Hack-Jutsu 101

by Demetris Papapetrou

Introduction

- What does Jutsu mean?
  - It is the Japanese word for Technique / Skill
- Hack Jutsu 101 means
  - Introduction to Hacking Techniques
- A Demonstration?
  - Risky Undertaking
  - Many things can go wrong
  - Easier for the audience to understand the impact of hacker attacks

Common Defense Claims

- We are very secure. We have a **firewall** deployed and therefore we are impenetrable !!! No one can get in!!!

- We have the best **antivirus** and/or **anti-spyware** software installed and hence malicious programs cannot run on our systems!!!

- **Who cares** about us?

What Ethical Hacking isn't

- It is not a full-proof solution.
  - It cannot detect all your vulnerabilities / weaknesses
  - It is as good as the Pentester/Hacker performing it
  - It is limited by many factors (e.g. scope, deadlines)
- It is not a Nessus scan!!!
- It is not a Metasploit autopwn attack!!!

What Ethical Hacking is

- It is about **gathering** and **analyzing** information, **understanding** how things work and **combining** everything together in very **creative** ways with the intend to **bypass** security controls.

- It is about thinking what others haven't thought about (e.g. a programmer, a web developer).

- It is about thinking **outside the box** on an every day basis!!!

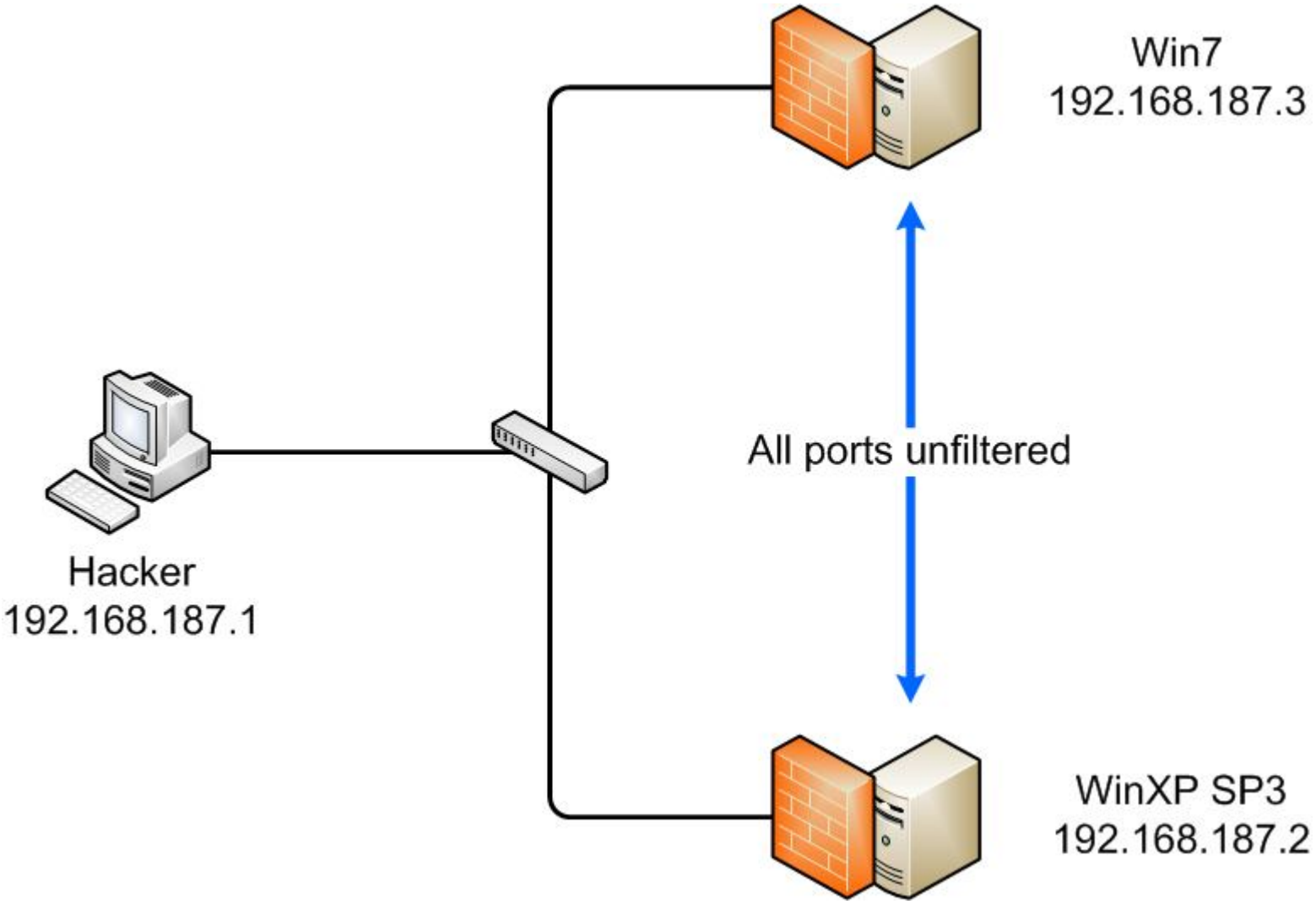
- And it provides a realistic view of an organization's security posture.

Network Penetration Testing

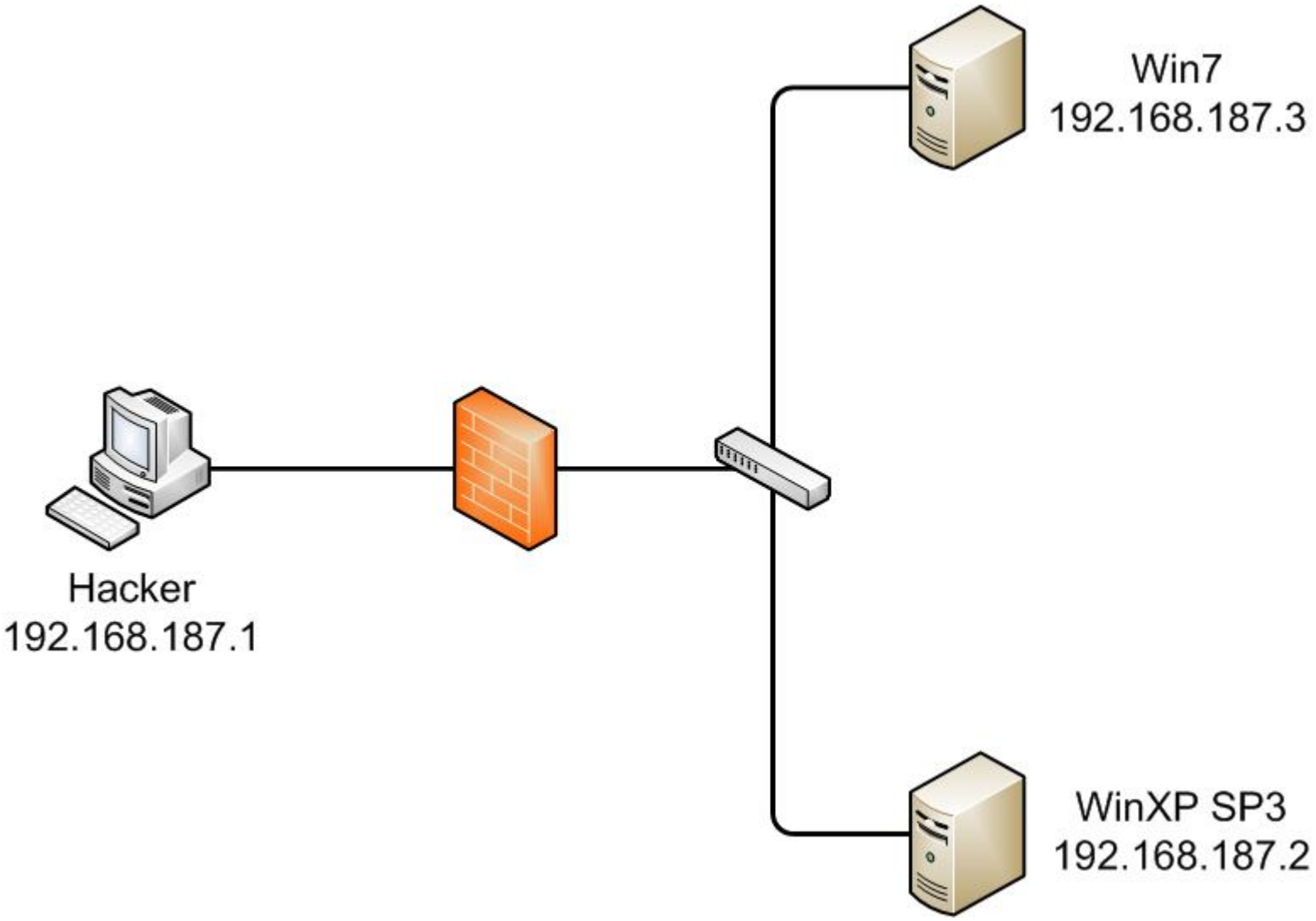
Network Pentesting Demo

- Systems involved.
  - MS Windows XP SP3, w/ Firewall, w/ Antivirus
  - MS Windows 7, w/ Firewall, w/o Antivirus
- Why not use Server versions of MS Windows?
  - Low budget
  - The security architecture is very similar between Server and Workstation versions (e.g. DEP, ASLR)

Network Pentesting Demo



Network Pentesting Demo



DEMO

Network Pentesting Demo

SecurityFocus™

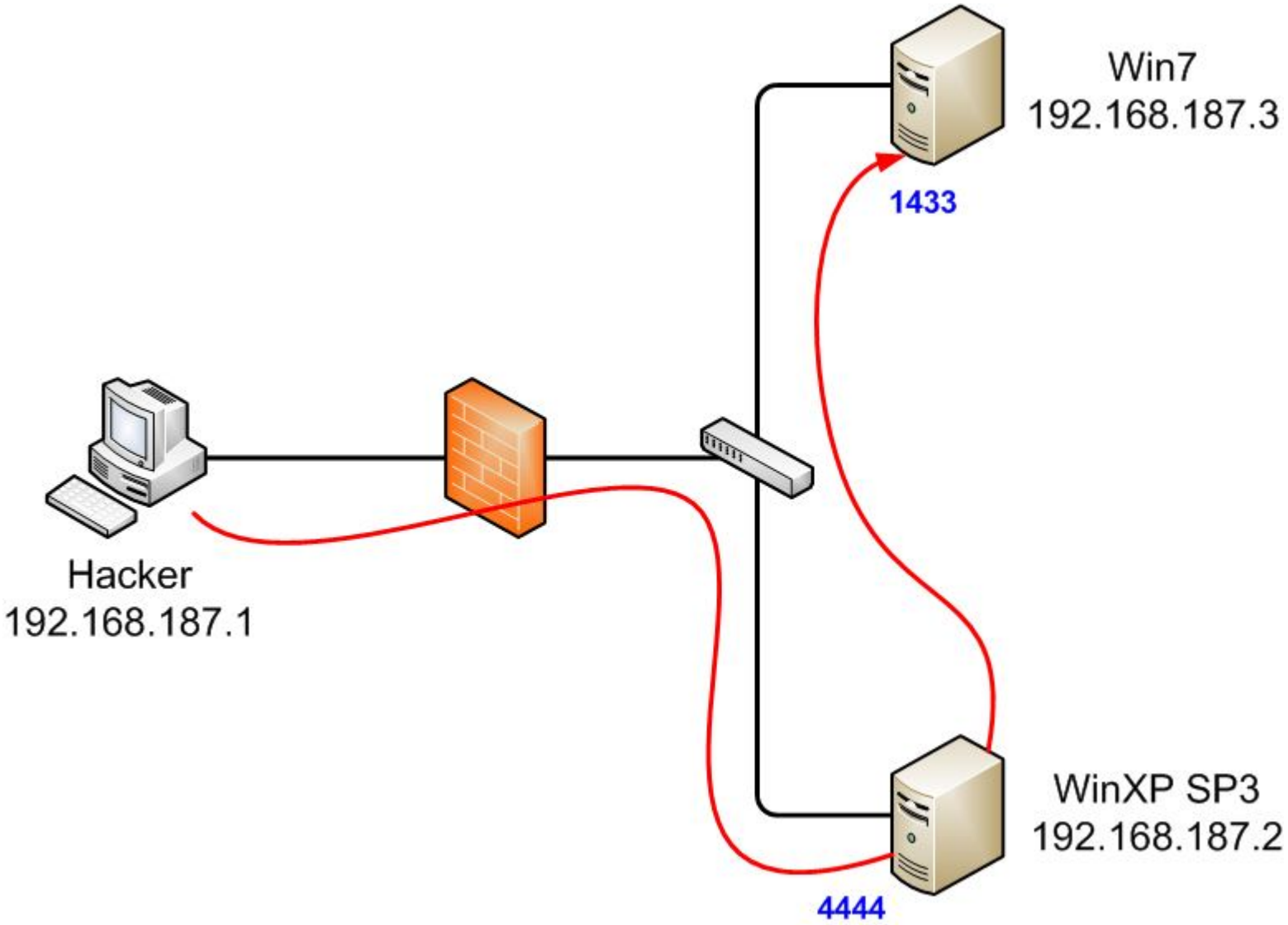
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation ▸

info | discussion | exploit | solution | references

Jarle Aase War FTPD USER/PASS Buffer Overflow Vulnerability

Bugtraq ID:	10078
Class:	Boundary Condition Error
CVE:	
Remote:	Yes
Local:	No
Published:	Mar 19 1998 12:00AM
Updated:	Mar 19 1998 12:00AM
Credit:	This vulnerability was discovered by ISS.
Vulnerable:	Jarle Aase War FTPD 1.65

Network Pentesting Demo



Network Pentesting Demo

RainbowCrack 1.5

File Edit Rainbow Table Help

Hash	Plaintext	Plaintext in Hex	Comment
e52cac67419a9a224a3b108f3fa6cb6d	password	70617373776f7264	Administrator
838f0388a3b8968155a2d7a878ac35f2	V3ryS3curePa55	563372795333637572655061353 5	ciso
0c1e9701632dd7f7eacbeb9271fb3e7a	FLOWERS???????	464c4f5745525 3?????????????	gardener
5646cd2988b0d4d5e069c2e2bc83daa5	???????S3NDMA4	????????????? 53334e444d4134	HelpAssistant
ccf9155e3e7db453aad3b435b51404ee	123	313233	test

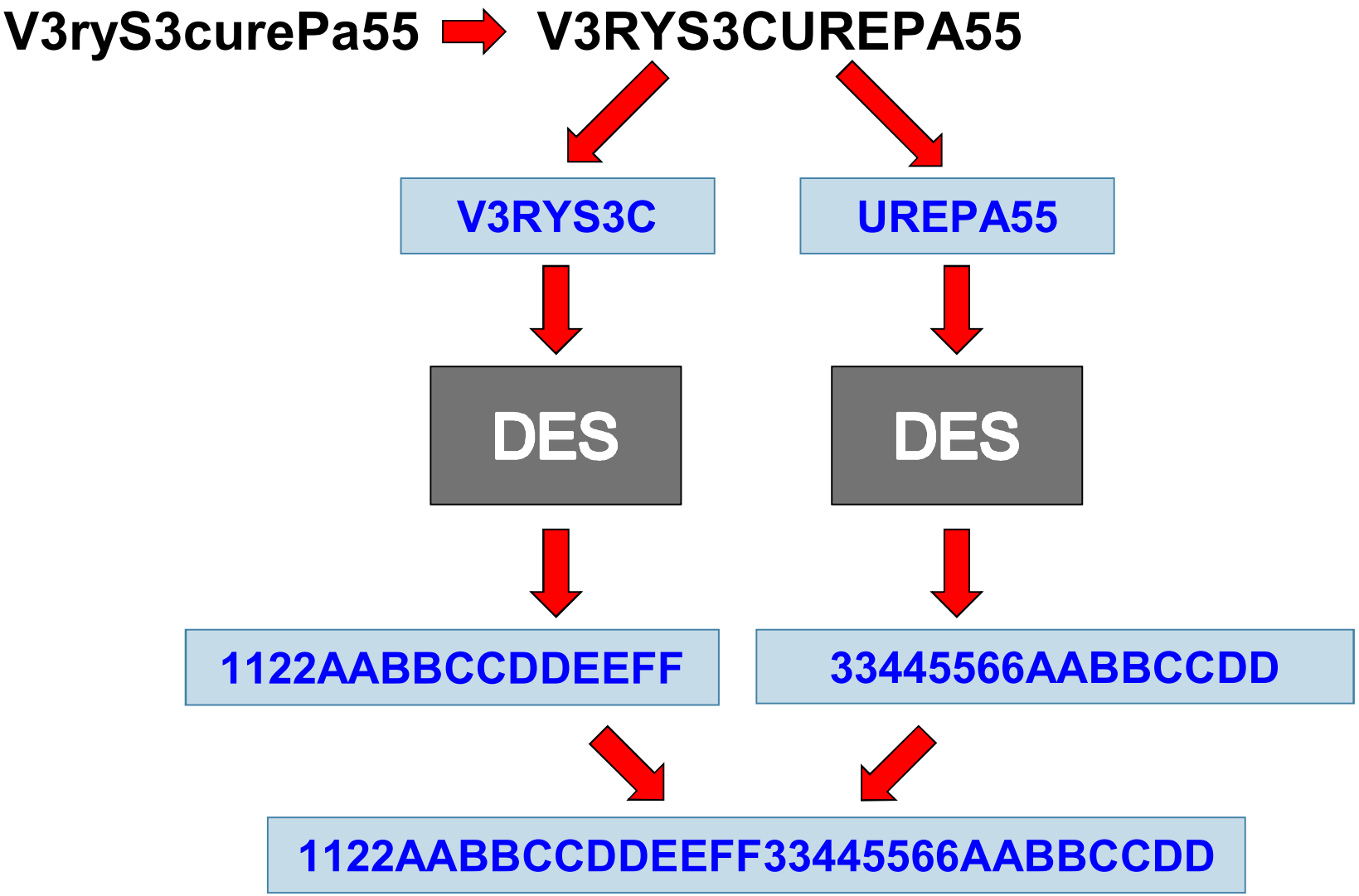
Messages

plaintext found: 7 of 9
total time: 127.50 s

Password Best Practices

- Passwords should be at least **eight (8) characters long**
- Passwords should meet **complexity requirements**.
- However… the victim's password was **fourteen (14) characters long**, met the MS Windows password **complexity requirements**…
- …But we manage to **crack** it in 2 minutes.
- WHY?… Because it was stored as **LM Hash**.

LM Hash Generation



Password Best Practices

- NTLM is **stronger** than LM.
- NTLM does not suffer from the same weakness as LM does (i.e. password splitting and hash concatenation).
- Hence **eight (8)** character long **complex** passwords are **secure** if **LM is disabled**. Right?
- **WRONG!!!**

Password Best Practices

- **Change** your password policy!!!
- Passwords must be at least **nine (9)** characters long…
- …**for now**!!!
- This applies to unsalted **MD5** hashes as well.

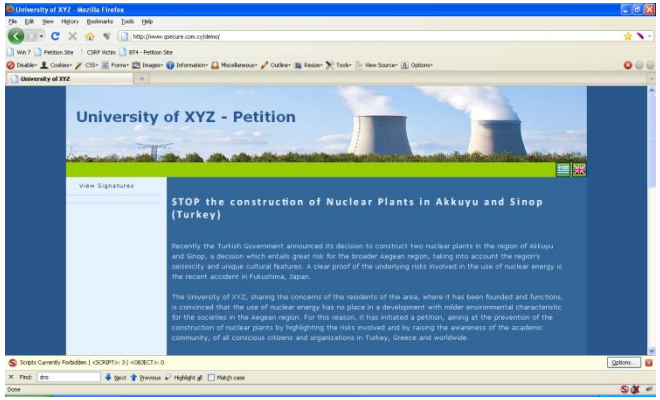
Cross-Site Request Forgery

Cross-Site Request Forgery

- An attacker **tricks** the victim into performing an **undesired function**, without his/her knowledge (e.g. change password, transfer money)

- Requirements:
  - The target Web App needs to be vulnerable to CSRF. The requested URL is always the same and does not change over time or per request.
  - The victim has authorized access to the URL (i.e. it is already authenticated).

Cross-Site Request Forgery



GET page

1

Here you go.
But you need this as well
www.ebank.com/transfer.php

2

Sent instruction to transfer money

3

e Banking

Cross-Site Request Forgery

- Attacks through HTTP GET Requests are usually easy to perform.
- Attacks through HTTP POST Requests are harder to perform but still possible.
  - Need some XSS and a bit of AJAX
  - Need to bypass browser Same Origin Policy (SOP)
- Attacks can utilize UPnP. No authentication required!!!
- Attacks against DSL routers may have devastating effects (e.g. change primary DNS, port forward, proxy).

DEMO

Client-Side Attacks

Client-Side Attacks

- They exploit applications installed on user workstation or the user himself/herself.
- They are the new type of remote attacks.
- They are massively exploited.
- They target the low hanging fruits. The users.
- They bypass firewalls and other infrastructure security systems.
- Attackers only need to succeed once.

Client-Side Attacks

- Why target the users?
  - They have unrestricted access to the corporate network
  - There is large number of security unaware users
  - User workstations are not monitored that well
  - There are a lot of unpatched 3rd party applications installed on user workstations
  - It is much easier than penetrating the firewall
- Victims can be contacted via email, Facebook, Google Ads, posters, etc.

DEMO

Conclusion

- Improving your organization's security posture is **not an easy task**. It goes beyond **security policies and procedures.**
- Your security posture is **as strong as** the **skills** of your **InfoSec Team** (incl. your consultants, etc).
- So choose them **wisely**!!!
- But the most important question **still remains…**

Conclusion

How can you tell who has got the necessary skills since you don't have those skills yourselves?

Do You Have Any Questions?

We would be happy to help.

The presentation was performed by
Demetris Papapetrou

Many thanks go to **QSecure** for their contribution!!!

Inaccuracies

- If a stateful firewall device was deployed, then Idle scanning could not be performed between the two victim hosts.
- If the XP machine was behind a NAT device, then TCP port 23 wouldn't be reachable from the Internet.
- The xp_cmdshell stored procedure is not enabled by default on MS SQL Server 2005. It needs to be enabled by a sys admin.