Penetrační testování firewallu

Číslo testu:..... Datum:.....

Adresa:.....
.....
.....

Kontaktní osoba:.....

Telefon:.....

Úvod

Tento dokument je vytvořen jako procedura, jak postupovat při externím síťovém penetračním testování. Současně jej lze použít jako report penetračního testování. Cílem je otestovat dostupnost a bezpečnost hraničního firewallu. Při testu se předpokládá použití paketového firewallu s demilitarizovanou zónou. Proxy systémy nejsou cílem testování. Jednotlivé části testů jsou následující:

- Průzkum vzdálené sítě,
- testování firewallu,
- skenování, identifikace operačního systému a služeb firewallu,
- testování hesel,
- testování bezpečnostních děr.

1 Známé údaje

1.1 Informace o společnosti (název, adresa, kontakty, zaměstnanci).

Není k dispozici

1.2 Informace o firewallu (IP adresa, typ zapojení firewallu).

IP adresa: 192.168.30.10 Zapojení: 3-Leg (LAN, DMZ, WAN)

1.3 Ostatní informace.

DMZ servery IP: 192.168.30.20 - web IP: 192.168.30.30 – web, mail

2 Průzkum vzdálené sítě

2.1 Identifikace doménového jména nebo ip firewallu.
nslookup $IP
nslookup $domain

není k dispozici, nepoužívá se doménových jmen pro experimentální sít

2.2 Informace o registracích domény a přidělených rozsazích ip adres.
whois $domain
whois $ip

není k dispozici, neexistují registrace pro experimentální sít

2.2 Informace o doméně. Zjistit případné servery umístěné za firewallem v dmz podle IP adres (adresy podobné firewalu, adresy přiděleného rozsahu).
dig $domain
./dnsenum.pl $domain

není k dispozici, neexistují dns záznamy pro experimentální sít

2.3 Zjistit cestu k firewallu.
Pro TCP traceroute je nutné
UDP traceroute
traceroute -n $IP_firewall
ICMP traceroute
traceroute -I -n $IP_firewall

Způsob: TCP
root@mentor-desktop:/opt/nessus/bin# traceroute -n 192.168.30.10
traceroute to 192.168.30.10 (192.168.30.10), 30 hops max, 40 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *

Způsob: ICMP
root@mentor-desktop:/opt/nessus/bin# traceroute -I -n 192.168.30.10
traceroute to 192.168.30.10 (192.168.30.10), 30 hops max, 40 byte packets
1 192.168.30.10 0.594 ms 0.662 ms 0.638 ms

2.4 Identifikovat, zda servery společnosti leží za testovaným firewallem.
Testují se známé servery společnosti a získané záznamy z bodu 2.2. Použití ip adres nebo doménového jména. Servery ležící za firewallem je možné považovat v případě identické cesty nebo delší se stejnou trasou jako u firewallu.
traceroute –n $IP_server
ICMP traceroute
traceroute –I –n $IP_server

192.168.30.20
Způsob: TCP
root@mentor-desktop:/opt/nessus/bin# traceroute -n 192.168.30.20
traceroute to 192.168.30.20 (192.168.30.20), 30 hops max, 40 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *

Způsob: ICMP
root@mentor-desktop:/opt/nessus/bin# traceroute -n -I 192.168.30.20
traceroute to 192.168.30.20 (192.168.30.20), 30 hops max, 40 byte packets
1 192.168.30.20 0.792 ms 0.725 ms 0.697 ms

192.168.30.30
Způsob: TCP
root@mentor-desktop:/opt/nessus/bin# traceroute -n 192.168.30.30
traceroute to 192.168.30.30 (192.168.30.30), 30 hops max, 40 byte packets
1 * * *
2 * * *
3 * * *
4 * * *

```
 5  * * *

Způsob: ICMP
root@mentor-desktop:/opt/nessus/bin# traceroute -n -I 192.168.30.30
traceroute to 192.168.30.30 (192.168.30.30), 30 hops max, 40 byte packets
 1  192.168.30.30  0.375 ms  0.397 ms  0.362 ms
```

2.5 Získat veřejně dostupné informace. Využití tzv. google-hacking.
Zkoušení vyhledat na internetu pomocí známých údajů informace o konfiguracích, technických dotazech, bezpečnostních dírách apod..

není dostupné, pro experimentální sít nejsou informace na internetu

3 Testování firewallu

3.1 Identifikace typu firewallu.
Test otevrených vyšších portů >1024. Pokud je nefiltrováno jedná se o nestavový. V opačném případě je stavový. Identifikace vychází z pravidla, kdy na bezstavovém firewallu musí být povoleny vyšší porty pro zpětná navázaná spojení.
nmap –sA -p1024-2000 $ip_firewall
nmap –sA -p1024-2000 $ip_serverl

firewall je stavový

```
root@mentor-desktop:/opt/nessus/bin# nmap -sA -p1024-2000 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:05 CEST
All 977 scanned ports on 192.168.30.10 are filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.71 seconds
```

vybraný server 192.168.30.20

```
root@mentor-desktop:/opt/nessus/bin# nmap -sA -p1024-2000 192.168.30.20

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:05 CEST
All 977 scanned ports on 192.168.30.20 are filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.86 seconds
```

3.2 Identifikace NATu.
Pokud jsou ip adresy veřejných serverů stejné jako firewall, jedná se pravděpodobně o směrování portů. Pokud jsou adresy odlišné jedná se pravděpodobně o NAT 1:1.

provádí se pravděpodobně NAT 1:1, pravděpodobně překlad na privátní adresy (stejná TTL vzdálenost jako firewall)

3.3 Zjistit povolené porty pro servery v dmz.
Servery z bodu 2.4 otestovat na povolené porty pomocí ruzných typů skenů.

nmap –sT -p 1-1024 $ip_serveru
nmap –sS -p 1-1024 $ip_serveru
nmap –sF -p 1-1024 $ip_serveru
nmap –sA -p 1-1024 $ip_serveru
nmap –sU -p 1-1024 $ip_serveru

192.168.30.20
Metoda: TCP
root@mentor-desktop:/opt/nessus/bin# nmap -sT -p 1-1024 192.168.30.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:14 CEST
Interesting ports on 192.168.30.20:
Not shown: 1021 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds

Metoda: SYN
root@mentor-desktop:/opt/nessus/bin# nmap -sS -p 1-1024 192.168.30.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:15 CEST
Interesting ports on 192.168.30.20:
Not shown: 1021 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds

Metoda: FIN
root@mentor-desktop:/opt/nessus/bin# nmap -sF -p 1-1024 192.168.30.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:34 CEST
All 1024 scanned ports on 192.168.30.20 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.44 seconds

Metoda: ACK
root@mentor-desktop:/opt/nessus/bin# nmap -sA -p 1-1024 192.168.30.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:16 CEST
Interesting ports on 192.168.30.20:
Not shown: 1021 filtered ports
PORT STATE SERVICE

22/tcp unfiltered ssh
80/tcp unfiltered http
443/tcp unfiltered https
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.71 seconds

Metoda: UDP
root@mentor-desktop:/opt/nessus/bin# nmap -sU -p 1-1024 192.168.30.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:17 CEST
All 1024 scanned ports on 192.168.30.20 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds

192.168.30.30
Metoda: TCP
root@mentor-desktop:/opt/nessus/bin# nmap -sT -p 1-1024 192.168.30.30

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:28 CEST
Interesting ports on 192.168.30.30:
Not shown: 1015 filtered ports
PORT   STATE SERVICE
22/tcp open   ssh
25/tcp open   smtp
80/tcp open   http
110/tcp open   pop3
143/tcp open   imap
443/tcp open   https
465/tcp closed smtps
993/tcp open   imaps
995/tcp open   pop3s
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.93 seconds

Metoda: SYN
root@mentor-desktop:/opt/nessus/bin# nmap -sS -p 1-1024 192.168.30.30

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:29 CEST
Interesting ports on 192.168.30.30:
Not shown: 1015 filtered ports
PORT   STATE SERVICE
22/tcp open ssh
25/tcp open   smtp
80/tcp open   http
110/tcp open   pop3
143/tcp open   imap

```
443/tcp open   https
465/tcp closed smtps
993/tcp open   imaps
995/tcp open   pop3s
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.41 seconds

Metoda: FIN
root@mentor-desktop:/opt/nessus/bin# nmap -sF -p 1-1024 192.168.30.30

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:35 CEST
All 1024 scanned ports on 192.168.30.30 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.21 seconds

Metoda: ACK
root@mentor-desktop:/opt/nessus/bin# nmap -sA -p 1-1024 192.168.30.30

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:36 CEST
Interesting ports on 192.168.30.30:
Not shown: 1015 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
110/tcp unfiltered pop3
143/tcp unfiltered imap
443/tcp unfiltered https
465/tcp unfiltered smtps
993/tcp unfiltered imaps
995/tcp unfiltered pop3s
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.50 seconds

Metoda: UDP
root@mentor-desktop:/opt/nessus/bin# nmap -sU -p 1-1024 192.168.30.30

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:28 CEST
All 1024 scanned ports on 192.168.30.30 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.51 seconds
```

3.3 Zjistit povolené icmp zprávy pro servery v dmz.
Servery z bodu 2.4 otestovat na povolené icmp zprávy.
sing -$icmp-type –c 1 $ip_serveru

192.168.30.20

Typ icmp: echo request
root@mentor-desktop:/opt/nessus/bin# sing -echo 192.168.30.20
SINGing to 192.168.30.20 (192.168.30.20): 16 data bytes
16 bytes from 192.168.30.20: seq=0 ttl=64 TOS=0 time=2.850 ms
16 bytes from 192.168.30.20: seq=1 ttl=64 TOS=0 time=0.384 ms

Typ icmp: timestamp
bez odezvy

Typ icmp: Address mask request
bez odezvy

Typ icmp: Information request
bez odezvy

192.168.30.30
Typ icmp: echo request
root@mentor-desktop:/opt/nessus/bin# sing -echo 192.168.30.30
SINGing to 192.168.30.30 (192.168.30.30): 16 data bytes
16 bytes from 192.168.30.30: seq=0 ttl=64 TOS=0 time=0.523 ms
16 bytes from 192.168.30.30: seq=1 ttl=64 TOS=0 time=0.331 ms

Typ icmp: timestamp
bez odezvy

Typ icmp: Address mask request
bez odezvy

Typ icmp: Information request
bez odezvy

3.4 Zjistit povolené porty pomocí TTL
firewalk –s $source_port –d$destination_port –p$packet_type $ip_firewall $ip_server_dmz

nelze použít

4 Skenování, identifikace operačního systému a služeb firewallu

4.1 Identifikovat operační systém.
nmap –O $ip_firewall

Linux
root@mentor-desktop:/opt/nessus/bin# nmap -O 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:44 CEST
Interesting ports on 192.168.30.10:
Not shown: 999 filtered ports
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 00:0C:29:43:1D:8A (VMware)

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.27
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.31 seconds
```

4.2 Zjistit povolené porty pro firewall.

Povolené porty pomocí ruzných typů skenů.

nmap –sT -p 1-1024 $ip_serveru
nmap –sS -p 1-1024 $ip_serveru
nmap –sA -p 1-1024 $ip_serveru
nmap –sF -p 1-1024 $ip_serveru
nmap –sU -p 1-1024 $ip_serveru
nmap –sN -p 1-1024 $ip_serveru

```
Metoda: TCP
root@mentor-desktop:/opt/nessus/bin# nmap -sT -p 1-1024 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:46 CEST
Interesting ports on 192.168.30.10:
Not shown: 1023 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds

Metoda: SYN
root@mentor-desktop:/opt/nessus/bin# nmap -sS -p 1-1024 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:48 CEST
Interesting ports on 192.168.30.10:
Not shown: 1023 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.28 seconds

Metoda: FIN
root@mentor-desktop:/opt/nessus/bin# nmap -sF -p 1-1024 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 01:48 CEST
All 1024 scanned ports on 192.168.30.10 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.71 seconds
```

Metoda: UDP
root@mentor-desktop:/opt/nessus/bin# nmap -sU -p 1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:49 CEST
All 1024 scanned ports on 192.168.30.10 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 24.71 seconds

Metoda: NULL
root@mentor-desktop:/opt/nessus/bin# nmap -sN -p 1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:50 CEST
All 1024 scanned ports on 192.168.30.10 are open|filtered
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.01 seconds

4.3 Zjistit povolené icmp zprávy pro firewall.
Otestovat firewall na povolené icmp zprávy.
sing -$icmp-type –c 1 $ip_serveru

Typ icmp: echo request
root@mentor-desktop:/opt/nessus/bin# sing -echo 192.168.30.10
SINGing to 192.168.30.10 (192.168.30.10): 16 data bytes
16 bytes from 192.168.30.10: seq=0 ttl=64 TOS=0 time=0.385 ms
16 bytes from 192.168.30.10: seq=1 ttl=64 TOS=0 time=0.365 ms

Typ icmp: timestamp
bez odezvy

Typ icmp: Address mask request
bez odezvy

Typ icmp: Information request
bez odezvy

4.4 Zjistit typ služby na portu.
Některé porty mohou být obsaženy i jinými službami než standardními nebo lze získat více informací o verzi apod..
nc $ip_firewall $port
připojení webovým prohlížečem

ssh
root@mentor-desktop:/opt/nessus/bin# nc 192.168.30.10 22
SSH-2.0-OpenSSH_5.2

4.5 Otestovat odolnost proti fragmentovému útoku.
Použít metodu skenování s možností fragmentace.
nmap –sS -f -p 1-1024 $ip_serveru

stejný výsledek jako bez fragmentace
root@mentor-desktop:/opt/nessus/bin# nmap -sS -f -p1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-18 01:53 CEST
Interesting ports on 192.168.30.10:
Not shown: 1023 filtered ports
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 00:0C:29:43:1D:8A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds

4.6 Otestovat odolnost na Syn flood.
hping3 –S $ip_firewall --flood

není zranitelný
root@mentor-desktop:/opt/nessus/bin# hping3 -S 192.168.30.10 --flood
HPING 192.168.30.10 (eth1 192.168.30.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

root@mentor-desktop:/# ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=1 ttl=64 time=0.313 ms
64 bytes from 192.168.30.10: icmp_seq=2 ttl=64 time=0.297 ms
64 bytes from 192.168.30.10: icmp_seq=3 ttl=64 time=0.274 ms
64 bytes from 192.168.30.10: icmp_seq=4 ttl=64 time=0.539 ms
64 bytes from 192.168.30.10: icmp_seq=5 ttl=64 time=3.56 ms
64 bytes from 192.168.30.10: icmp_seq=6 ttl=64 time=0.265 ms
64 bytes from 192.168.30.10: icmp_seq=7 ttl=64 time=0.185 ms
64 bytes from 192.168.30.10: icmp_seq=8 ttl=64 time=0.206 ms

4.6 Otestovat odolnost na Land attack.
hping3 –S –a $ip_firewall –p $port $ip_firewall

není zranitelný
root@mentor-desktop:/opt/nessus/bin# hping3 -S -a 192.168.30.10 192.168.30.10
HPING 192.168.30.10 (eth1 192.168.30.10): S set, 40 headers + 0 data bytes

root@mentor-desktop:/# ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=1 ttl=64 time=0.969 ms
64 bytes from 192.168.30.10: icmp_seq=30 ttl=64 time=0.343 ms
64 bytes from 192.168.30.10: icmp_seq=31 ttl=64 time=0.265 ms
64 bytes from 192.168.30.10: icmp_seq=32 ttl=64 time=0.330 ms
64 bytes from 192.168.30.10: icmp_seq=33 ttl=64 time=0.364 ms
64 bytes from 192.168.30.10: icmp_seq=34 ttl=64 time=0.252 ms

5 Testování hesel

5.1 Otestovat defaultní hesla administrace.
Otestovat služby poskytující možnost administrace na defaultní hesla. Tyto služby jsou identifikovány v bode 4.2 a 4.4.

není k dispozici

5.2 Otestovat sílu hesel.
Použít aplikaci umožňující brute-force metodu louskání hesel na podporovaný port.

Ssh
bez nálezů - 5 znaků abecedy

6 Testování bezpečnostních děr

6.1 Identifikovat bezpečnostní díry v aplikacích a operačním systému.
Spustit aplikaci umožňující vyhledávání bezpečnostních děr.
nesus

2 lehce závažné – detekce výrobce sítové karty, detekce virtualního stroje

6.2 Případné otestování zneužití bezpečnostních děr.
Spouštění expploitů pomocí metasploit.

Nezjištěny zranitelné bezpečnostní díry viz bod 6.1

Nálezy:

- Neblokované skenování. Umožňuje mapovat firewall a prostředí sítě.
- Povolený ping. Umožňuje zjišťovat dostupnost serverů v adresním rozsahu.
- Detekce operačního systému.
- Detekce verze ssh.

Jméno auditora:..... Datum:.....

Převzal:..... Datum:.....