

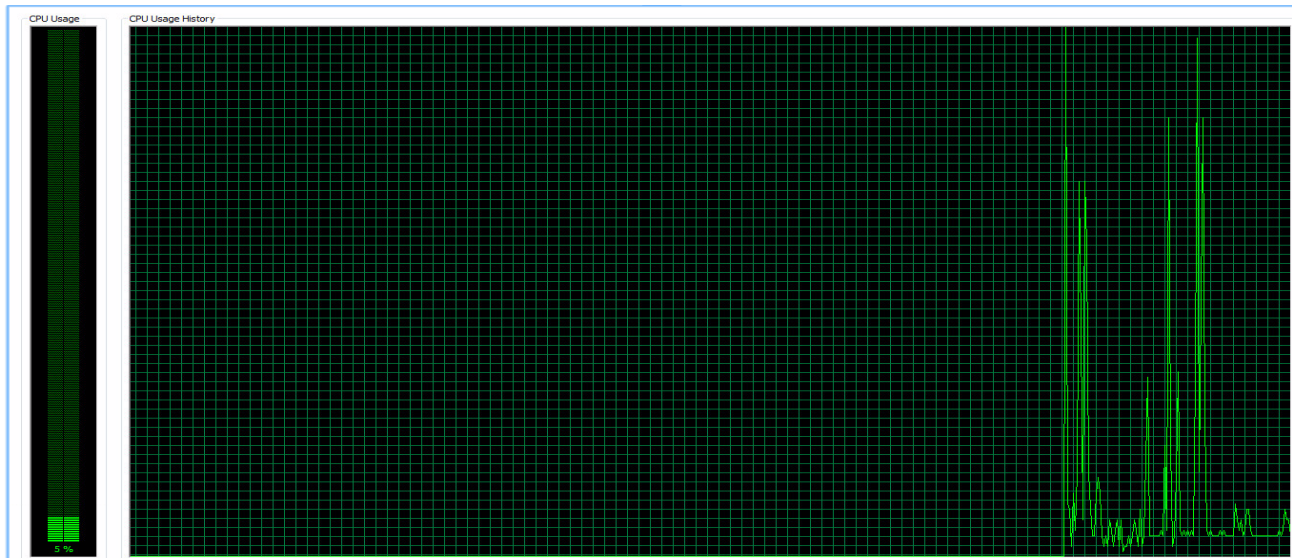
# Analysis Report

by

**Team 6 (Dhivya Govindarajan, Sushant Murdeshwar, Ashish Pandit)**

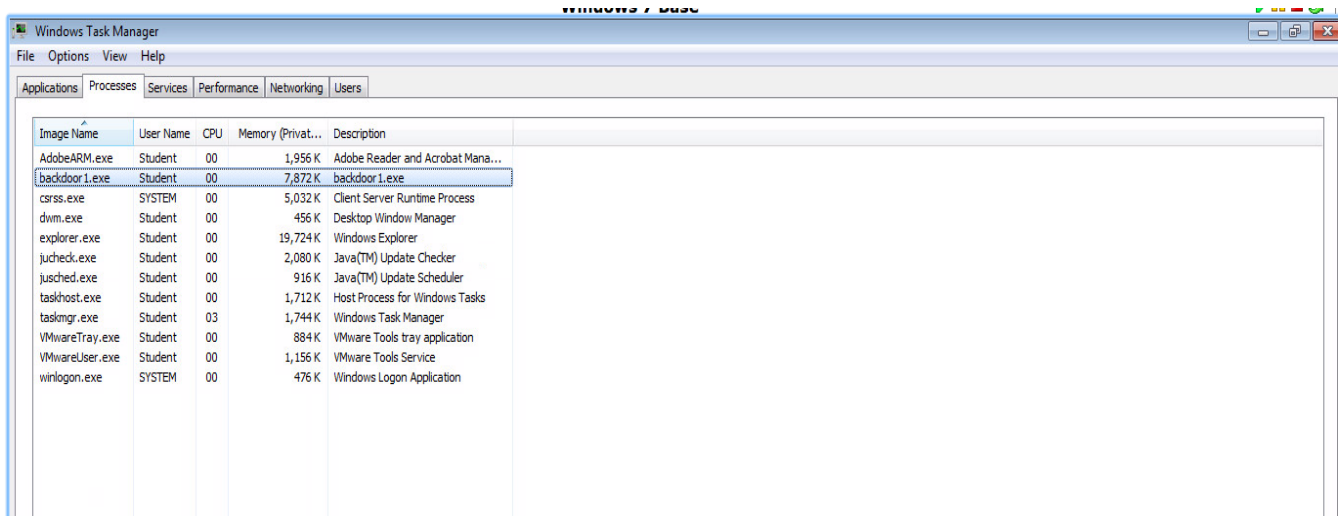
This report is the analysis report of **Team 8** malware (Nitish Ganesan; Pradeepkumar Duvvur; Nandakumar Gunalan). The malware identified is the Keylogger which captures the keystrokes and sends it through the server using a TCP connection. The following section provides the detailed analysis performed to detect the malware.

1. We started with the system's CPU usage in the task manager. We saw the usage spiked almost upto 100. This seemed unusual for the system to spike 100% when none of the applications were open.



**Figure 1 : CPU usage of the system**

2. Observing the spikes, we looked at the Processes section to identify what processes were open and running. We observed that two processes backdoor1.exe and explorer.exe were consuming significant amount of resources, as shown in the Fig 2. On analysing, we found that the explorer.exe is the process of the windows system for the user interface functions and it was not the malware. So, we focussed on the backdoor1.exe



**Figure 2 : Identified the active Processes in the Task Manager**

- 3 . Although we doubted that backdoor1.exe was malicious, we were unable to find what exactly the .exe was doing. To explore more on it, we used the process hacker tool. The tool gives the detailed information of the system's activity. We found that the backdoor1.exe was consuming significant resources.

Name	PID	CPU	I/O Total...	Private B...	User Name	Description
System Idle Process	0	94.52		0	NT AUTHORITY\SYSTEM	
System	4	0.46		48 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	252			216 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Interrupts		0.25		0		Interrupts and DPCs
csrss.exe	352			1.24 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	408			876 kB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	488	1.63		4.12 MB	NT AUTHORITY\SYSTEM	Services and Controller app
lsass.exe	504			2.51 MB	NT AUTHORITY\SYSTEM	Local Security Authority Process
lsmd.exe	512			1.14 MB	NT AUTHORITY\SYSTEM	Local Session Manager Service
csrss.exe	416	0.61	24 B/s	9.3 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	464			1.53 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
explorer.exe	940	0.35		26.02 MB	WIN732VL\Student	Windows Explorer
VMwareTray.exe	1368			2.26 MB	WIN732VL\Student	VMware Tools tray application
VMwareUser.exe	1444	0.13		2.92 MB	WIN732VL\Student	VMware Tools Service
AdobeARM.exe	1264			2.48 MB	WIN732VL\Student	Adobe Reader and Acrobat Manager
jusched.exe	1492			1.2 MB	WIN732VL\Student	Java(TM) Update Scheduler
backdoor1.exe	2888	0.20	770 B/s	8.64 MB	WIN732VL\Student	
ProcessHacker.exe	2360	1.64		6.77 MB	WIN732VL\Student	Process Hacker

**Figure 3 : Identified backdoor1.exe using the Process Hacker Tool**

4. Analysing the possibilities, we found in the Network section of the Process Hacker that the backdoor1.exe established a TCP connection and kept listening all the time as shown in the Fig 4. We also verified all the other connections established and we confirmed that the other .exe files are the Windows processes.

Name	Local Address	Local...	Remote Address	Rem...	Prot...	State	Owner
backdoor1.exe	WIN732VLrit.edu	1235	Windows7Bas-001	49405	TCP	Established	
backdoor1.exe	WIN732VLrit.edu	1235			TCP	Listen	
jucheck.exe	WIN732VLrit.edu	49186	a23-37-29-200.dep...	443	TCP	Close Wait	
jussched.exe	WIN732VLrit.edu	49254	a172-231-148-131....	443	TCP	Close Wait	
lsass.exe	WIN732VL	49156			TCP	Listen	
lsass.exe	WIN732VL	49156			TCP6	Listen	
services.exe	WIN732VL	49155			TCP	Listen	
services.exe	WIN732VL	49155			TCP6	Listen	
svchost.exe	WIN732VL	5355			UDP		Dnscache
svchost.exe	WIN732VL	1900			UDP		SSDPSRV
svchost.exe	WIN732VLrit.edu	1900			UDP		SSDPSRV
svchost.exe	WIN732VL	3702			UDP		FDResPub
svchost.exe	WIN732VL	49382			UDP		FDResPub
svchost.exe	WIN732VLrit.edu	49468			UDP		SSDPSRV
svchost.exe	WIN732VL	49469			UDP		SSDPSRV
svchost.exe	WIN732VL	1900			UDP6		SSDPSRV
svchost.exe	WIN732VL	3702			UDP6		FDResPub
svchost.exe	WIN732VL	49383			UDP6		FDResPub
svchost.exe	WIN732VL	49467			UDP6		SSDPSRV
svchost.exe	WIN732VL	49157			TCP	Listen	PolicyAgent
svchost.exe	WIN732VL	49157			TCP6	Listen	PolicyAgent
svchost.exe	WIN732VL	135			TCP	Listen	RpcSs
svchost.exe	WIN732VL	135			TCP6	Listen	RpcSs
svchost.exe	WIN732VL	49153			TCP	Listen	eventlog
svchost.exe	WIN732VL	49153			TCP6	Listen	eventlog
svchost.exe	WIN732VL	49154			TCP	Listen	Schedule
svchost.exe	WIN732VL	49154			TCP6	Listen	Schedule
svchost.exe	WIN732VL	500			UDP		IKEEXT

**Figure 4 : Network connection established by the backdoor1.exe**

- Tracking the backdoor1.exe file, we also found the backdoor1.exe.log file. We had to change the folder options to unhide the files as all of these files were hidden. The log file contained information about the source file backdoor.pyw written in python, the network connection using socket and the socket's source file socket.pyc

```

backdoor1.exe.log - Notepad
File Edit Format View Help
Traceback (most recent call last):
  File "backdoor.pyw", line 8, in <module>
    File "socket.pyc", line 228, in meth
socket.error: [Errno 10048] only one usage of each socket address (protocol/network address/port) is normally permitted
Traceback (most recent call last):
  File "backdoor.pyw", line 8, in <module>
    File "socket.pyc", line 228, in meth
socket.error: [Errno 10048] only one usage of each socket address (protocol/network address/port) is normally permitted

```

**Figure 5 : Identified the malware's Log file**

- We then used the TCPView tool to identify where and how much data is been sent. We found that the backdoor1.exe established a TCP connection and was listening at the local port 1235. We noticed that whenever a key was pressed, the data packets were sent. In the below fig 6, we noticed that 9 bytes of data packets were sent to the address "windows7bas-001".

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
backdoor1.exe	2320	TCP	win732v.lit.edu	1235	windows7bas-001	49405	ESTABLISHED	9		9	
backdoor1.exe	2320	TCP	win732v.lit.edu	1235	WIN732VL	0	LISTENING				
lsass.exe	528	TCP	win732v.lit.edu	49156	WIN732VL	0	LISTENING				
lsass.exe	528	TCPV6	win732v.lit.edu	49156	win732v.lit.edu	0	LISTENING				
services.exe	512	TCP	win732v.lit.edu	49155	WIN732VL	0	LISTENING				
services.exe	512	TCPV6	win732v.lit.edu	49155	win732v.lit.edu	0	LISTENING				
svchost.exe	704	TCP	win732v.lit.edu	49157	WIN732VL	0	LISTENING				
svchost.exe	752	TCP	win732v.lit.edu	49153	WIN732VL	0	LISTENING				
svchost.exe	960	TCP	win732v.lit.edu	49154	WIN732VL	0	LISTENING				
svchost.exe	1828	TCP	win732v.lit.edu	49157	WIN732VL	0	LISTENING				
svchost.exe	704	TCPV6	win732v.lit.edu	49157	win732v.lit.edu	0	LISTENING				
svchost.exe	752	TCPV6	win732v.lit.edu	49153	win732v.lit.edu	0	LISTENING				
svchost.exe	960	TCPV6	win732v.lit.edu	49154	win732v.lit.edu	0	LISTENING				
svchost.exe	1828	TCPV6	win732v.lit.edu	49157	win732v.lit.edu	0	LISTENING				
System	4	TCP	win732v.lit.edu	netbios-ssn	WIN732VL	0	LISTENING				
System	4	TCP	WIN732VL	microsoft-ds	WIN732VL	0	LISTENING				
System	4	TCP	WIN732VL	wsd	WIN732VL	0	LISTENING				
System	4	TCPV6	win732v.lit.edu	microsoft-ds	win732v.lit.edu	0	LISTENING				
System	4	TCPV6	win732v.lit.edu	wsd	win732v.lit.edu	0	LISTENING				
wininit.exe	412	TCP	WIN732VL	49152	WIN732VL	0	LISTENING				
wininit.exe	412	TCPV6	win732v.lit.edu	49152	win732v.lit.edu	0	LISTENING				
[System Proc...]	0	TCP	win732v.lit.edu	49342	vlinf155.1e100.net	https	TIME_WAIT				
[System Proc...]	0	TCP	win732v.lit.edu	49337	vlinf155.1e100.net	https	TIME_WAIT	1		37	
[System Proc...]	0	TCP	win732v.lit.edu	49335	unsubscrib...entain.com	http	TIME_WAIT				

**Figure 6 : Observed the Network connection details using TCPView**

7. We resolved for the ip address using the TCPview tool and found the ip address as 192.168.206.248 to which the keystrokes are sent as shown in fig 7.

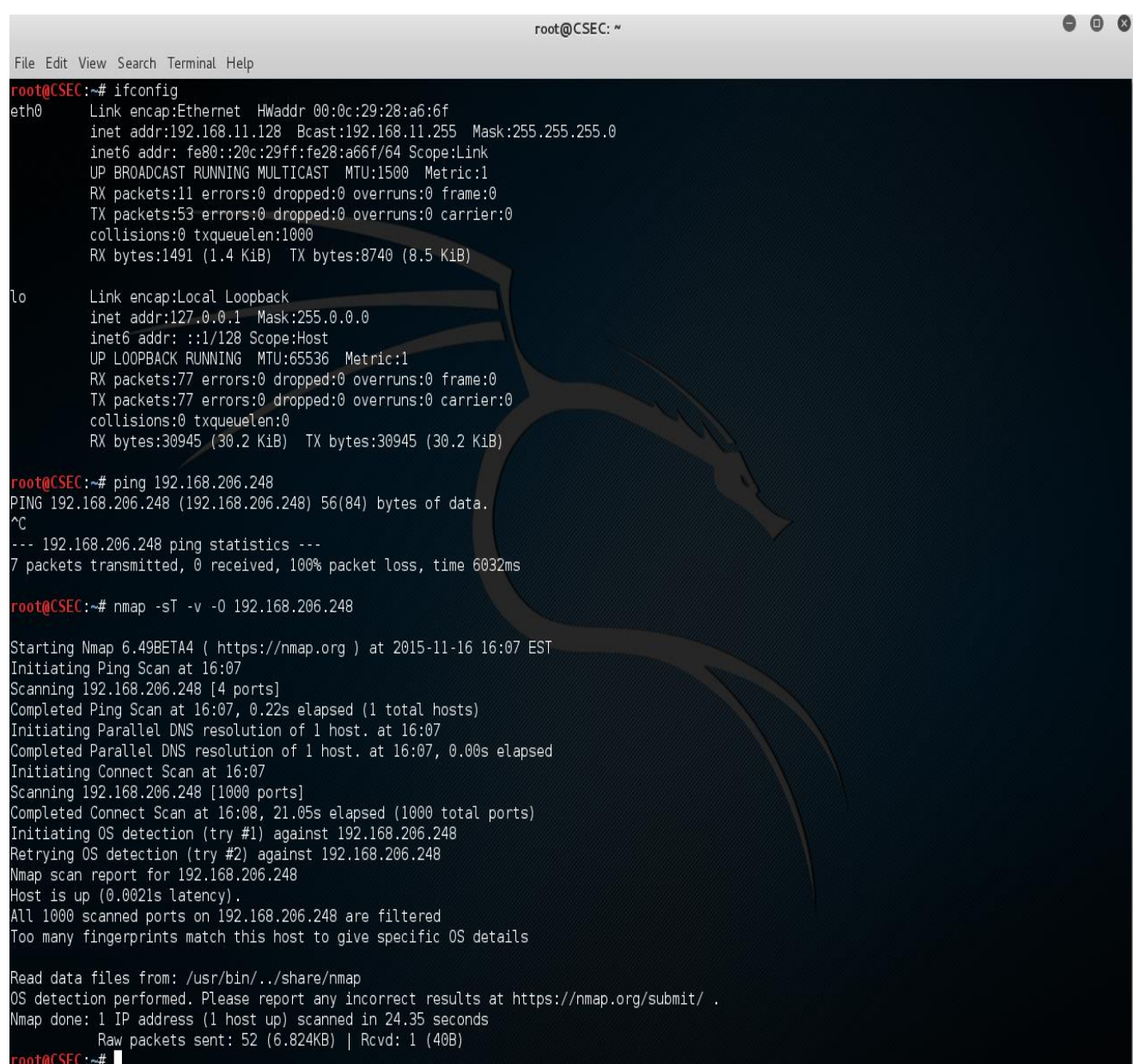
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
backdoor1.exe	2320	TCP	192.168.206.140	1235	192.168.206.248	49405	ESTABLISHED	9		9	
backdoor1.exe	2320	TCP	192.168.206.140	1235	0.0.0.0	0	LISTENING				
lsass.exe	528	TCP	0.0.0.0	49156	0.0.0.0	0	LISTENING				
lsass.exe	528	TCPV6	[0:0:0:0:0:0:0:0]	49156	[0:0:0:0:0:0:0:0]	0	LISTENING				
services.exe	512	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING				
services.exe	512	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	704	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING				
svchost.exe	752	TCP	0.0.0.0	49153	0.0.0.0	0	LISTENING				
svchost.exe	960	TCP	0.0.0.0	49154	0.0.0.0	0	LISTENING				
svchost.exe	1828	TCP	0.0.0.0	49157	0.0.0.0	0	LISTENING				
svchost.exe	704	TCPV6	[0:0:0:0:0:0:0:0]	135	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	752	TCPV6	[0:0:0:0:0:0:0:0]	49153	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	960	TCPV6	[0:0:0:0:0:0:0:0]	49154	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1828	TCPV6	[0:0:0:0:0:0:0:0]	49157	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCP	192.168.206.140	139	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	5357	0.0.0.0	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	445	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	5357	[0:0:0:0:0:0:0:0]	0	LISTENING				
wininit.exe	412	TCP	0.0.0.0	49152	0.0.0.0	0	LISTENING				
wininit.exe	412	TCPV6	[0:0:0:0:0:0:0:0]	49152	[0:0:0:0:0:0:0:0]	0	LISTENING				
[System Proc...]	0	TCP	192.168.206.140	49342	74.125.141.155	443	TIME_WAIT				
[System Proc...]	0	TCP	192.168.206.140	49337	74.125.141.155	443	TIME_WAIT	1		37	

**Figure 7 : Resolving the IP address to which the data is sent**

We then tried to find the host/server name of the ip address. The ip address of the target machine is 192.168.206.248, which is a private ip address. The ip address of the virtual machine used to scan the target to obtain it's hostname is 192.168.11.128, which is also a



private ip address of the lab network we worked from. Hence when we tried to scan the target using Nmap tool, it scanned the machine which has the target's ip address in the Lab environment and displayed the results; but it didn't connect to the server where the keystrokes were sent as the server was in a separate private network. The test is shown in fig 8. So we were unable to resolve it.

A screenshot of a terminal window titled 'root@CSEC: ~'. The terminal shows the output of several commands. First, 'ifconfig' is run, showing details for the 'eth0' interface (IP: 192.168.11.128) and the 'lo' loopback interface (IP: 127.0.0.1). Next, a 'ping' command is executed to 192.168.206.248, resulting in a 100% packet loss. Finally, an 'nmap -sT -v -O 192.168.206.248' command is run, showing a detailed scan report where all 1000 ports are filtered. A large, faint dragon watermark is visible in the background of the terminal window.

```
root@CSEC:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:28:a6:6f
          inet addr:192.168.11.128  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:a66f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1491 (1.4 KiB)  TX bytes:8740 (8.5 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:30945 (30.2 KiB)  TX bytes:30945 (30.2 KiB)

root@CSEC:~# ping 192.168.206.248
PING 192.168.206.248 (192.168.206.248) 56(84) bytes of data.
^C
--- 192.168.206.248 ping statistics ---
 7 packets transmitted, 0 received, 100% packet loss, time 6032ms

root@CSEC:~# nmap -sT -v -O 192.168.206.248

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-16 16:07 EST
Initiating Ping Scan at 16:07
Scanning 192.168.206.248 [4 ports]
Completed Ping Scan at 16:07, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:07
Completed Parallel DNS resolution of 1 host. at 16:07, 0.00s elapsed
Initiating Connect Scan at 16:07
Scanning 192.168.206.248 [1000 ports]
Completed Connect Scan at 16:08, 21.05s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.206.248
Retrying OS detection (try #2) against 192.168.206.248
Nmap scan report for 192.168.206.248
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.206.248 are filtered
Too many fingerprints match this host to give specific OS details

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.35 seconds
Raw packets sent: 52 (6.824KB) | Rcvd: 1 (40B)

root@CSEC:~#
```

**Figure 8: Using Ping and NMap to find the host/server name**

## **Conclusion**

Through this investigation phase, we learnt that detecting keyloggers is all about knowing what to look and where to look for.