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

není k dispozici

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

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

3. Ostatní informace.

DMZ servery IP: 192.168.40.20 - web IP: 192.168.40.30 – 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 síť

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

není k dispozici, neexistují registrace pro experimentální síť

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 se záznamy pro experimentální síť

2.3 Zjistit cestu k firewallu.
Pro TCP traceroute je nutné znát otevřený port na firewallu. Pokud není znám, je potřeba provést nejprve skenování firewallu.
UDP traceroute
traceroute -n $IP_firewall
ICMP traceroute
traceroute -I -n $IP_firewall

Způsob: UDP
root@mentor-desktop:~# 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:~# 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 73.750 ms 73.735 ms 74.469 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.
UDP traceroute
traceroute –n $IP_server
ICMP traceroute
traceroute –I –n $IP_server

192.168.40.20 leží za firewallem
Způsob: UDP
root@mentor-desktop:~# traceroute -n 192.168.40.20
traceroute to 192.168.40.20 (192.168.40.20), 30 hops max, 40 byte packets

```
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *

Způsob: ICMP
root@mentor-desktop:~# traceroute -I -n 192.168.40.20
traceroute to 192.168.40.20 (192.168.40.20), 30 hops max, 40 byte packets
 1  192.168.30.10  83.817 ms  85.548 ms  86.449 ms
 2  192.168.40.20  86.971 ms  87.418 ms  87.885 ms
```

192.168.40.30 leží za firewallem

```
Způsob: UDP
root@mentor-desktop:~# traceroute -n 192.168.40.30
traceroute to 192.168.40.30 (192.168.40.30), 30 hops max, 40 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *

Způsob: UDP
root@mentor-desktop:~# traceroute -I -n 192.168.40.30
traceroute to 192.168.40.30 (192.168.40.30), 30 hops max, 40 byte packets
 1  192.168.30.10  73.639 ms  73.552 ms  73.644 ms
 2  192.168.40.30  73.798 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..

pro experimentální sít nelze najít žádné informace

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_server

firewall je stavový

```
root@mentor-desktop:~# nmap -sA -p 1024-2000 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 21:55 CEST
All 977 scanned ports on 192.168.30.10 are filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 23.53 seconds

vybraný server 192.168.40.20
root@mentor-desktop:~# nmap -sA -p 1024-2000 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 21:56 CEST
All 977 scanned ports on 192.168.40.20 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.32 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.

za firewallem, jedná se o statický NAT 1:1 (veřejné adresy se směrováním)

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

192.168.40.20
Metoda: TCP
root@mentor-desktop:~# nmap -sT -p 1-1024 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 21:59 CEST
Interesting ports on 192.168.40.20:
Not shown: 1022 filtered ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https

Metoda: SYN
root@mentor-desktop:~# nmap -sS -p 1-1024 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:03 CEST
Interesting ports on 192.168.40.20:
Not shown: 1022 filtered ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds

Metoda: FIN
root@mentor-desktop:~# nmap -sF -p 1-1024 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:02 CEST
All 1024 scanned ports on 192.168.40.20 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 22.32 seconds

Metoda: ACK
Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
root@mentor-desktop:~# nmap -sA -p 1-1024 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 21:58 CEST
All 1024 scanned ports on 192.168.40.20 are filtered

Nmap done: 1 IP address (1 host up) scanned in 22.59 seconds

Metoda: UDP
root@mentor-desktop:~# nmap -sU -p 1-1024 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:05 CEST
All 1024 scanned ports on 192.168.40.20 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds

192.168.40.30
Metoda: TCP
root@mentor-desktop:~# nmap -sT -p 1-1024 192.168.40.30

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:07 CEST
Interesting ports on 192.168.40.30:
Not shown: 1016 filtered ports
PORT   STATE SERVICE
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

Nmap done: 1 IP address (1 host up) scanned in 10.01 seconds

Metoda: SYN
root@mentor-desktop:~# nmap -sS -p 1-1024 192.168.40.30

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:07 CEST
Interesting ports on 192.168.40.30:
Not shown: 1016 filtered ports
PORT   STATE SERVICE
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

Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds

Metoda: FIN
root@mentor-desktop:~# nmap -sF -p 1-1024 192.168.40.30

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 22:08 CEST
All 1024 scanned ports on 192.168.40.30 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds

Metoda: ACK
root@mentor-desktop:~# nmap -sA -p 1-1024 192.168.40.30

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 22:08 CEST
All 1024 scanned ports on 192.168.40.30 are filtered

Nmap done: 1 IP address (1 host up) scanned in 14.80 seconds

Metoda: UDP
root@mentor-desktop:~# nmap -sU -p 1-1024 192.168.40.30

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 22:09 CEST
All 1024 scanned ports on 192.168.40.30 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.61 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

192.168.40.20

```
Typ icmp: echo request
root@mentor-desktop:~# sing -echo 192.168.40.20
SINGing to 192.168.40.20 (192.168.40.20): 16 data bytes
16 bytes from 192.168.40.20: seq=0 ttl=63 TOS=0 time=6.320 ms
16 bytes from 192.168.40.20: seq=1 ttl=63 TOS=0 time=2.103 ms

Typ icmp: timestamp
bez odpovědi


Typ icmp: Address Mask Request
```

bez odpovědi

Typ icmp: Information Request
bez odpovědi

192.168.40.30
Typ icmp: echo request
root@mentor-desktop:~# sing -echo 192.168.40.30
SINGing to 192.168.40.30 (192.168.40.30): 16 data bytes
16 bytes from 192.168.40.30: seq=0 ttl=63 TOS=0 time=3.161 ms
16 bytes from 192.168.40.30: seq=1 ttl=63 TOS=0 time=1.886 ms

Typ icmp: timestamp
bez odpovědi

Typ icmp: Address Mask Request
bez odpovědi

Typ icmp: Information Request
bez odpovědi

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

192.168.40.20
TCP porty
80, 443

192.168.40.30
TCP porty
80, 443, 25, 110,143, 465,993,995

4 Skenování, identifikace operačního systému a služeb firewallu

4.1 Identifikovat operační systém.
nmap –O $ip_firewall

Microsoft windows server 2003 SP2
root@mentor-desktop:~# nmap -O 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:34 CEST
Interesting ports on 192.168.30.10:
Not shown: 999 filtered ports
PORT STATE SERVICE
3389/tcp open ms-term-serv
MAC Address: 00:0C:29:43:E9:7A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|switch|WAP

Running (JUST GUESSING) : Microsoft Windows XP|2003|2000 (95%), Xylan embedded (92%), DEC Digital UNIX 4.X (90%), Apple embedded (86%)
Aggressive OS guesses: Microsoft Windows XP SP3 (95%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows XP Professional SP2 (firewall enabled) (92%), Microsoft Windows XP SP2 (92%), Xylan OmniStack switch (version 3.2.5) (92%), Xylan OmniStack switch (version 3.4.7) (92%), Microsoft Windows XP Embedded SP2 (91%), Microsoft Windows 2000 SP4 (90%), DEC Digital UNIX OSF1 v4.0 1229 (90%)
No exact OS matches for host (test conditions non-ideal).
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 24.95 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:~# nmap -sT -p1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:37 CEST
All 1024 scanned ports on 192.168.30.10 are filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.28 seconds

Metoda: SYN
root@mentor-desktop:~# nmap -sS -p1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:44 CEST
All 1024 scanned ports on 192.168.30.10 are filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.31 seconds

Metoda: ACK
root@mentor-desktop:~# nmap -sA -p1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:45 CEST
All 1024 scanned ports on 192.168.30.10 are filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds

```
Metoda: FIN
root@mentor-desktop:~# nmap -sF -p1-1024 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 22:45 CEST
All 1024 scanned ports on 192.168.30.10 are open|filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.39 seconds

Metoda: UDP
root@mentor-desktop:~# nmap -sU -p1-1024 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 22:46 CEST
All 1024 scanned ports on 192.168.30.10 are open|filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.86 seconds

Metoda: Null
root@mentor-desktop:~# nmap -sN -p1-1024 192.168.30.10

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-17 22:47 CEST
All 1024 scanned ports on 192.168.30.10 are open|filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.23 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:~# 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=128 TOS=0 time=2.046 ms
16 bytes from 192.168.30.10: seq=1 ttl=128 TOS=0 time=0.822 ms

Typ icmp: timestamp
bez odpovědi


Typ icmp: Address Mask Request
bez odpovědi

Typ icmp: Information Request
bez odpovědi
```

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

Porty souhlasí se standardním přidělením

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

firewall nepropouští zranitelné fragmentované pakety
root@mentor-desktop:~# nmap -sS -f -p 1-1024 192.168.30.10

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:50 CEST
All 1024 scanned ports on 192.168.30.10 are filtered
MAC Address: 00:0C:29:43:E9:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.34 seconds

192.168.40.20
root@mentor-desktop:~# nmap -sS -f -p 1-1024 192.168.40.20

Starting Nmap 5.00 (http://nmap.org) at 2010-05-17 22:50 CEST
All 1024 scanned ports on 192.168.40.20 are filtered

Nmap done: 1 IP address (1 host up) scanned in 22.76 seconds

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

zhoršení odezvy
root@mentor-desktop:~# 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=8 ttl=128 time=0.255 ms
64 bytes from 192.168.30.10: icmp_seq=9 ttl=128 time=0.701 ms
64 bytes from 192.168.30.10: icmp_seq=10 ttl=128 time=0.302 ms
64 bytes from 192.168.30.10: icmp_seq=11 ttl=128 time=0.212 ms
64 bytes from 192.168.30.10: icmp_seq=13 ttl=128 time=0.453 ms
64 bytes from 192.168.30.10: icmp_seq=14 ttl=128 time=7.65 ms
64 bytes from 192.168.30.10: icmp_seq=16 ttl=128 time=8.63 ms
64 bytes from 192.168.30.10: icmp_seq=18 ttl=128 time=0.480 ms
64 bytes from 192.168.30.10: icmp_seq=19 ttl=128 time=14.7 ms
64 bytes from 192.168.30.10: icmp_seq=22 ttl=128 time=27.0 ms
64 bytes from 192.168.30.10: icmp_seq=24 ttl=128 time=71.2 ms

4.6 Otestovat odolnost na Land attack.

hping3 –S –a $ip_firewall –p $port $ip_firewall

není zranitelný

```
root@mentor-desktop:~# hping3 -S  -a 192.168.30.10 192.168.30.10 -p 3389 -V
using eth1, addr: 192.168.30.12, MTU: 1500
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=47 ttl=128 time=0.463 ms
64 bytes from 192.168.30.10: icmp_seq=48 ttl=128 time=0.409 ms
64 bytes from 192.168.30.10: icmp_seq=49 ttl=128 time=5.03 ms
64 bytes from 192.168.30.10: icmp_seq=50 ttl=128 time=0.276 ms
64 bytes from 192.168.30.10: icmp_seq=51 ttl=128 time=0.435 ms
64 bytes from 192.168.30.10: icmp_seq=52 ttl=128 time=0.378 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 aplikací umožňující brute-force metodu louskání hesel na podporovaný port.

nepodporovaný protokol

6 Testování bezpečnostních děr

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

1 středně závažná - upozornění na možnost Man-in-Middle u RDP
7 lehce závažných – Detekce OS, Traceroute k firewallu apod.

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

nezjištěna zranitelná bezpečnostní díra viz bod 6.1

Nálezy:

- Neblokované skenování. Umožňuje mapovat firewall a prostředí sítě.
- Povolený ping. Umožňuje zjišťovat dostupnost serverů v adresním rozsahu.
- SYN flood způsobuje zhoršení odezvy firewallu. V kritickém případě by mohlo dojít k Denial of service?
- Detekce operačního systému.

Jméno auditora:..... Datum:.....

Převzal:..... Datum:.....