Do you...

- have an User Account on any Computer?
- visit unknown web-links from any search engine?
- host a Web Service?
- use a Proxy?
- log-in to your Web based accounts?
- use any Web Service?
- access any private data?

You are InSecure if you don't...

- apply security policies over your User Account.
- use patched Web Browsers.
- use Intrusion Detection System.
- use trusted SSL Proxy.
- log-in to your Web Accounts over encrypted connection.
- use Firewall.
- delete and format your storage media.

YOU ARE INSECURE

EVEN IF YOU DO

ALL THIS.

Security is just maintained, it's never achieved.

INSECURITY IN SECURITY

By : (m0727) Abhishek Kumar

Guide : Mr. Ramdas N. Karmali

O.S. User Account Log-In

- O.S. strongly encrypts the user password to hash.

- These hashes are stored in files with highly restricted user rights.

O.S. User Account Log-In
(ACTIVE MODE) :: HACKS ::

Hackers have tools:

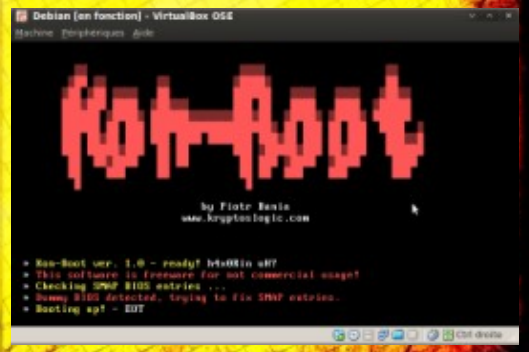
- Live Boot Discs to steal Password-Hash files (otherwise inaccessible).
- Tool “John-The-Ripper” can try cracking passwords by matching hash of guessed passwords.
- Tool “Rainbow Crack” and “OPHCrack” have precomputed hash tables of several passwords to match the hash in the stolen password file.

O.S. User Account Log-In
(PASSIVE MODE) :: BYPASS ::

Cracking password consumes a lot of time against strong passwords.

Hackers have tools:

- Grub/Lilo (Unix/Linux)
- Kon-Boot (Windows, Unix/Linux)
- Keyboard (Macintosh only)



Visiting Unknown Websites

:: SMBENUM ::

Reconnaissance via simple HTML Web Page

- IE supports "***file://***" and "***res://***" protocol for accessing local machine resources' URI.
- Firefox has also started support for a similar "resource://" protocol.
- Javascript can use these protocols to enumerate resources.
- Could gather User Names using Brute Force.
- e.g. if "***file:///c:/oracle/ora81/bin/orclcontainer.bmp***" loads, means "Oracle 8" is present on system.

Visiting Unknown Websites

:: RES-TIMING ATTACK ::

The 'res(ource)://' protocol hack using CPU Cycles.

- An attacker can even get resources to execute on your machine.
- Could measure CPU Cycles for resource enumeration, the CPU cycle count for existing resources is almost twice the CPU cycle count for non-existing resources.
- Could even exhaust Victim's machine by generating infinite CPU cycles.

Hosting Vulnerable Web Server

:: SLOWLORIS ::

The slow HTTP Denial-of-Service Attack..

- It's a stealth-mode attack.
- Allows single machine to attack Web-Server with minimal bandwidth.
- Uses Partial HTTP Connections to keep Web Server sockets busy, and slowly consumes all the sockets.
- It works ***successfully over Apache 1.x, Apache 2.x, dhttpd, GoAhead, WebSense,*** etc. but ***fails against IIS 6.0, IIS 7.0, lighttpd, squid, nginx***, etc.

:: SIDEJACKING ::

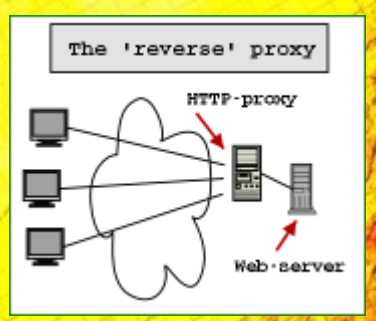
Intercept and Hijack an engaged web session.

- Websites protect against sniffing of passwords by encrypting the log-in mechanism, and create a session for further authenticated access.
- But after log-in, if this Session Information is transferred in plain-text, it can be sniffed.
- Attackers sniff this session information and use them to replicate the required cookies or session state managing file.
- Now, an user can access the same Account without knowing the password.

:: DEANONYMIZE PROXY ::

Trojan infected proxy tools are the problem.

- Onion Proxy is one of the best Anonymizer.
- TOR works on it, using a chain of random proxy servers between the entry node and the exit node.
- According to Research, several TOR exit clients are Trojan-infected, sniffing all the sensitive data passed.
- e.g. doing a Reverse DNS Lookup on POP3 packets and harvesting usernames and passwords.



Protector Of Protocols

:: SSL (SECURE SOCKET LAYER) ::

Faulty Design and Poor Implementation.

- Earlier it allowed any Digital Certificate Owner to sign any Digital Certificate (e.g. haxor.com can sign certificate for paypal.com and use itself)
- It was patched by specifying signing authority field in Digital Certificate
- If attacker send a forged certificate with expired validity date, several applications ask for date confirmation and perform no more checks for certificate validation.

Defeating SSL

:: SSL STRIPPING ATTACK ::

Poor Implementation is an easy hack.

- Default behaviour of maximum Websites is non-SSL. SSL is implemented by Redirecting to a SSL Link or let user click the SSL Service link.
- e.g. opening ***Facebook.com***, opens ***http://www.Facebook.com,*** here log-in button has https:// link for SSL based Log-in.
- Attacker can modify webpage replacing ***https://login*** link to ***http://login*** link
- Now log-in credentials transfer in plain-text mode, thus they can be sniffed.

Defeating SSL

::SSL DIGITAL CERTIFICATE MOD ATTACK::

Faulty Design is hard to find, best to exploit.

- Authority grants a digital certificate to an organisation ***Y.org*** for all sub-domains it asks say ***X.Y.org***, irrespective of value of ***X***.

- If X is "***www.PayPal.com\0***", then too it issues the certificate to ***Y.org*** for ***www.PayPal.com\0Y.org***.

Defeating SSL

::SSL DIGITAL CERTIFICATE MOD ATTACK::

Null Character Insertion (except WebKit, Opera)

www.PayPal.com\0Y.org get stored in a String and read back only as ***www.PayPal.com\0 .***

Null Character Escape (for WebKit, Opera)

www.Pay\0Pal.com\0 get stored in a String and read back only as ***www.PayPal.com\0 .***

Wildcard ('*', '|') Match

Matching several website certificates at once.

Defeating SSL's Security

Certificate Revocation

Uses **OCSP** (Online CertificateRevocation Policy) with two fields ***ResponseStatus*** and ***ResonseBytes (with signature)***.
Setting "**ResponseStatus=3**" for "**Try Later**" has no ResponseBytes, so no signature and hence the victim does not see any effect of the attack.

Software Updates

Software Updates also work over SSL channel, which is already compromised.

:: DNS ::

The base of all Network Services is Vulnerable.

- Man-in-the-Middle attack are a major threat to DNS.
- DNS Cache Poisoning is possible even if machines are behind a Firewall.
  When DNS queries about IP of any Domain, attacker spoofs as one of domain's NameServer and answers a specially crafted response making the Victim record the attacker's IP for requested Domain.

Security over DNS
:: DNSSEC ::

Does not fulfill the basic requirement of Security.

- It provides Origin Authentication, Integrity Protection, PKI, and even authenticated denial of existence of data.
- But no Confidentiality, and confidentiality is one of the fundamental requirement of Security.
- DNS NameServer Enumeration is much deeper because of 'DNS Query Espionage'.
- CPU Flooding is possible as it uses exhaustive encryption/decryption.

Forensic eXpert Hackers

:: DATA STEALING ::

You loaded it in Main Memory, Hackers stole it.

- Data Carving.
- Cold Boot Attack.
- Imaging RAM.
- Dig Information from O.S.
- Dig information from Files.
- Timestomp.

:: COUNTERMEASURES :: #1

O.S. User Account Log-in Hack/Bypass

- Restrict any kind of physical access to your machine, nothing else can counter it.

RES-Timing and SMBEnum Attack

- Turning off Javascript is a partial solution, victim is vulnerable till correct patches are provided by Microsoft and Mozilla.

Slowloris Attack

- Applying patches to Web Servers & IDSes, but no optimal patch is available.

:: COUNTERMEASURES :: #2

SideJacking

- Use private secure VPN.
- Don't log-in at any Public Hotspot.

DeAnonymize Proxy

- Use your own encryption channel for data exchange over proxy.

Defeating SSL

- Use secure proxy channel.
- Check URL in Certificate with one in Address Bar, do a WHOIS on both & match them.

:: COUNTERMEASURES :: #3

DNSSEC Vulnerabilities

- Use static address mapping for important domains.
- Use DNSCurve instead of DNSSEC.

Forensic eXpert Hackers

- Encrypt your content or even entire disc.
- Apply 'Secure Recursive Delete' on sensitive data.
- Use ZipBomb to trouble the Hacker.

Conclusion

Security is just maintained, it's never achieved.

So keep track of latest vulnerabilities and start/stop using resources based on them.

Refer sites like ***SecurityFocus.com***, ***CERT.org/vuls***, ***updates.ZDNet.com/tags/security. html***, etc.

Most of the Insecurity In Security comes from badly written piece of code and we have only careless developers to thank for them.

Reference

I referred to the work of :

Thorkill (piotrbania, KryptosLogic)

Billy Rios (Security Engg., Verisign)

Robert Hansen (SecTheory)

Joshua 'Jabber' Abraham (Rapid7)

Robert Graham (Errata Security)

Moxy Marlinspike (ThoughtCrime)

Dan Kaminsky (Director, IOActive)

Adrian Crenshaw (InfoSec Enthu)

Presentaions from:

- BlackHat 2009
- DefCon 17
- DefCon 16

MY CRIME IS THAT OF CUROSITY

My Crime is of Judging people by what they say and think,
And not by what they look like.