FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Post Exploit

Agenda

- Review of Lab Activities
- Scope of work
- Post-Exploit Activities
- Environmental analysis
- Pillaging
- Data exfiltration
- Lab 10 Overview

Lab Review

Backdoor Connections

One way to connect to the backdoor is from the attacking system

- Set up a netcat server on the target VM, listening for an incoming connection on port 1234
  - What options let you know it is a server instance you are setting up?
- This allowed us to connect at will, but it also lets anyone else connect
- Seen by vulnerability scanners

Backdoor Connections

Another way is to modify your registry entry so the target machine will phone home to a netcat server listening on Kali

- This is a more realistic use of netcat as a backdoor
- It won’t be seen by vulnerability scanners
- It will only attempt to connect to the Kali machine
- You aren’t leaving a hole in the defenses of the target machine that others could connect to
    - Very bad in a production environment
    - Hackers don’t stop trying to get in when you are doing a pentest

msfvenom

Msfvenom replaced msfpayload and msfencode

- The functionality of both msfpayload and msfencode have been combined into a single tool

Msfvenom still has the same two primary functions

Creating a payload

- Generating the executable binary from the payload

Encoding the payload

- Changing the binary structure of the payload to avoid detection by antivirus programs

Msfvenom Options

Some of the most used options:

- **l** used to generate a list of payloads, encoders, etc.

- **p** specifies the payload to use

- **e** specifies the encoder to use

- **b** allows you to specify bad characters to avoid (\x00)
  - \x00 represents a null byte

- **a** specifies the architecture (x86, x64, etc.)

-- **platform** specifies the target platform

-- **payload-options** lists the payloads options

- **f** specifies the output format

-- **help-formats** lists the possible formats

Bash Scripting

- At their simplest from, they allow you to run several terminal commands one after another
  - The commands are specified in a file
  - You need to make the file executable to run it
- Allows you to create useful scripts to perform common tasks
- Automates simple tasks to save time
- It is good practice to specify the shell you want the terminal to run the script in
  - #! /bin/bash

Scope of Work

Scope of Work

Pen testers need to protect themselves by establishing a clear set of rules for engagement:

- Contract or statement of work needs to be signed
- Review any existing security policies
- Ensure all local laws and regulations are followed
- Have an incident response plan in case of unexpected findings

Client Security Policies

Acceptable Use Policy – What does it cover?

The following needs to be taken into consideration:

- Personal use of company equipment
- Personal employee data on systems
- Ownership of data/rights on client systems
- Ownership of data/rights on company systems

Protect the client

Protecting the client – What does that mean?

The following needs to be taken into consideration:

- Any modifications must be previously approved in writing
- Establish which systems are mission critical of “off limits”
- Document any actions against systems

Protect the client

- Document any changes or modifications so that they can be returned to their original configurations
- Ensure that any data that is uncovered remains protected using encryption (client and tester)
- Ensure any compromised systems require a form of authentication for access
  - Reverse connections
  - Login prompts
  - Certificates

Protect the client

- All sensitive data or information gathered for a pen test report needs to be properly sanitized
  - Screenshots
  - Databases
  - Passwords
- All data needs to be destroyed once the test is complete and the report is submitted

Protect the client

- If the pen tester finds any previous compromise to the systems being tested:
  - Record all actions taken (timestamped)
  - Gather all logs and any evidence of the intrusion
  - Report findings to the client
  - Invoke appropriate incident response

Note: Logs should be backed up prior to testing and not removed, cleared or modified unless specific authorization has been obtained in the contract or statement of work

Environmental Analysis

Network Infrastructure

Compromised systems can be used to:

- Scan for additional subnets
- Identify network routers/switches
- DNS Servers
- Identify network servers

Network Infrastructure

Check for any services running on the compromised system

- Domain accounts
- Neighbor discovery
- VPN connections
- Video Surveillance

Check for installed software on the compromised system

Network Infrastructure

Are there external services being used or third party vendors?

- Office 365
- Hosting
- IT Support
- Social Media

Post-Exploit Activities

Post-Exploit

Once a system has been exploited there are a few things to consider:

- How valuable is the data on the compromised system?
- Can persistent access be maintained?
- Can the system be used to elevate privileges?
- Can the system be used to further exploit the network?

EoP: Escalation of Privilege

There are several techniques an attacker can use to elevate their privileges once they have a compromised a system

- Use a local exploit
- Upgrade to meterpreter shell

Goal is to bypass UAC on Windows and obtain system or admin level privileges

On Linux, root privileges are the goal

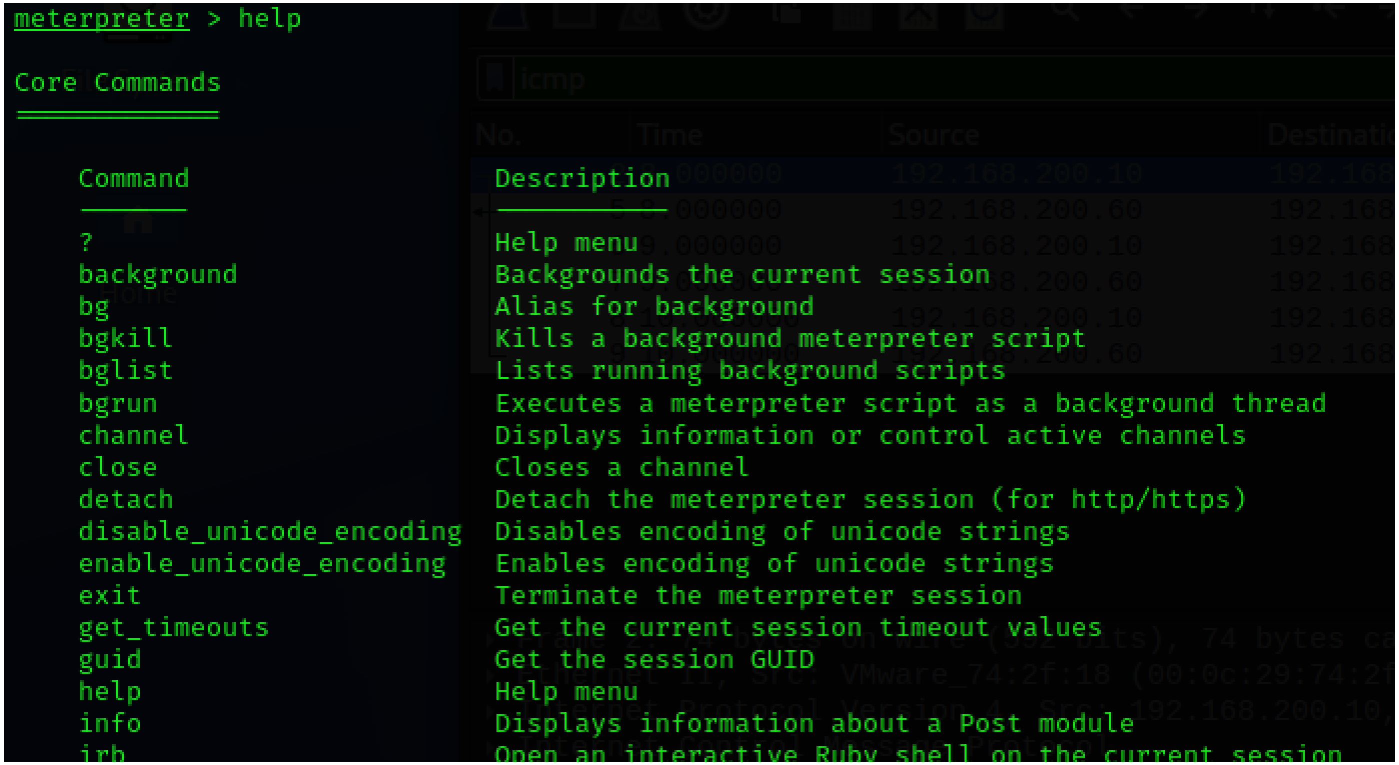
Meterpreter

There are several techniques an attacker can use to elevate their privileges once they have a meterpreter session

- Use getsystem from within meterpreter to attempt to get system privileges
- getprivs can be used to try to turn on all the privileges for the current service
- Migrate to a process running with higher privileges
- Do a hashdump then attack the Administrator account
- Add another account with elevated privileges

Meterpreter Commands

You can get a list of all the commands available in meterpreter by issuing the **help** command



```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
```

psexec

Module that is used to gain access to a system that the attacker has the password or hash for

- Allows the attacker use the actual username and password, or the username and the hash of the password
- Using the hash removes the need to spend time cracking the hash
- Once the attacker gets the Admin hash, they will likely have access to multiple machines

psexec

- Allows you to compromise a system remotely if you have either the password, or hash, for an account
- We can use multi/handler and **freegame.exe** to get the hashes, then we can use psexec to establish a new meterpreter session
  - Allows you to connect at will
  - Multi/handler requires an action by the user
    - Running freegame.exe

clearev

Many of the activities a hacker performs to exploit a machine will leave traces in the event log

- System administrators are notorious for not looking at their event logs

clearev is a meterpreter tool that will wipe the event logs on the remote machine

- This can be a sign to an alert administrator that someone has attacked the machine
  - They still need to find out what the attacker did

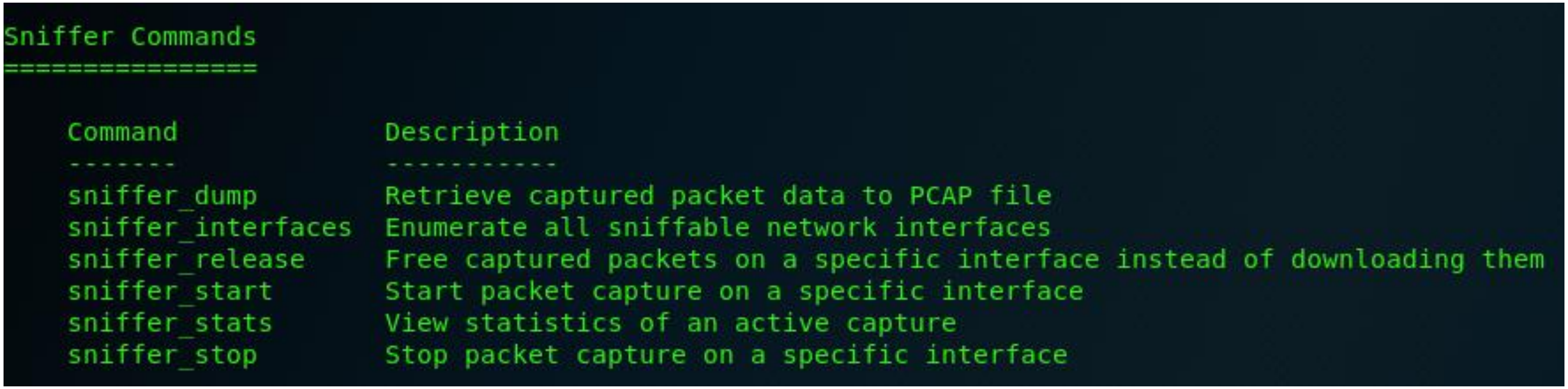
Sniffing

Once an attacker has a machine on the remote network, they can use it as a scanner

- meterpreter's sniffer tool can dump PCAP files to the attacking system for later analysis
- PCAP files should be saved with the .cap file extension

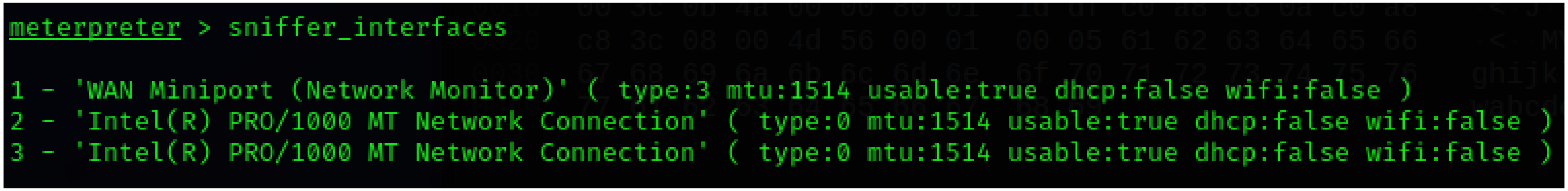
Sniffing from a remote machine is often better because it will likely have access to more internal networks

Sniffer Options



```
Sniffer Commands
================

    Command             Description
    -------             -----------
    sniffer_dump        Retrieve captured packet data to PCAP file
    sniffer_interfaces  Enumerate all sniffable network interfaces
    sniffer_release     Free captured packets on a specific interface instead of downloading them
    sniffer_start       Start packet capture on a specific interface
    sniffer_stats       View statistics of an active capture
    sniffer_stop        Stop packet capture on a specific interface
```



```
meterpreter > sniffer_interfaces

1 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dhcp:false wifi:false )
2 - 'Intel(R) PRO/1000 MT Network Connection' ( type:0 mtu:1514 usable:true dhcp:false wifi:false )
3 - 'Intel(R) PRO/1000 MT Network Connection' ( type:0 mtu:1514 usable:true dhcp:false wifi:false )
```

Pivoting

Pivoting refers to using an exploited machine as a staging point for further attacks

autoroute is a meterpreter tool that allows attackers to exploit dual-homed machines

- Computers with NICs on two different networks
- Sets up a route to the second network and passes the packets though
    - allows for scanning and attacking the second network

Timestomp

- Timestomp is a meterpreter tool that allows an attacker to modify time related file attributes
  - Date Modified
  - Date Accessed
  - Date Created
- This information is often used during digital forensics to track an attack
  - Investigators find an obviously malicious file, then search for other files that were modified around the same time

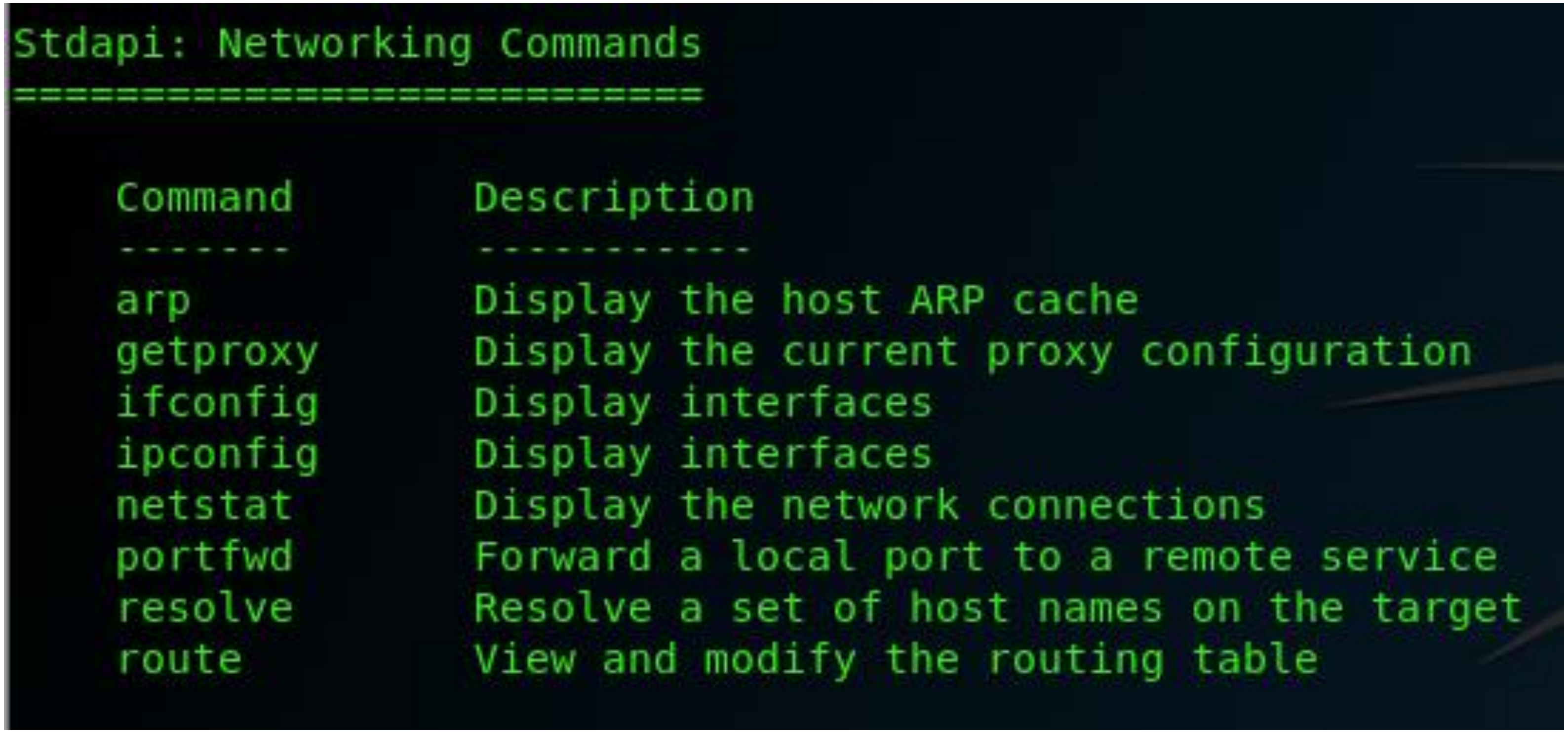
getgui

- Tool for creating remote desktop sessions
  - Allows an attacker to enable remote desktop on the target machine
  - Allows for the creation of user accounts with remote desktop privileges
    - Accounts don’t show up on login screens or in the under user access in control panel
- Has a built in feature that creates a script to remove all traces after it has been used

More Useful Commands

- getuid
  - Get the user ID of the meterpreter sessions
- migrate
  - Migrate your meterpreter session to another process PID
- set, unset, setg, unsetg and save
  - Temporarily and globally setting options
  - **save** can be used in combination with setg to save state
- eventvwr (on Windows machine)
  - Open event viewer

Troubleshooting Commands



```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configuration
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote service
    resolve       Resolve a set of host names on the target
    route         View and modify the routing table
```

hashdump and run hashdump

In the previous lab we needed to have enough privileges associated with our exploit to have enough permissions to use hashdump

- There are two ways to get around this problem
  - You can migrate to a process with appropriate permissions
    - I make you do it this way in the lab to highlight the different privileges associated with different processes
  - If you used getsystem first, you could use the run command in combination with hashdump

http://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/

getgui

Tool for creating remote desktop sessions

- Allows an attacker to enable remote desktop on the target machine
- Allows for the creation of user accounts with remote desktop privileges
  - Accounts don’t show up on login screens or in the user access in control panel

Has a built-in feature that creates a script to remove all traces after it has been used

Password Cracking

Pen testers will need to have their own curated password lists

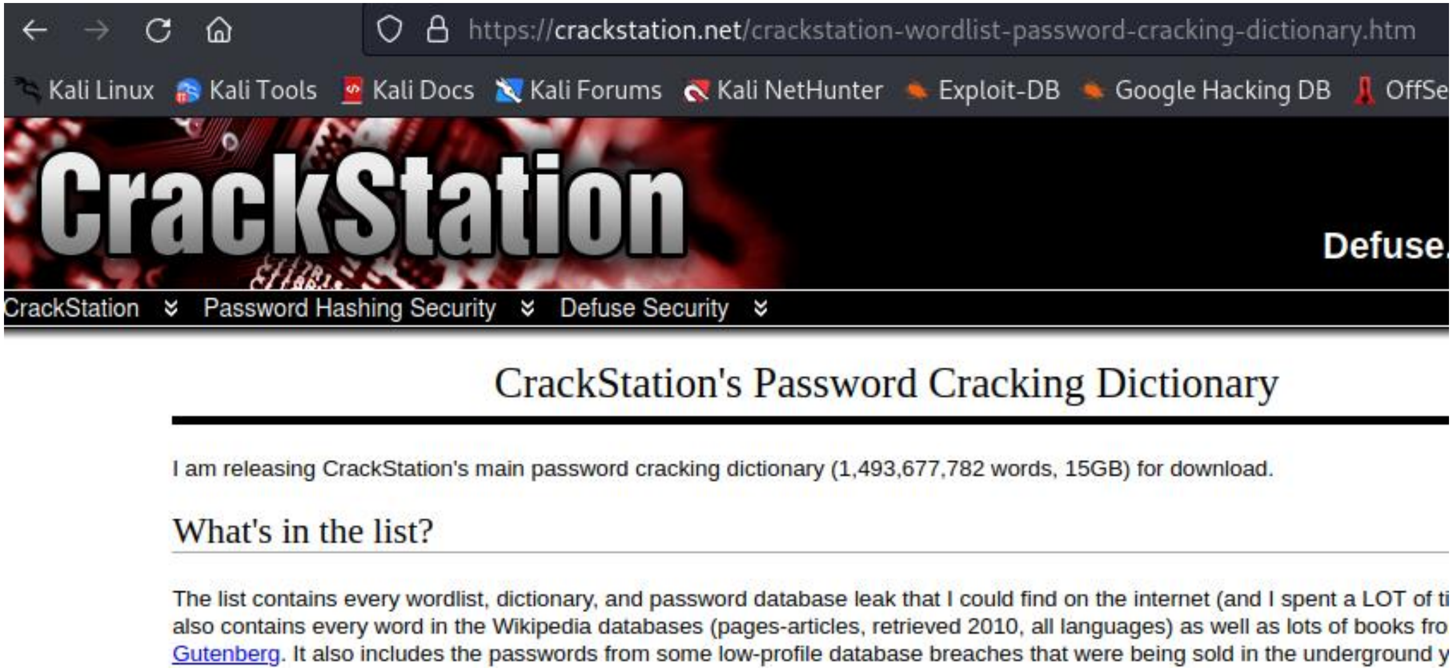
Lists can be trimmed or appended depending on needs

- Password policies (>6 characters, etc.)
- **CeWL** adding organizational keywords

Password Cracking

CrackStation.net has a 15GB (uncompressed) wordlist file:

https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm



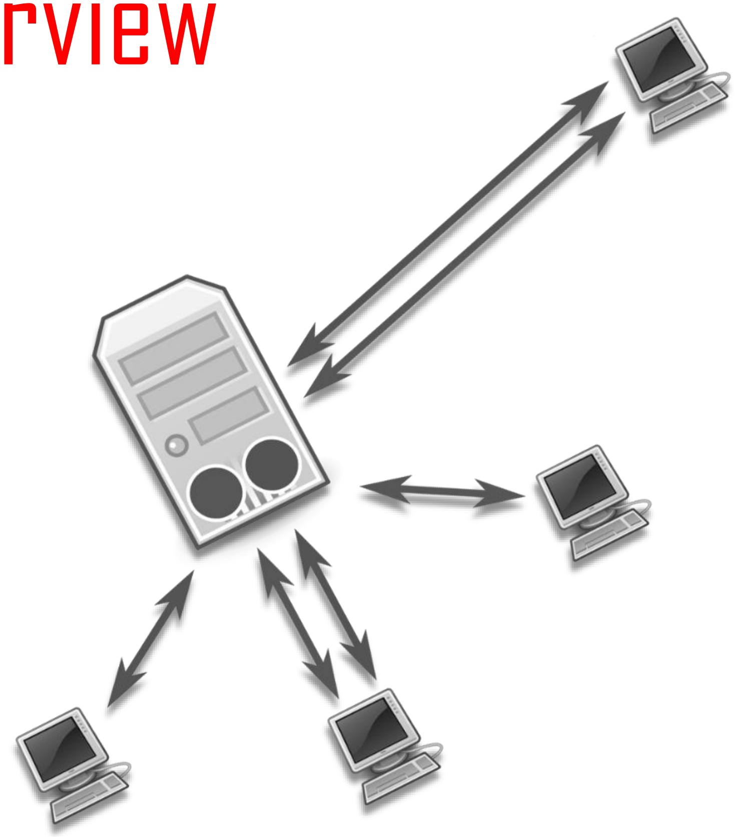
CrackStation's Password Cracking Dictionary

I am releasing CrackStation's main password cracking dictionary (1,493,677,782 words, 15GB) for download.

What's in the list?

The list contains every wordlist, dictionary, and password database leak that I could find on the internet (and I spent a LOT of ti
also contains every word in the Wikipedia databases (pages-articles, retrieved 2010, all languages) as well as lots of books fro
Gutenberg. It also includes the passwords from some low-profile database breaches that were being sold in the underground y

Lab 10 Overview



Lab 10: Post-Exploit Activities

- Meterpreter
- **MS17-010:** EternalBlue
- Post Exploit
- Creating remote desktop sessions
- Event Viewer
- Timestomp
- Sniffing traffic from a compromised Dual Homed machine