nmap2nessus

Keith Lee & Michael Gianarakis

Blackhat Asia Arsenal 2015

Trustwave®
SpiderLabs®

#whoami

@keith55

Security Consultant at SpiderLabs

@mgianarakis

Managing Consultant at SpiderLabs

Application Security

What Is This Presentation About?

- What is nmap2nessus
- Usage scenarios
- How nmap2nessus works
- How to use nmap2nessus

How nmap2nessus was born ?

How nmap2nessus was born

- When performing a vulnerability scan, I prefer to run a nmap scan first to have a good overview of the services/ports that are open.

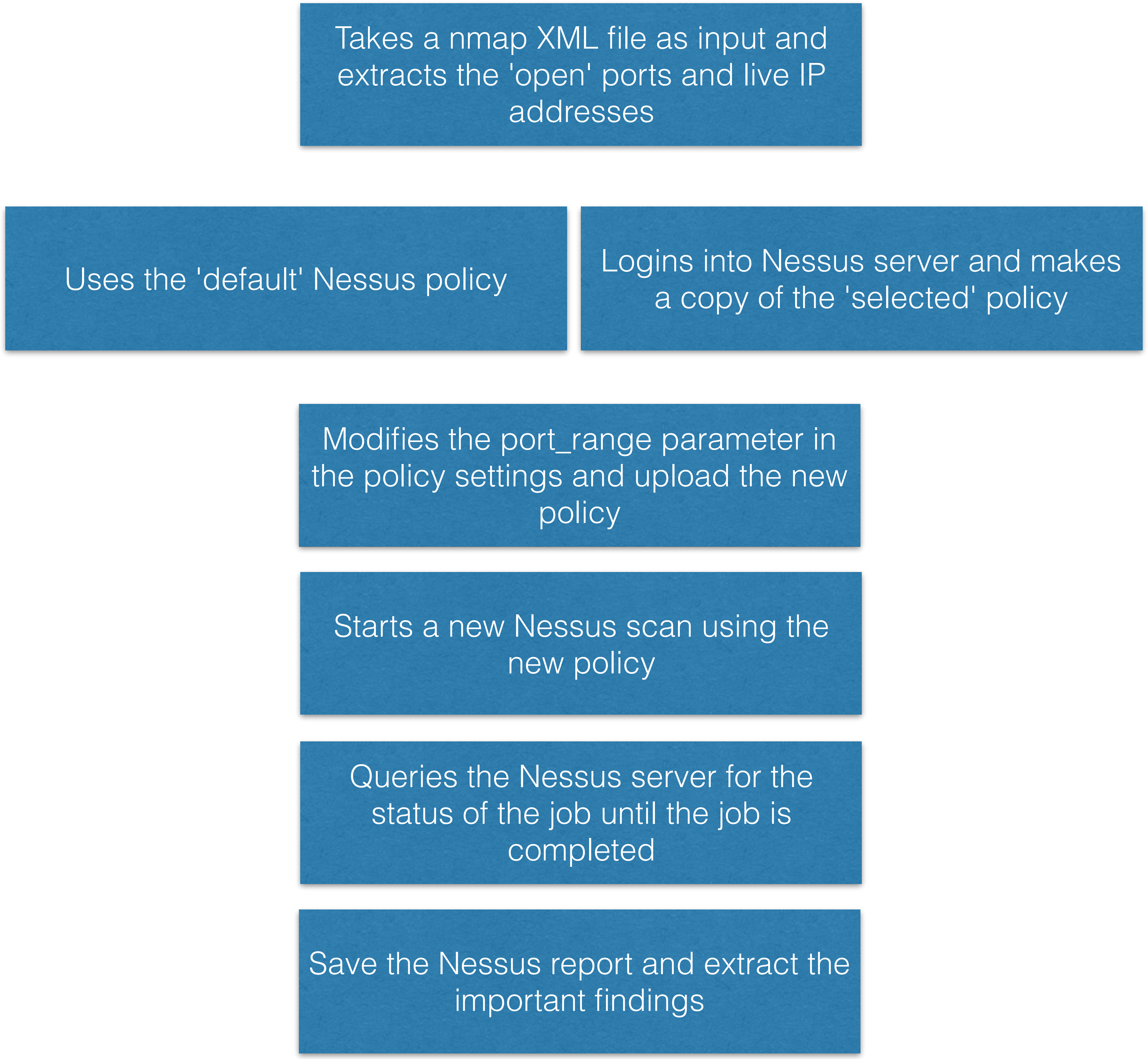
- The benefits of running a nmap scan first is that there are many tools that you might want to use later that supports nmap files as a input file.

- Running a Nessus scan after performing a Nmap scan takes a long time as Nessus has to scan all the ports again.

- Nessus has a NASL script that allows importing of Nmap XML file (http://static.tenable.com/documentation/nmapxml.nasl) via the Nessus admin console. However, it is not working in Nessus version 6.3.2.

How nmap2nessus works ?

How nmap2nessus works



Takes a nmap XML file as input and extracts the 'open' ports and live IP addresses

Uses the 'default' Nessus policy

Logins into Nessus server and makes a copy of the 'selected' policy

Modifies the port_range parameter in the policy settings and upload the new policy

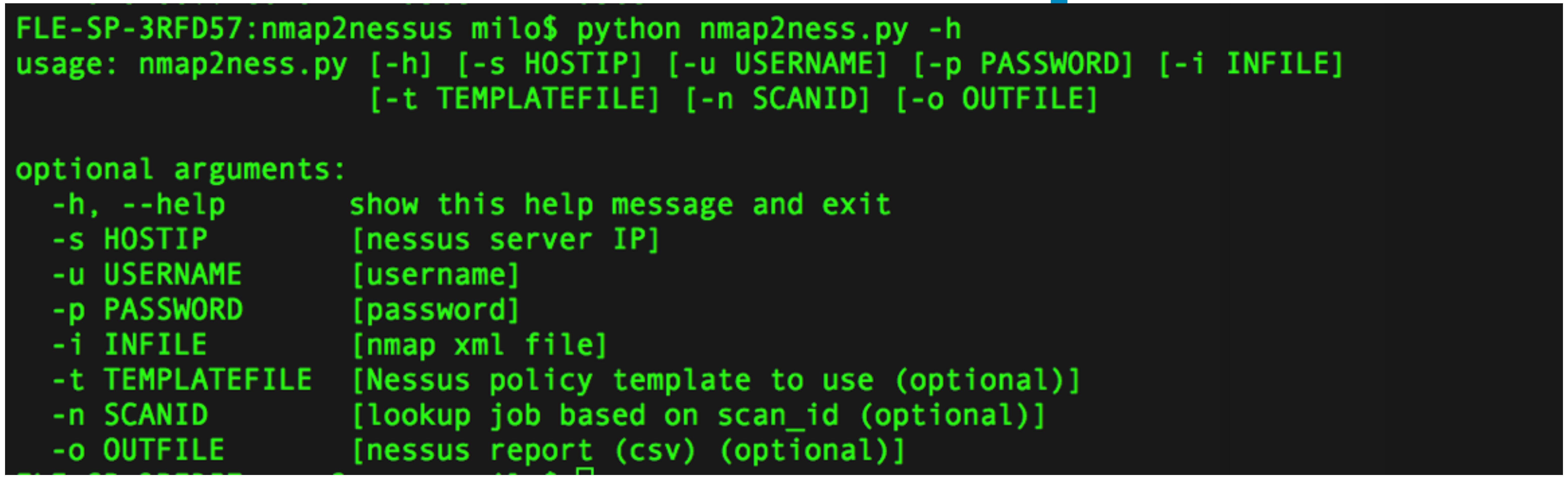
Starts a new Nessus scan using the new policy

Queries the Nessus server for the status of the job until the job is completed

Save the Nessus report and extract the important findings

How to use nmap2nessus ?

How to use nmap2nessus



```
FLE-SP-3RFD57:nmap2nessus milo$ python nmap2ness.py -h
usage: nmap2ness.py [-h] [-s HOSTIP] [-u USERNAME] [-p PASSWORD] [-i INFILE]
                    [-t TEMPLATEFILE] [-n SCANID] [-o OUTFILE]

optional arguments:
  -h, --help       show this help message and exit
  -s HOSTIP        [nessus server IP]
  -u USERNAME      [username]
  -p PASSWORD      [password]
  -i INFILE        [nmap xml file]
  -t TEMPLATEFILE  [Nessus policy template to use (optional)]
  -n SCANID        [lookup job based on scan_id (optional)]
  -o OUTFILE       [nessus report (csv) (optional)]
```

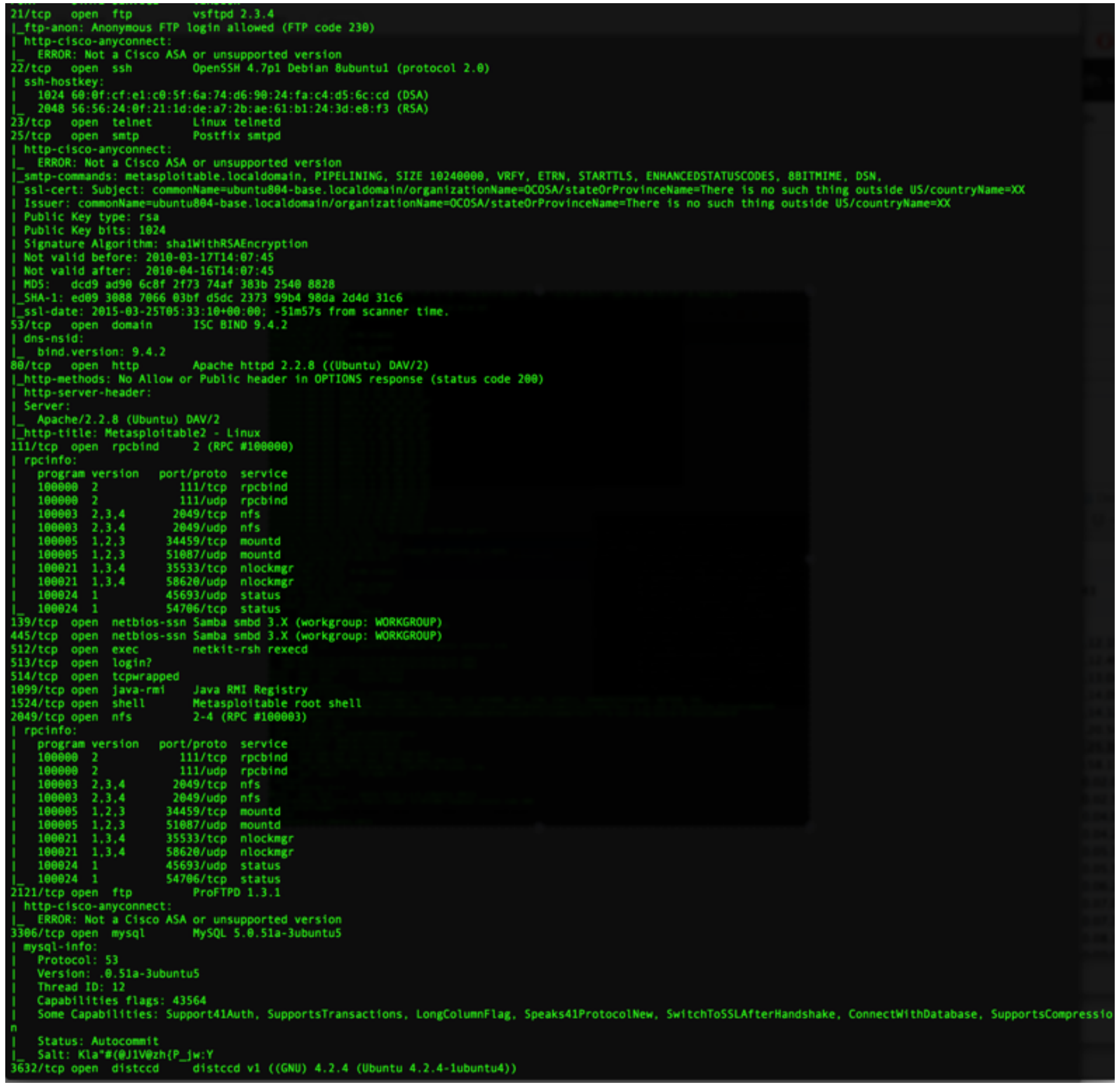
- **Uses the default nessus policy**
  python nmap2ness.py -u root -p xxxxxxx -s 192.168.112.132 -i nmapt_target.xml

- **Uses nessus policy "policy1"**
  python nmap2nessus.py -u root -p xxxxxx -s 192.168.112.132 -t policy1 -i nmapt_target.xml

- **Connects to Nessus server and queries for scan job 232**
  python nmap2nessus.py -u root -p xxxxx -s 192.168.112.132 -n 232

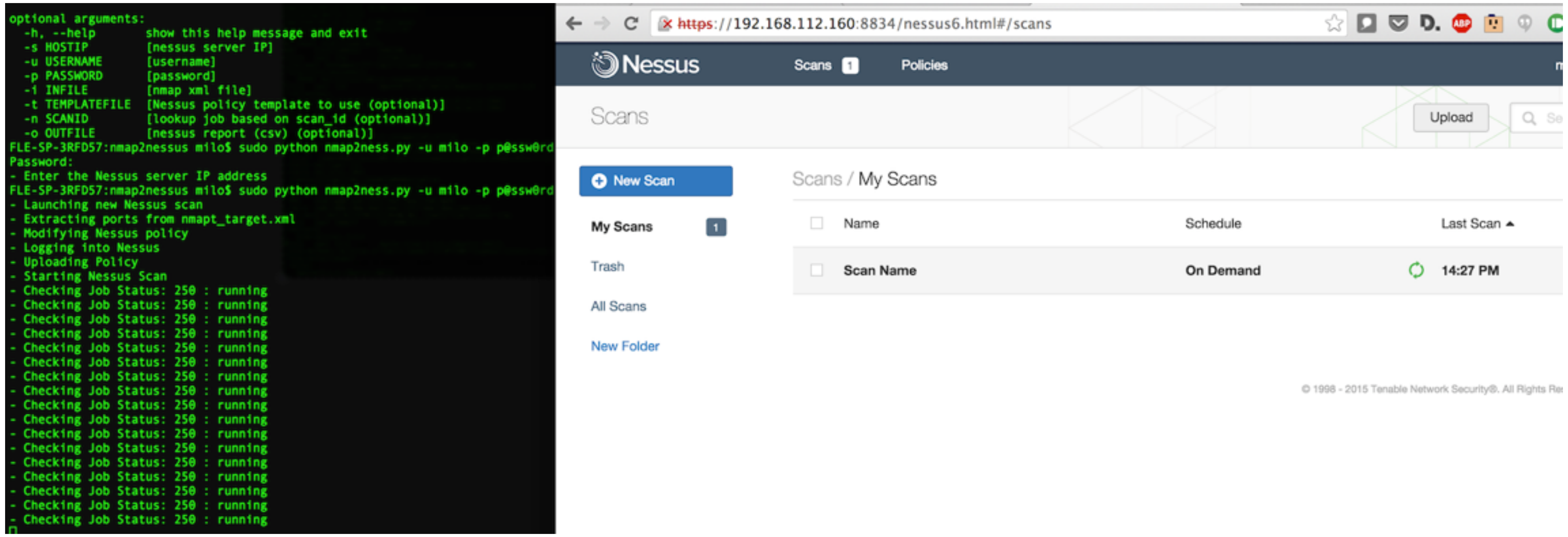
Demo

Nmap scan against Metasploitable2 VM



```
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| http-cisco-anyconnect:
|_  ERROR: Not a Cisco ASA or unsupported version
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
| http-cisco-anyconnect:
|_  ERROR: Not a Cisco ASA or unsupported version
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
|_ssl-date: 2015-03-25T05:33:10+00:00; -51m57s from scanner time.
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-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-server-header:
| Server:
|_  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      34459/tcp  mountd
|   100005  1,2,3      51087/udp  mountd
|   100021  1,3,4      35533/tcp  nlockmgr
|   100021  1,3,4      58620/udp  nlockmgr
|   100024  1          45693/udp  status
|_  100024  1          54706/tcp  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  tcpwrapped
1099/tcp open  java-rmi    Java RMI Registry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
| 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      34459/tcp  mountd
|   100005  1,2,3      51087/udp  mountd
|   100021  1,3,4      35533/tcp  nlockmgr
|   100021  1,3,4      58620/udp  nlockmgr
|   100024  1          45693/udp  status
|_  100024  1          54706/tcp  status
2121/tcp open  ftp         ProFTPD 1.3.1
| http-cisco-anyconnect:
|_  ERROR: Not a Cisco ASA or unsupported version
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 53
|   Version: .0.51a-3ubuntu5
|   Thread ID: 12
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompressio
n
|   Status: Autocommit
|_  Salt: Kla"#(@J1V@zh{P_jw:Y
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

Running nmap2nessus



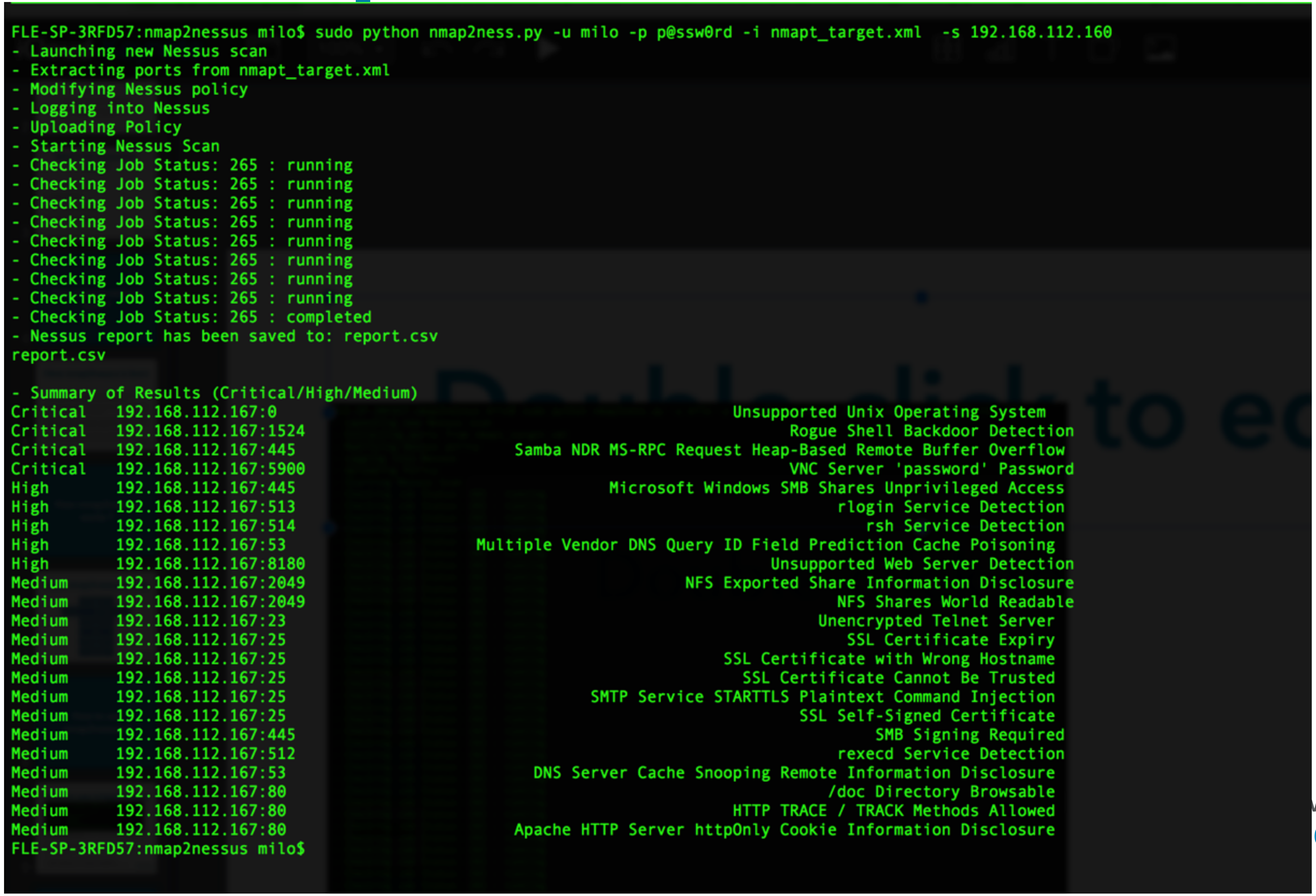
```
optional arguments:
  -h, --help         show this help message and exit
  -s HOSTIP          [nessus server IP]
  -u USERNAME        [username]
  -p PASSWORD        [password]
  -i INFILE          [nmap xml file]
  -t TEMPLATEFILE    [Nessus policy template to use (optional)]
  -n SCANID          [lookup job based on scan_id (optional)]
  -o OUTFILE         [nessus report (csv) (optional)]
FLE-SP-3RFD57:nmap2nessus milo$ sudo python nmap2ness.py -u milo -p p@ssw0rd
Password:
- Enter the Nessus server IP address
FLE-SP-3RFD57:nmap2nessus milo$ sudo python nmap2ness.py -u milo -p p@ssw0rd
- Launching new Nessus scan
- Extracting ports from nmapt_target.xml
- Modifying Nessus policy
- Logging into Nessus
- Uploading Policy
- Starting Nessus Scan
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
- Checking Job Status: 250 : running
```

Scans / My Scans

□	Name	Schedule	Last Scan ▲
□	Scan Name	On Demand	14:27 PM

© 1998 - 2015 Tenable Network Security®. All Rights Re

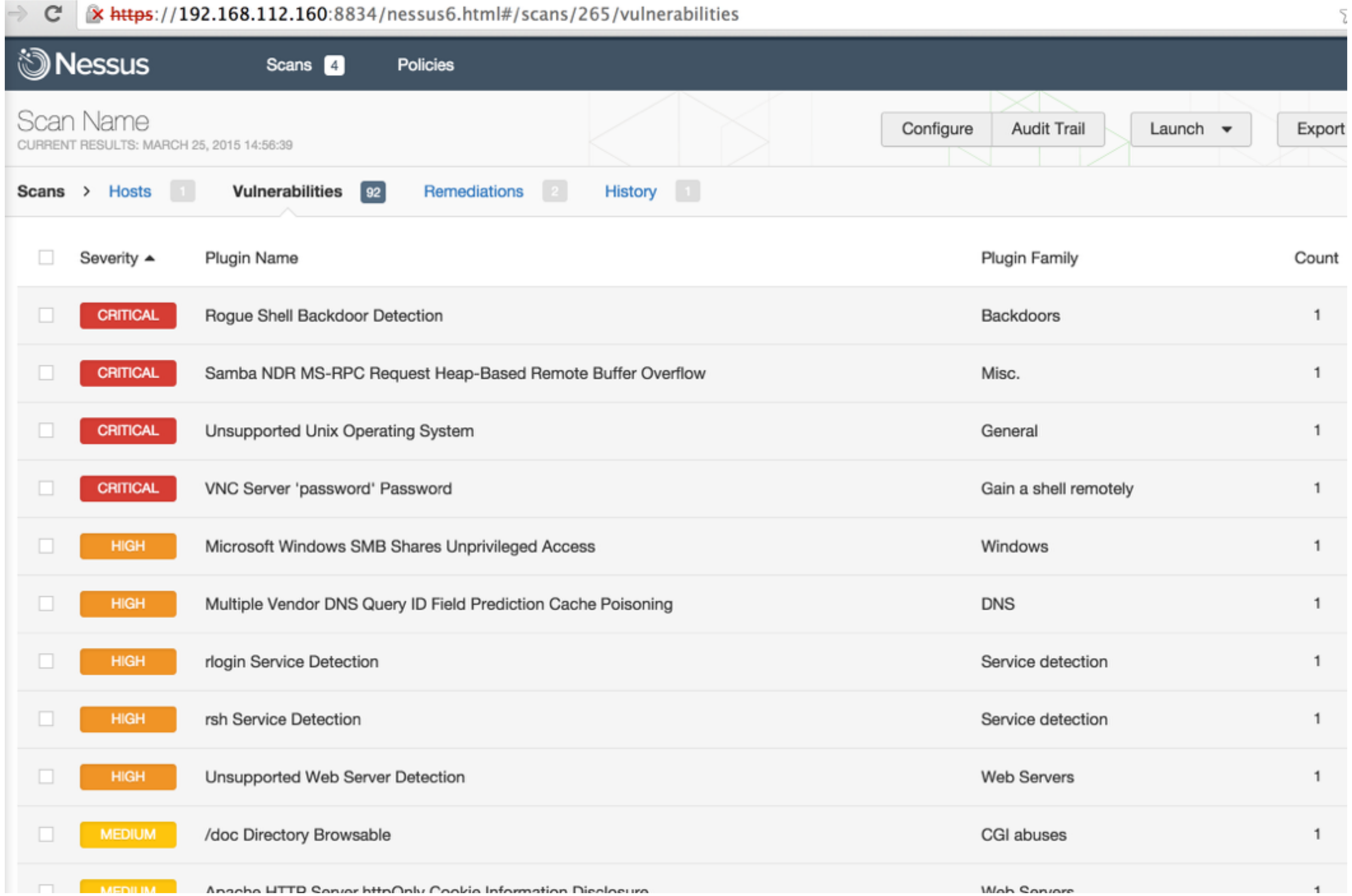
Nmap2nessus Results



```
FLE-SP-3RFD57:nmap2nessus milo$ sudo python nmap2ness.py -u milo -p p@ssw0rd -i nmapt_target.xml  -s 192.168.112.160
- Launching new Nessus scan
- Extracting ports from nmapt_target.xml
- Modifying Nessus policy
- Logging into Nessus
- Uploading Policy
- Starting Nessus Scan
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : running
- Checking Job Status: 265 : completed
- Nessus report has been saved to: report.csv
report.csv

- Summary of Results (Critical/High/Medium)
Critical   192.168.112.167:0                                                Unsupported Unix Operating System
Critical   192.168.112.167:1524                                                   Rogue Shell Backdoor Detection
Critical   192.168.112.167:445                       Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow
Critical   192.168.112.167:5900                                                   VNC Server 'password' Password
High       192.168.112.167:445                                  Microsoft Windows SMB Shares Unprivileged Access
High       192.168.112.167:513                                                        rlogin Service Detection
High       192.168.112.167:514                                                           rsh Service Detection
High       192.168.112.167:53                    Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
High       192.168.112.167:8180                                                 Unsupported Web Server Detection
Medium     192.168.112.167:2049                                        NFS Exported Share Information Disclosure
Medium     192.168.112.167:2049                                                        NFS Shares World Readable
Medium     192.168.112.167:23                                                        Unencrypted Telnet Server
Medium     192.168.112.167:25                                                           SSL Certificate Expiry
Medium     192.168.112.167:25                                              SSL Certificate with Wrong Hostname
Medium     192.168.112.167:25                                                SSL Certificate Cannot Be Trusted
Medium     192.168.112.167:25                                SMTP Service STARTTLS Plaintext Command Injection
Medium     192.168.112.167:25                                                      SSL Self-Signed Certificate
Medium     192.168.112.167:445                                                            SMB Signing Required
Medium     192.168.112.167:512                                                        rexecd Service Detection
Medium     192.168.112.167:53                          DNS Server Cache Snooping Remote Information Disclosure
Medium     192.168.112.167:80                                                         /doc Directory Browsable
Medium     192.168.112.167:80                                               HTTP TRACE / TRACK Methods Allowed
Medium     192.168.112.167:80                        Apache HTTP Server httpOnly Cookie Information Disclosure
FLE-SP-3RFD57:nmap2nessus milo$
```

Results in Nessus console



https://192.168.112.160:8834/nessus6.html#/scans/265/vulnerabilities

Scan Name

CURRENT RESULTS: MARCH 25, 2015 14:56:39

Scans > Hosts 1 Vulnerabilities 92 Remediations 2 History 1

□	Severity ▲	Plugin Name	Plugin Family	Count
□	CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
□	CRITICAL	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	Misc.	1
□	CRITICAL	Unsupported Unix Operating System	General	1
□	CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
□	HIGH	Microsoft Windows SMB Shares Unprivileged Access	Windows	1
□	HIGH	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1
□	HIGH	rlogin Service Detection	Service detection	1
□	HIGH	rsh Service Detection	Service detection	1
□	HIGH	Unsupported Web Server Detection	Web Servers	1
□	MEDIUM	/doc Directory Browsable	CGI abuses	1
□	MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	1

Trustwave®
SpiderLabs®

Vulnerabilities not found by Nessus

- Port 22 is vulnerable to CVE-2008-0166 (Debian OpenSSL - Predictable PRNG Bruteforce SSH Exploit) - http://www.exploit-db.com/exploits/5632/.

- Port 6667 is vulnerable to CVE-2010-2075. (exploits/unix/irc/unreal_ircd_3281_backdoor)

- Port 80 is running a vulnerable version of TWiki. The history component is vulnerable to CVE-2015-2877). (exploit/unix/webapp/twiki_history)

- Port 139 is running a vulnerable version of Samba. (exploit/multi/samba/usermap_script)

- Port 8180 is running a vulnerable version of Apache Tomcat. The account (tomcat|tomcat) is found in use. (exploit/multi/http/tomcat_mgr_deploy)

- Complete walkthrough found at https://community.rapid7.com/docs/DOC-1875.

Conclusion

- nmap2nessus is designed to do one thing well - quickly and simply initiate a Nessus scan based on the output of Nmap
- Vulnerability assessments have their place, but a good penetration test will always be a more realistic assessment of security risk
- The script can be downloaded from https://github.com/milo2012/nmap2nessus.