

logo

TITLE:	Vulnerability Assessment Plan
DATE:	_____, 200__

SUBJECT

Vulnerability Assessment - Utilizing vulnerability scanners all discovered hosts can then be tested for vulnerabilities. The result would then be analyzed to determine if there any vulnerability that could be exploited to gain access to a target host on a network. A number of tests carried out by these scanners are just banner grabbing/ obtaining version information, once these details are known, the version is compared with any common vulnerability and exploits (CVE) that have been released and reported.

BENEFITS OF ASSESSMENTS

- Build and broaden awareness.
- Establish or evaluate against a baseline.
- Identify vulnerabilities and develop responses.
- Categorize key assets and drive the risk management process.
- Develop and build internal skills and expertise.

SCOPE OF ASSESSMENT

- Identify all critical vulnerabilities—physical and cyber—and develop appropriate response options.
- Identify and rank all key assets from a security perspective.
- Develop the business case for making security investments and organizational changes that will enhance security.
- Enhance awareness and make security an integral part of the business strategy.

Manual

Patch Levels

Result: _____

Vulnerability Assessment Tool

Nessus (Windows)

Result: _____

Enumeration Tools

```
nmap  
nmap -n -A -P0 -p- -T Agressive -iL nmap.targetlist -oX nmap.syn.results.xml
```

```
nmap -sU -P0 -v -O -p 1-30000 -T polite -iL nmap.targetlist > nmap.udp.results
```

```
nmap -sV -P0 -v -p 21,22,23,25,53,80,443,161 -iL nmap.targets > nmap.version.results  
grep "appears to be up" nmap_saved_filename | awk -F\ '{print $2}' | awk -F\ '{print $1}' > ip_list
```

Cisco Specific Testing

Nmap To effectively scan a Cisco device, both TCP and UDP ports across the whole range must be checked. TCP scan: - This will perform a TCP scan, fingerprint, be verbose, scan ports 1-65535 against IP 10.1.1.1 and output the results in normal mode to TCP.scan.txt file.

```
nmap -sT -O -v -p 1-65535 <IP> -oN TCP.scan.txt
```

UDP scan: - This will perform a UDP scan, be verbose, scan ports 1.65535 against IP 10.1.1.1 and output the results in normal mode to UDP.scan.txt file.

```
nmap -sU -v -p 1-65535 <IP> -oN UDP.scan.txt
```

netcat

nc -v -w 2 -z IP_Address port_range/port_number

nc -v -n IP_Address port

amap

amap [-A|-B|-P|-W] [-1buSRHUdqv] [[-m] -o <file>] [-D <file>] [-t/-T sec] [-c cons] [-C retries] [-p proto] [-i <file>] [target port [port] ...]

amap -bqv IP_Address port

nbtscan

nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] (-f filename) | (<scan_range>)

NetBIOS enumeration

Null Session

```
net use \\192.168.1.1\ipc$ "" /u:""
```

```
net view \\ip_address
```

Firewall Tools

```
firewalk -p [protocol] -d [destination_port] -s [source_port] [internal_IP] [gateway_IP]
```

```
ftester host 1 ./ftestd -i eth0 -v host 2 ./ftest -f ftest.conf -v -d 0.01 then ./report ftest.log ftestd.log
```

FTP port 21

Fingerprint server

```
telnet ip_address 21 (Banner grab)
```

Run command ftp ip_address

Check for anonymous access
ftp ip_address
Username: anonymous OR anon
Password: any@email.com

Password guessing

Hydra brute force
Brutus

Examine configuration files

/etc/inetd.conf

/etc/xinetd.d/telnet

/etc/xinetd.d/stelnet

LDAP Port 389

ldap enumeration

ldapminer

ldapminer -h ip_address -p port (not required if default) -d

openldap

ldapsearch [-n] [-u] [-v] [-k] [-K] [-t] [-A] [-L[L[L]]] [-M[M]] [-d debuglevel] [-f file] [-D binddn] [-W] [-w passwd] [-y passwdfile] [-H ldapuri] [-h ldaphost] [-p ldapport] [-P 2|3] [-b searchbase] [-s base|one|sub] [-a never|always|search|find] [-l timelimit] [-z sizelimit] [-O security-properties] [-l] [-U authcid] [-R realm] [-x] [-X authzid] [-Y mech] [-Z[Z]] filter [attrs...]

ldapadd [-c][-S file][-n][-v][-k][-K][-M[M]][-d debuglevel][-D binddn][-W][-w passwd][-y passwdfile][-h ldaphost][-p ldap-port][-P 2|3][-O security-properties][-l][-Q][-U authcid][-R realm][-x][-X authzid][-Y mech][-Z[Z]][-f file]

ldapdelete [-n][-v][-k][-K][-c][-M[M]][-d debuglevel][-f file][-D binddn][-W][-w passwd][-y passwdfile][-H ldapuri][-h ldaphost][-p 2|3][-p ldapport][-O security-properties][-U authcid][-R realm][-x][-l][-Q] [-X authzid][-Y mech][-Z[Z]][dn]

ldapmodify [-a][-c][-S file][-n][-v][-k][-K][-M[M]][-d debuglevel][-D binddn][-W][-w passwd][-y passwdfile][-H ldapuri][-h ldaphost][-p ldapport][-P 2|3][-O security-properties][-l][-Q][-U authcid][-R realm][-x][-X authzid][-Y mech][-Z[Z]][-f file]
