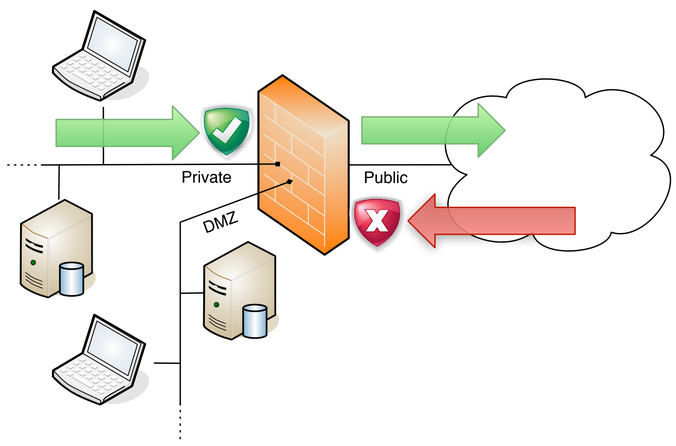
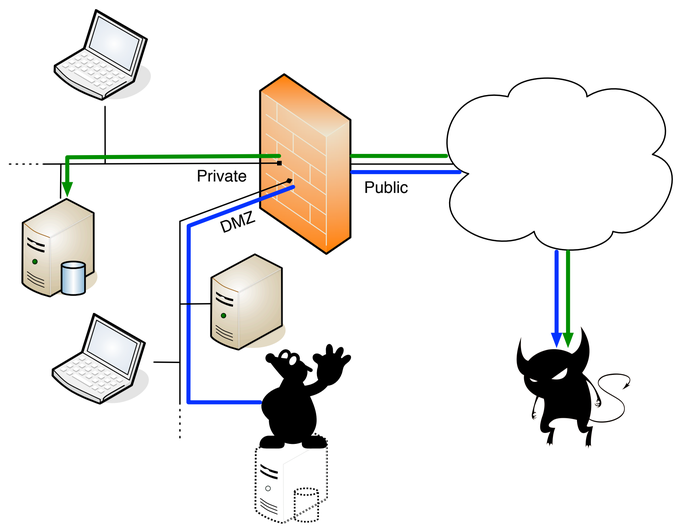
CERIAS

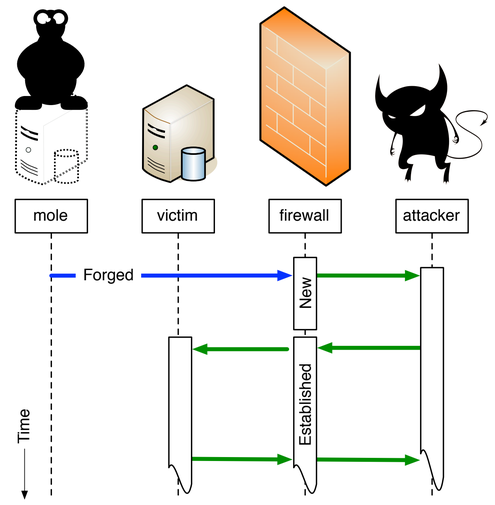
the center for education and research in information assurance and security

DEFEATING STATEFUL FIREWALLS

Dannie M. Stanley <ds@cs.purdue.edu>







Premise

Firewalls often allow traffic out of the network and deny traffic into the network. Firewalls use stateful packet inspection (SPI) and connection tracking to determine the origin of the connection and allow related traffic back into the network.

Vulnerability

If a mole could forge a datagram that would be recognized by the firewall, then he could punch a hole in the firewall for an outside attacker. To do this he impersonates the victim host. The mole doesn't necessarily have to be on the private network. Depending on firewall configuration, the mole could be positioned on the public network.

Attack

Once a hole is punched in the firewall, then the attacker can establish a connection to the victim host. Once the connection is established, the attacker can interact with network services on the protected victim host. The attack works against both UDP and TCP. The basic UDP datagram sequence is illustrated above.

Results

UDP

All tested firewalls (Cisco, Linux, BSD, Linksys) were vulnerable to a UDP attack. From an outside position we were able to perform the following on a protected host:

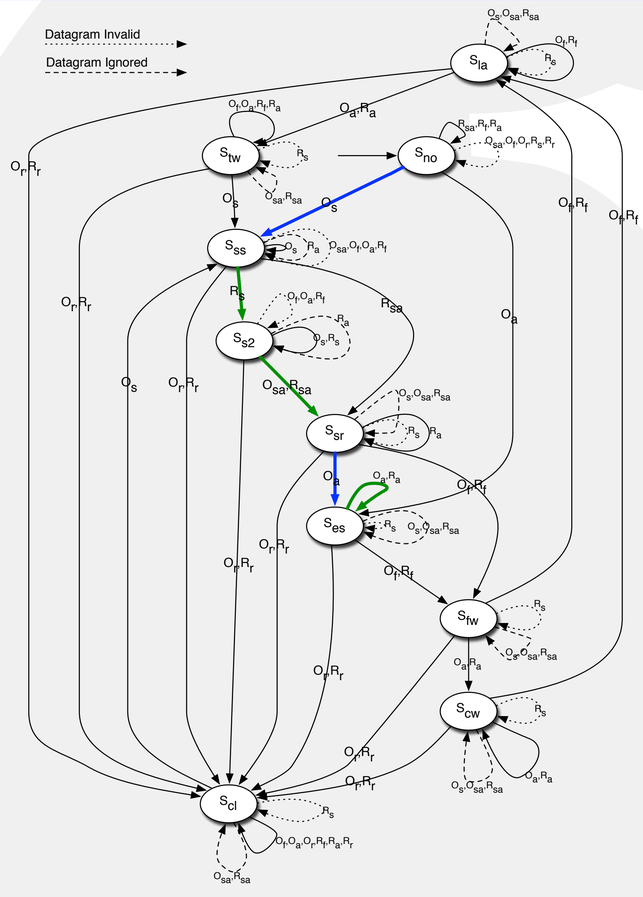
- Read SNMP data
- Mount an NFS file share

TCP

A TCP attack was developed for the Linux firewall (Netfilter). TCP is stateful and can more accurately be tracked by the firewall. From an outside position we were able to perform the following on a protected host:

- Complete a TCP 3-way handshake
- Complete HTTP request

TCP Attack

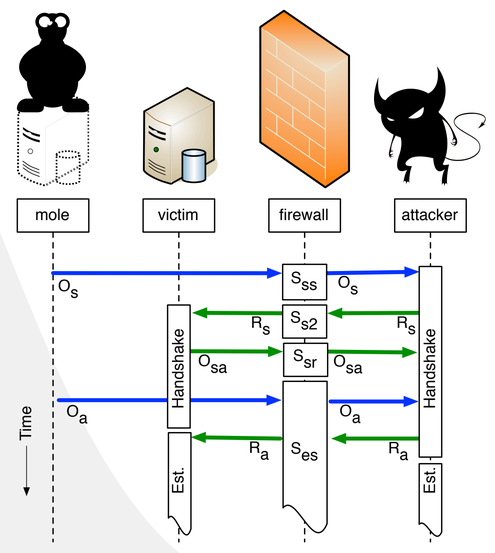


Connection States

S_{no}: None
S_{ss}: SYN Sent
S_{s2}: SYN Sent 2
S_{sr}: SYN Received
S_{es}: Established

Datagrams

O_s: SYN
R_s: SYN
O_{sa}: SYN+ACK
O_a: ACK
R_a: ACK



PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center