



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.....	4
Koncepti etik (Defense cyber security)	5
Çka është “footprinting”	5
Analiza e parë “I”	5
Rekomandim	5
Analiza e dytë “II”	6
Rekomandim	7
Çka është Scanning Network	8
Analiza e parë “I”	8
Analiza e dytë “II”	9
Analiza e trete “III”	10
Rekomandim	10
Çka është Enumeration.....	10
Analiza e parë “I”	10
Çka është System Hacking	11
Analiza e parë “I”	11
Analiza e dyte “II”	12
Analiza e trete “III”	13
Rekomandim	15
Analiza e katert “IV”	15
Çka është Trojans and Backdoors	15
Analiza e parë “I”	15
Analiza e dyte “II”	16
Analiza e trete “III”	17
Rekomandim	17
Çka është Viruses and Worms	17
Analiza e parë “I”	17
Rekomandim	18
Çka është Sniffers.....	18
Analiza e parë “I”	18
Analiza e dyte “II”	20
Çka është Social Engineering	21

Rekomandim	21
Çka është DoS, DDoS.....	21

UBT-CERT

Hyrje

Ky dokument është përgatitur me qëllim që të vetëdijsoj të gjithë ata që janë të angazhuar në fushën e TIK-ut dhe i dedikohet komunitetit të TIK-ut.

Përmirëson nivelin e sigurisë të sistemeve kompjuterike të një kompanie ose organizate, ndihmon përdoruesit e këtyre sistemeve për shfrytëzim sa më të sigurt të tyre.

UBT-CERT

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”

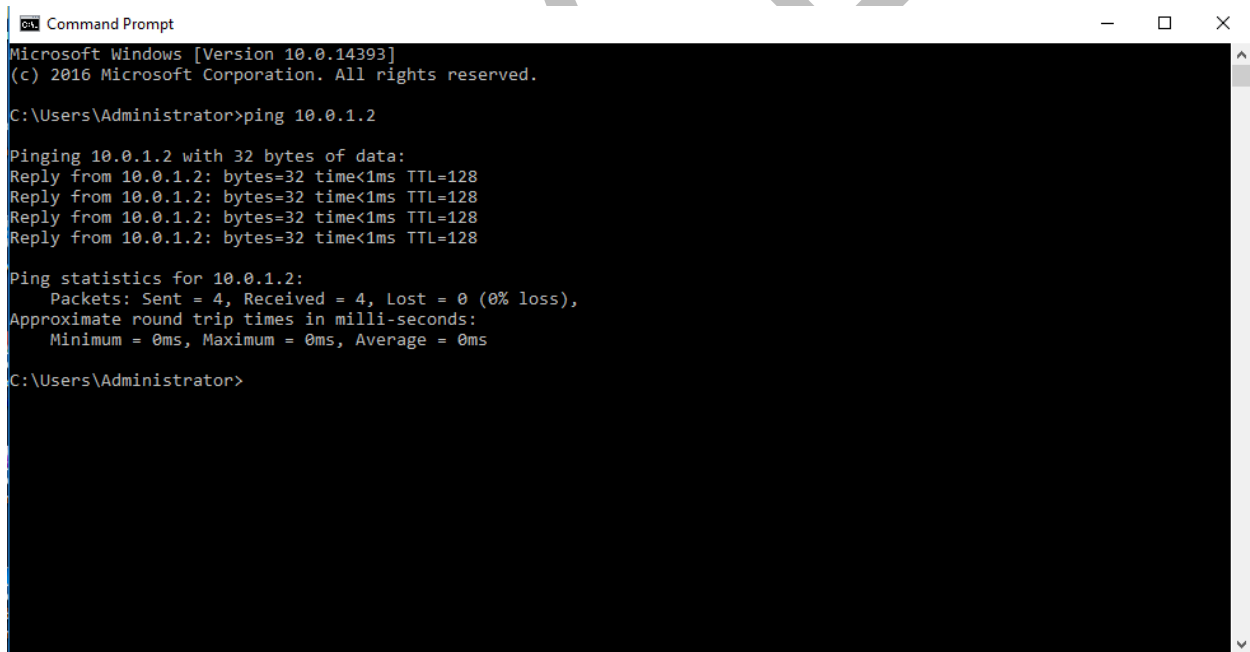
Ky proces “footprinting” i referohet funksioneve të zbulimit dhe mbledhjes të sa më shumë informatave për një target të caktuar në rrjetë p.sh. institucion publik, privat, akademik ose kompani. Si rezultat i këtij procesi “footprinting” ne krijojmë në mendjen tonë një skemë vizuale të arkitekturës së 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:



```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.0.1.2

Pinging 10.0.1.2 with 32 bytes of data:
Reply from 10.0.1.2: bytes=32 time<1ms TTL=128
Reply from 10.0.1.2: bytes=32 time<1ms TTL=128
Reply from 10.0.1.2: bytes=32 time<1ms TTL=128
Reply from 10.0.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

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 ISP₁-së
- Pronari i domain-t dhe IP adresës
- Informata për pronarin e domain-t
- Data regjistrimit dhe skadimit domain-t

Skenari i përdorur:

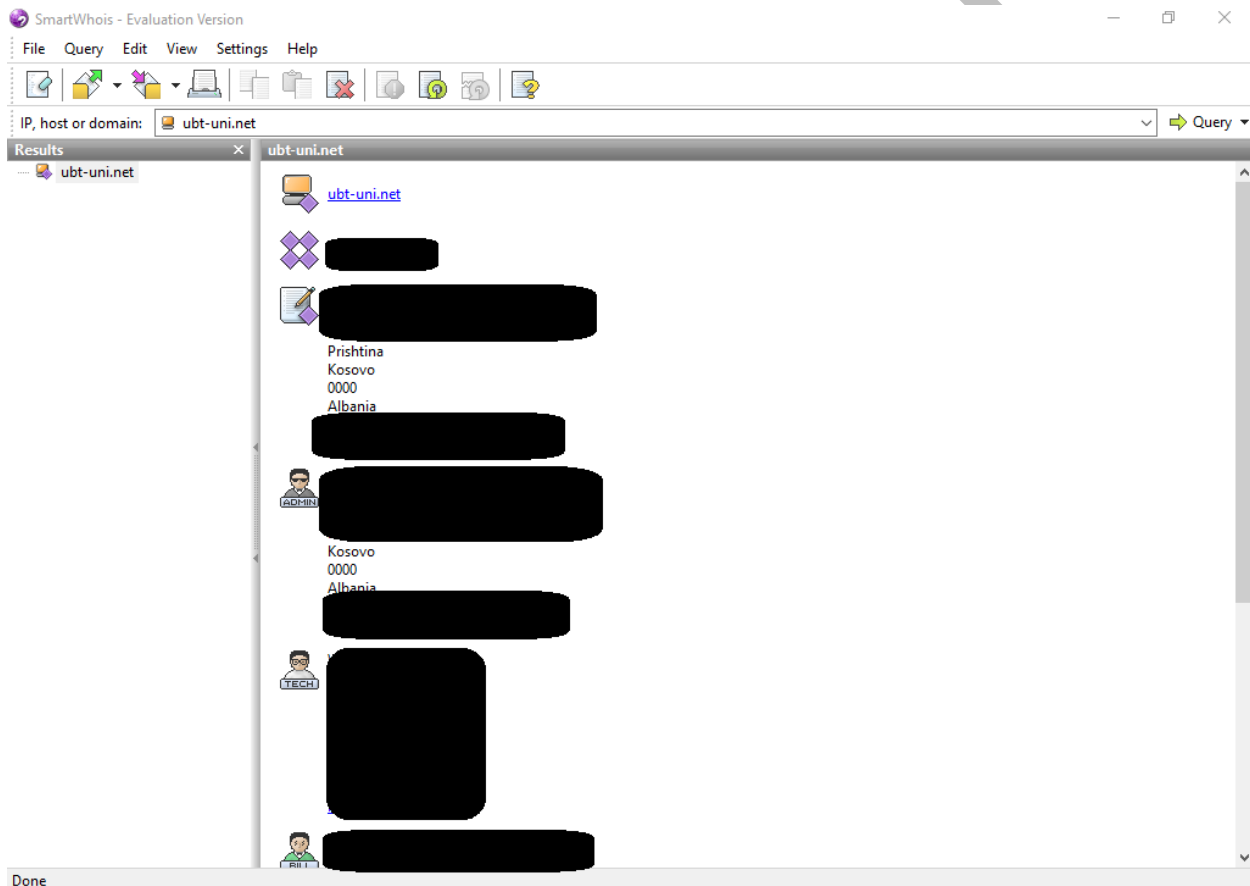


Figura 2

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:

eMailTrackerPro v10.0b Advanced Edition. Trial day 13 of 15

File Help

My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition

View New Email Trace Configure

Home internshiptest828@gmail... x

The trace is complete, the information found is displayed on the right New Trace View Report

Map

Mountain View, California, USA

Hop #	Hop IP	Hop Name	Location
1	10.0.1.1		
2	192.168.0.254		
3	10.90.77.1		
4	192.168.90.1		
5	10.114.113.45		
6	10.114.113.33		
7	10.40.0.1		
8	10.40.0.101		
9	79.101.106.233		Belgrade, RS

Email Summary

Email Address: internshiptest828@gmail.com
IP: 74.125.28.26
Location: Mountain View, California, USA
Abuse Address: network-abuse@google.com

System Information:

- The system is running a mail server (ESMTP *a21si14695721pjh.134 - gsmtp*) on port 25. This means that this system can be used to send email.
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

Network Whois

Domain Whois

You are on day 13 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

New spam fighting product by Visualware. Introducing InboxGuardian. [Check it out here.](#)

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” është proces që i referohet një grupi të procedurave për identifikimin e hosts, porteve dhe shërbimeve që funksionojnë në rrjetet. Skenimi i rrjetit ka për qëllim kontrollin e sistemeve kompjuterike që përdoren, porteve të hapura dhe mbledhjen e informatave me detaje për sistemin operativ, dobesive në infrastrukturën e rrjetit etj.

Analiza e parë “1”

“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 rrjetin lokal.

Skenari i përdorur:

The screenshot shows the Angry IP Scanner interface. The IP Range is set to 10.0.1.0 to 10.0.1.23, and the Hostname is OFFICER. The scan results table is as follows:

IP	Ping	Hostname	Ports [0+]
10.0.1.1	0 ms	[n/a]	[n/s]
10.0.1.2	0 ms	QUEEN	[n/s]
10.0.1.3	[n/a]	[n/s]	[n/s]
10.0.1.4	0 ms	OFFICER	[n/s]
10.0.1.5	[n/a]	[n/s]	[n/s]
10.0.1.6	[n/a]	[n/s]	[n/s]
10.0.1.7	[n/a]	[n/s]	[n/s]
10.0.1.8	[n/a]	[n/s]	[n/s]
10.0.1.9	[n/a]	[n/s]	[n/s]
10.0.1.10	[n/a]	[n/s]	[n/s]
10.0.1.11	[n/a]	[n/s]	[n/s]
10.0.1.12	[n/a]	[n/s]	[n/s]
10.0.1.13	[n/a]	[n/s]	[n/s]
10.0.1.14	[n/a]	[n/s]	[n/s]
10.0.1.15	[n/a]	[n/s]	[n/s]
10.0.1.16	[n/a]	[n/s]	[n/s]
10.0.1.17	[n/a]	[n/s]	[n/s]
10.0.1.18	[n/a]	[n/s]	[n/s]
10.0.1.19	[n/a]	[n/s]	[n/s]
10.0.1.20	[n/a]	[n/s]	[n/s]
10.0.1.21	[n/a]	[n/s]	[n/s]
10.0.1.22	[n/a]	[n/s]	[n/s]
10.0.1.23	0 ms	KING	[n/s]

The 'Scan Statistics' dialog box displays the following information:

- Scanning completed
- Total time: 5.65 sec
- Average time per host: 0.25 sec
- IP Range: 10.0.1.0 - 10.0.1.23
- Hosts scanned: 23
- Hosts alive: 4

Figura 4

Analiza e dytë "II"

"Friendly pinger" është një aplikacion lehtë i përdorshëm për administrimin, monitorimin dhe inventarizimin e rrjetës dhe pajisjeve të tjera të TI-së.

Skenari I përdorur:

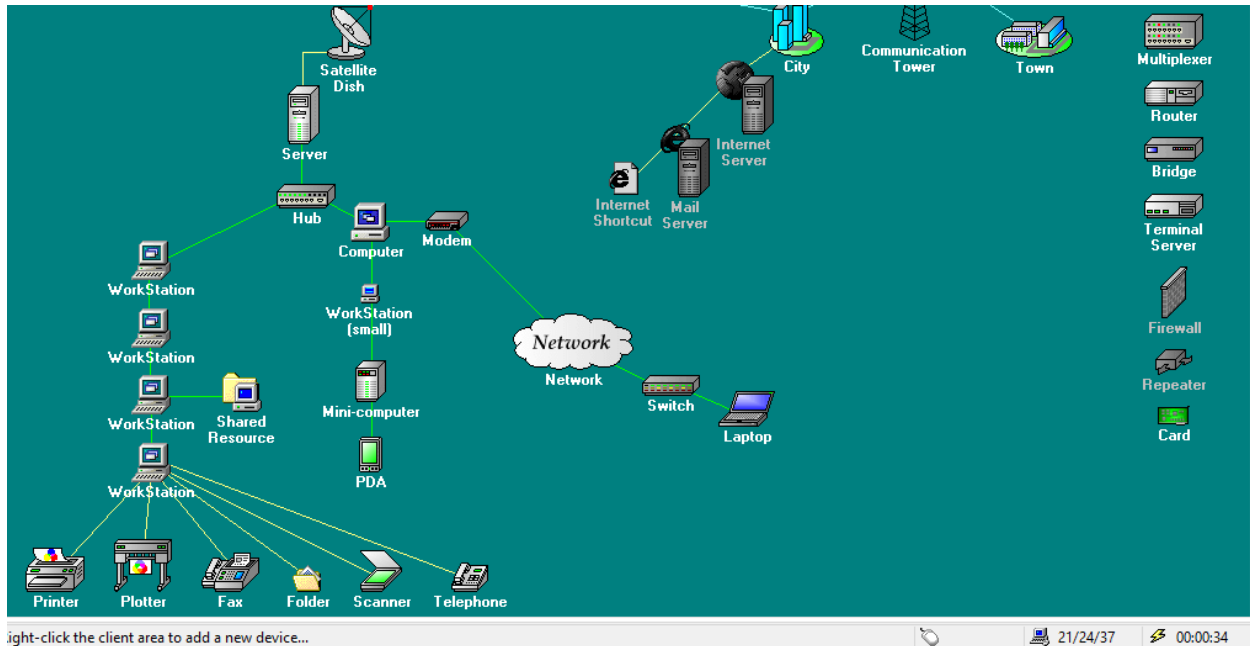


Figura 5

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:

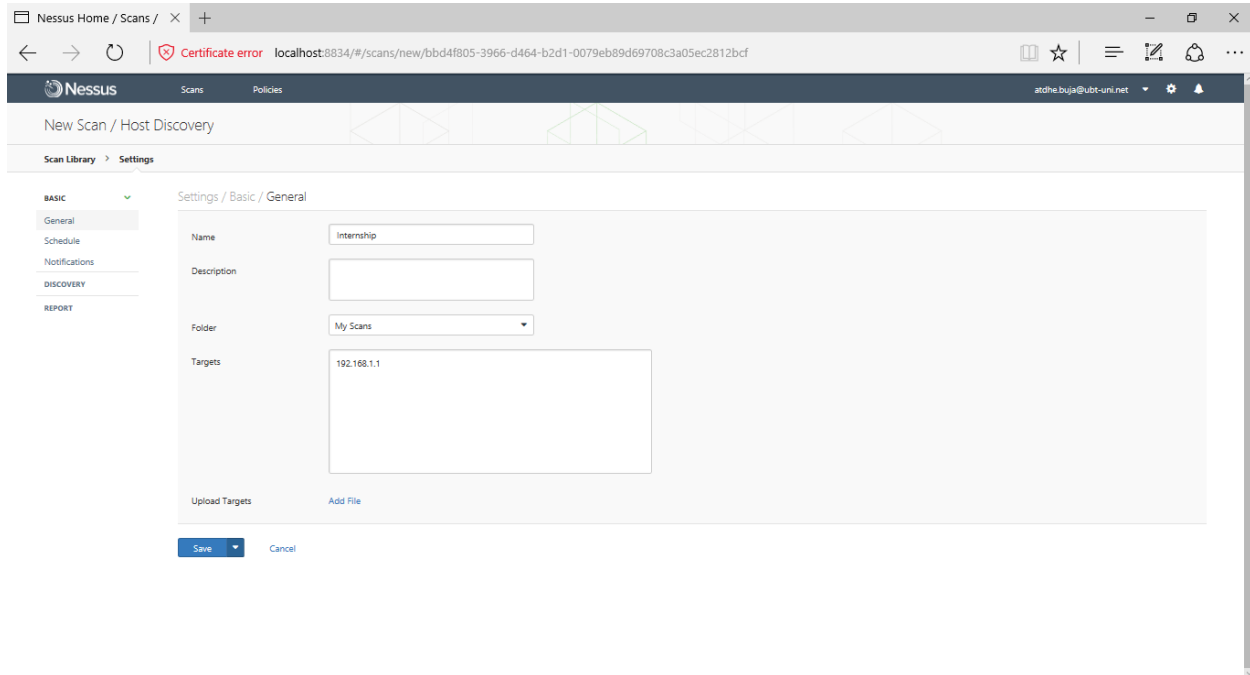


Figura 6

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 konfiguruar 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 të bënin me shume me mbledhjen e informatave për infrastrukturen dhe sistemet kompjuterike. **Enumeration** është procesi i trete dhe me i rëndësishëm, përmes të cilit provohet të merren të dhëna për përdoruesit, emrat e makinave, informata të infrastruktures së rrjetës dhe shërbimeve (ang. services) nga sistemi kompjuterik.

Analiza e pare “I”

“SuperScan” mundëson skanimin, marrjen e të dhënave nga e gjithë rrjeta dhe pajisjeve që gjenden në të, varësisht nga lloji që ne zgjedhim (Enumeration type). Për më shumë shihni figurën në vazhdim.

Skenari I përdorur:

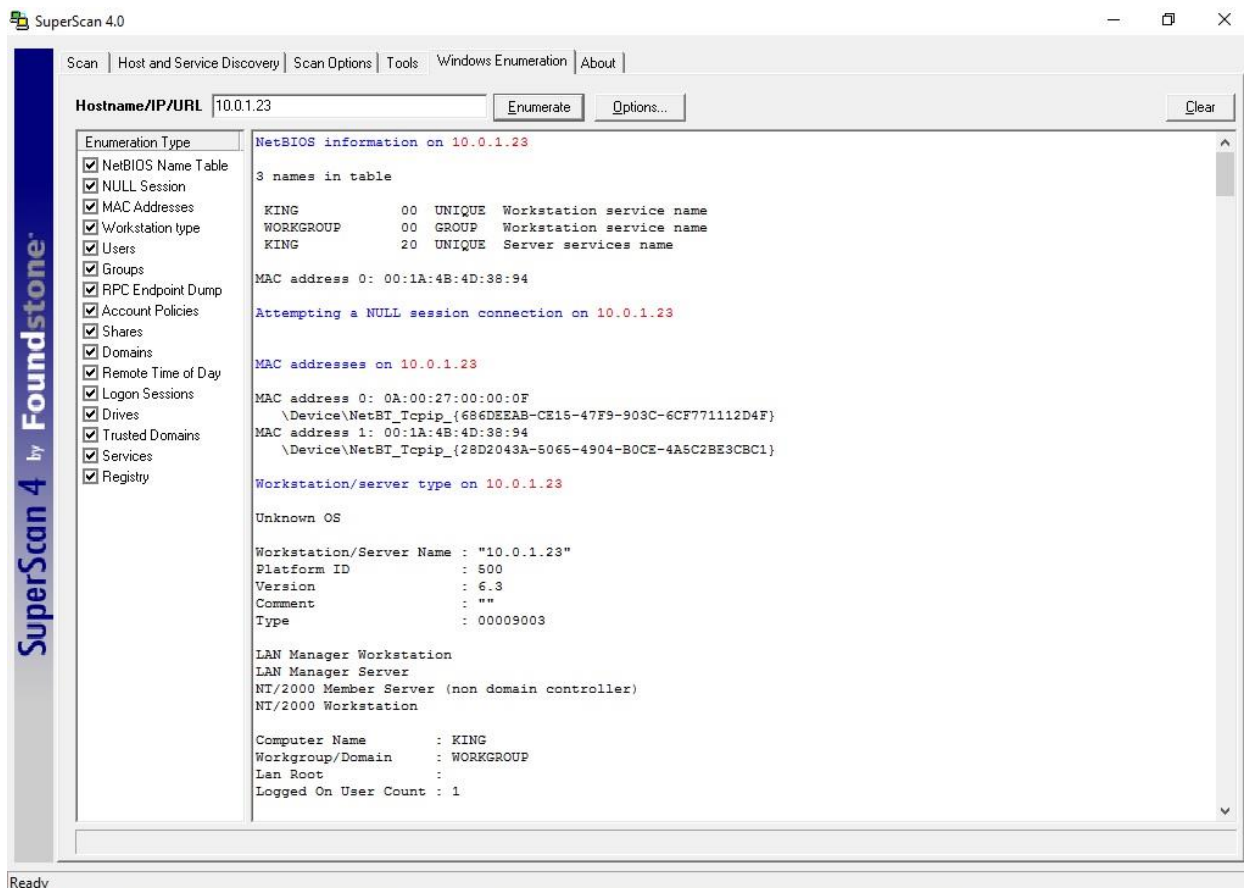


Figura 7

Çka është System Hacking

“System Hacking” është një shkencë e testimit të sistemeve kompjuterike rrjetes dhe vete paisjeve kompjuterike për dobësit (ang. Vulnerabilities) që mund të i kenë.

Analiza e parë “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:

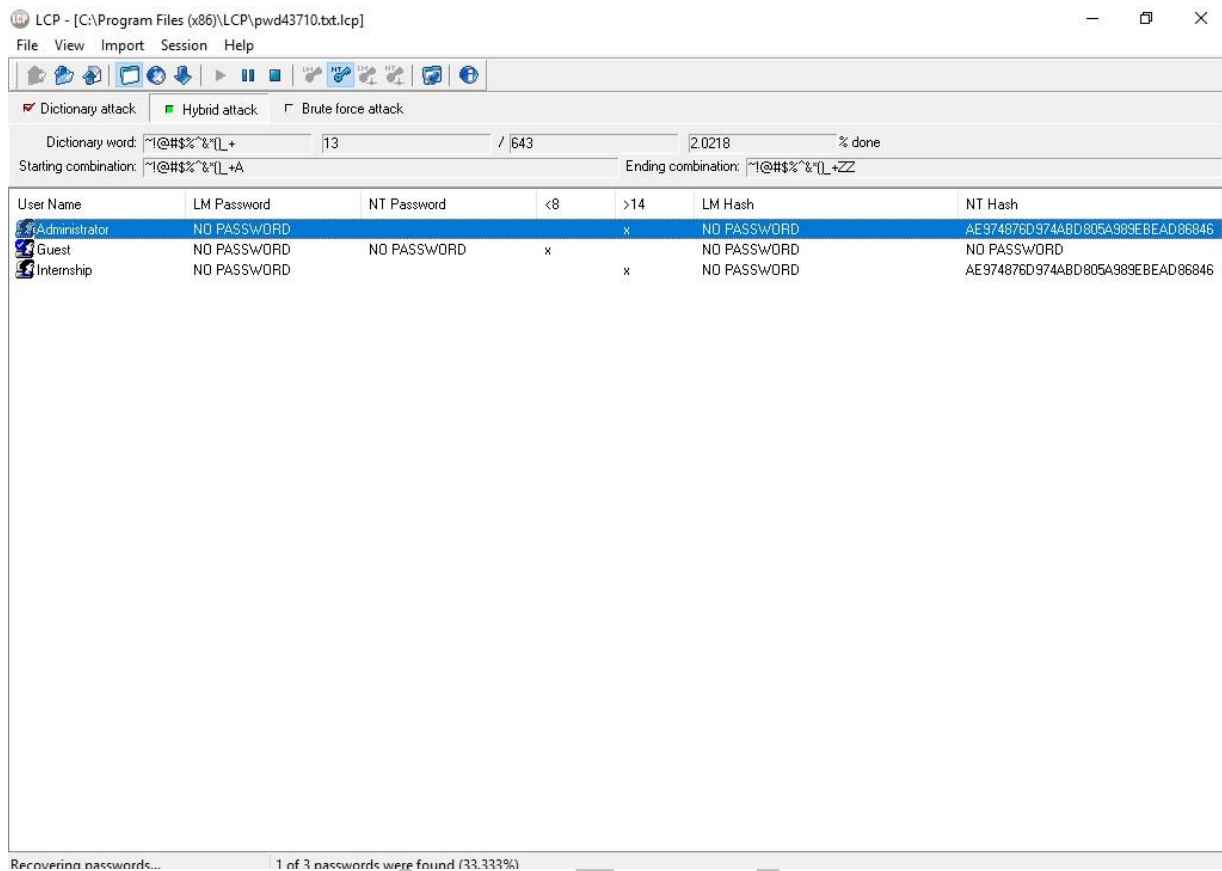


Figura 8

Analiza e dytë "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 përdorur:

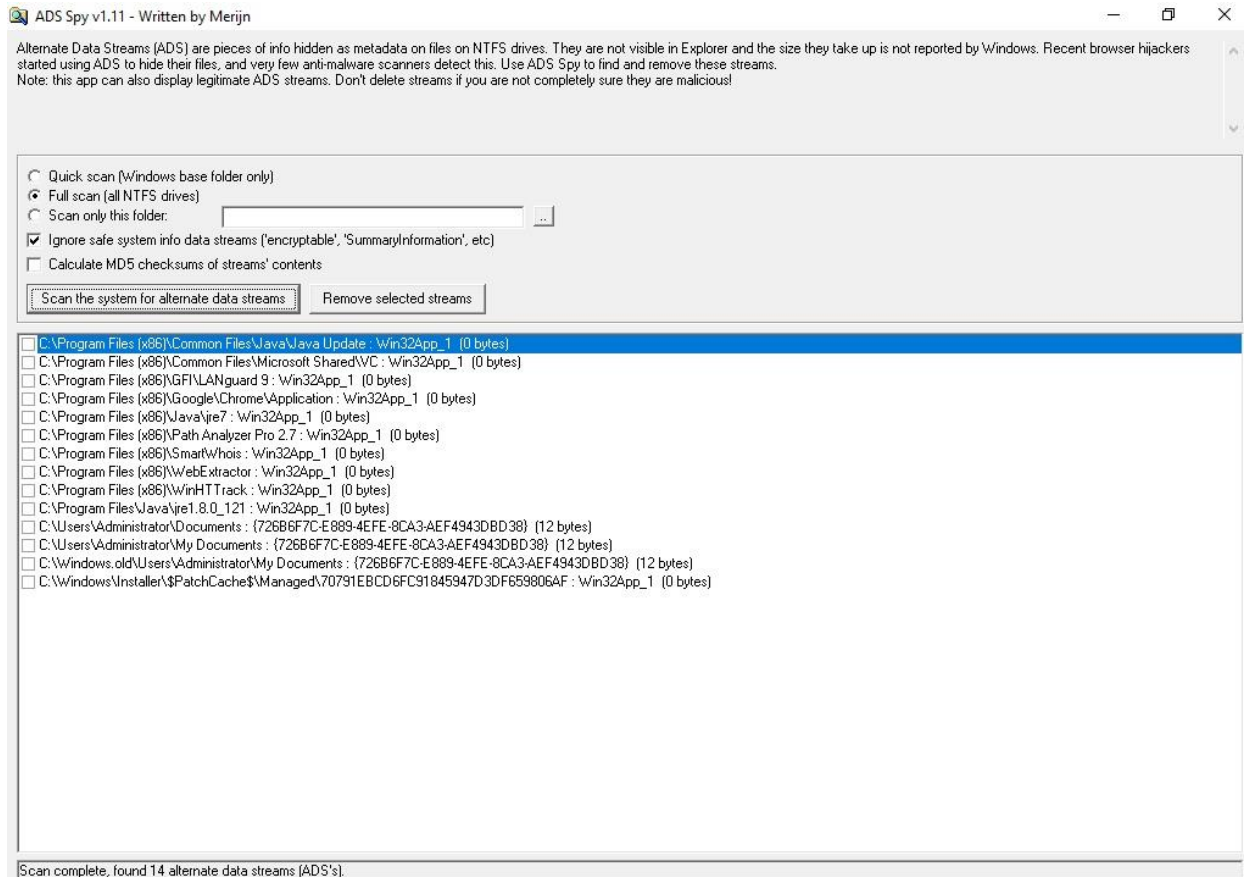


Figura 9

Analiza e trete“III”

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

Skenari I përdorur:

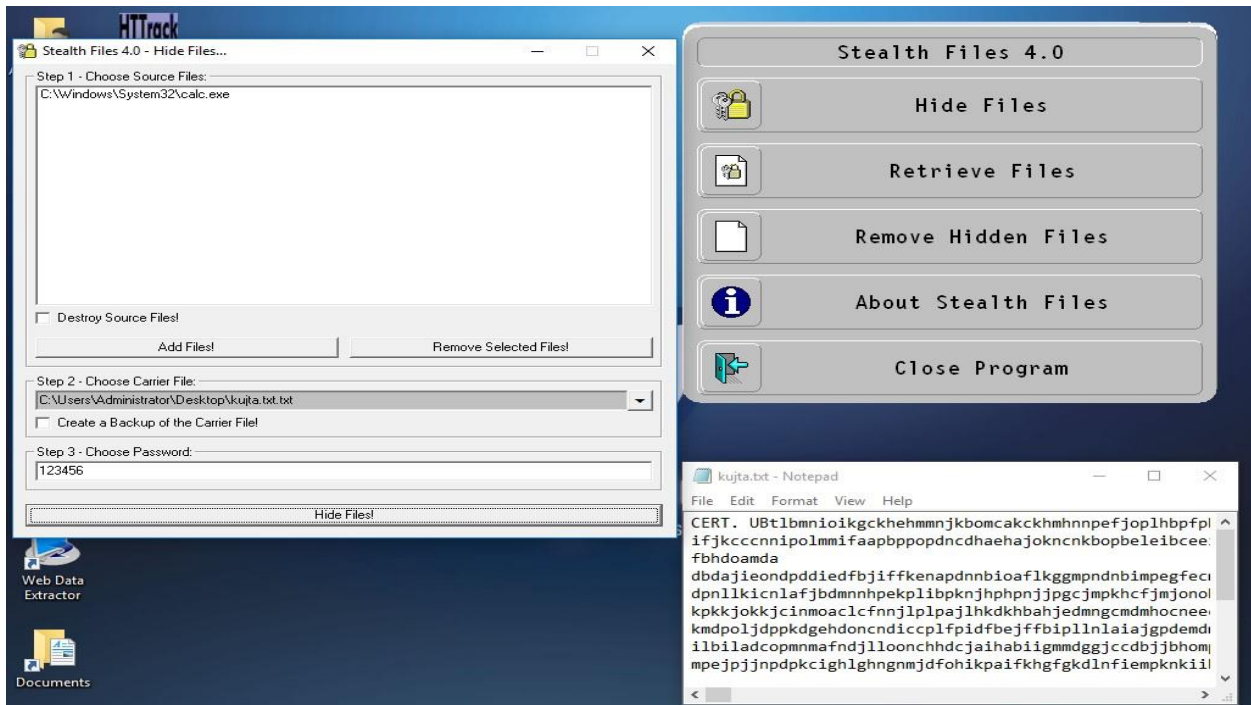


Figura 10

Stealth Retrieve procesi, në figurën mëposhtme:

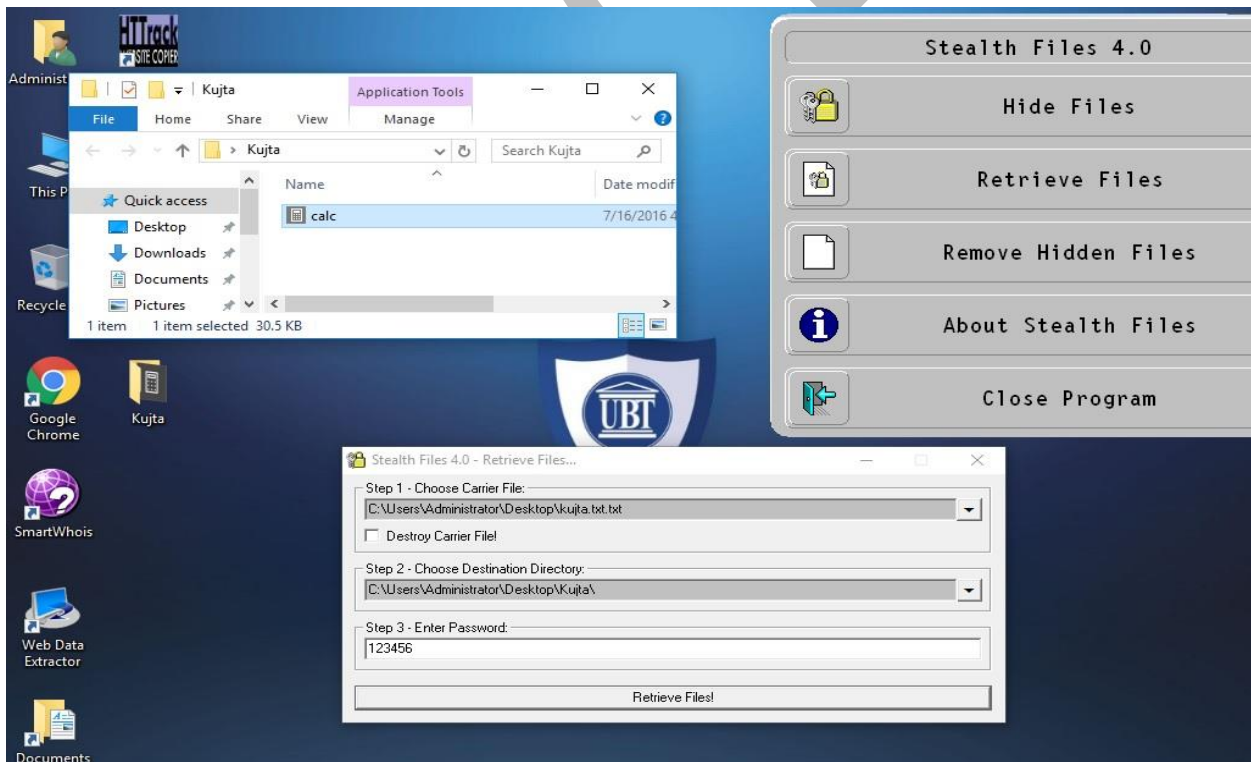


Figura 11

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:

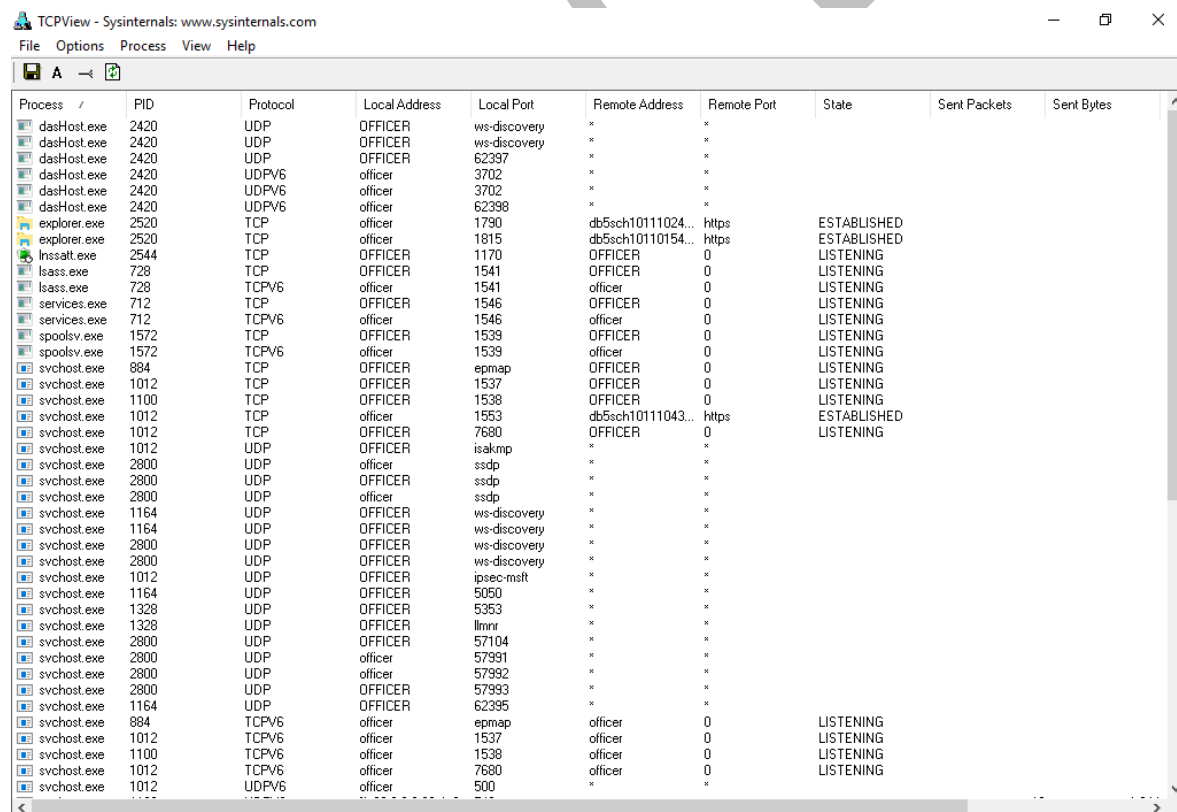
Çka është Trojans and Backdoors

Trojani është program që përmban kod të demshëm dhe mund të jetë i rrezikshëm për sistemet kompjuterike dhe largohet me veshitësi, por ka programe të posaqme për 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 të pajisja e fundme.

Skenari I perdorur:



The screenshot shows the TCPView application window with the following columns: Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, and Sent Bytes. The data is as follows:

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		
lsass.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	linwe	*	*			
svchost.exe	2600	UDP	OFFICER	57104	*	*			
svchost.exe	2600	UDP	officer	57391	*	*			
svchost.exe	2600	UDP	officer	57392	*	*			
svchost.exe	2600	UDP	OFFICER	57393	*	*			
svchost.exe	2600	UDP	OFFICER	57395	*	*			
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:

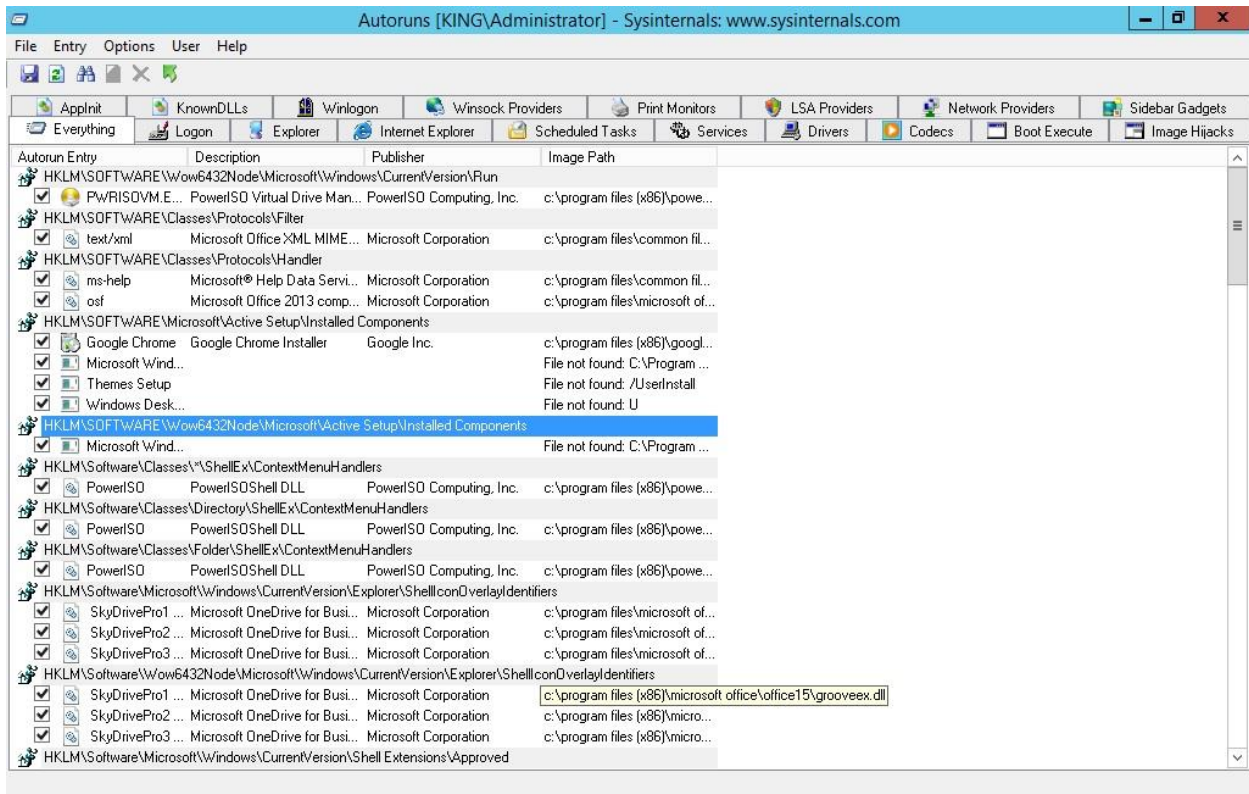
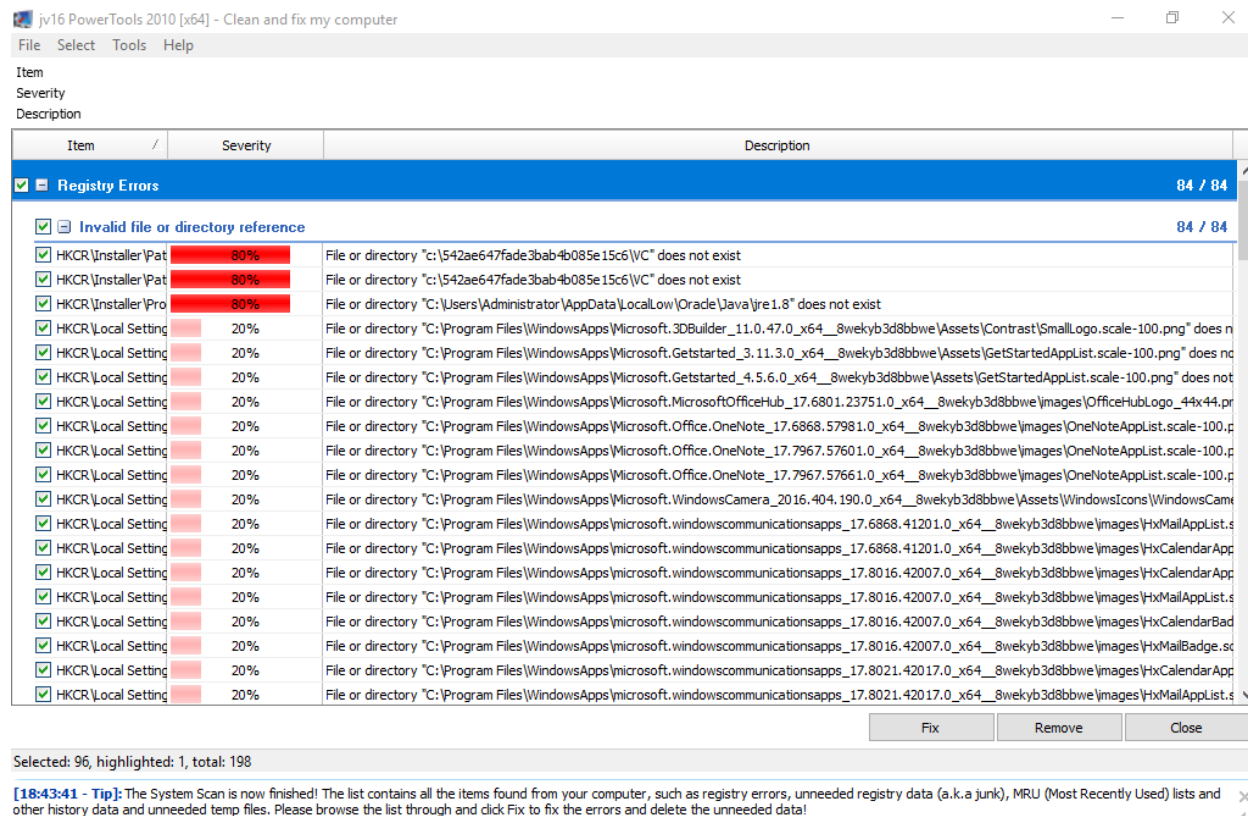


Figura 13

Analiza e trete "III"

JV 16

Skenari I perdorur:



The screenshot shows the 'Clean and fix my computer' window in PowerTools 2010. It displays a list of registry errors under the heading 'Registry Errors' (84 / 84). The errors are categorized as 'Invalid file or directory reference' (84 / 84). The list includes items like 'HKCR\Installer\Pat' with 80% severity and 'HKCR\Local Setting' with 20% severity. The description for each error is 'File or directory "C:\Users\Administrator\AppData\Local\Oracle\Java\re1.8" does not exist' or similar paths. At the bottom, there are buttons for 'Fix', 'Remove', and 'Close'. A status bar indicates 'Selected: 96, highlighted: 1, total: 198'. A tip at the bottom states: '[18:43:41 - Tip]: The System Scan is now finished! The list contains all the items found from your computer, such as registry errors, unneeded registry data (a.k.a junk), MRU (Most Recently Used) lists and other history data and unneeded temp files. Please browse the list through and click Fix to fix the errors and delete the unneeded data!'

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 është program i vet-replikueshem që prodhon kodin e vet duke u kopjuar në kode të tjera të ekzekutueshme dhe është i demshëm për sistemin kompjuterik, ndërsa ekzekutimi i kodit të Worms-it ka mundësi të infektimit të shumë pajisjeve të 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:

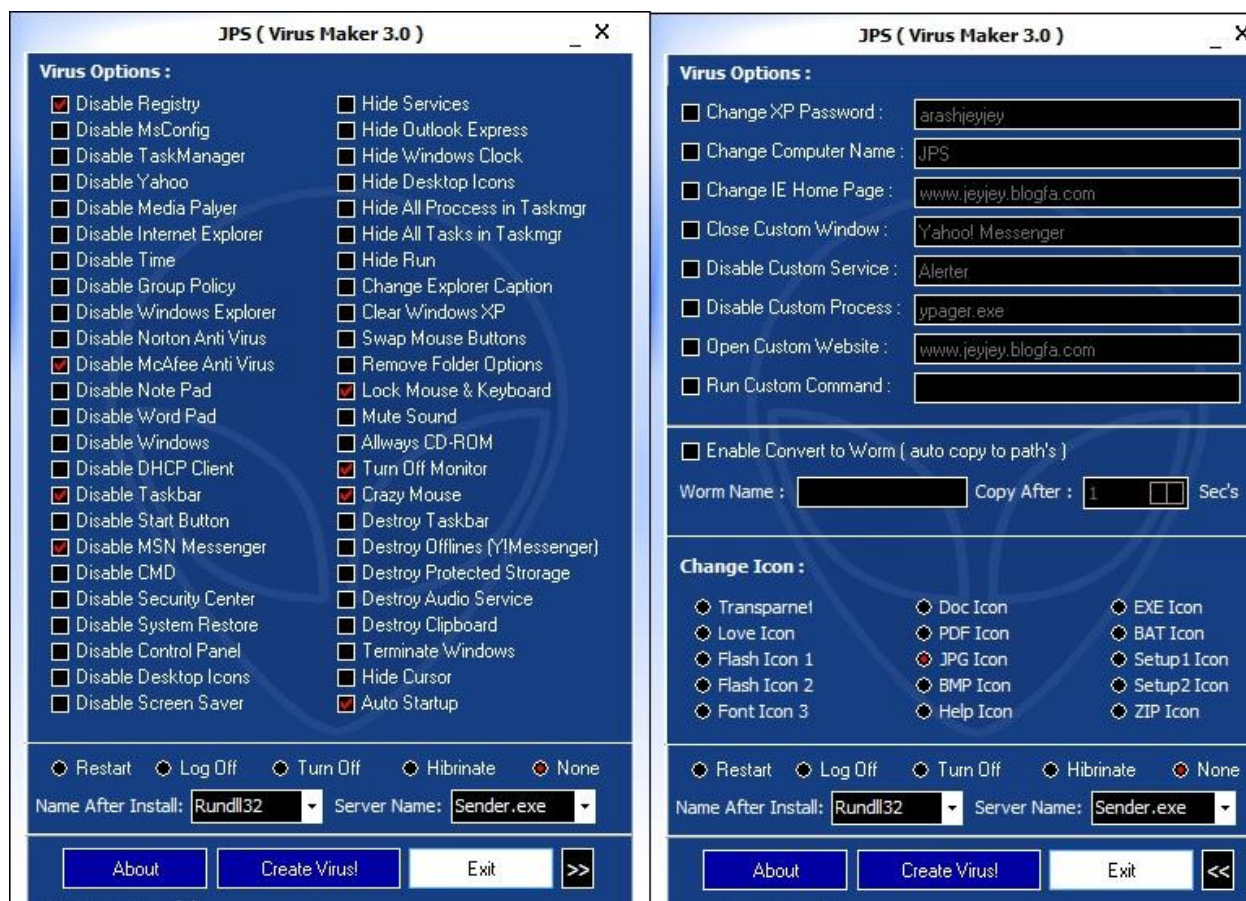


Figura 15

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 përgjuesit janë lloje të programeve apo pajisje harduer-ke që monitorojnë çdo bit të informates, që hyn ose del nga rrjeti kompjuterik.

Analiza e pare “I”

“TheDude”

Skenari I perdorur:

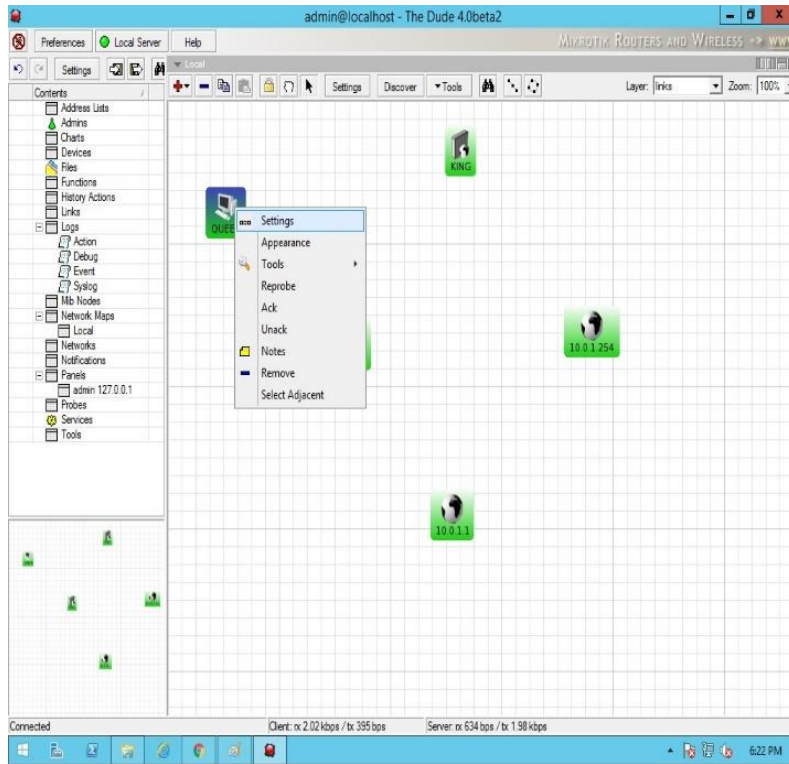


Figura 16

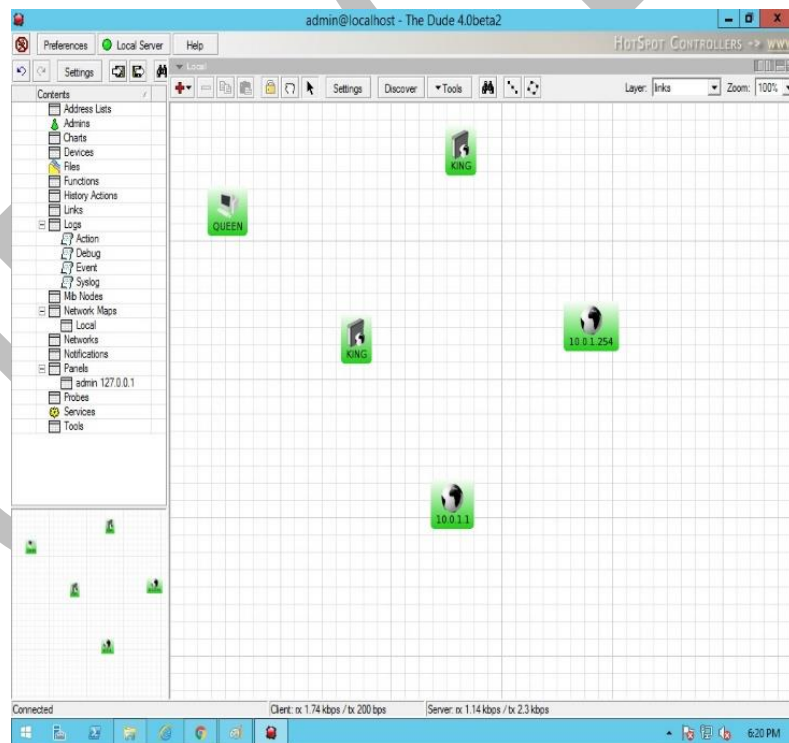


Figura 17

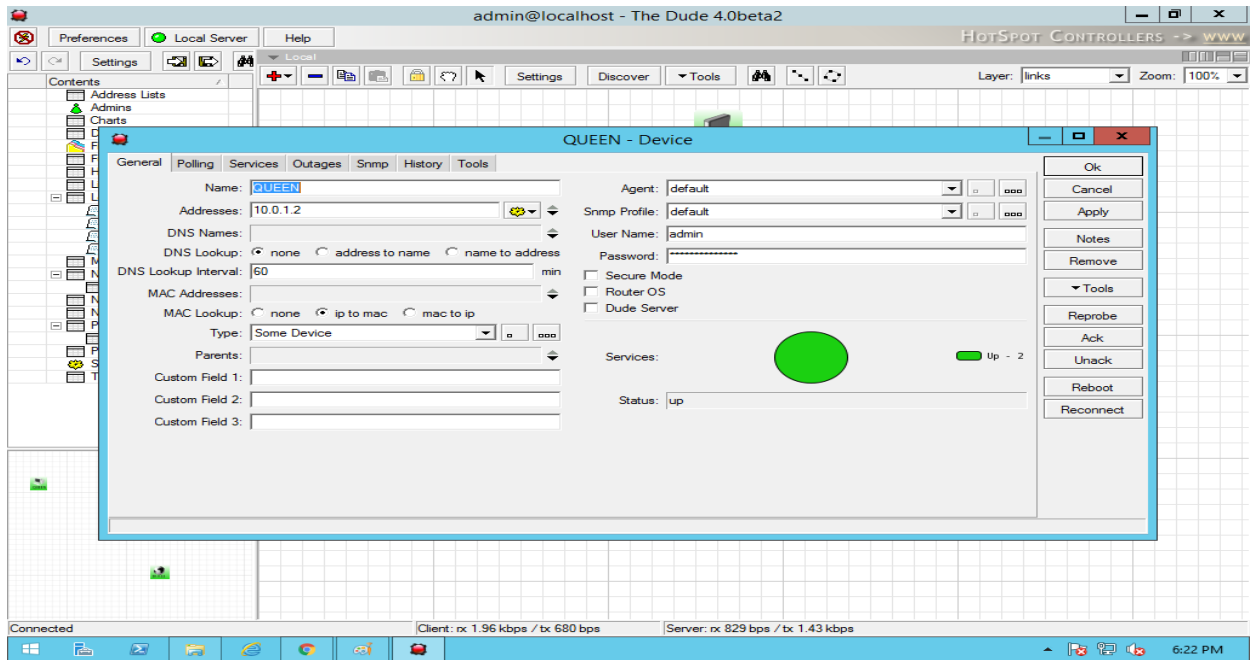


Figura 18

Analiza e dyte "II" "WireShark"

Skenari I perdorur:

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Info. Key packets include:

- Packet 2: ARP request from 10.0.1.2 to 10.0.1.4 asking for the MAC address of 10.0.1.23.
- Packet 3: ARP reply from 10.0.1.23 to 10.0.1.2.
- Packet 4: CDP packet from Cisco_2d:40:a5 to Cisco_2d:40:a5.
- Packet 5: CDP packet from Cisco_2d:40:a5 to Cisco_2d:40:a5.
- Packet 6: CDP packet from Cisco_2d:40:a5 to Cisco_2d:40:a5.
- Packet 8: NBNS Name query for NBSTAT from 10.0.1.2 to 10.0.1.4.
- Packet 9: NBNS Name query response for NBSTAT from 10.0.1.4 to 10.0.1.2.
- Packets 10-16: SMB2 Close Request and Close Response sequence between 10.0.1.2 and 10.0.1.4.
- Packet 16: TCP ACK from 10.0.1.4 to 10.0.1.2 for a Microsoft-DS connection.

The packet details pane for Frame 1 shows the structure: IEEE 802.3 Ethernet, Logical-Link Control, and Spanning Tree Protocol. The packet bytes pane shows the raw hex and ASCII data.

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

- Trajtime 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:f9bfff02::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	Dynam	
12	5.160801	Cisco_2d:40:a5	CDP/VTP/DTP/PagP/UD DTP	Dynam	
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	NBSS
20	7.094165	10.0.1.2	10.0.1.4	TCP	microSOFT-RE > 8888 [ACK] Seq=1 ACK=7 Win=2031 Len=0 SFE=1 SDF

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..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

User Agent

Sockets Requests

[Legal Disclaimer](http://www.socketsoft.net/) <http://www.socketsoft.net/>

Ready

Figura 20