nmap2nessus

Keith Lee & Michael Gianarakis Blackhat Asia Arsenal 2015



Trustwave® SpiderLabs®





- Security Consultant at SpiderLabs
 - @mgianarakis
- Managing Consultant at SpiderLabs
 - **Application Security**

#whoami

@keith55



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

- input file.
- time as Nessus has to scan all the ports again.
- version 6.3.2.

• 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

• Running a Nessus scan after performing a Nmap scan takes a long

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



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

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

y

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



How to use nmap2nessus ?

How	to use
•	<pre>2nessus milo\$ python nma 7 [-h] [-s HOSTIP] [-u U 7 [-t TEMPLATEFILE] [-n</pre>
optional arguments:	
-h,help -s HOSTIP	<pre>show this help message [nessus server IP]</pre>
-u USERNAME	[username]
-p PASSWORD	[password]
-i INFILE	[nmap xml file]
-t TEMPLATEFILE	[Nessus policy template
-n SCANID	[lookup job based on sc
-o OUTFILE	[nessus report (csv) (o

- Uses the default nessus policy
- 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



ap2ness.py -h SERNAME] [-p PASSWORD] [-i INFILE] SCANID] [-0 OUTFILE]

and exit

to use (optional)] an id (optional)] ptional)

python nmap2ness.py -u root -p xxxxxxx -s 192.168.112.132 -i nmapt_target.xml





Nmap scan against Metasploitable2 VM

<pre>[ftp-anon: Anonymous FTP login allowed (FTP code 230) https-tics-anyconnect: </pre>			vsftpd 2.3.4
<pre>L ERON: Not a Cisco ASA or unsupported version 22/tCc open ssh OpenS04 4.7pl Debian Bubuntui (protocol 2.0) 1 ssh-hostkey: 1024 66.0Ft(crtel:c0:Sf:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA) 2.7btCp open relation 1025 fb:25:24:0Ft(21:1d:de:a7:Bb:ac:61:B1:24:34:68:13 1025 fb:25:24:0Ft(21:1d:de:a7:Bb:ac:61:B1:24:34:68:13 1025 fb:25:24:0Ft(21:1d:de:a7:Bb:ac:61:B1:24:34:68:13 1025 fb:25:24:0Ft(21:1d:de:a7:B1:24:13:1:42:13:1:68:13 1025 fb:25:24:0Ft(21:1d:de:a7:B1:24:13:1:68:13:1:42:13:1:68:13:1:42:13:1:68:13:1:42:13:1:68:13:1:42:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:14:15:15:15:15:15:15:15:15:15:15:15:15:15:</pre>			igin allowed (FIP code 230)
<pre>issi-hootkey: iB24 669/icfreicel.cellsfise.72/idf:90:22/ifa:celld5/6C:Cd (DSA) j2488 56:56:24:07:21:16:04:a7:25:ba:e61:01:22:13:04:06:13 (DSA) j24/EQ 0000 mint issi-cert:Suprometed issi-cert:Suprometed issi-cert:Subject:Commonwae-ubuntu804-base.localdomain/organizationName=COSA/stateOrProvinceName=There issi-cert:Subject:Commonwae-ubuntu804-base.localdomain/organizationName=COSA/stateOrProvinceName=There issi-cert:Subject:Commonwae-ubuntu804-base.localdomain/organizationName=COSA/stateOrProvinceName=There is no such i Public Key Diger:Subject:Commonwae-ubuntu804-base.localdomain/organizationName=COSA/stateOrProvinceName=There is Diger:</pre>	ERROR: No	ot a Cisco ASA o	
<pre>1 ID24 60:0F:cfc:lc0:5f:6a:74.06:90:24:f:ccid5:05:ccid (DSA) 27/cp open telnet Linux telnetd 27/cp open stp Postfix stpd 1 http-cisco-anyconnect: 8RAOK.Not & Cisco AAA or unsupported version 1 stp:cc_open stp1 Postfix stpd 1 http-cisco-anyconnect: 1 stp:cc_open stp1 Postfix stpd 2 stp:cc_open stp1 Postfix stpd 2 stp:cc_open stp1 Postfix stpd 2 stp.cc_open stp1 Postfix stpd 2 stp:cc_open stp2 Postfix stpc 2 stp:cc_open stp2 Postfix stpd 2</pre>			penSSH 4.7pl Debian Bubuntul (protocol 2.0)
<pre>1 2048 56:56:24:0F:21:10:de:a7:20:ae:61:01:24:30:e8:F3 (RSA) 25/tcp open setp Postfix setpd 15tp-cisco-anyconnect: 1 ERRD: Not a Cisco ASA or unsupported version 1 ERRD: Not a Cisco ASA or unsupported version 1 ERRD: Not a Cisco ASA or unsupported version 1 ERRD: Not a Cisco ASA or unsupported version 1 ERRD: Not a Cisco ASA or unsupported version 1 Sincer: Componence-upuntu804-base.localdomain/organizationMame=OCOSA/stateOrProvinceMame=There 1 Signature Algorithms: shallHithRAAncryption 1 Not valid before: 2010-04-16714:07:45 1 Not valid before: 2010-04-16714 1 Not valid before: 2010-04-16714 1 Not valid before: 2010 1 Not valid bef</pre>			6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
5/tcp open smtp Postfix smtpd bitp-cisco-anyconnect:	2048 56:5	6:24:0f:21:1d:d	de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
<pre>http-cisco-anyconnect: _smpp-commands: metasplotable.localdomain, PIPELINING, SIZE 18240000, VEFY, ETRN, STARTILS, ENHANCEDSTATUS _smlp-commands: metasplotable.localdomain/organizationName=OCOSA/stateOrProvinceName=There is use isl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such /built Key type: rsa Public Key 1015: 1024 Sinature Algorithm: shaWithRSAEncryption Not: valid before: 3080-83-1771-09735 Not: valid before: 3080-83-1771-09735 Not: valid before: 3080-83-1771-09735 Sinature Algorithm: shaWithRSAEncryption Not: valid before: 3080-83-1771-09735 Not: valid before: 3080-83-1771-09735 Sinature Algorithm: shaWithRSAEncryption Not: valid before: 3080-8777 Alaf XBB 2540 8828 _SiN-ti: c009 3080 7066 8Drf ddc 2373 3994 9840 204d 31c6 _ssi-date: 2081-50-32705-331:0460-009 - SinB75 from scanner time. Sitep open domain ISC BIND 9.4.2 (ms-nsid: bind.version: 9.4.2 Bitp: open nttp Aaache httpd 2.2.8 ((Ubuntu) DAV/2) [http-methods: No Allow or Public header in OPTIONS response (status code 200) [rpcind: server: _apache/2.2.8 (Ubuntu) DAV/2 [rttp-title: Metasploitable3 - Linux 11/tcp open probind 2 (RC 410000) [rpcind: 100000 2.3.4 2049/tcp nfs 100000 2.3.4 2049/tcp nfs 100000 1.3.4 3533/tcp nlockmgr 100001 1.3.4 3533/tcp nlockmgr 100002 1.3.4 3667/upg mountd 100001 1.3.4 3533/tcp nlockmgr 100021 1.3.4 3533/tcp nlockmgr 100021 1.3.4 3543/tcp nlockmgr 100021 1.3.4 2449/tcp nfs 100005 1.2.3 34439/tcp nset 100005 1.2.3 34439/tcp nset 100006 2 111/tcp probind 100008 1.2.3 4249/tcp nfs 100009 2 1.3.4 2049/tcp nfs 100009 2 1.3.4 2049/tcp nfs 100000 2 1.3.4 2049/tcp nfs 100000 2 1.3.4 2049/tcp nfs 100000 2 1.3.4 2049/tcp nfs 100000 1.3.4 2049/tcp</pre>			
SRD: Not a Cisco ASA or unsupported version SRD: commonXime=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There 			οστηχ επτρο
<pre></pre>	ERROR: No	ot a Cisco ASA o	
<pre>Issuer: commonRemevubuntu884-base.localdomain/organizationName=COSA/stateOrProvinceName=There is no such ' Public Key bits: 1024 Signature Algorithm: shalwithRSAEncryption Not valid before: 2010-03-17114/07:45 Not valid before: 2010-03-17114/07:45 Not valid 9408 6c8f 2f713 744f 383b 2540 8828 Sin-1 ecd09 3086 7066 0317 33:16+00:00; -51m37 sfrom scanner time. Jitcp open domain 15C BIND 9.4.2 dns.ns1d: bind.version: 9.4.2 P/top open http Apache httpd 2.2.8 ((Ubuntu) DAV/2) Litp.methods: No Allow or Public header in OPTIONS response (status code 200) http:server-header: server: ind.version: 9.2.8 (Ubuntu) DAV/2 Litp.methods: No Allow or Public header in OPTIONS response (status code 200) http:server-header: server: ind.version port/proto service 100000 2 111/dcp rpcbind 100000 2 111/dcp rpcbind 100000 2 111/dcp rpcbind 100000 2 111/dcp rpcbind 100000 1 1.3.4 35537/ccp mountd 1000001 1.3.4 35537/ccp mountd 1000001 1.3.4 35537/ccp nolockmgr 100001 1.3.4 5563/udp status 33/ccc open netblois-ssn Samba smbd 3.X (workgroup: WORKGROUP) 13/ccp open http reprane version port/proto service i00001 1.3.4 5566/clp status i00003 2.3.4 249/dcp nis 100002 1.3.4 53337/ccp nlockmgr i00021 1.3.4 5563/udp status i00003 1.2.3 34459/ccp mountd i00003 1.3.4 5459/cdp mountd i00003 1.3.4 5459/cdp mountd i00001 1.3.4 55337/ccp nlockmgr i00021 1.3.4 55337/ccp nlockmgr i00021 1.3.4 5553/dcg mountd i00003 2.3.4 249/dcg nis i00021 1.3.4 5563/udp status i00003 1.3.4 546/ccp status i00003 1.3.4 546/ccp status i00003 1.3.4 546/ccp respond i00003 1.3.4 546/ccp respond i00003 1.3.4 546/ccp status i00003 1.3.4 5456/cdp nlockmgr i00003 1.3.4</pre>	_smtp-comman	ds: metasploita	able.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCO
Public Key type: rsaSignature Algorithm: shalkithRSAEncryptionNot valid effore: 2010-00-17114:07:45Not valid effore: 2010-00-17114:07:45Not valid effore: 2010-00-17114:07:45JS: date: 2015-00-2715:31:04:00:06: -51875 from scanner timeSM-ta: e009 J088 7066 Bbf dsdc 2373 9bb 906a 2044 J1c6_SM-ta: e009 J088 7066 Bbf dsdc 2373 9bb 906a 2044 J1c6_SM-ta: e009 J088 7066 Bbf dsdc 2373 9bb 906a 2044 J1c6_SM-ta: e009 J088 7066 Bbf dsdc 2373 9bb 906a 2044 J1c6_SM-ta: e009 J088 7066 Bbf dsdc 2373 9bb 906a 2044 J1c6_Bind.version: 9.4.2Øftcp open domain ISC BIND 9.4.2Int:-server:_ Apache http Apache httpd 2.2.8 ((Ubuntu) DAV/2)_Http-server-neader:Server:_ Apache/2.2.8 (Ubuntu) DAV/2_http-server-neader:_ Program version port/proto service100000 2.3.4 J049/udp nfs100000 1.3.4 J049/udp nfs1000001 1.3.4 J353/tcp nountd1000001 2.3.4 J049/udp nfs1000001 1.3.4 J353/tcp nountd1000001 1.3.4 J353/tcp nountd100001 1.3.4 J353/tcp nountd100000 1.3.4 J353/tcp nountd100000 2 111/tcp rpcbind100000 2 111/tcp rpcbind100000 2 111/tcp rpcbind			
<pre>Signature Algorithm: shalWithRSAEncryption Not valid pefore: 2010-00-15714:07:45 Not valid pefore: 2010-00-15714:07:45 Not valid pefore: 2010-00-15714:07:45 Not valid pefore: 2010-00-15714:07:45 Sector: 2015-00-25705:31:04:00.081; -51n575 from scanner time. 37.tcp open domain ISC BIND 9.4.2 (dms.nsid: bind.version: 9.4.2 bind.version: 9.4.2 bitd.version: 9.4.2 bitd.v</pre>			na-nase: constronments of Banty sector mane-or observations and the endine-there is no shell on
Not valid before: 2010-09-17114:07:45 Not valid before: 2010-09-15114:07:45 NDS: dcd9 ad90 6c87 2773 7447 381b 2540 8828 _ssl-date: 2015-08-25T05:33:10+00:00; -51875 from scanner time. _ssl-date: 2015-08-25T05:33:10+00:00; -51875 from scanner time. _strate: 2015-08-25T05:30:10+00:00; -51875 from scanner time. _strate: 2015-08-25T05:30:00; -51855 from from scanner time. _strate: 2015-08-25T05:30:00; -51855 from from scanner time. _strate: 200600 2:111/tcp: probind 1000001 2:1,3; 4:3555710; notextse: _strate: 200600 1:1,3; 4:3555710; notextse: _strate: 2005-08-	Public Key	bits: 1024	
Not valid after: 2010-04-16714:07:45 MDS: dc04 a090 6C8 2717 747 343 3bb 2540 8278 _SHA:: ed09 3088 7066 03bf d5dc 2373 9904 90da 2d4 31c6 _SH.dic: 03b-03-2750:33:10-00:00; -51875 from scanner time. Jtcp open domain ISC BIND 9.4.2 dns.nsid: _bind.version: 9.4.2 Dictp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2) _http-serverNebader: Server: _Apache/2.2.8 (Ubuntu) DAV/2 _http-serverNebader: Server: _Apache/2.2.8 (Ubuntu) DAV/2 _http-serverNebader: _Server: _Apache/2.2.8 (Ubuntu) DAV/2 _http-serverNebader: _Server: _Apache/2.2.8 (Ubuntu) DAV/2 _http-serverNebader: _Server: _Apache/2.2.8 (Ubuntu) DAV/2 _http-serverNebader: _Server: _Ser			
<pre>MDS: dcd9 ad90 6c8f 2/73 744f 331b 2540 8828 _ssl-date: 2015-03-25705:33:10+00:00; -51m57s from scanner time. Jottp open domain isC BIND 9.4.2 dns-nsid: bind.version: 9.4.2 Pitp-methods: No Allow or Public header in OPTIONS response (status code 200) http-server-header: Server: </pre>			
_ssl-date: 2015-03-25705:33:10+00:00: -51m57s from scanner time. jitcp open domain ISC BIND 9.4.2 dns-nsid: 	MD5: dcd9	ad90 6c8f 2f73	3 74af 383b 2540 8828
3/tcp open domain ISC BIND 9.4.2 dms-nsid: bind.version: 9.4.2 0/tcp open http Apache/2.2.8 (Ubuntu) DAV/2) http:server-header: Server: Apache/2.2.8 (Ubuntu) DAV/2 _http:title: Netasplotable2 - Linux I/tcp open rpcbind 2 (RPC #10000) rpcinfo: program version port/proto service 100000 2 11/tup rpcbind 100000 2, 13.4 2049/tup nfs 100000 1, 2.3 Side57/udp mountd 100000 1, 2.3 Side57/udp mountd 100001 1, 3.4 \$6503/udp nlockmgr 100002 1, 1.3, 4 \$6503/udp nlockmgr 100002 1, 2.3 Side57/udp mountd 100002 1, 2.3 Side57/udp mountd 100002 1, 2.3 Side57/udp status 100002 1, 3.4 2049/tup status 100002 1, 3.4 Seconvertistable 2.4 (workgroup: WORKGROUP) 45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 11/tcp open login7 100002 1, 3.4 2049/tup nlockmgr 100002 1 11/tup rpcbind			
<pre>dmainstd: bind.version: 9.4-2 @/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: </pre>			
Ø/tcpopenhttpApachehttp://dim.http-methods:No Allow or Public header in OPTIONS response (status code 200)http-server:.Apache/2.2.8 (Ubuntu) DAV/2.http-strict: Metasploitable2 - LinuxIl/tcp open rpcbind100000 211/tcp open rpcbind100000 21100000 2111/tcp open100000 2111/tcp interver100000 2111/tcp interver100000 2111/tcp interver100000 2111/tcp interver100000 2111/tcp interver100000 2111/tcp interver100000 1100000 2111/tcp interver100000 2111/tcp interver100000 2111/tcp interver100000 1111/tcp interver100001 1111/tcp interver100002 1111/tcp interver100003 1111/tcp interver100001 1111/tcp interver111/tcp interver	dns-nsid:		
_http:methods: No Allow or Public header in OPTIONS response (status code 200) http:server:Apache/2.2.8 (Ubuntu) DAV/2 Apache/2.2.8 (Ubuntu) DAV/2 Dttp-title: Metasploitable2 - Linux li/tcp open rpcbind 2 (RPC #100000) rpcinfo: program version port/proto service 1000000 2 111/tcp rpcbind 1000003 2.3.4 2049/tcp nfs 1000003 2.3.4 2049/tcp nfs 1000021 1.3.4 35533/tcp nlockmgr 100024 1 45639/udp status 30/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 13/tcp open shell Metasploitable root shell 100005 1.2.3 34459/tcp mountd 1000061 1.3.4 35533/tcp mountd 1000062 1.3.4 2049/tcp nfs 1000061 1.3.4 35533/tcp nlockmgr 1000624 1 \$4706/tcp status 110/tcp open ftp ProFTP 1.3.1 110/tcp open ftp ProFTP 1.3.1 ttp-cisco-amyconnect: _ ERROR: Not a Cisco ASA or unsupported version			anche https:////ibuntu/ DAV/25
Titp-server-header:_ Apache/2.2.8 (Ubuntu) DAV/2 http-title: Metasploitable2 - Linux11/tcp open rpcbind 2 (RPC #100000)rpcinfo:program version port/proto service100000 2111/tcp rpcbind100000 2,3.4100000 2,3.4100000 1,2.334459/tcp mountd100001 1,3.43533/tcp nlockmgr100021 1,3.43507/tcp open netbios-sn Samba smbd 3.X (workgroup: WORKGROUP)12/tcp open			
Intro-title: Metasploitable2 - Linux 11/tcp open rpcbind 2 (RPC #100000) rpcinfo: program version port/proto 100000 2 111/tdp 100000 2 111/tdp 100000 2 111/tdp 100000 2 111/tdp 100003 2.3.4 2049/tcp 100003 2.3.4 2049/tcp 100003 1.3.3 St897/tdp 100021 1.3.4 35533/tcp 100021 1.3.4 S5629/udp 100024 1 45693/udp 100024 1 54766/tcp 11/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 145/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 137/tcp open ntogin7 14/tcp open stell		2.0.000	W/2
<pre>II/tcp open rpcbind 2 (RPC #100000) rpcinfo: program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100000 2 3.3.4 2049/tcp nfs 100000 1 3.3.4 35459/tcp mountd 100000 1 3.3.4 35533/tcp nlockmgr 100021 1.3.4 35533/tcp nlockmgr 100024 1 45603/udp status 100025 1.2.3 34459/tcp status 100024 1 45603/udp status 100024 1 45603/udp status 100025 1.2.3 4459/tcp status 100024 1 45603/udp status 100024 1 45603/udp status 100025 1.2.3 4459/tcp status 100025 1.2.3 4459/tcp status 100025 1.2.3 4459/tcp status 100025 1.2.3 4459/tcp status 11/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 11/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 12/tcp open sec netkit-rsh rexecd 13/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100000 1 13.4 35533/tcp nlockmgr 100025 1.2.3 51087/udp nlockmgr 100025 1.2.3 51087/udp nlockmgr 100024 1 3.4 45503/udp nlockm</pre>			
program version port/proto service 100000 2 111/tcp rpcbind 100003 2,3,4 2049/tcp nfs 100003 2,3,4 2049/tcp nfs 100005 1,2,3 34459/tcp mountd 100005 1,2,3 S1007/udp mountd 100001 1,3,4 S533/tcp mountd 100021 1,3,4 S533/tcp nlockmgr 100021 1,3,4 S533/tdp staus 100021 1,3,4 S6520/udp nlockmgr 100021 1,3,4 S6520/udp Norkgroup: WORKGROUP) 12/tcp open netbios-ssn Samba snbd 3.X (workgroup: WORKGROUP) S32/tcp open netbios-ssn Samba snbd 3.X (workgroup: WORKGROUP) 12/tcp open ntsion-ssn Samba snbd 3.X (workgroup: WORKGROUP) S32/tcp open ntsion-ssn Samba snbd 3.X (workgroup: WORKGROUP) 12/tcp open shell Maa RHI Registry S32/tcp open ntsion-ssn Samba Snbd 3.X (workgroup: WORKGROUP)	111/tcp open		
100000 2 111/tcp rpcbind 100000 2 111/tudp rpcbind 100000 2 2.3.4 2049/tudp nfs 100000 1.2.3 34459/tcp mountd 100001 1.3.4 35533/tcp nlockmgr 100021 1.3.4 58620/tudp nlockmgr 100024 1 54706/tcp status 100024 1 54706/tcp status 39/tcp open netbios-ssn Samba snbd 3.X (workgroup: WORKGROUP) 12/tcp open netpios-ssn Samba snbd 3.X (workgroup: WORKGROUP) 12/tcp open shell Metasploitable root shell 099/tcp open java-rmi Java RHI Registry 524/tcp open shell Metasploitable root shell 0499/tcp open java-rmi Java RHI registry 524/tcp open shell Metasploitable root shell 100000 2 111/tcp rpcbind 100000 2,3.4<	rpcinfo:		
100000 2 111/udp rpcbind 1000003 2,3,4 2049/tcp nfs 1000005 1,2,3 34459/tcp mountd 1000005 1,2,3 34459/tdp mountd 1000011,3,4 35533/tcp nlockmgr 100021 1,3,4 35533/tcp nlockmgr 100021 1,3,4 35620/udp nlockmgr 100021 1,3,4 35620/udp nlockmgr 100021 1,3,4 35620/udp nlockmgr 100021 1,3,4 35620/udp nlockmgr 100024 1 54706/tcp status 100021 1,3,4 35620/udp status 100024 1 54706/tcp status 13/tcp open netkit=rsh rexecd 13/tcp open netkit=rsh rexecd 13/tcp open status status 14/tcp open status status 14/tcp open status status 100496 111/tcp rpcbind status 1000003 2,3,4			
100003 2.3.4 2049/udp nfs 100003 2.3.4 2049/udp nfs 100005 1.2.3 31459/tcp mountd 100021 1.3.4 35533/tcp nlockmgr 100021 1.3.4 36528/udp nlockmgr 100021 45629/udp nlockmgr 100024 45629/udp status 100024 54706/tcp status 100024 54706/tcp status 100024 54706/tcp status 100024 54706/tcp status 39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 12/tcp open netpi-status Nlaves Nlaves			
1000051,2,334459/tcp mountd1000211,3,435533/tcp mlockmgr1000211,3,458620/udp nlockmgr100024154766/tcp status39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)12/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)10002411/tcp reptind1000251,2,3100024112/tcp open nfs12/tcp open nfs12/tcp open nfs10002414706/tcp status	100003 2	2,3,4 2049	a/tcp nfs
1000051,2,3S1087/udp mountd1000211,3,4S553/udp mockmgr100024145693/udp status100024145693/udp status39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)12/tcp open login?14/tcp open tcpwrapped009/tcp open nfs2-4 (RPC #100003)rpcinfo:program version port/proto service1000092,3,41000092,3,41000091,1,41000091,2,31000091,2,31000091,3,41000091,3,41000091,3,41000011,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,41000021,3,410000211000241500021000021000241500021000021000241500231000241500244100024150024450024450024450024450024450024450033502444 </td <td></td> <td></td> <td></td>			
100021 1.3.4 3553/tcp nlockmgr 100024 1 4563/udp status 100024 1 54706/tcp status 39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 12/tcp open exec netkit-rsh rexecd 13/tcp open login? 14/tcp open login? 14/tcp open ftpwrapped 099/tcp open fst 2-4 (RPC #100003) rpcinfo: program version port/proto service 100000 2 111/tcp rpcbind 100000 2,3,4 2049/tcp nfs 100005 1.2,3 34459/tcp mountd 100005 1.2,3 51087/udp mountd 100005 1.2,3 51087/udp mountd 100021 1.3,4 35533/tcp nlockmgr 100024 1 54706/tcp status 112/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconmect: _ ERROR: Not a Cisco ASA or unsupported version			
<pre>100024 1 45693/udp status 39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 12/tcp open networks set in the status 13/tcp open tcpwrapped 099/tcp open java-rmi Java RMI Registry 524/tcp open shell Metasploitable root shell 049/tcp open nfs 2-4 (RPC #100003) rpcinfo: program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100000 2,3,4 2049/tcp nfs 100005 1,2,3 51007/udp mountd 100005 1,2,3 51007/udp mountd 100021 1,3,4 35533/tcp nlockmgr 100021 1,3,4 3553/tcp nlockmgr 100024 1 54706/tcp status 112/tcp open ftp ProTTPD 1.3.1 http-cisco-anyconnect: _ ERROR: Not a Cisco ASA or unsupported version</pre>	100021 1	1,3,4 35533	3/tcp_nlockmgr
<pre>100024 1 54706/tcp status 39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 145/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 12/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 13/tcp open login? 14/tcp open tcpwrapped 1099/tcp open java-rmi Java RMI Registry 524/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 100003 2,3,4 2049/tcp nfs 100005 1,2,3 31459/tcp mountd 100005 1,2,3 51087/udp mountd 100005 1,2,3 51087/udp mountd 100021 1,3,4 38520/udp nlockmgr 100024 1 45693/udp status 121/tcp open ftp ProFTPD 1,3,1 http-fiseo-anyconnect: _ ERROR: Not a Cisco ASA or unsupported version</pre>			
39/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 145/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 512/tcp open exec netkit-rsh rexecd 13/tcp open login? 514/tcp open tcpwrapped 1099/tcp open java-rmi Java RMI Registry 1524/tcp open nfs 2-4 (RPC #100003) rpcinfo: program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100000 2 111/tdp rpcbind 100000 1,2,3 34459/tcp mountd 100005 1,2,3 51087/udp mountd 100005 1,2,3 51087/udp mountd 100001 1,3,4 35533/tcp nlockmgr 100002 1,3,4 35620/udp nlockmgr 100002 1,3,4 5630/udp status 100002 1,3,4 5633/udp status 1000024 54706/tcp status 12/tcp open ftp ProFFPD 1.3.1 http-cisco-anyconnect:			
<pre>H45/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP) 12/tcp open exec netkit-rsh rexecd S13/tcp open login? 14/tcp open login? 14/tcp open topwrapped 1009/tcp open java-rmi Java RMI Registry 1524/tcp open nfs 2-4 (RPC #100003) 17ptinfo: program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/tcp rpcbind 100003 2.3.4 2049/tcp nfs 100005 1.2.3 34459/tcp mountd 100005 1.2.3 S1007/udp mountd 100005 1.2.3 S1007/udp mountd 100005 1.2.3 S1007/udp mountd 100001 1.3.4 S5533/tcp nlockmgr 100021 1.3.4 S5620/udp nlockmgr 100024 1 45693/udp status 1100024 1 54706/tcp status 1121/tcp open ftp ProFTPD 1.3.1 http://sco-anyconnect: ERROR: Not a Cisco ASA or unsupported version</pre>	39/tcp open	netbios-ssn S	Samba smbd 3.X (workgroup: WORKGROUP)
<pre>S13/tcp open login? 14/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 2,3,4 2049/tcp nfs 100003 2,3,4 2049/tcp 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 100021 1 45693/udp status 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</pre>	45/tcp open	netbios-ssn S	Samba smbd 3.X (workgroup: WORKGROUP)
S14/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: 1 program version port/proto service 1 100000 2 111/tcp rpcbind 1 100003 2,3,4 2049/tcp nfs 1 100003 2,3,4 2049/tcp nfs 1 100005 1,2,3 34459/tcp mountd 1 100005 1,2,3 51087/udp mountd 1 100021 1,3,4 35533/tcp nlockmgr 1 100021 1,3,4 58620/udp nlockmgr 1 100024 1 45693/udp status 1 100024 1 54706/tcp status 1212/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect: _ ERROR: Not a Cisco ASA or unsupported version	12/tcp open 513/tcp open	exec r	NETRIC-ISH TEXECO
<pre>l099/tcp open java-rmi Java RMI Registry l524/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 2,3,4 2049/tcp nfs 100003 2,3,4 2049/tcp 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 l_ 100024 1 54706/tcp status 2121/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect: L_ ERROR: Not a Cisco ASA or unsupported version</pre>			
20049/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 58537/tcp nlockmgr 100021 1,3,4 58620/udp nlockmgr 100024 1 45693/udp status 1100024 1 54706/tcp status 121/tcp open ftp ProFTPD 1,3.1 http-cisco-anyconnect:	1099/tcp open	i java-rmi J	
rpcinfo: program version port/proto 100000 2 111/tcp rpcbind 100000 2 111/udp rpcbind 100003 2,3,4 2049/tcp nfs 100005 2,3,4 2049/udp nfs 100005 1,2,3 34459/tcp mountd 100005 1,2,3 51087/udp mountd 100021 1,3,4 5533/tcp nlockmgr 100021 1,3,4 58620/udp nlockmgr 100024 1 45693/udp status 100024 1 54706/tcp status 1121/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect: ERROR: Not a Cisco ASA or unsupported version			
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 100003 2,3,4 2049/udp 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 121/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect:		1115	(NC #100003)
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 1100024 1 54706/tcp status 1110000000000000000000000000000000000	program v		
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 121/tcp Open ftp ProFTPD http-cisco-anyconnect:		11	
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 121/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect:			
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:	100003 2	2,3,4 2049	a/udp_nfs
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:	100005 1	,2,3 34459	
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:			
100024 1 45693/udp status 100024 1 54706/tcp status 2121/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect:			
121/tcp open ftp ProFTPD 1.3.1 http-cisco-anyconnect: ERROR: Not a Cisco ASA or unsupported version	100024 1	45693	3/udp_status
http-cisco-anyconnect: ERROR: Not a Cisco ASA or unsupported version			/tcp status
ERROR: Not a Cisco ASA or unsupported version		anyconnect:	TOFIPU 1.3.1
			or unsupported version
306/tcp open mysql NySQL 5.0.51a-3ubuntu5	306/tcp open	n mysql 🕴	
mysql-info: Protocol: 53			
Protocol: 53 Version: .0.51a-3ubuntu5			
Thread ID: 12	Thread ID	0: 12	
Capabilities flags: 43564	Capabilit	ies flags: 4350	
Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSL	Some Capa	bilities: Suppo	<pre>rt41Auth, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAf</pre>
Status: Autocommit	Status: A	utocommit	
Salt: Kla"#(@J1V@zh{P_jw:Y	Salt: Kla	*#(@J1V@zh{P_jv	
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))	3632/tcp open	distccd o	<pre>istccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-lubuntu4))</pre>





Running nmap2nessus

optional argumen	show this help message and exit	← → C 🕼 https://192.1
-s HOSTIP	[nessus server IP]	
-u USERNAME	[username]	🕲 Nessus
-p PASSWORD	[password]	Winessus
-1 INFILE	[nmap xml file]	
-t TEMPLATEFIL	<pre>E [Nessus policy template to use (optional)]</pre>	
-n SCANID	[lookup job based on scan_id (optional)]	Scans
-o OUTFILE	[nessus report (csv) (optional)]	
FLE-SP-3RFD57:nm	ap2nessus milo\$ sudo python nmap2ness.py -u milo -p p@ssw0rd	
Password:		
	sus server IP address	New Scan
	<pre>map2nessus milo\$ sudo python nmap2ness.py -u milo -p p@ssw0rd</pre>	
- Launching new		
	ts from nmapt_target.xml	My Scans 1
- Modifying Ness		
- Logging into N		
- Uploading Poli		Trash
- Starting Nessu		
	tatus: 250 : running	1.0
	tatus: 250 : running	All Scans
	itatus: 250 : running itatus: 250 : running	
	itatus: 250 : running	New Folder
	itatus: 250 : running	101110100
	itatus: 250 : running	
- Checking Job S	itatus: 250 : running	
Π		

.168.112.160:8834/nessus6.html#/	scans	☆ 🖸 🤝 D. 💩 🔨 🗘
Scans 1 Policies		n
		Upload Q Se
Scans / My Scans		
Name	Schedule	Last Scan 🔺
Scan Name	On Demand	14:27 PM

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



Nmap2nessus Results

		python nmap2ness.py -u milo -
	ng new Nessus scan	
	ing ports from nmapt_target	t.xml
	ng Nessus policy	
	into Nessus	
	ng Policy	
	g Nessus Scan	
	g Job Status: 265 : running	
	g Job Status: 265 : running	
- Checkin	g Job Status: 265 : running	5
- Checkin	g Job Status: 265 : running	5
- Checkin	g Job Status: 265 : running	ş
- Checkin	g Job Status: 265 : running	ξ.
- Checkin	g Job Status: 265 : running	ξ.
- Checkin	g Job Status: 265 : running	3
- Checkin	g Job Status: 265 : complet	ted
- Nessus	report has been saved to: r	report.csv
report.cs	v	
- Summary	of Results (Critical/High/	(Medium)
Critical	192.168.112.167:0	
Critical	192.168.112.167:1524	
Critical	192.168.112.167:445	Samba NDR MS-
Critical	192.168.112.167:5900	
High	192.168.112.167:445	Mic
High	192.168.112.167:513	
High	192.168.112.167:514	
High	192.168.112.167:53	Multiple Vendor D
High	192.168.112.167:8180	
Medium	192.168.112.167:2049	
Medium	192.168.112.167:2049	
Medium	192.168.112.167:23	
Medium	192.168.112.167:25	SMTP
Medium	192.168.112.167:25	
Medium	192.168.112.167:445	
Medium	192.168.112.167:512	
Medium	192.168.112.167:53	DNS Server
Medium	192.168.112.167:80	
Medium	192.168.112.167:80	
Medium	192.168.112.167:80	Apache HTTP S
	FD57:nmap2nessus milo\$	

-p p@ssw0rd -i nmapt_target.xml -s 192.168.112.160

Unsupported Unix Operating System Rogue Shell Backdoor Detection RPC Request Heap-Based Remote Buffer Overflow VNC Server 'password' Password rosoft Windows SMB Shares Unprivileged Access rlogin Service Detection rsh Service Detection DNS Query ID Field Prediction Cache Poisoning Unsupported Web Server Detection NFS Exported Share Information Disclosure NFS Shares World Readable Unencrypted Telnet Server SSL Certificate Expiry SSL Certificate with Wrong Hostname SSL Certificate Cannot Be Trusted Service STARTTLS Plaintext Command Injection SSL Self-Signed Certificate SMB Signing Required rexecd Service Detection Cache Snooping Remote Information Disclosure /doc Directory Browsable HTTP TRACE / TRACK Methods Allowed Server httpOnly Cookie Information Disclosure

vave[®] erLabs[®]

Results in Nessus console

→ C	🖹 https://1	92.168.112.160:8834/nessus6.html#	/scans/265/vulnerabilities		2
۱	lessus	Scans 4 Policies			
	Name	25, 2015 14:56:39		Configure Audit Trail Launch -	Export
Scans	> Hosts 1	Vulnerabilities 92 Remediation	s 2 History 1		
	Severity -	Plugin Name		Plugin Family	Count
	CRITICAL	Rogue Shell Backdoor Detection		Backdoors	1
	CRITICAL	Samba NDR MS-RPC Request Heap-Base	ed 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 Predic	tion Cache Poisoning	DNS	1
	HIGH	GH 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
	MEDILIM	Anacha HTTP Saniar http://phy.Coakia.info	mation Disclosuro	Web Servers	1

	Plugin Family	Count
	Backdoors	1
w	Misc.	1
	General	1
	Gain a shell remotely	1
	Windows	1
	DNS	1
	Service detection	1
	Service detection	1
	Web Servers	1
	CGI abuses	1
	Wab Sarvars	1



Vulnerabilities not found by Nessus

- Bruteforce SSH Exploit) <u>http://www.exploit-db.com/exploits/5632/</u>.
- Port 6667 is vulnerable to CVE-2010-2075. (exploits/unix/irc/ unreal_ircd_3281_backdoor)
- vulnerable to CVE-2015-2877). (exploit/unix/webapp/twiki_history)
- usermap_script)
- Complete walkthrough found at <u>https://community.rapid7.com/docs/</u> <u>DOC-1875</u>.

• Port 22 is vulnerable to CVE-2008-0166 (Debian OpenSSL - Predictable PRNG)

• Port 80 is running a vulnerable version of TWiki. The history component is

• Port 139 is running a vulnerable version of Samba. (exploit/multi/samba/

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



Conclusion

- the output of Nmap
- good penetration test will always be a more realistic assessment of security risk
- The script can be downloaded from <u>https://</u> github.com/milo2012/nmap2nessus.

 nmap2nessus is designed to do one thing well quickly and simply initiate a Nessus scan based on

Vulnerability assessments have their place, but a

