Port Scanning 101
Author - Natalia Wadden

Matrix Reloaded, Bourne Ultimatium and a brief glimpse in Girl with the Dragon Tattoo – these are just a few movies which feature a port scanning technique called nmap.
Before we go to far, let's define nmap. It sounds glamorous, it must be, it is featured in at least 3 major Hollywood films. Nmap aka Network Mapper is a security scanner that is used to detect hosts and services on a computer network – in short it can determine which ports are open, what the operating system (OS) and version is, services that are offered, and what firewalls are used – basically it can create a map of the computer network and hosts.

Nmap is portable, it can be used across multiple platforms, Windows, Mac and Linux, but it is most commonly used in Linux. For this article, I will be using Kali Linux, it's easy and many tools are already built into the OS. My mentor described ports as windows in a building, which means that nmap is looking for the open windows aka ports. So let's dive in and scan our test machine and see if we can find any open ports.

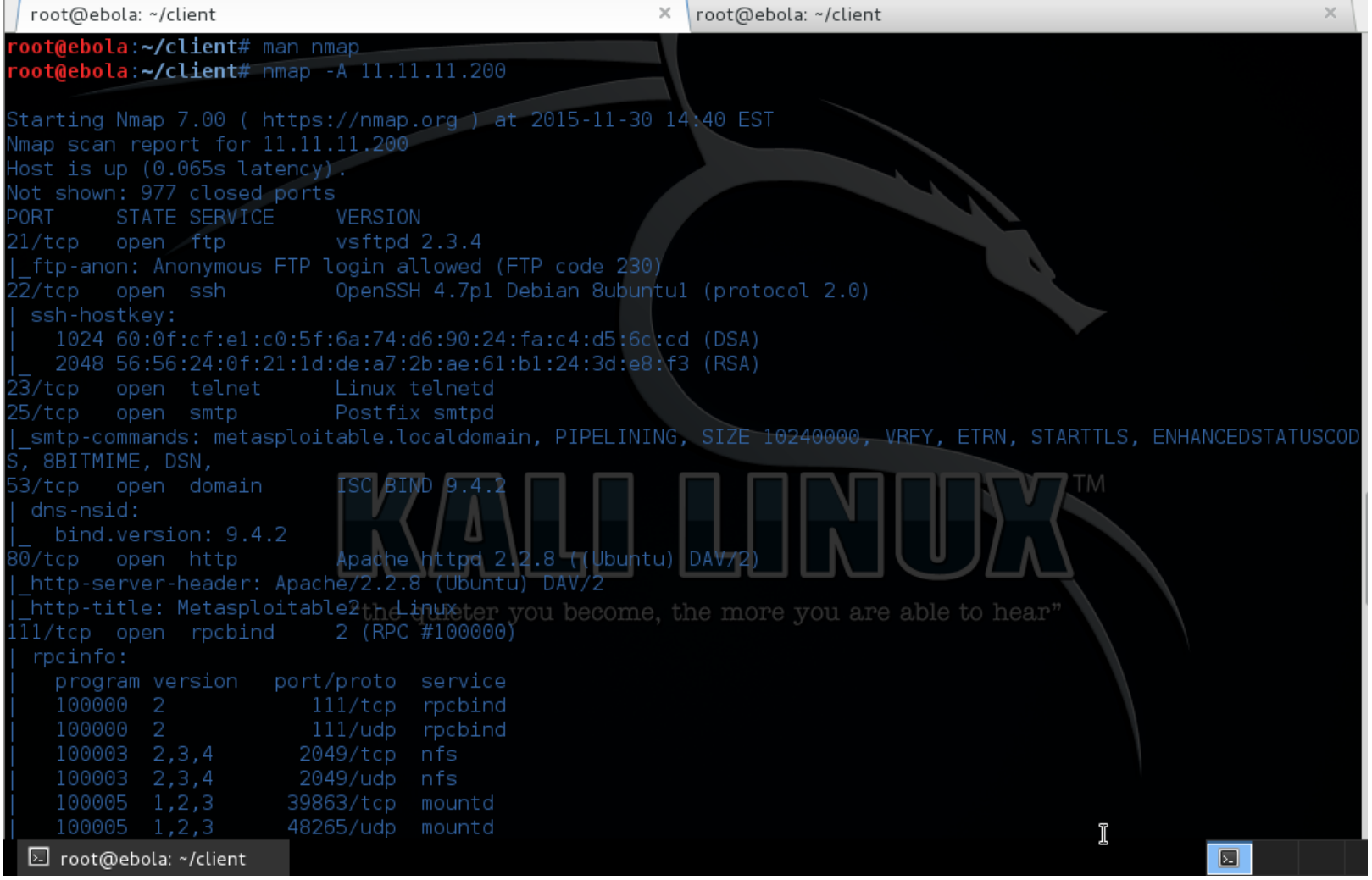
Our simple nmap scan provided us with a significant amount of information, this can be over whelming if you don't know what to look for – let's try to break it down. Nmap has shown us that each of these ports are open via the 3 way TCP handshake. A SYN was sent to an open port, in the case above port 80 (web) and responded with a SYN ACK, the client answered SYN ACK with an ACK, thereby completing the response. An open port 80 is not uncommon, many websites have this open as they require it as part of their business, for example, Amazon, Ebay and Google, all have port 80 open, if they weren't open nobody could see their website.
Now let's try this again but use a UDP (User Datagram Protocol) scan along with nmap, and see what happens. UDP scan does not require the 3 way handshake, which means a request will be sent out, but a response is not necessarily received, there is no guarentee of delivery. UDP is typically used for streaming audio media and real-time video as it is designed to handle occasional lost packets, so only slight degradation in quality occurs, rather than large delays if lost packets were retransmitted.

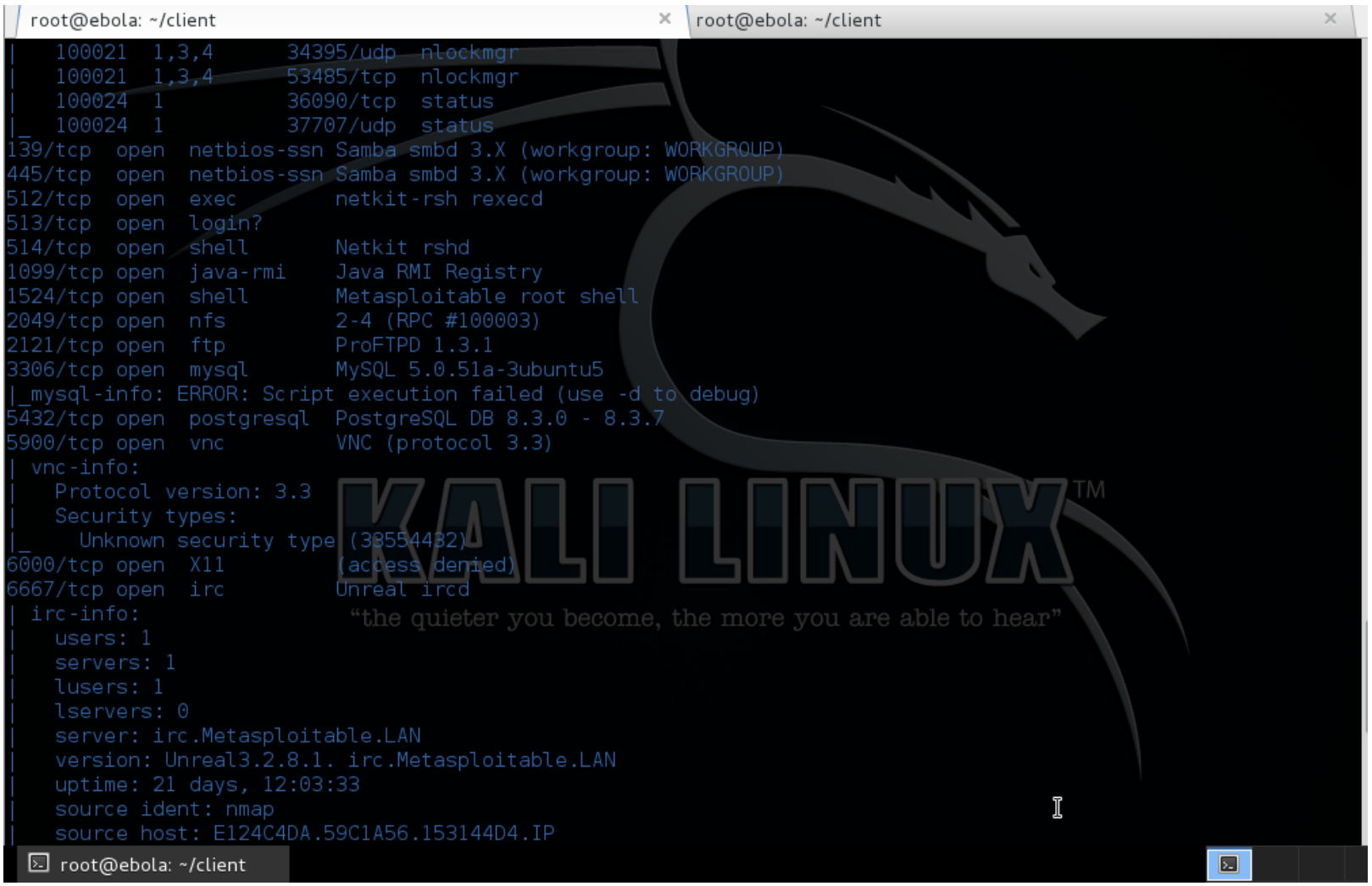
```
root@ebola:~/client# nmap -sU 11.11.11.200

Starting Nmap 7.00 ( https://nmap.org ) at 2015-11-30 13:57 EST
Nmap scan report for 11.11.11.200
Host is up (0.030s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs

Nmap done: 1 IP address (1 host up) scanned in 1071.39 seconds
```

The results of our UDP nmap scan above provides us with a datagram of possible vulnernabilities, ports which if we were curious could continue investigating, such as Port 53, Port 69 , Port 137 and Port 2049 – if we listen to these ports, we potentially might be pleasantly surprised with what we find. Let's do one more, let's see if we can find out what versions are running on each port.

```
Starting Nmap 7.00 ( https://nmap.org ) at 2015-11-30 14:23 EST
Nmap scan report for 11.11.11.200
Host is up (0.057s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:
/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.57 seconds
root@ebola:~/client#
```

Let's try another one, this time, this time, type in nmap man, this will bring up the nmap manual. In our next example, let's try a built-in shorthand for the most popular options "-A". This type of scan provides additional information about the remote system to the ports provided by a typical nmap scan.


root@ebola: ~/client
root@ebola: ~/client
root@ebola:~/client# man nmap
root@ebola:~/client# nmap -A 11.11.11.200
Starting Nmap 7.00 (https://nmap.org) at 2015-11-30 14:40 EST
Nmap scan report for 11.11.11.200
Host is up (0.065s latency).
Not shown: 977 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCOD
S, 8BITMIME, DSN,
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 39863/tcp mountd
| 100005 1,2,3 48265/udp mountd
root@ebola: ~/client


root@ebola: ~/client
root@ebola: ~/client
| 100021 1,3,4 34395/udp nlockmgr
| 100021 1,3,4 53485/tcp nlockmgr
| 100024 1 36090/tcp status
|_ 100024 1 37707/udp status
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi Java RMI Registry
1524/tcp open shell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
|_mysql-info: ERROR: Script execution failed (use -d to debug)
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ Unknown security type (38554432)
6000/tcp open X11 (access denied)
6667/tcp open irc Unreal ircd
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 21 days, 12:03:33
| source ident: nmap
| source host: E124C4DA.59C1A56.153144D4.IP
root@ebola: ~/client

```
|_  error: Closing Link: ewyjtvgja[11.11.11.100] (Quit: ewyjtvgja)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.00%E=4%D=11/30%OT=21%CT=1%CU=44596%PV=N%DS=2%DC=T%G=Y%TM=565CA6
OS:67%P=x86_64-pc-linux-gnu)SEQ(SP=C4%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%TS=7)OPS(
OS:O1=M536ST11NW6%O2=M536ST11NW6%O3=M536NNT11NW6%O4=M536ST11NW6%O5=M536ST11
OS:NW6%O6=M536ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(
OS:R=Y%DF=Y%T=40%W=16D0%O=M536NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%R
OS:UCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe
/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2015-11-30T19:39:48-05:00

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1   75.08 ms 12.12.12.1
```


root@ebola: ~/client

```
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.00%E=4%D=11/30%OT=21%CT=1%CU=44596%PV=N%DS=2%DC=T%G=Y%TM=565CA6
OS:67%P=x86_64-pc-linux-gnu)SEQ(SP=C4%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%TS=7)OPS(
OS:O1=M536ST11NW6%O2=M536ST11NW6%O3=M536NNT11NW6%O4=M536ST11NW6%O5=M536ST11
OS:NW6%O6=M536ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(
OS:R=Y%DF=Y%T=40%W=16D0%O=M536NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%R
OS:UCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe
/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2015-11-30T19:39:48-05:00

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1   75.08 ms 12.12.12.1
2   46.60 ms 11.11.11.200

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.42 seconds
```

Take a close look at the results of our scan - With a simple command, we have now discovered the OS version, the various hosts as well as the version of Tomcat.
Nmap is used by many individuals, and not all of them are “bad”, some are malicious individuals looking to sniff around networks looking for open ports, to get information, others are security professionals, using nmaping to conduct penetration testing to safely exploit system vulnerabilities to evalute the security.