneve, kjo vegël të mundëson identifikimin dhe largimin e streams të dyshimtë “malicious”.

Skenari I perdorur:

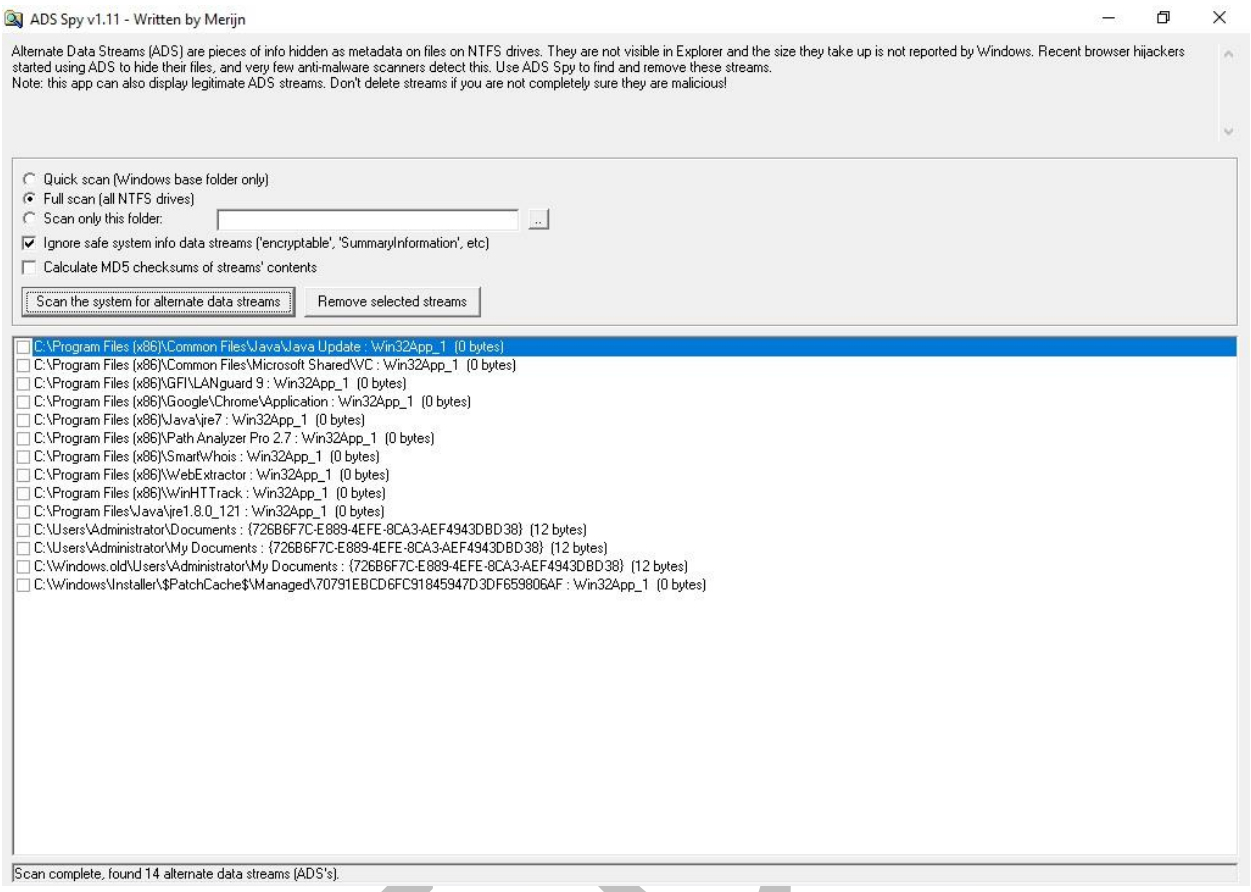


Figura 9

Analiza e trete“III”

“**Stealth**” vegla përdor procesin e njëjtë të Steganografisë që çdo skedar që maskohet brenda një skedari.

Skenari I perdorur:

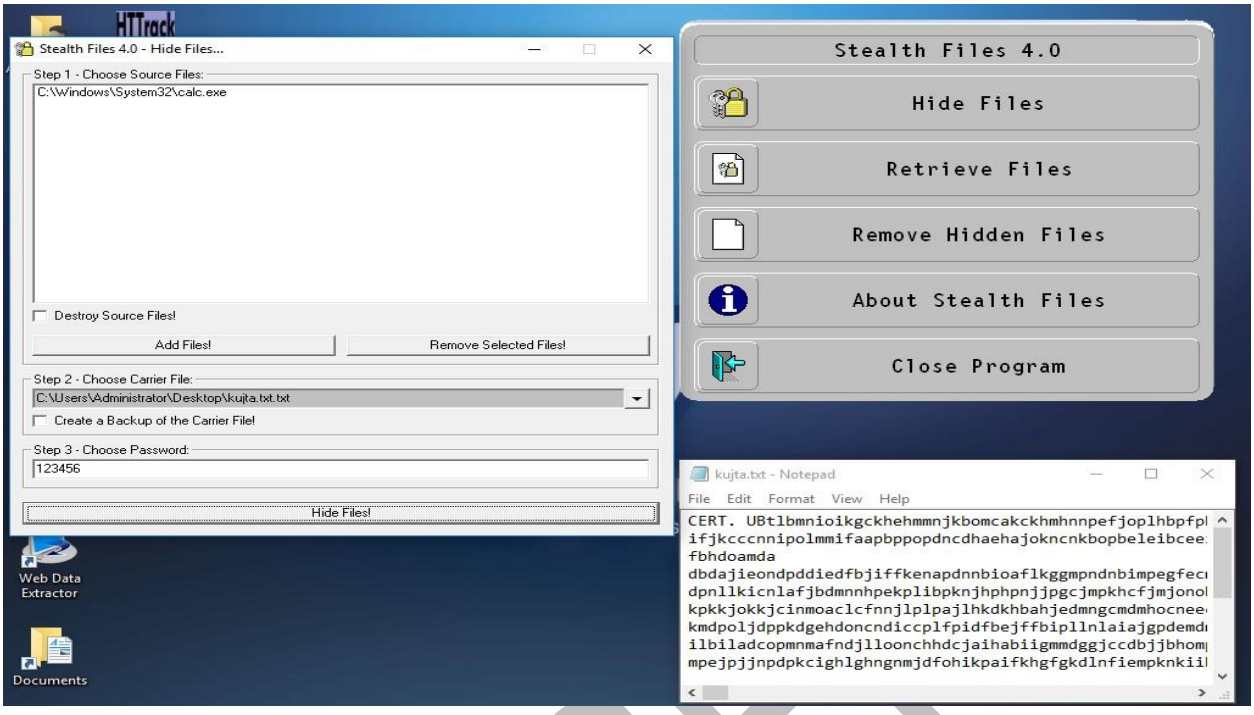


Figura 10

Stealth Retrieve procesi, në figurën mëposhtme:

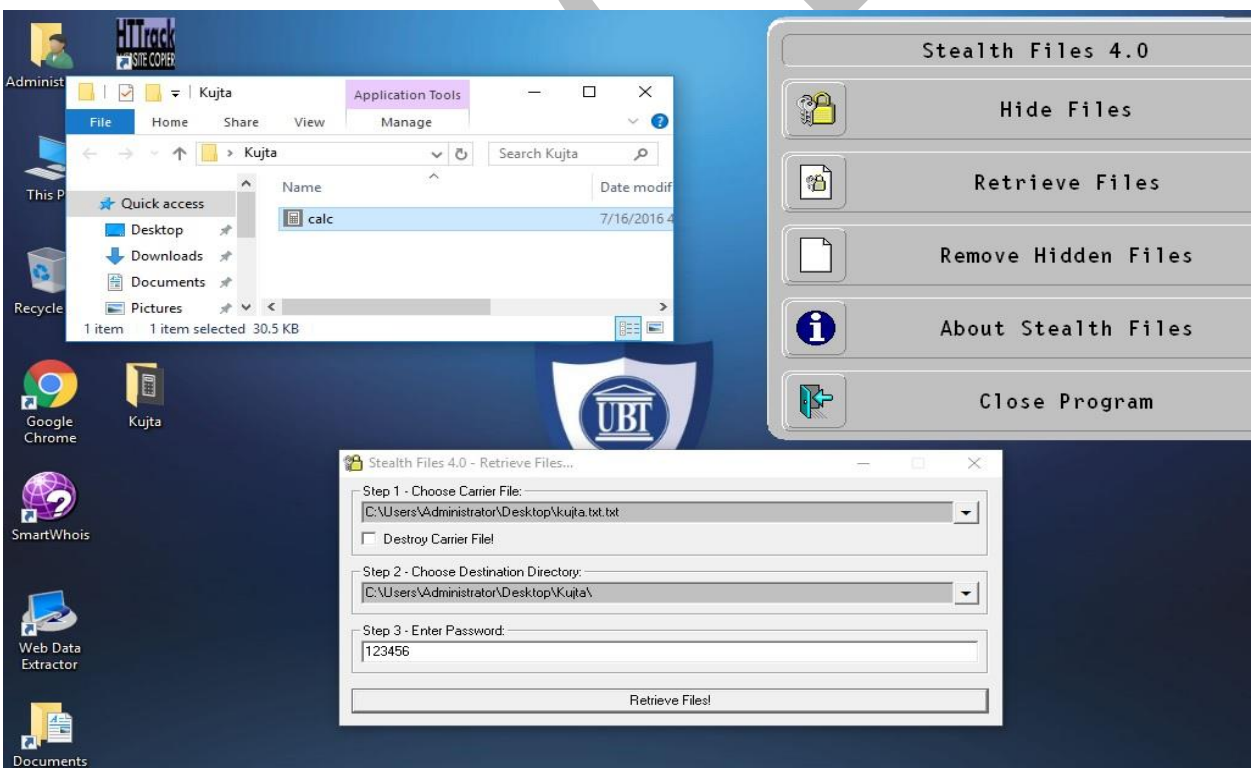


Figura 11

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).

[Të provohet në Windows Server 2008] Skenari I perdorur:

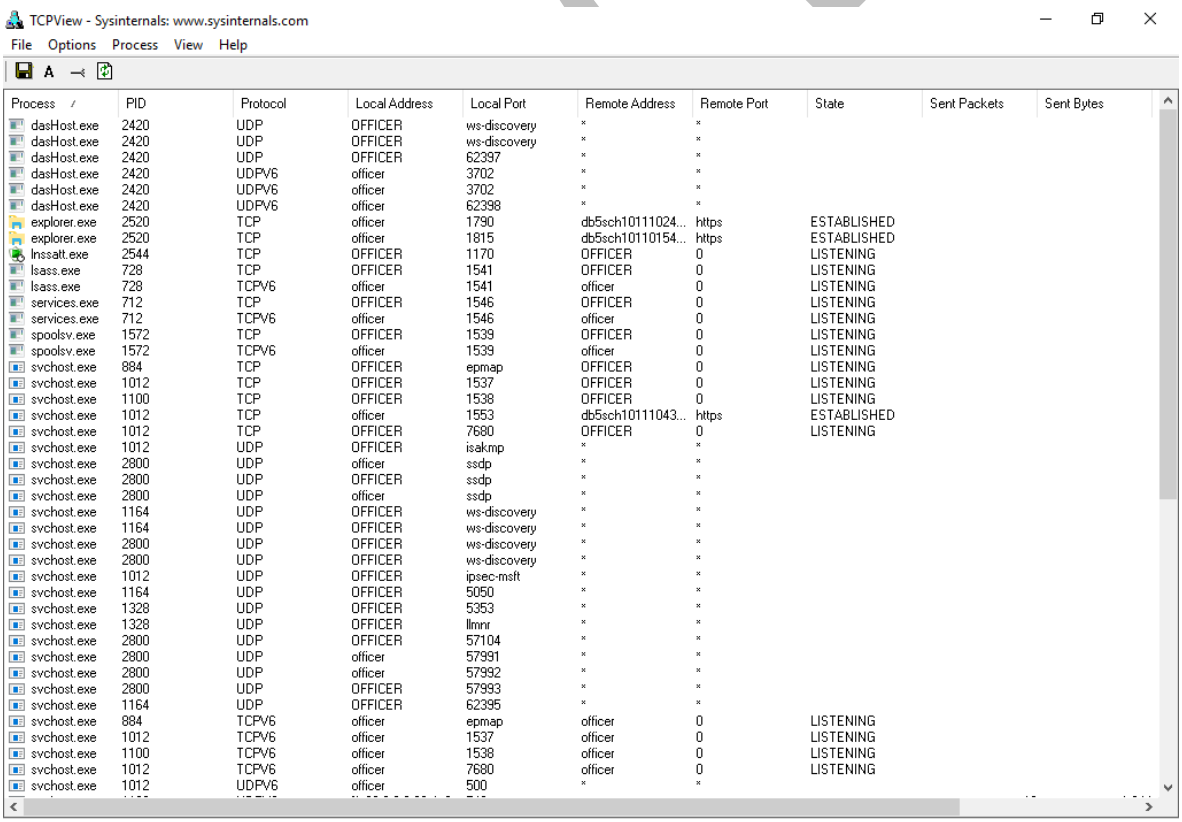
Çka është Trojans and Backdoors

Trojani eshte program qe permban kod te demshem dhe mund te jete I rrezikshem per sistemet kompjuterike dhe largohet me veshtiresi, por ka programe te posaqme per identifikimin e Trojanit dhe Backdoors sulmeve.

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.

Skenari I perdorur:



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
dasHost.exe	2420	UDP	OFFICER	ws-discovery	*	*			
dasHost.exe	2420	UDP	OFFICER	ws-discovery	*	*			
dasHost.exe	2420	UDP	OFFICER	62397	*	*			
dasHost.exe	2420	UDPV6	officer	3702	*	*			
dasHost.exe	2420	UDPV6	officer	3702	*	*			
dasHost.exe	2420	UDPV6	officer	62398	*	*			
explorer.exe	2520	TCP	officer	1790	db5sch10111024...	https	ESTABLISHED		
explorer.exe	2520	TCP	officer	1815	db5sch10110154...	https	ESTABLISHED		
lnssatt.exe	2544	TCP	OFFICER	1170	OFFICER	0	LISTENING		
lsass.exe	728	TCP	OFFICER	1541	OFFICER	0	LISTENING		
lsass.exe	728	TCPV6	officer	1541	officer	0	LISTENING		
services.exe	712	TCP	OFFICER	1546	OFFICER	0	LISTENING		
services.exe	712	TCPV6	officer	1546	officer	0	LISTENING		
spoolsv.exe	1572	TCP	OFFICER	1539	OFFICER	0	LISTENING		
spoolsv.exe	1572	TCPV6	officer	1539	officer	0	LISTENING		
svchost.exe	884	TCP	OFFICER	epmap	OFFICER	0	LISTENING		
svchost.exe	1012	TCP	OFFICER	1537	OFFICER	0	LISTENING		
svchost.exe	1100	TCP	OFFICER	1538	OFFICER	0	LISTENING		
svchost.exe	1012	TCP	officer	1553	db5sch10111043...	https	ESTABLISHED		
svchost.exe	1012	TCP	OFFICER	7680	OFFICER	0	LISTENING		
svchost.exe	1012	UDP	OFFICER	isakmp	*	*			
svchost.exe	2800	UDP	officer	ssdp	*	*			
svchost.exe	2800	UDP	OFFICER	ssdp	*	*			
svchost.exe	2800	UDP	officer	ssdp	*	*			
svchost.exe	1164	UDP	OFFICER	ws-discovery	*	*			
svchost.exe	1164	UDP	OFFICER	ws-discovery	*	*			
svchost.exe	2800	UDP	OFFICER	ws-discovery	*	*			
svchost.exe	2800	UDP	OFFICER	ws-discovery	*	*			
svchost.exe	1012	UDP	OFFICER	ipsec-msft	*	*			
svchost.exe	1164	UDP	OFFICER	5050	*	*			
svchost.exe	1328	UDP	OFFICER	5353	*	*			
svchost.exe	1328	UDP	OFFICER	llmnr	*	*			
svchost.exe	2800	UDP	OFFICER	57104	*	*			
svchost.exe	2800	UDP	officer	57991	*	*			
svchost.exe	2800	UDP	officer	57992	*	*			
svchost.exe	2800	UDP	OFFICER	57993	*	*			
svchost.exe	1164	UDP	OFFICER	62395	*	*			
svchost.exe	884	TCPV6	officer	epmap	officer	0	LISTENING		
svchost.exe	1012	TCPV6	officer	1537	officer	0	LISTENING		
svchost.exe	1100	TCPV6	officer	1538	officer	0	LISTENING		
svchost.exe	1012	TCPV6	officer	7680	officer	0	LISTENING		
svchost.exe	1012	UDPV6	officer	500	*	*			

Figura 12

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. Pasyra përmbledhëse tregon qartë si nga pjesa hardware poashtu edhe software me detajet për proceset që zhvillohen brenda një kompjuteri.

Skenari I perdorur:

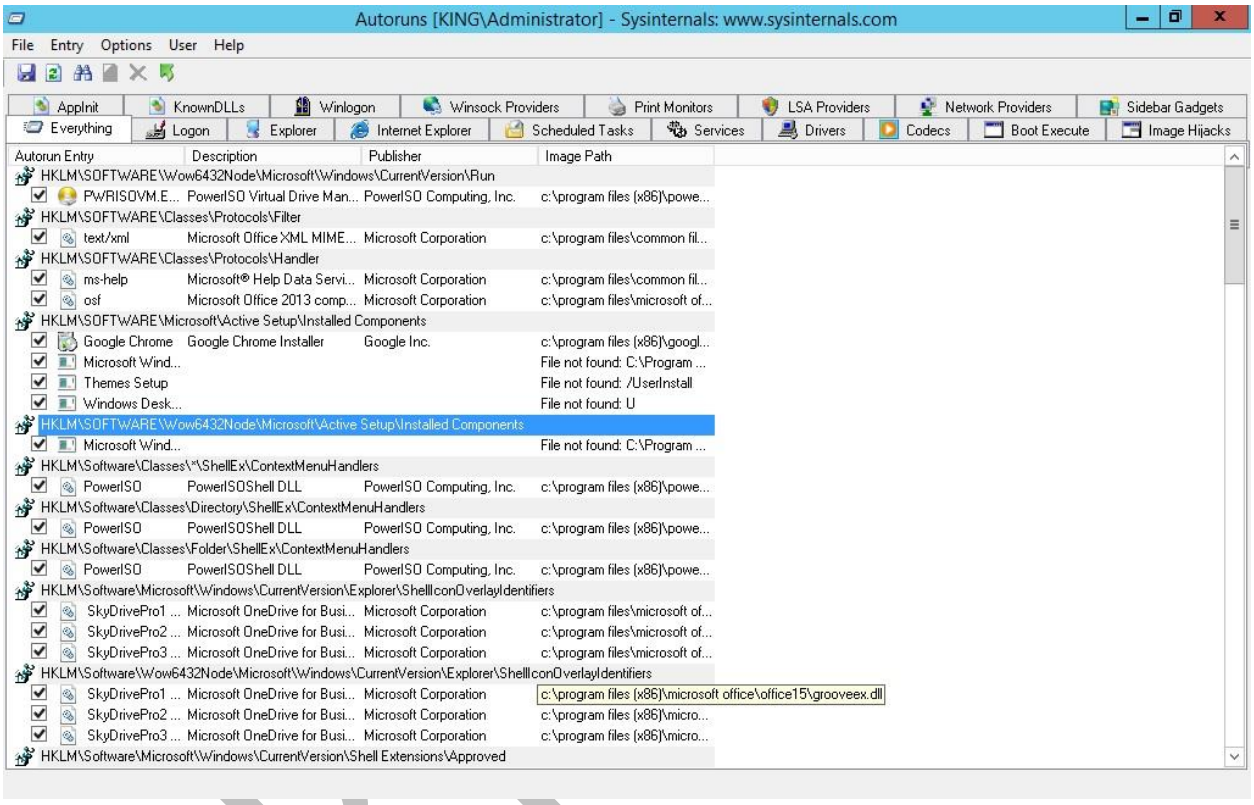


Figura 13

Analiza e trete “III”

JV 16

Skenari I perdorur:

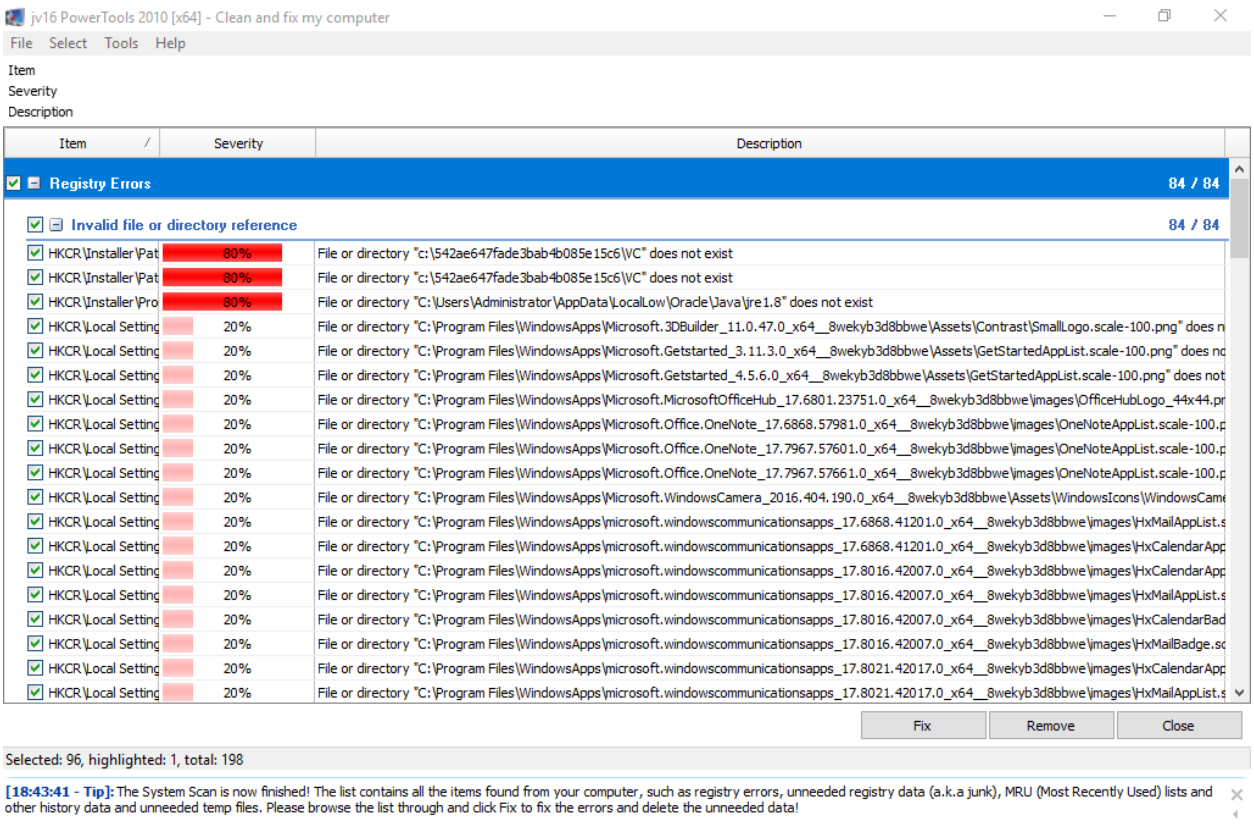


Figura 14

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:

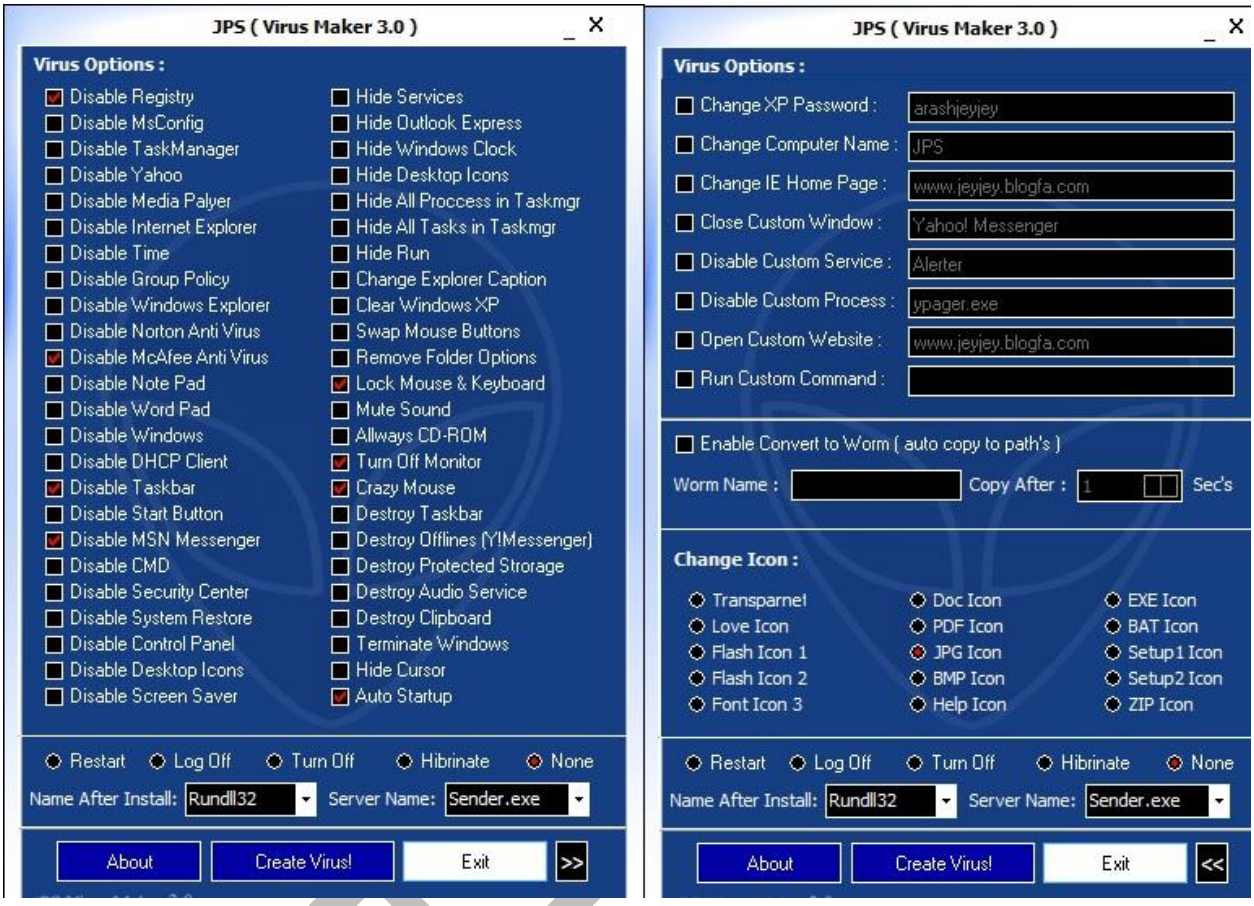


Figura 15

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:

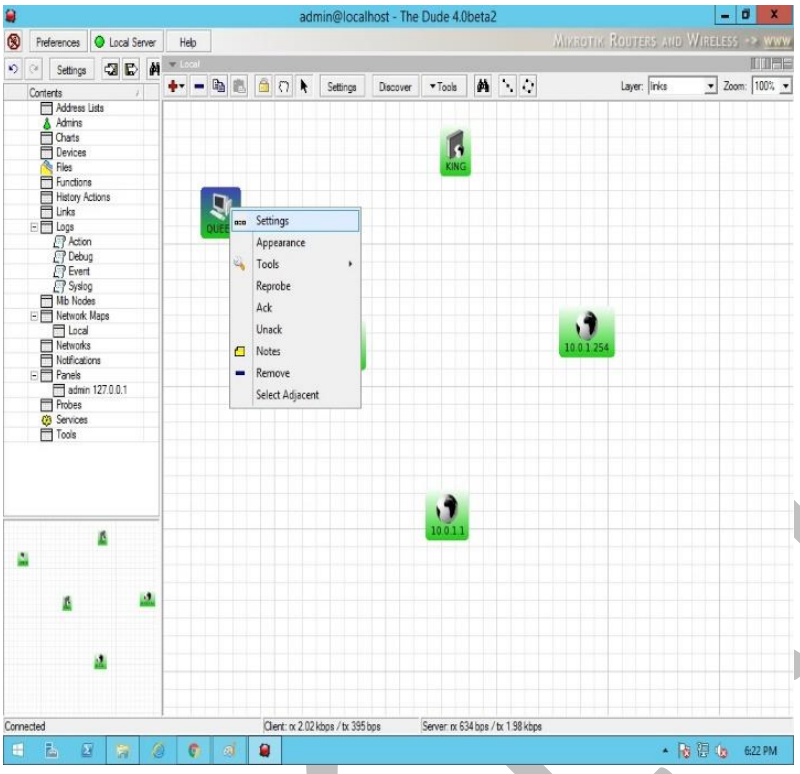


Figura 16

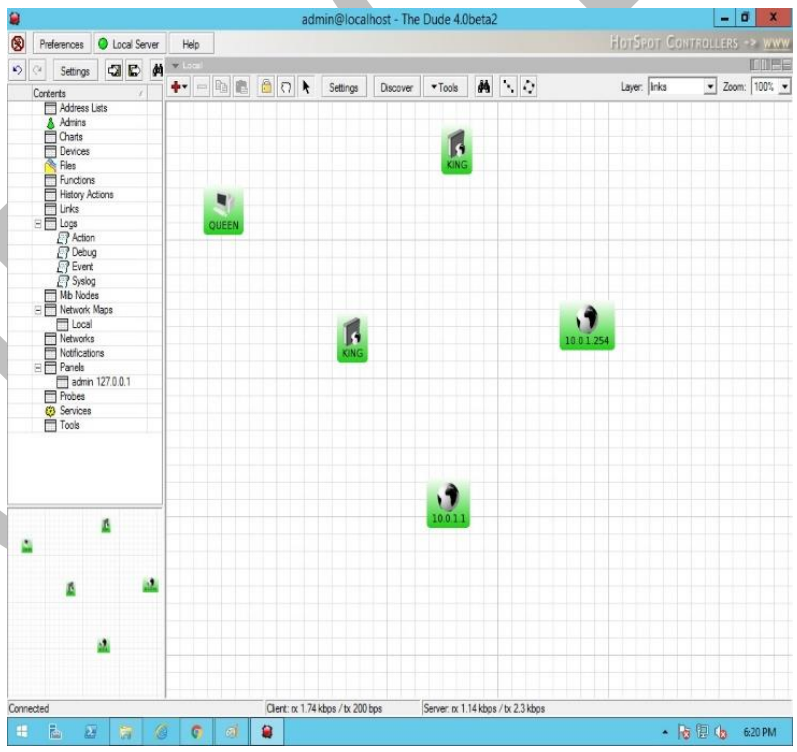


Figura 17

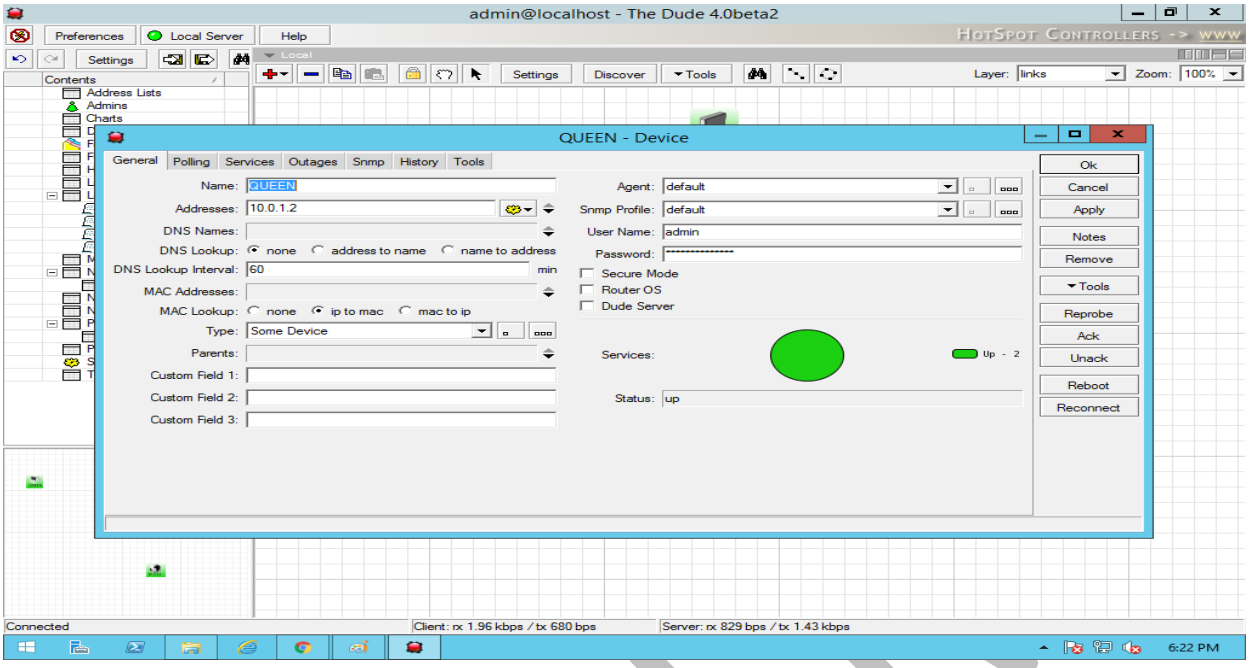


Figura 18

Analiza e dyte "II"

"**WireShark**"

Skenari I perdorur:

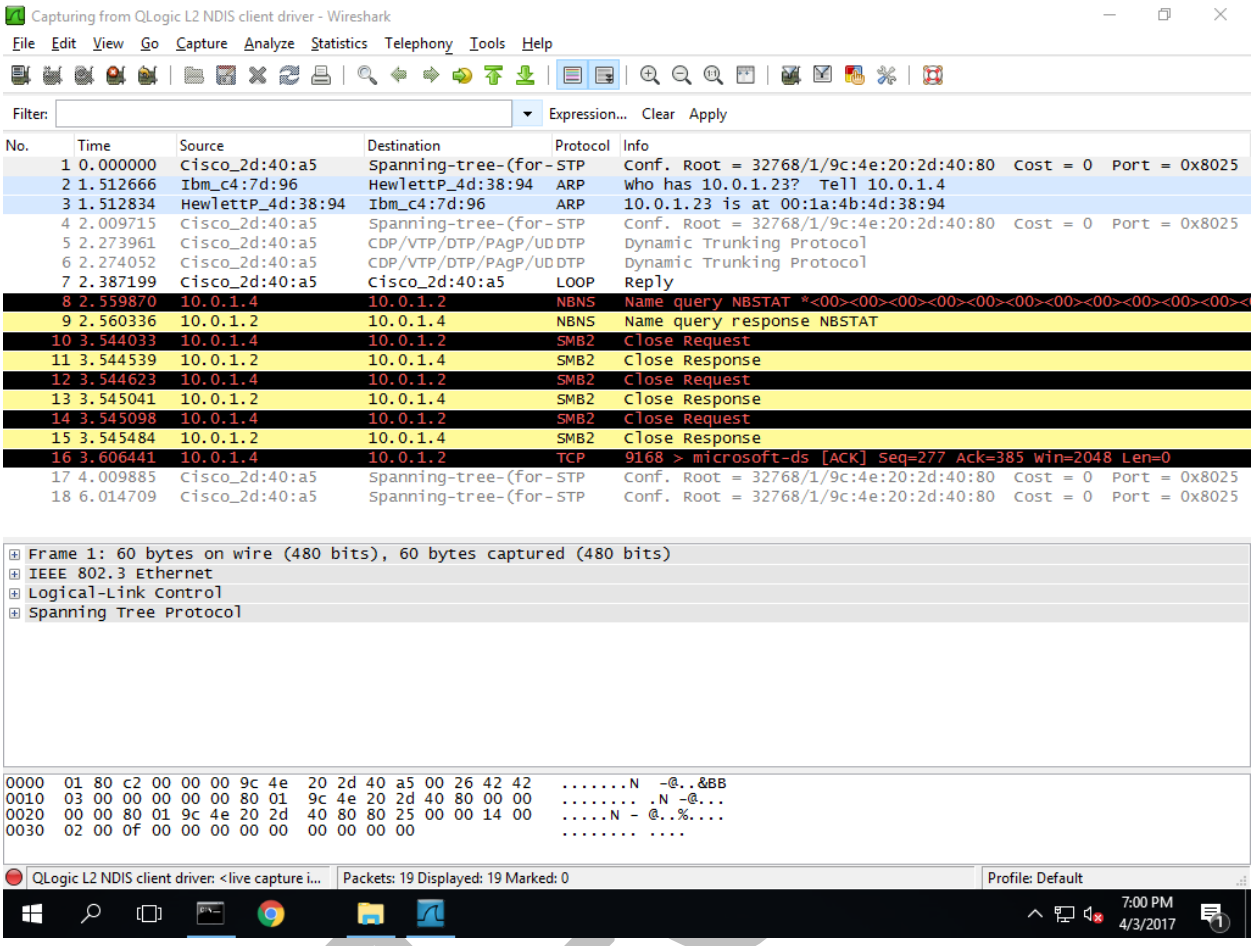


Figura 19

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.

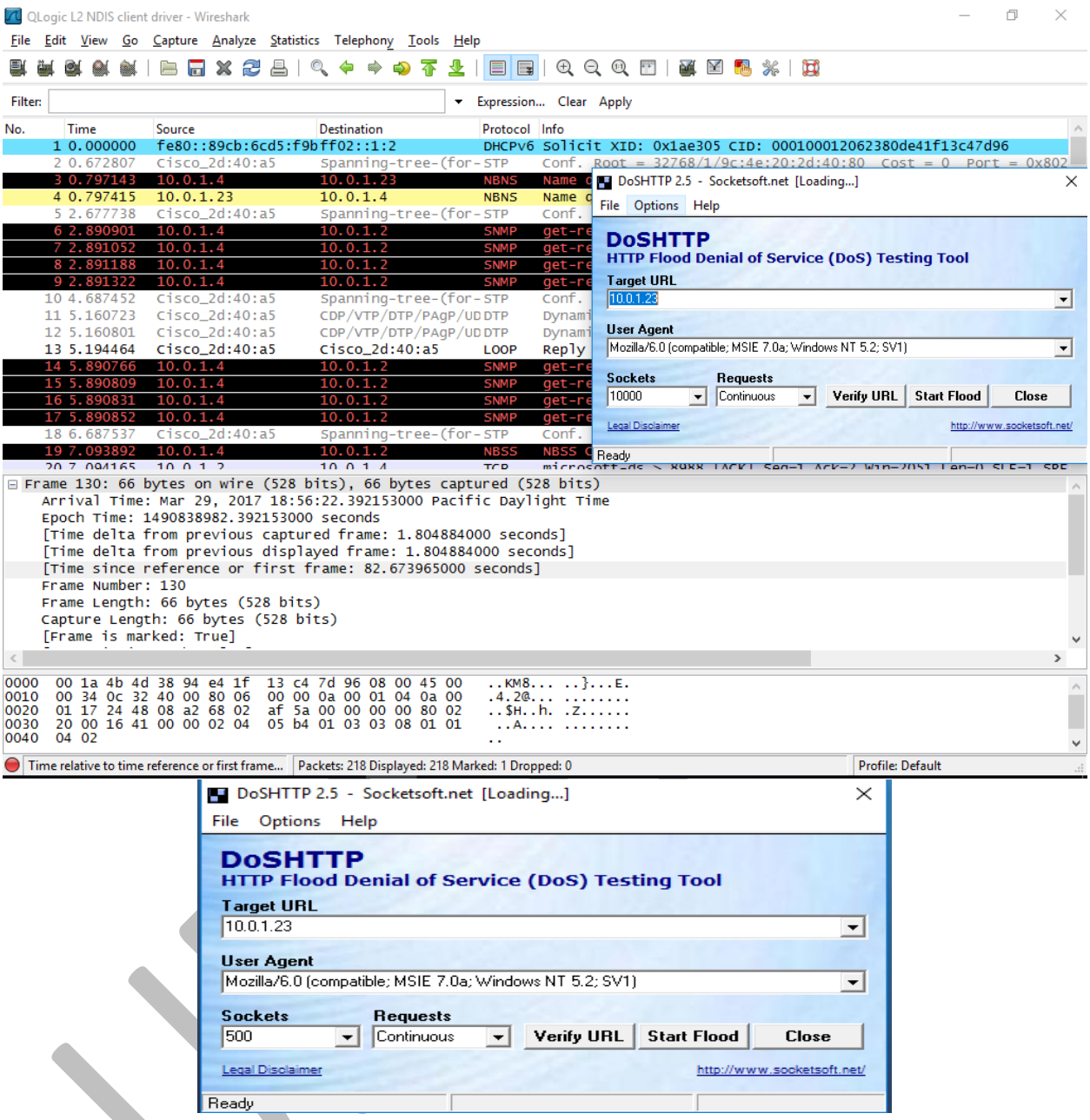
Rekomandim

- 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:


QLogic L2 NDIS client driver - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 fe80::89cb:6cd5:f9bf f02::1:2 DHCPv6 Solicit XID: 0x1ae305 CID: 000100012062380de41f13c47d96
2 0.672807 Cisco_2d:40:a5 Spanning-tree-(for- STP Conf. Root = 32768/1/9c:4e:20:2d:40:80 Cost = 0 Port = 0x802
3 0.797143 10.0.1.4 10.0.1.23 NBNS Name
4 0.797415 10.0.1.23 10.0.1.4 NBNS Name
5 2.677738 Cisco_2d:40:a5 Spanning-tree-(for- STP Conf.
6 2.890901 10.0.1.4 10.0.1.2 SNMP get-re
7 2.891052 10.0.1.4 10.0.1.2 SNMP get-re
8 2.891188 10.0.1.4 10.0.1.2 SNMP get-re
9 2.891322 10.0.1.4 10.0.1.2 SNMP get-re
10 4.687452 Cisco_2d:40:a5 Spanning-tree-(for- STP Conf.
11 5.160723 Cisco_2d:40:a5 CDP/VTP/DTP/PAgP/UD DTP Dynami
12 5.160801 Cisco_2d:40:a5 CDP/VTP/DTP/PAgP/UD DTP Dynami
13 5.194464 Cisco_2d:40:a5 Cisco_2d:40:a5 LOOP Reply
14 5.890766 10.0.1.4 10.0.1.2 SNMP get-re
15 5.890809 10.0.1.4 10.0.1.2 SNMP get-re
16 5.890831 10.0.1.4 10.0.1.2 SNMP get-re
17 5.890852 10.0.1.4 10.0.1.2 SNMP get-re
18 6.687537 Cisco_2d:40:a5 Spanning-tree-(for- STP Conf.
19 7.093892 10.0.1.4 10.0.1.2 NBSS
DoSHTTP 2.5 - Socketsoft.net [Loading...]
File Options Help
DoSHTTP
HTTP Flood Denial of Service (DoS) Testing Tool
Target URL
10.0.1.23
User Agent
Mozilla/6.0 (compatible; MSIE 7.0a; Windows NT 5.2; SV1)
Sockets
10000
Requests
Continuous
Verify URL
Start Flood
Close
Legal Disclaimer
http://www.socketsoft.net/
Ready
Frame 130: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Arrival Time: Mar 29, 2017 18:56:22.392153000 Pacific Daylight Time
Epoch Time: 1490838982.392153000 seconds
[Time delta from previous captured frame: 1.804884000 seconds]
[Time delta from previous displayed frame: 1.804884000 seconds]
[Time since reference or first frame: 82.673965000 seconds]
Frame Number: 130
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: True]
0000 00 1a 4b 4d 38 94 e4 1f 13 c4 7d 96 08 00 45 00 ..KM8... ..}...E.
0010 00 34 0c 32 40 00 80 06 00 00 0a 00 01 04 0a 00 .4.2@... ....
0020 01 17 24 48 08 a2 68 02 af 5a 00 00 00 00 80 02 ..$H..h. .Z......
0030 20 00 16 41 00 00 02 04 05 b4 01 03 03 08 01 01 ..A.... ....
0040 04 02 ..
Time relative to time reference or first frame...
Packets: 218 Displayed: 218 Marked: 1 Dropped: 0
Profile: Default

DoSHTTP 2.5 - Socketsoft.net [Loading...]
File Options Help
DoSHTTP
HTTP Flood Denial of Service (DoS) Testing Tool
Target URL
10.0.1.23
User Agent
Mozilla/6.0 (compatible; MSIE 7.0a; Windows NT 5.2; SV1)
Sockets
500
Requests
Continuous
Verify URL
Start Flood
Close
Legal Disclaimer
http://www.socketsoft.net/
Ready

Figura 20