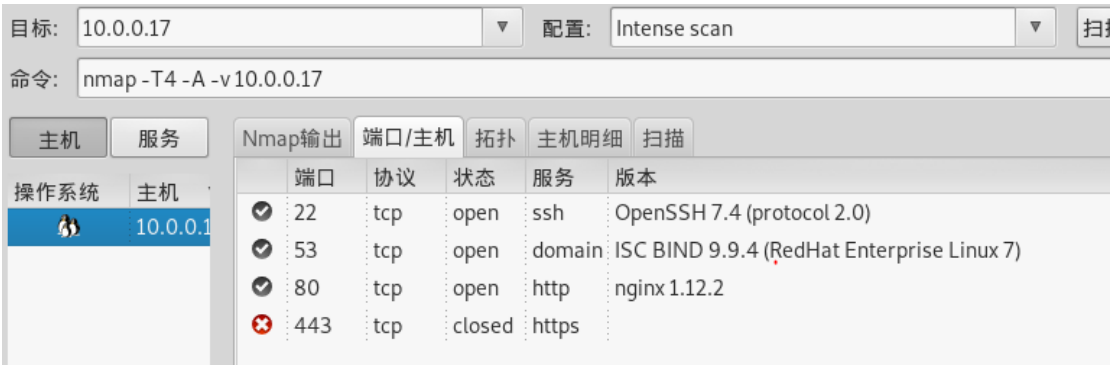
CF assignment 3

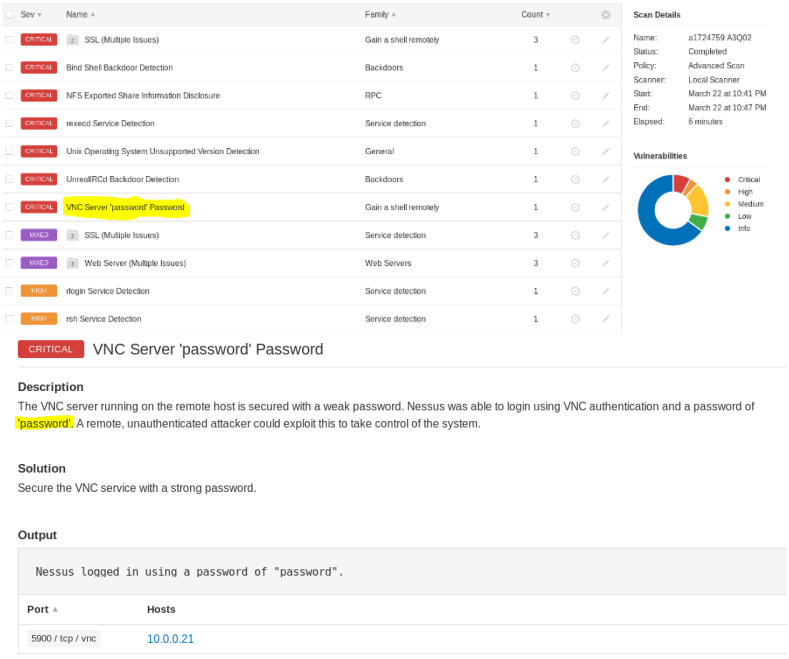
A1691850

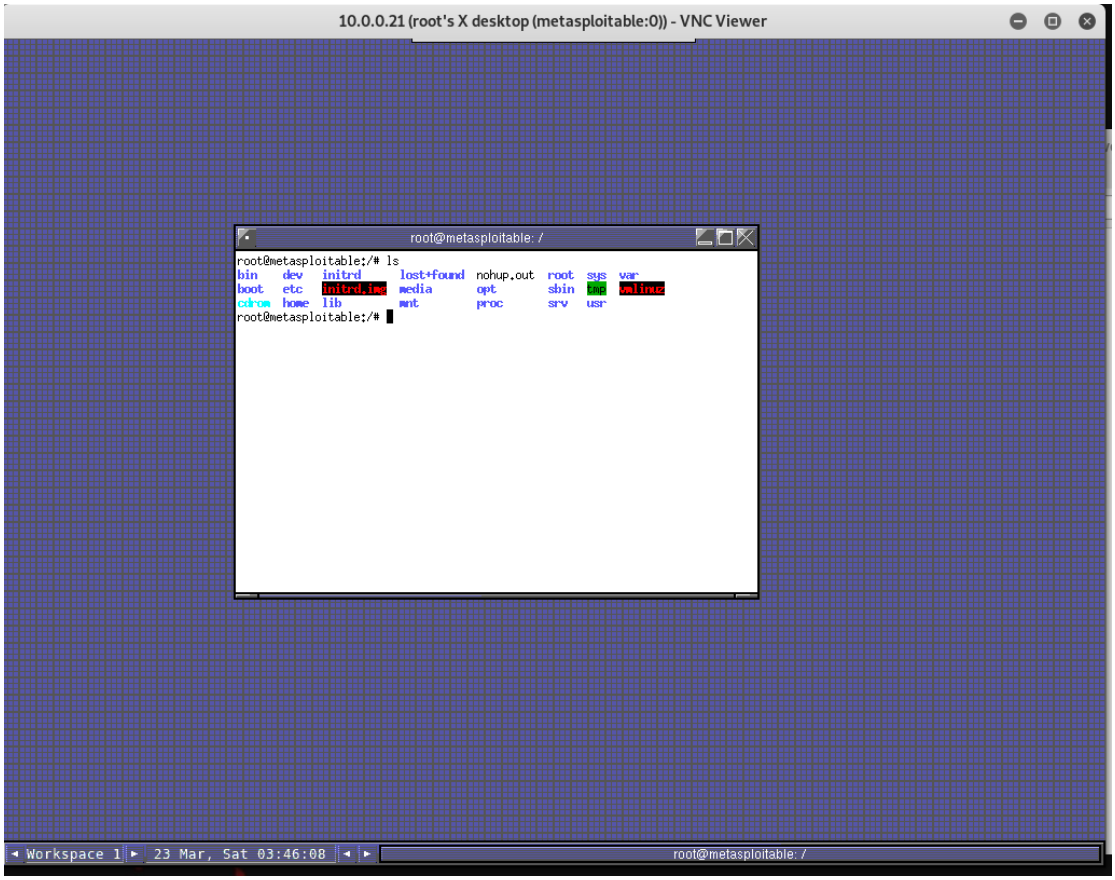
2019/3/23

Q1.



Q2.



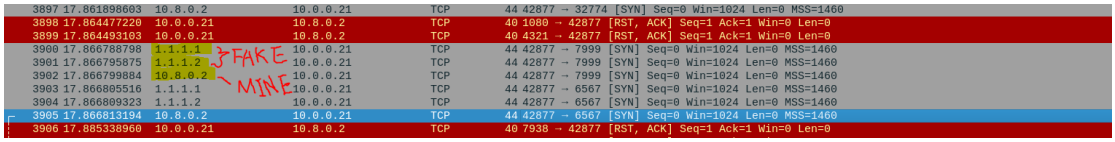


Q3.

How could the decoy option be useful for a black hat hacker?

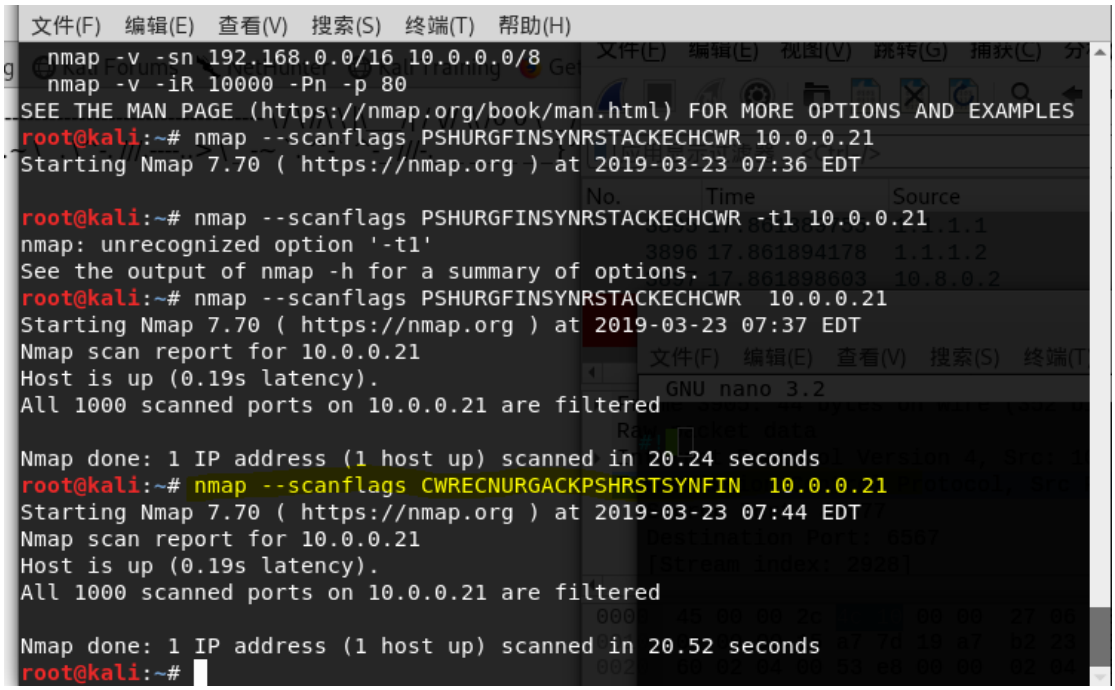
Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. Thus, their IDS might report 5–10 port scans from unique IP addresses, but they won't know which IP was scanning them and which were innocent decoys. While this can be defeated through router path tracing, response-dropping, and other active mechanisms, it is generally an effective technique for hiding your IP address.

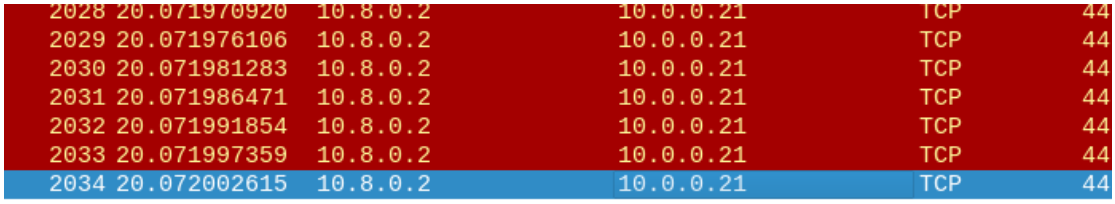
```
root@kali:~/Downloads# nmap -D 1.1.1.1,1.1.1.2,ME 10.0.0.21
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-23 04:03 EDT
Nmap scan report for 10.0.0.21
Host is up (0.19s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
```

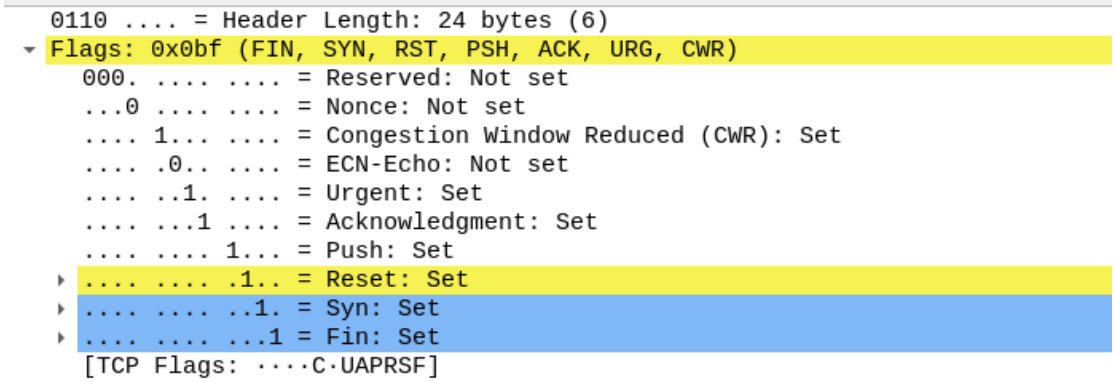


Q4.

Btw, i set-up seven flag bits to 1.





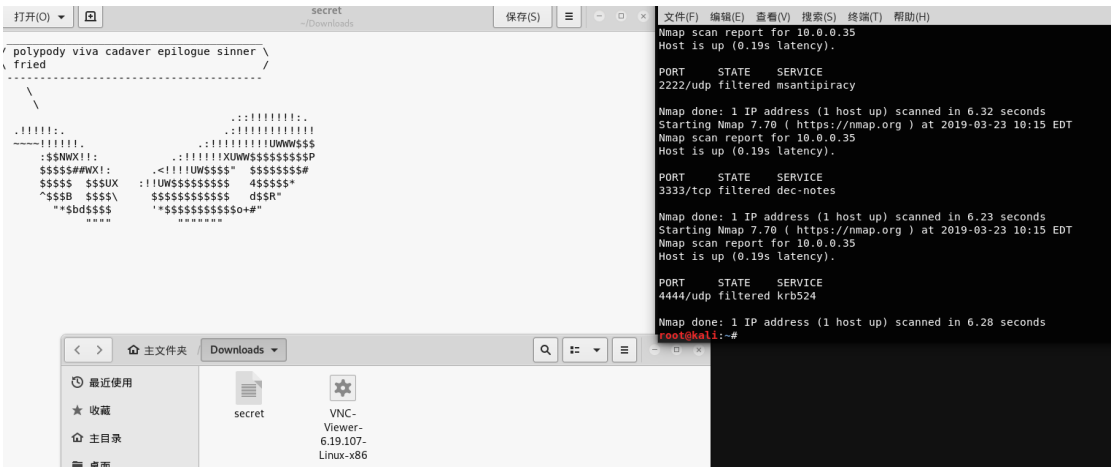


Q5.

```
SYN Stealth Scan Timing: About 56.05% done; ETC: 08:10 (0:01:22 remaining)
Nmap scan report for 10.0.0.35
Host is up (0.19s latency).
Not shown: 40000 filtered ports
PORT      STATE SERVICE
54127/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 176.91 seconds
root@kali:~# nc 10.0.0.35 54127
 _____________________________________
/ demure martial wellborn finochio \
\ shindig echidna                   /
 -------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
root@kali:~#
```

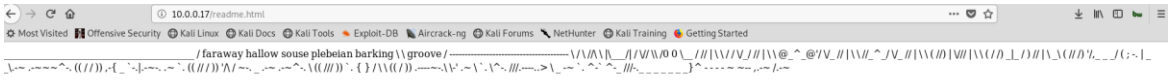
Q6.

```
root@kali: ~
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
  GNU nano 3.2                          q6.sh

#! /bin/bash

#for PORT in  2222 3333 4444;
#do
#nmap --scanflags SYN -PN 10.0.0.35 -p $PORT;
#nmap -sT -PN 10.0.0.35 -p $PORT;
#done
nmap -p 2222 -sU 10.0.0.35
nmap -p 3333 -sT 10.0.0.35
nmap -p 4444 -sU 10.0.0.35


#nmap -F 10.0.0.35
#sleep 1s
#nmap -sT -F 10.0.0.35
x-www-browser 'http://10.0.0.35/secret'
```

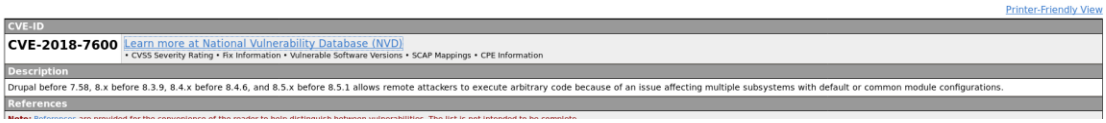


Q7.

```
NSE Timing: About 99.22% done; ETC: 06:45 (0:00:03 remaining)
Nmap scan report for 10.0.0.17
Host is up (0.19s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
53/tcp  open   domain  ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
80/tcp  open   http    nginx 1.12.2
| http-enum:
|_  /readme.html: Interesting, a readme.
|_http-server-header: nginx/1.12.2
443/tcp closed https
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 433.96 seconds
root@kali:~/Downloads# nmap -sV --script http-enum 10.0.0.17
```



Q8.



About CVE-2018-7600

On 28 March 2018, the Drupal core security team released security advisory SA-CORE-2018-002 which discusses a highly critical vulnerability CVE-2018-7600, later nicknamed drupalgeddon2. The vulnerability is present on all Drupal versions 7.x before 7.58, 8.3.x versions before 8.3.9, 8.4.x versions before 8.4.6, and 8.5.x before 8.5.1.

```
$form['account']['mail'] = [
  '#type' => 'email',
  '#title' => $this->t('Email address'),
  '#description' => $this->t('A valid email address. All emails from the system will be sent to this
      address. The email address is not made public and will only be used if you wish to receive a new
      password or wish to receive certain news or notifications by email.'),
  '#required' => !(!$account->getEmail() && $admin),
  '#default_value' => (!$register ? $account->getEmail() : ''),
];
```

Figure 1. Drupal core example of render array key-value pairs

A quick examination of the Drupal security patch revealed the addition of a class called RequestSanitizer. Of note is the method stripDangerousValues, which is called in another method called sanitize. The previous function stripped a control character, '#', from index zero of an array parameter. Below is a snippet of the patch function.

```
protected static function stripDangerousValues($input, array $whitelist, array &$sanitized_keys) {
  if (is_array($input)) {
    foreach ($input as $key => $value) {
      if ($key !== '' && $key[0] === '#' && !in_array($key, $whitelist, TRUE)) {
        unset($input[$key]);
        $sanitized_keys[] = $key;
      }
      else {
        $input[$key] = static::stripDangerousValues($input[$key], $whitelist, $sanitized_keys);
      }
    }
  }
  return $input;
}
```

Figure 2. Drupal patch stripping '#' from parameterized input

CVE-2018-7600 Detail

Current Description

Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.

Source: MITRE
Description Last Modified: 03/29/2018
+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:

Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service