DNS, SMTP, and XDMCP

Tom Kelliher, CS 325

Nov. 20, 2006

1 Administrivia

Announcements

Projects due now.

Assignment

Read 7.3.

From Last Time

Introduction to networks.

Outline

1. DNS.
2. SMTP.
3. XDMCP.

Coming Up

Controls.

2 DNS

1. Domain names and IP addresses.

2. Host files, the early days.

3. The need for delegating authority within the namespace.

4. Two components: the nameserver and the resolver.

5. A sample DNS query.

6. Host files, today.

   Exploits.

7. Caching name servers.

8. Poisoning the cache:

   (a) By redirecting the target domain's (goucher.edu) nameserver. Force the target to make a request from hacker.com domain. Request:

   ```
   ;; QUESTION SECTION:
   evil.hacker.com IN A
   ```

   Response from hacker.com's nameserver:

   ```
   ;; ANSWER SECTION:
   evil.hacker.com.   2331    IN      A       10.67.1.26

   ;; AUTHORITY SECTION:
   hacker.com. 3600 IN NS boone.goucher.edu

   ;; ADDITIONAL SECTION:
   boone.goucher.edu. IN A w.x.y.z
   ```

An "unknowing" nameserver would cache and serve the poisoned entry in the additional section. `w.x.y.z` is an IP address of the attacker's choice. It will point to a nameserver with entries hand-crafted by the attacker.

What is the name for this type of an exploit?

(b) By redirecting the NS record of the target domain. Request:

```
;; QUESTION SECTION:
evil.hacker.com IN A
```

Response from hacker.com's nameserver:

```
;; ANSWER SECTION:
evil.hacker.com.   2331    IN      A       10.67.1.26

;; AUTHORITY SECTION:
goucher.edu. 3600 IN NS ns.whatever.com

;; ADDITIONAL SECTION:
ns.whatever.com. IN A w.x.y.z
```

This time, an "unknowing" nameserver would cache and serve the poisoned records in both the authority and additional sections. Such an attack could be used to trick goucher.edu nameservers into directing NS requests for, say, microsoft.com, to the attackers nameserver.

(c) By responding before the real nameserver.

This involves peppering the target nameserver with numerous requests, guessing the nonce and the (randomized) source port and replying back with a query response before the real nameserver can respond. This might involve hitting the real nameserver with a DOS attack.

The success of this also depends upon a lack of authenticity checking by the target nameserver.

3 SMTP

1. The SMTP protocol. Note that the mail client is connecting to the local SMTP server (127.0.0.1). The server will relay the message to its destination. (Open relays are one problem.)

```
220 bluebird.goucher.edu ESMTP Sendmail 8.12.11.20060308/8.12.11; Mon, 20
Nov 2006 08:56:52 -0500
>>> EHLO bluebird.goucher.edu
250-bluebird.goucher.edu Hello localhost.localdomain [127.0.0.1], pleased
to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI
250-DELIVERBY
250 HELP
>>> MAIL From:<kelliher@bluebird.goucher.edu> SIZE=64
AUTH=kelliher@bluebird.goucher.edu
250 2.1.0 <kelliher@bluebird.goucher.edu>... Sender ok
>>> RCPT To:<kelliher@phoenix.goucher.edu>
>>> DATA
250 2.1.5 <kelliher@phoenix.goucher.edu>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 kAKDuqvS032182 Message accepted for delivery
kelliher@phoenix.goucher.edu... Sent (kAKDuqvS032182 Message accepted for
delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 bluebird.goucher.edu closing connection
```

2. MX records.

3. Spoofing techniques used by hackers.

   Manipulation of the `MAIL From:` header allows a sender to masquerade as anyone else.

4. Sender Policy Framework:

   (a) Uses an existing DNS record type, `TXT`, to specify allowed senders from a domain.

   IETF has also assigned a new resource record type for SPF data.

   Example:

   ```
   amazon.com. 6752 IN TXT  "spf2.0/pra ip4:207.171.160.0/19
   ```

```
ip4:87.238.80.0/21 ip4:72.21.196.0/24 ip4:72.21.208.0/24 ?all"
amazon.com. 6752 IN TXT "v=spf1 ip4:207.171.160.32/28
ip4:207.171.180.176/28 ip4:207.171.164.32/28 ip4:207.171.190.0/28
ip4:87.238.80.24/29 ip4:87.238.84.24/29 ip4:72.21.196.0/24
ip4:72.21.208.0/24 ?all"
```

(b) Only prevents forgeries of `Return-Path`, not `From` or `Sender`.

(c) Intentionally will not work with forwarders that don't rewrite `Return-Path`

5. Slowing down "spam cannons" via Greylisting.

4 XDMCP

1. X and XDM are notoriously exploitable. They should always be hidden behind a firewall.

2. GDM and authenticating the host system using PTR and A DNS queries.

3. The result of incorrect, or stale, PTR entries in a nameserver in a DHCP environment.

4. TCP Wrappers.