



Reverse Shells Enable Attackers To Operate From Your Network

Richard Hammer

August 2006



Reverse Shells?

- Why should you care about reverse shells?
- How do reverse shells work?
- How do reverse shells get installed on your systems?
- What covert channels do reverse shells use?
- How do you detect reverse shells on your network?



Reverse Shells? (Cont)

- Will firewall egress rules stop reverse shells?
- How do you test firewall egress rules?
- Is there a positive use for reverse shells?
- How do you protect your network against reverse shells?

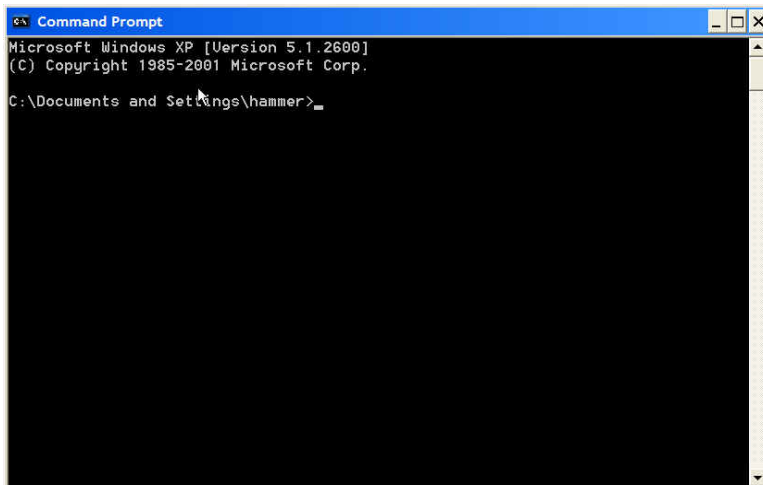


Why should you care about reverse shells?

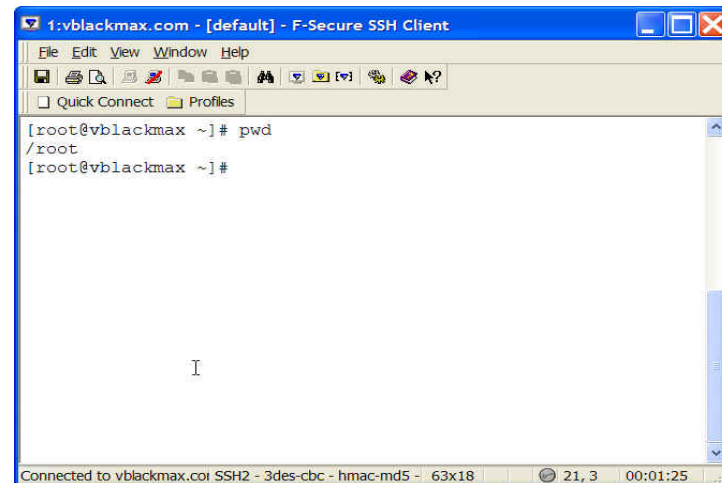
- Reverse shells give attackers full control of the systems they are installed on
- Reverse shells allow attackers to collect and send your data out of your network
- Reverse shells allow attackers to capture usernames and passwords
- Reverse shells allow attackers to scan your network from the inside

What the heck is a shell?

- Command line user interface for a computer
- Users enter text commands for the computer system to execute



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\hammer>
```

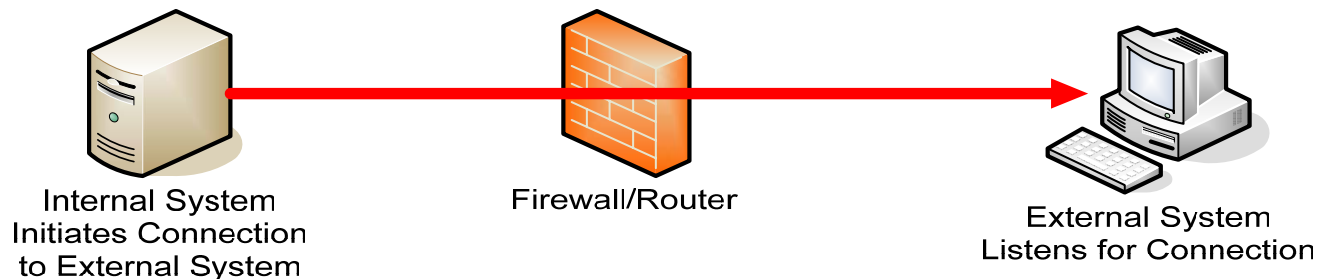


```
1:vblackmax.com - [default] - F-Secure SSH Client
File Edit View Window Help
Quick Connect Profiles
[root@vblackmax ~]# pwd
/root
[root@vblackmax ~]#
```

Connected to vblackmax.col SSH2 - 3des-cbc - hmac-md5 - 63x18 21,3 00:01:25

How do reverse shells work?

- Reverse shells allow access to internal systems without having incoming access to the network
- Reverse shells force an internal system to actively connect out to an external system





How do reverse shells get installed on your systems?

- Physical access
 - Reverse shell installed using auto-play feature
 - Skilled intruder with private physical access can defeat all installed security mechanisms and install reverse shells
 - Insider installing reverse shells
- Social Engineering someone into installing the reverse shell program
- Users executing e-mail attachments that install the reverse shell program
- Users downloading and executing reverse shell program
- Legitimate programs that can act like reverse shells

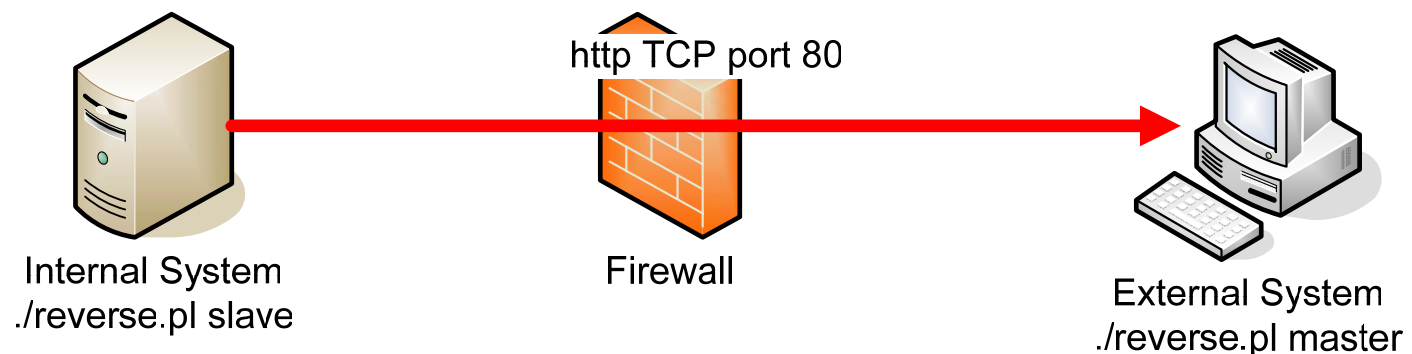


What covert channels do reverse shells use?

- Reverse shells can operate using any protocol/port combination that is allowed out of your network
- Netcat – any TCP/UDP port
- Cryptcat - any TCP/UDP port with encryption
- Loki & Ping Tunnel - ICMP
- Reverse WWW Shell – HTTP
- DNS Tunnel – DNS
- Sneakin – Telnet
- Stunnel – SSL
- Secure Shell - SSH
- Custom Reverse Shell ???

Reverse WWW Shell

- Attacker configures variables
 - External system IP address
 - Port
 - Time of day to execute
 - Proxy information if needed
- Attacker must find a way to execute on the internal system





Application aware firewalls and proxies

- Application aware firewalls and proxies are capable of making filtering decisions based on the embedded application data in the network traffic
 - An application aware firewall will not pass telnet traffic through the http port
- When picking a reverse shell to exploit your network the attacker must know if your perimeter protection is application aware

Do you know if your perimeter protection is application aware?



Will firewall egress rules stop reverse shells?

- Egress filters will stop reverse shells if the protocol/port combination is closed
- Application aware firewalls and proxies will stop reverse shells that do not communicate using the expected application layer protocol
- Reverse shell programs are a good reason to only open outgoing service ports required for business

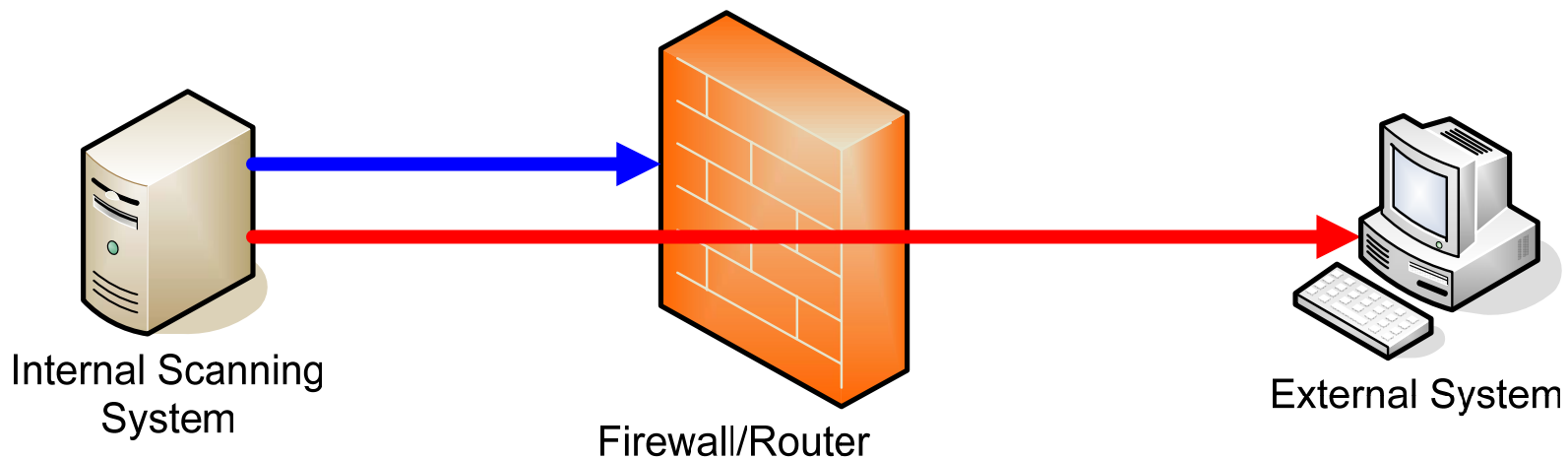
Are egress filters installed on your network?



How do you test firewall egress rules?

- Port scanning the firewall from the inside is not a valid test of egress filter rules
- Testing egress rules requires passing traffic through the firewall from the inside to a system outside the firewall
- Application aware firewalls and proxies must have the correct application layer traffic passed through them for a valid test

How do you test firewall egress rules?





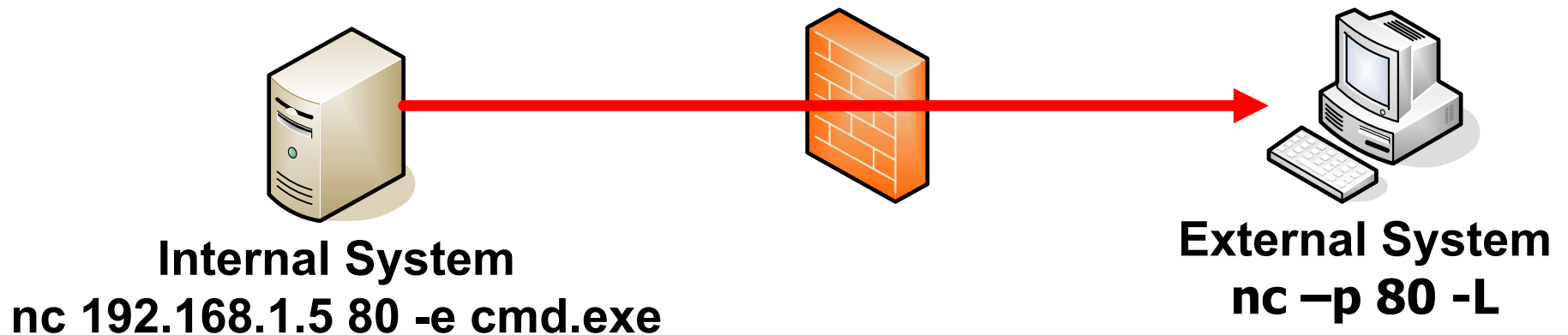
Is there a positive use for reverse shells?

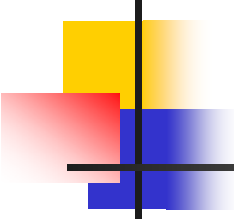
- Reverse shells can be used to test firewall filter rules
- Reverse shells can be used to test if application firewalls and proxies are really application aware
- Reverse shells can be used to test IDS rules
- Reverse shells can be used to work from home and not bother getting official access to the company network 😊

Netcat Example

- Netcat can push a shell to another system:
 - Using any TCP/UDP port
 - Through any non-application aware firewall or proxy
 - Running on most operating systems

Packet Filtering Firewall



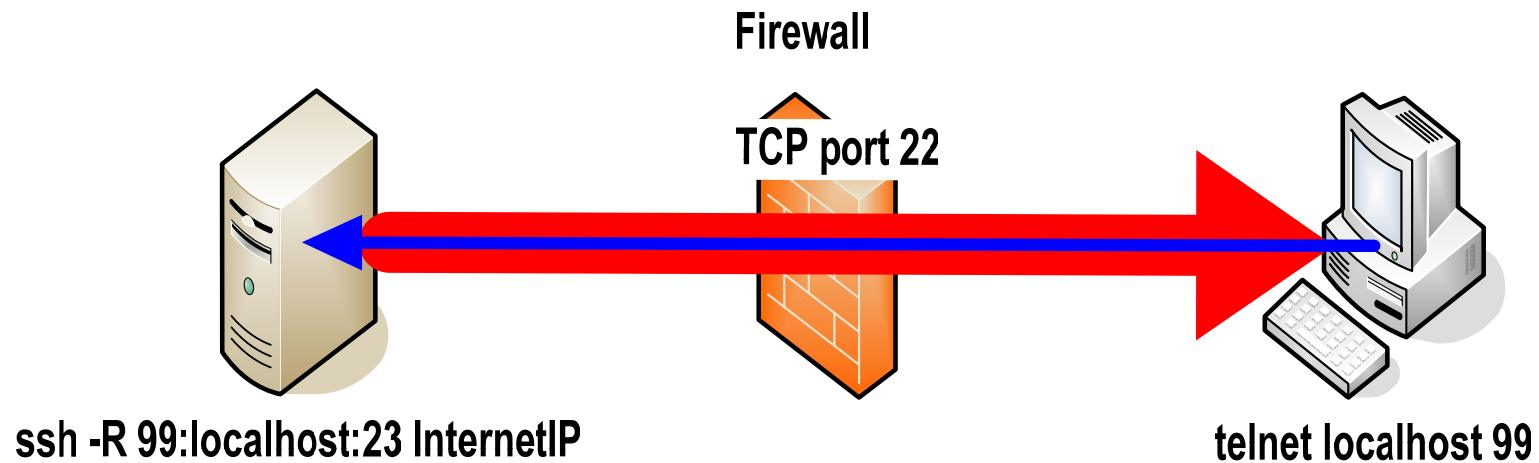


How do you detect reverse shells on your network?

- Detecting working reverse shells is difficult
- Scrutinize drop logs on firewall and proxies
- Tune IDS to alert on traffic that is not expected
 - E-mail server that starts surfing the web
 - DNS server that telnets out of the network
- Host based firewall logs
- Check server baselines against known good configurations

SSH - Friend or Foe?

- SSH can tunnel any TCP traffic
- -R reverse port forwarding
- Hides traffic inside an encrypted tunnel
- Network traffic at perimeter looks like SSH





How do you protect your network against reverse shells?

- Restrict physical access to your network
- Only allow outgoing services that are required for your business
- Install application aware host or client based firewalls
- Train users to:
 - NOT execute e-mail attachments they are NOT expecting
 - NOT download and install unauthorized programs



How do you protect your network against reverse shells? (Cont)

- Install application aware firewalls and proxies
- Authenticating outgoing web proxies
- Tune IDS rules for the specific network segment it is installed on
- Split DNS
- Separate incoming and outgoing e-mail servers
- Dedicated servers



Conclusion

- Reverse shell programs pose a real threat to your network
- Application aware firewalls help protect against reverse shell exploits
- Egress filters help protect against reverse shells
- Detecting reverse shells is difficult
- Protecting your network from reverse shell exploits requires an understanding of how they work and the protocols they use
- Your network perimeter is secured from the outside-in, now start looking from the inside-out