

## CF assignment 3

A1691850

2019/3/23

Q1.

目标: 10.0.0.17 配置: Intense scan 扫描

命令: nmap -T4 -A -v 10.0.0.17

主机	服务	Nmap输出	端口/主机	拓扑	主机明细	扫描	
操作系统	主机		端口	协议	状态	服务	版本
	10.0.0.17		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
			443	tcp	closed	https	

Q2.

Sev	Name	Family	Count	Scan Details
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	Name: a1724759 A3Q02 Status: Completed Policy: Advanced Scan Scanner: Local Scanner Start: March 22 at 10:41 PM End: March 22 at 10:47 PM Elapsed: 6 minutes
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1	
CRITICAL	NFS Exported Share Information Disclosure	RPC	1	
CRITICAL	rexec Service Detection	Service detection	1	
CRITICAL	Unix Operating System Unsupported Version Detection	General	1	
CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1	
MED	SSL (Multiple Issues)	Service detection	3	
MED	Web Server (Multiple Issues)	Web Servers	3	
HIGH	rlogin Service Detection	Service detection	1	
HIGH	rsh Service Detection	Service detection	1	

**CRITICAL** VNC Server 'password' Password

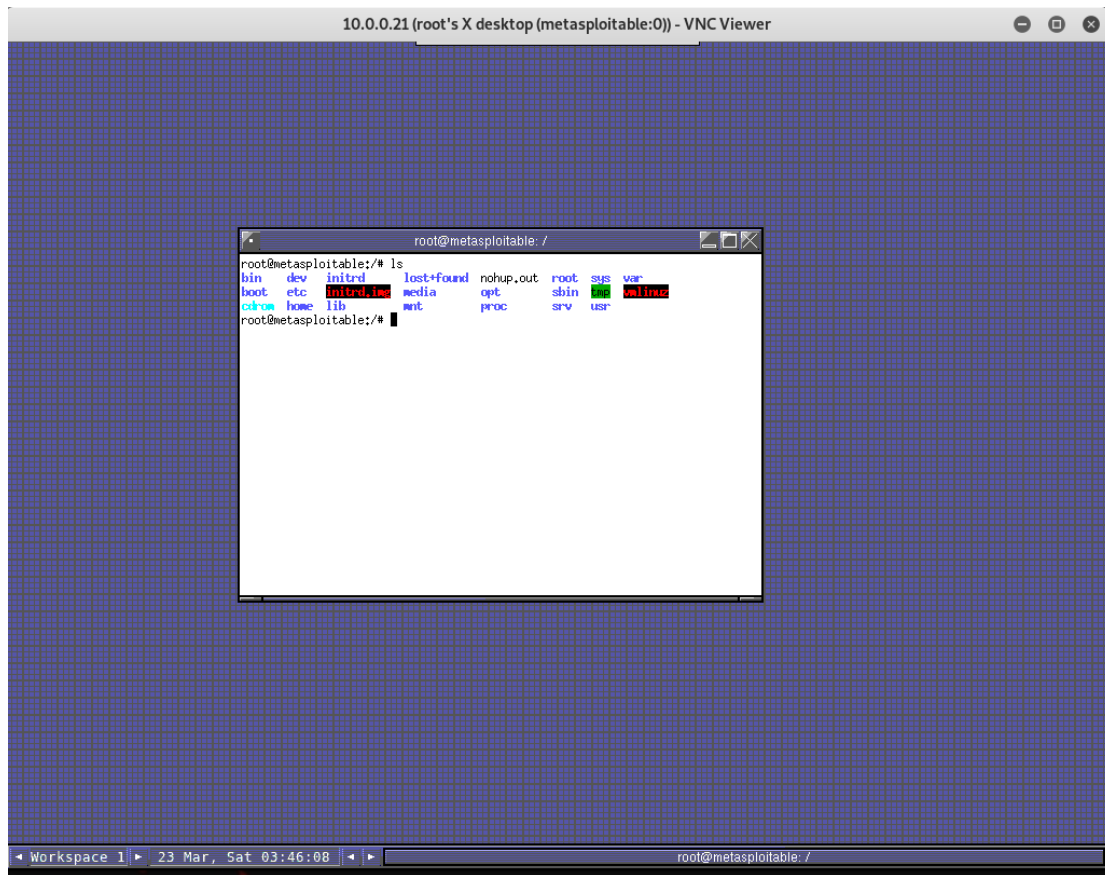
**Description**  
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

**Solution**  
Secure the VNC service with a strong password.

**Output**

Nessus logged in using a password of "password".

Port	Hosts
5900 / tcp / vnc	10.0.0.21



### 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

```

3897	17.861898603	10.8.0.2	10.0.0.21	TCP	44 42877 → 32774 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3898	17.861898603	10.0.0.21	10.8.0.2	TCP	40 4080 → 42877 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3899	17.864493103	10.0.0.21	10.8.0.2	TCP	40 4321 → 42877 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3900	17.866788798	1.1.1.1	10.0.0.21	TCP	44 42877 → 7999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3901	17.866795875	1.1.1.2	10.0.0.21	TCP	44 42877 → 7999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3902	17.866799884	10.8.0.2	10.0.0.21	TCP	44 42877 → 7999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3903	17.866805516	1.1.1.1	10.0.0.21	TCP	44 42877 → 6567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3904	17.866809323	1.1.1.2	10.0.0.21	TCP	44 42877 → 6567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3905	17.866813194	10.8.0.2	10.0.0.21	TCP	44 42877 → 6567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3906	17.885338960	10.0.0.21	10.8.0.2	TCP	40 7938 → 42877 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Q4.

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

```

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap --scanflags PSHURGFINSYNRSTACKECHCWR 10.0.0.21
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-23 07:36 EDT

root@kali:~# nmap --scanflags PSHURGFINSYNRSTACKECHCWR -tl 10.0.0.21
nmap: unrecognized option '-tl'
See the output of nmap -h for a summary of options.
root@kali:~# nmap --scanflags PSHURGFINSYNRSTACKECHCWR 10.0.0.21
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-23 07:37 EDT
Nmap scan report for 10.0.0.21
Host is up (0.19s latency).
All 1000 scanned ports on 10.0.0.21 are filtered

Nmap done: 1 IP address (1 host up) scanned in 20.24 seconds
root@kali:~# nmap --scanflags CWRECNURGACKPSHRSTSYNFIN 10.0.0.21
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-23 07:44 EDT
Nmap scan report for 10.0.0.21
Host is up (0.19s latency).
All 1000 scanned ports on 10.0.0.21 are filtered

Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds
root@kali:~#

```

2028	20.071970920	10.8.0.2	10.0.0.21	TCP	44
2029	20.071976106	10.8.0.2	10.0.0.21	TCP	44
2030	20.071981283	10.8.0.2	10.0.0.21	TCP	44
2031	20.071986471	10.8.0.2	10.0.0.21	TCP	44
2032	20.071991854	10.8.0.2	10.0.0.21	TCP	44
2033	20.071997359	10.8.0.2	10.0.0.21	TCP	44
2034	20.072002615	10.8.0.2	10.0.0.21	TCP	44

```

0110 .... = Header Length: 24 bytes (6)
Flags: 0x0bf (FIN, SYN, RST, PSH, ACK, URG, CWR)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 1... = Congestion Window Reduced (CWR): Set
.... 0... = ECN-Echo: Not set
.... ..1. = Urgent: Set
.... ...1 = Acknowledgment: Set
.... .... 1... = Push: Set
> .... .... 1.. = Reset: Set
> .... .... ..1. = Syn: Set
> .... .... ...1 = Fin: Set
[TCP Flags: ....C-UAPRSF]

```

Q5.

```

root@kali:~# nc -nvzu 10.0.0.35 20000-60000
GNU nano 3.2

```





```

$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