Logical jump from external to internal

LOGICAL CHAOS

Outline

I. **Introduction**
   I. Who am I?
   II. What to expect from this talk?
   III. Trends
   IV. Motivation
II. Logical Chaos
III. Conclusions
IV. Questions

Who Am I?

- David Llorens - @c4an
- .mx
- No certifications
- 10 years of experience in sec (like if this mattered nowadays)
- Pentester, consultant, auditor, etc

Note: All the material presented here describes my personal opinion and by no means represents the opinion of my employer or any co-worker.

What to expect from this talk?

- A chaotic way of trying to gain access to some corporate networks from the Internet
- Simple way to extract data out of systems without using known vulnerabilities but through logical flaws
- Most of the content in this presentation is explained from the attacker’s perspective

Trends

- Centralization of authentication: Same user access, Single Sign On (SSO), Access Manager (AM) and Identify Management (IDM)
- Remote connectivity / Mobility – “Work” from home or third party access
- Third party services and outsourcing of IT operations
- Automation of IT support processes
  - Self password reset after lockout
- Centralized Log Correlation tools are rarely well implemented

Motivation

- What do we want in an external pentest?
  - Domain Admin or root?
  - Access to sensitive data handled by web applications or other services
  - At the very least persistent low privilege access to the internal network from the Internet
- What is important to your client?
  - Sensitive Information
  - Did you get in?

Motivation

- Avoiding giving a false sense of security
- Don’t like to be the one that says to clients:
  - “I couldn’t get in“
  - “There are no high risk vulns from the outside”
- Dependence on automated tools is ridiculous
  - Scanner didn’t report anything so there are no critical vulnerabilities << *REAALLY?!*
  - Tools have their own limitations. Great tools out there but it is impossible to cover every single scenario or test every vulnerability with a tool.
- I would like to hold accountable companies that sell software for their security flaws

Motivation

Before starting (tools)

- Everybody uses
  - fierce.pl
  - dnsenum
  - Shodan
  - Maltego
  - metagoofil
- Great tools not that commonly used
  - The harvester
  - FOCA
  - Discovery framework
  - Every Routable IP project (DB)

Outline

I. Introduction

II. **Logical Chaos**

   I. Enumeration

   II. Bruteforce

III. Conclusions

IV. Questions

Logical Chaos

Tool designed to identify a large number of user accounts (Active Directory) and gain access to the internal network from the Internet. Applicable to web applications as well.

Two different stages of the attack:

- User enumeration (when possible)
- User bruteforce

Developed in ruby using selenium-webdriver
Supports socks proxy

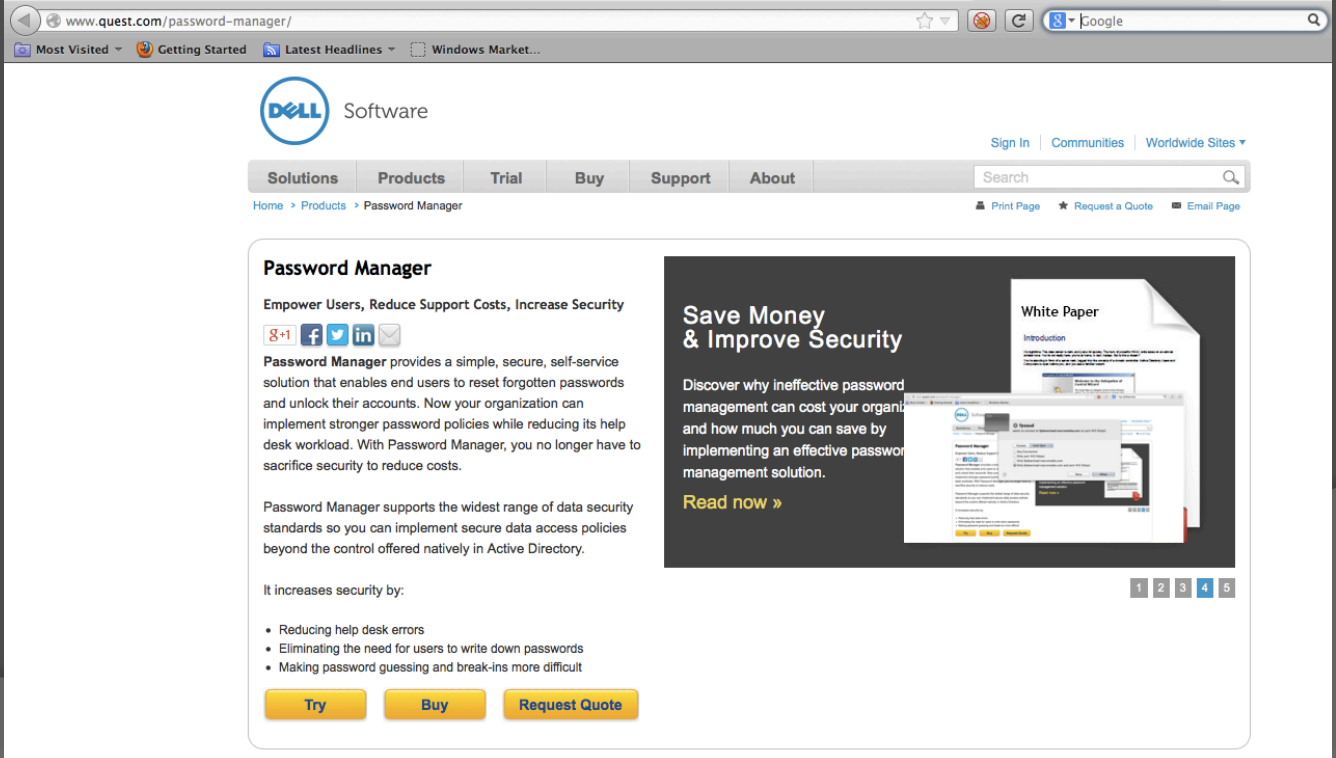
Logical Chaos

User Enumeration

- WebSphere Web portal
- SAP (still in process)
- ***Quest Password Manager (QPM)***
- ***Automated***

Quest Password Manager (QPM)

- Here is where it all started!
- So far identified a several large important companies using it



Password Manager

Empower Users, Reduce Support Costs, Increase Security

Password Manager provides a simple, secure, self-service solution that enables end users to reset forgotten passwords and unlock their accounts. Now your organization can implement stronger password policies while reducing its help desk workload. With Password Manager, you no longer have to sacrifice security to reduce costs.

Password Manager supports the widest range of data security standards so you can implement secure data access policies beyond the control offered natively in Active Directory.

It increases security by:

- Reducing help desk errors
- Eliminating the need for users to write down passwords
- Making password guessing and break-ins more difficult

Save Money & Improve Security

Discover why ineffective password management can cost your organi

and how much you can save by implementing an effective passwor

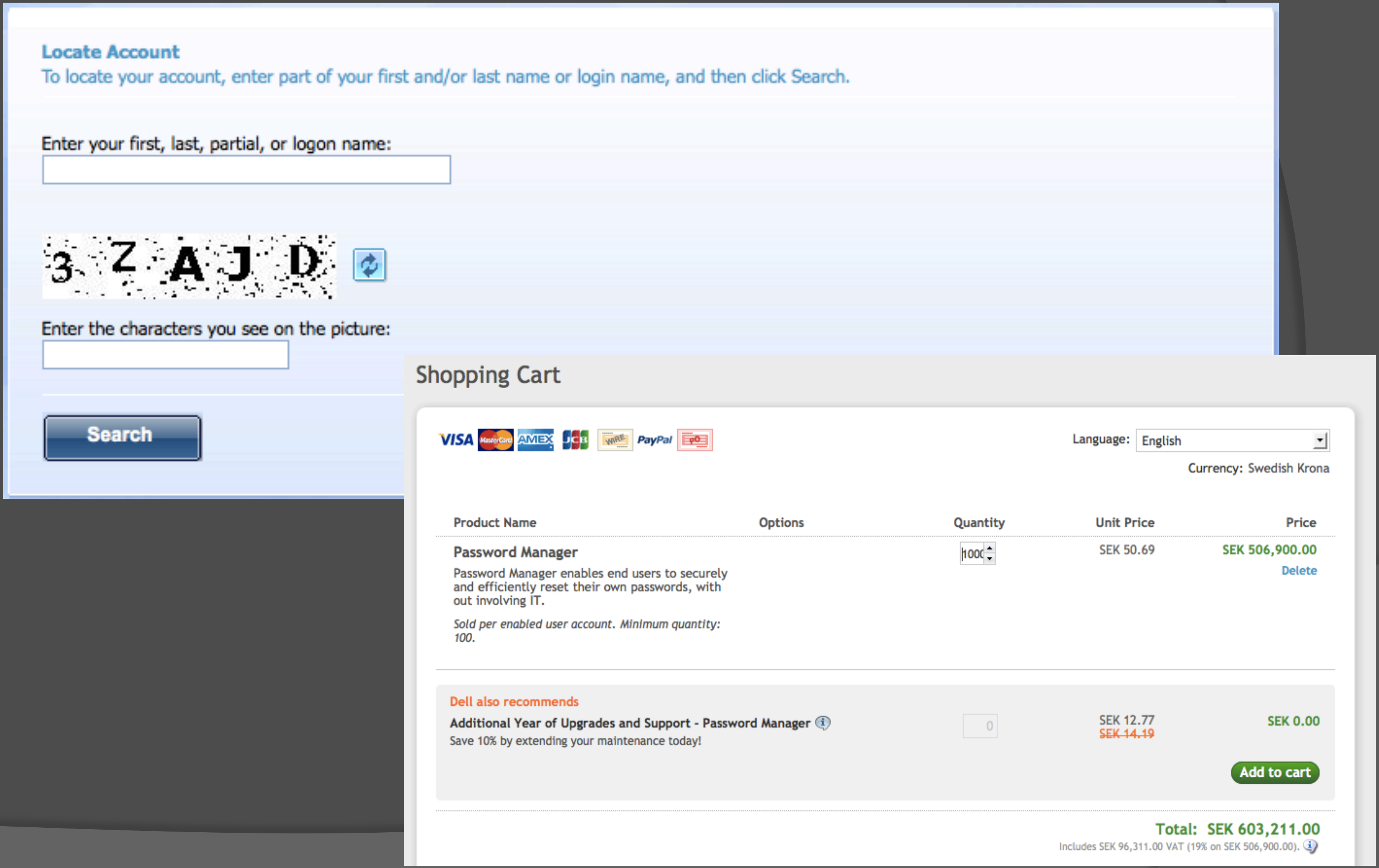
management solution.

Read now »

White Paper

Introduction

Quest Password Manager



Locate Account

To locate your account, enter part of your first and/or last name or login name, and then click Search.

Enter your first, last, partial, or logon name:

Enter the characters you see on the picture:

Shopping Cart

Language: English

Currency: Swedish Krona

Product Name	Options	Quantity	Unit Price	Price
Password Manager Password Manager enables end users to securely and efficiently reset their own passwords, with out involving IT. *Sold per enabled user account. Minimum quantity: 100.*		1000	SEK 50.69	SEK 506,900.00 Delete

Dell also recommends

Additional Year of Upgrades and Support - Password Manager Save 10% by extending your maintenance today!		0	SEK 12.77 ~~SEK 14.19~~	SEK 0.00

Total: SEK 603,211.00

Includes SEK 96,311.00 VAT (19% on SEK 506,900.00).

Quest Password Manager

- By default no Captchas
- Search functionality allows you to speed up the user enumeration process
- Always linked to Active Directory
- Worst case scenario you can manually try users until you get tired
- When Captchas are enabled are mishandled… Easy to bypass

Quest Password Manager

DEMO

Quest Password Manager

Automated

- Automatically detects a form with one field and tries a file of user accounts to identify valid users in the application

IBM WebSphere

- Default configuration allows you to register to the websphere portal
- Even though other parameters might be needed for the application the only 3 parameters are required: UserId, Password, and Lastname
- After log in the “hidden” pages can be accessed
- Lots of servers are linked to an LDAP server which is usually a specific subset of users in Active Directory

SAP Netweaver Portal

- Default authentication depending on client (client 100 ,101, etc)
  - TSMADM
  - SAP
- When a valid user is discovered enumeration of employees is possible (Last Name and First Name)
- Build users list based on employees names and user structure from a quick google search or using metadata of documents (FOCA)

When there is no enumeration

- Identify how a user account is constructed
  - john.smith , jsmith , jsmith1 , smithj, eNNNNN, etc
  - Look at the discovery tools slide. Metadata!! The harvester or FOCA are my recommendation
- Peoplesoft as HR system linked to AD
  - Almost all corporate users will start with an “e” or “u”. After that is their employee ID. Usually the employee ID is 5 to 7 digits. Example:
    - John Smith => *e27819*

    Really easy to come up with a list of all possible users
- Play with probability building your own user base using census data. Some US data in the “dictionaries” folder of the tool.
  - My source common last names and first names in census.gov and wikipedia ;)

Bruteforce

- Almost all companies allow 8 character long passwords as a minimum requirement and enforce password complexity
- Almost all companies have a Lockout Policy of 10 attempts for 30 minutes lockout duration
- Who has been in an internal pentest and not identified weak passwords?
- *Trustwave Global Security Report 2013*
  - Most passwords are around 8 characters and are LLLLLLNN
    - Wellcome1
    - Password1
    - *NameOfCompanyYEAR   << I will add this one*
    - *SummerYEAR   << I will add this one for places in the North*
- To brute force passwords remotely without locking out users we need:
  - One user and NO Lockout Policies << low probability
  - **Or …**

Reference: http://technet.microsoft.com/en-us/library/dd349793(v=ws.10).aspx

Bruteforce

Lots of users and weak lockout policies!

- Can go through a large number of users testing one password without locking out anyone
- Password lockout will reset after 30 minutes so you are free to try as many passwords you want
- Only restriction seems to be time ;)

Bruteforce

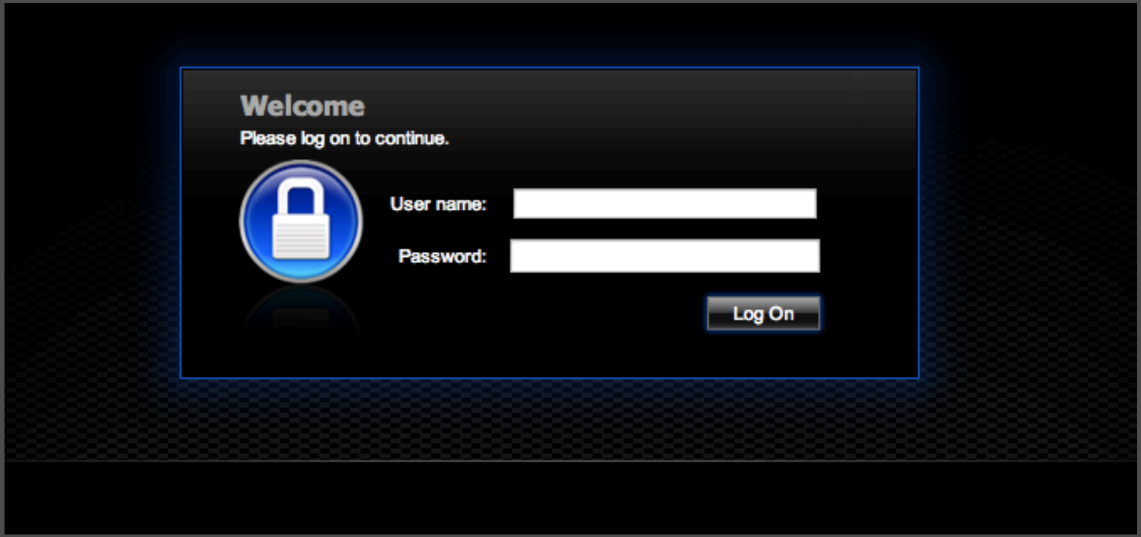
- My experience is that if you have around 1000 valid user accounts you are in. Time is the only restriction not lockout policies
- The crazy part of most tools used for web based remote access don´t have CAPTCHAS by default or don´t even support them
- Two factor authentication is not considered

Logical Chaos

User Bruteforce

- XenApp – A.K.A Citrix Metaframe
- Citrix vpn
- Outlook Web mail
- Web Forefront access
- Cisco Web VPN
- Juniper Web VPN
- PeopleSoft
- *RSA SecureID selfservice*
- Automated

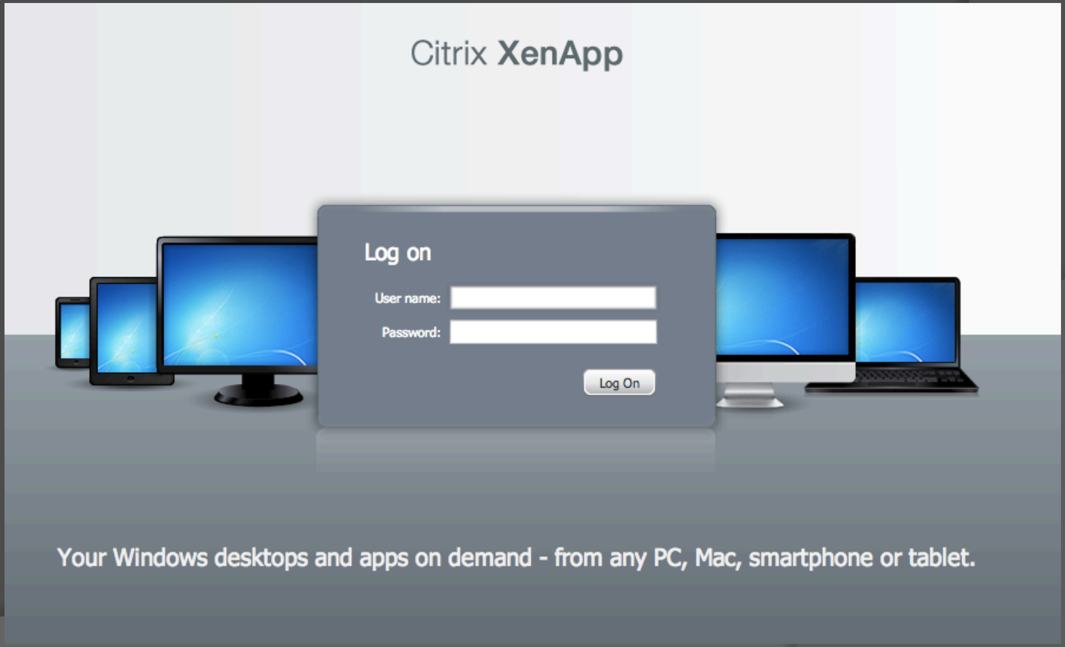
Citrix VPN



Welcome

Please log on to continue.

Citrix XenApp

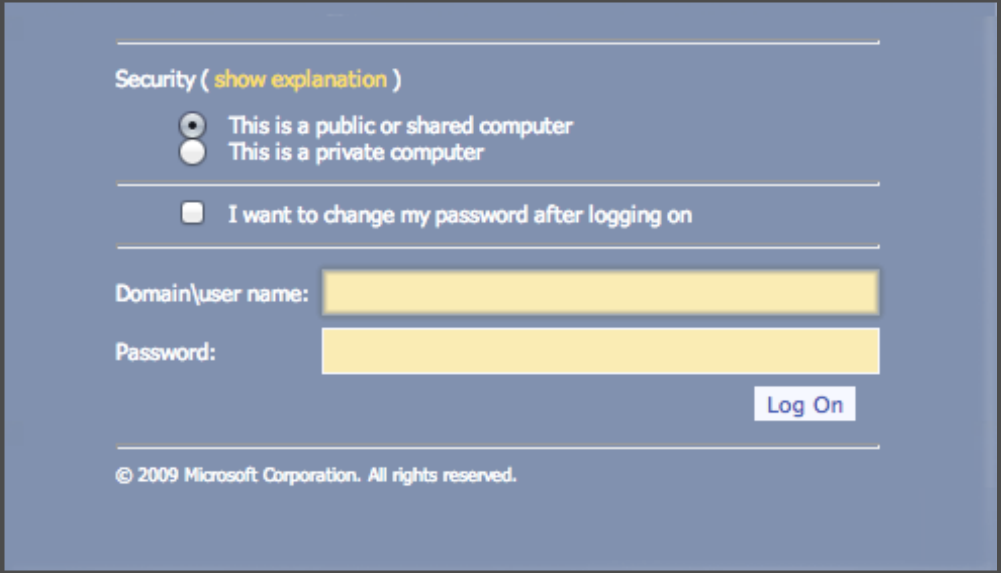


Citrix XenApp

Log on

Your Windows desktops and apps on demand - from any PC, Mac, smartphone or tablet.

Microsoft Forefront



Security (show explanation)

● This is a public or shared computer
○ This is a private computer

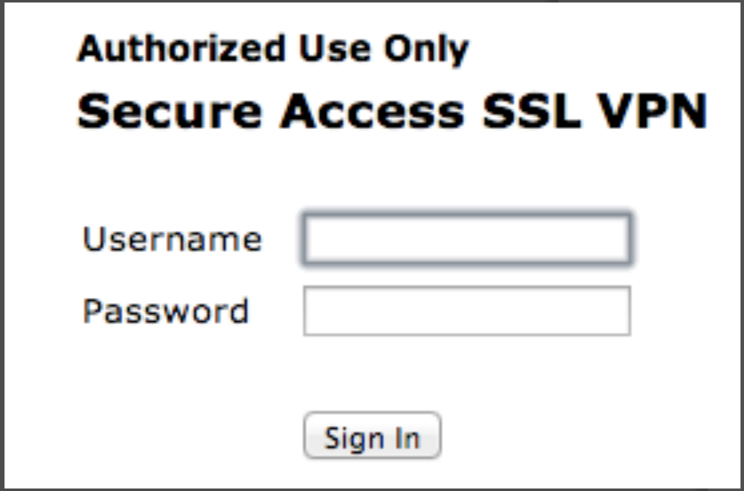
□ I want to change my password after logging on

Domain\user name:

Password:

Log On

Juniper VPN



Authorized Use Only

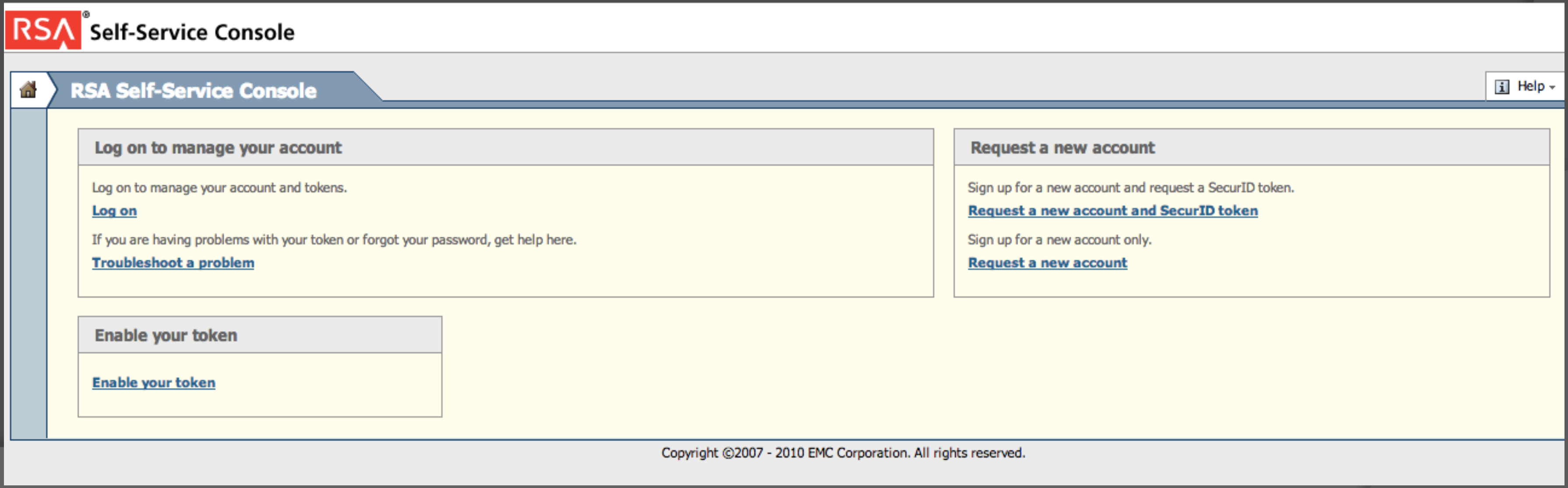
Secure Access SSL VPN

Username

Password

Sign In

RSA Self Service Console



Log on to manage your account

Log on to manage your account and tokens.

Log on

If you are having problems with your token or forgot your password, get help here.

Troubleshoot a problem

Request a new account

Sign up for a new account and request a SecurID token.

Request a new account and SecurID token

Sign up for a new account only.

Request a new account

Enable your token

Enable your token

FACEPALM

DEMOS

Outline

I. Introduction

II. Logical Chaos

III. **Conclusions**

    I. Pros of this attack

    II. Cons of this attack

    III. My thoughts

IV. Questions

Pros of this attack

- Usually IDS will be bypassed since you are acting as a regular user will do and using SSL
- Other monitoring tools like log correlation might not detect this as a ‘high’ risk problem. Sysadmins will usually not respond to this unless you block users
- Socks proxy can be used so even if you are blocked or identified you can change IP once you have a valid user
- Can leave it running at night or while you test for other attack vectors like SQLi, XSS, Session Hijack, code upload, etc
- If you get a large number of user accounts there is a **HIGH** probability you will succeed
- No one I know is actively testing this therefore lots of opportunities from outside and few are protecting against it

Cons of this attack

- Difficult to identify password policies from the outside
- Difficult to know if you locked someone
- If you don’t know what you are doing might create a huge DoS on your client
- Will work better against large companies. Small companies with few users in AD might not be a good target for this attack
- Specific conditions, like user enumeration, have to be present to exploit and have a high probability of success however you can always try without user enumeration
- Log correlation tools will scream ATTACK at people that are really monitoring. However, monitoring controls are usually relaxed at night. If they understand what happened the next day, it is just too late ;)

My thoughts

- Many other vectors on external pentests should always be tested. However, it is my opinion that part of a comprehensive testing approach should always try to check **SAFELY** for weak passwords. It is the basics, right?
- Passwords (a.k.a people) are still the weakest link in companies and we will be using them for a long time
- Leverage any technology, system and vulnerability that a target presents and try to put everything together on a greater scheme. Sometimes is really hard to get into one application but if you look at the bigger picture things might become clearer.

My thoughts

- 2 factor authentication should be a must for remote connectivity. Duh!
- Captchas?
- Why everyone needs remote access?
- How about creating profiles for remote users or restricting access only to certain systems?
- It is all pretty basic security stuff, right?

Thanks

- ET - @etlow – Efrain Torres

  For all the good ideas and input

- F4Lc0N LoWNOISE - @falcon_lownoise For being the first beta tester and identifying bugs

Q & A