Hacking Corporations using Unconventional Chained Exploits

Gianni Gnesa <research@ptrace-security.com>

Presentation

Summary

1. Introduction
    - The State of Exploit Development
    - Unconventional Exploits
2. Trust Relationships
3. Case 0x01 – Inaccessible system
4. Case 0x02 – Who is who?
5. Penetration Testing in 2020
6. Conclusion

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Presentation

Summary

1. **Introduction**
    - The State of Exploit Development
    - Unconventional Exploits
2. Trust Relationships
3. Case 0x01 – Inaccessible system
4. Case 0x02 – Who is who?
5. Penetration Testing in 2020
6. Conclusion

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Introduction

The State of Exploit Development

- Nobody is running (or should run) a company's critical service on a Windows XP machine!

- **Modern operating systems**, such as Windows Server 2008, Windows Server 2012, Linux 3.x, **are widely deployed**.

- **An exploit for Windows XP will fail miserably against Windows 8**, because of the numerous improvements made to the latest version of Windows.

- Similarly, an exploit for Linux 2.4 will fail against Linux 3.12.

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Introduction

The State of Exploit Development (part 2)

- Software houses know that insecure software can be very costly in terms of money spent to fix bugs, distribute patches, re-establish trust, etc.

- **ExploitCost = CostOfVulnerabilityResearch + CostOfExploitDevelopment**

- A key defensive strategy adopted by several software houses is to **increase the cost of vulnerability research and of exploit development** by making it harder to analyze an application and by forcing researchers to deal with several security mitigations (e.g. ASLR, DEP, Sandboxes, etc.).

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

- **The cost of a reliable exploit will keep rising!**

Introduction

Unconventional exploits

- Is there any other way to get into a system or escalate privileges without using software vulnerabilities?

- Yes, there is. Unconventional exploits.

- Unconventional exploits is a term coined at Defcon

- **It refers to all those exploits that do not rely on software vulnerabilities or insecure passwords but on trust relationships, weak designs and misconfigurations.**

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Presentation

Summary

1. Introduction
    - The State of Exploit Development
    - Unconventional Exploits
2. **Trust Relationships**
3. Case 0x01 – Inaccessible system
4. Case 0x02 – Who is who?
5. Penetration Testing in 2020
6. Conclusion

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Trust Relationships

The Concept

- **Everything and everyone trust something**!

- Some examples:
  - A database trusts Web applications
  - A LAN trusts another LAN
  - Your company trusts its ISPs
  - Your browser trusts the DNS
  - You trust your coworkers
  - …

- All these trust relationships can be a **possible point of access**!

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Presentation

Summary

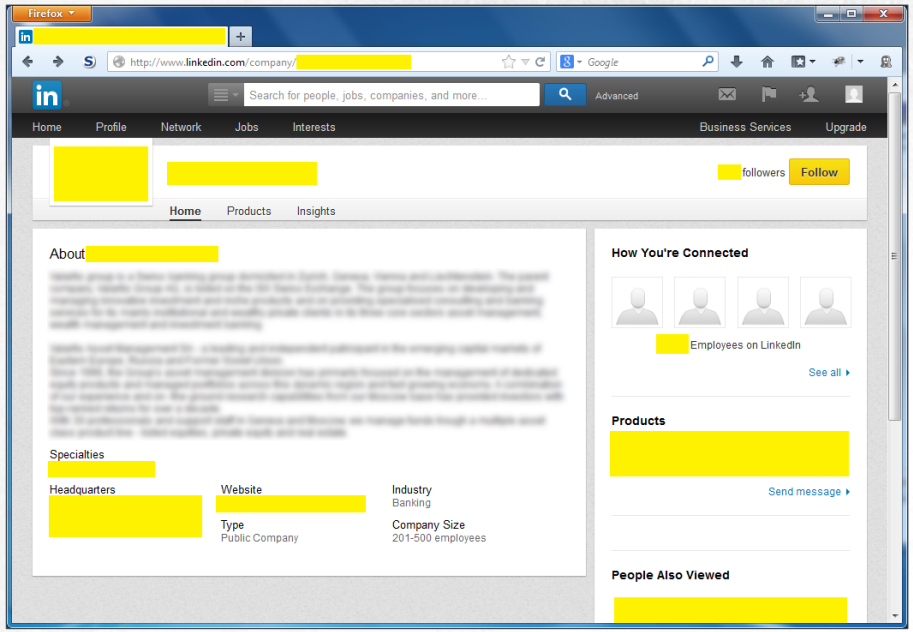
1. Introduction
    - The State of Exploit Development
    - Unconventional Exploits
2. Trust Relationships
3. **Case 0x01 – Inaccessible system**
4. Case 0x02 – Who is who?
5. Penetration Testing in 2020
6. Conclusion

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Few information about the target

- Swiss-based Private company
- 200 – 500 employees
- Most of its employees have a LinkedIn account with tons of interesting details about the target.
- The target is available also on Twitter and Facebook.

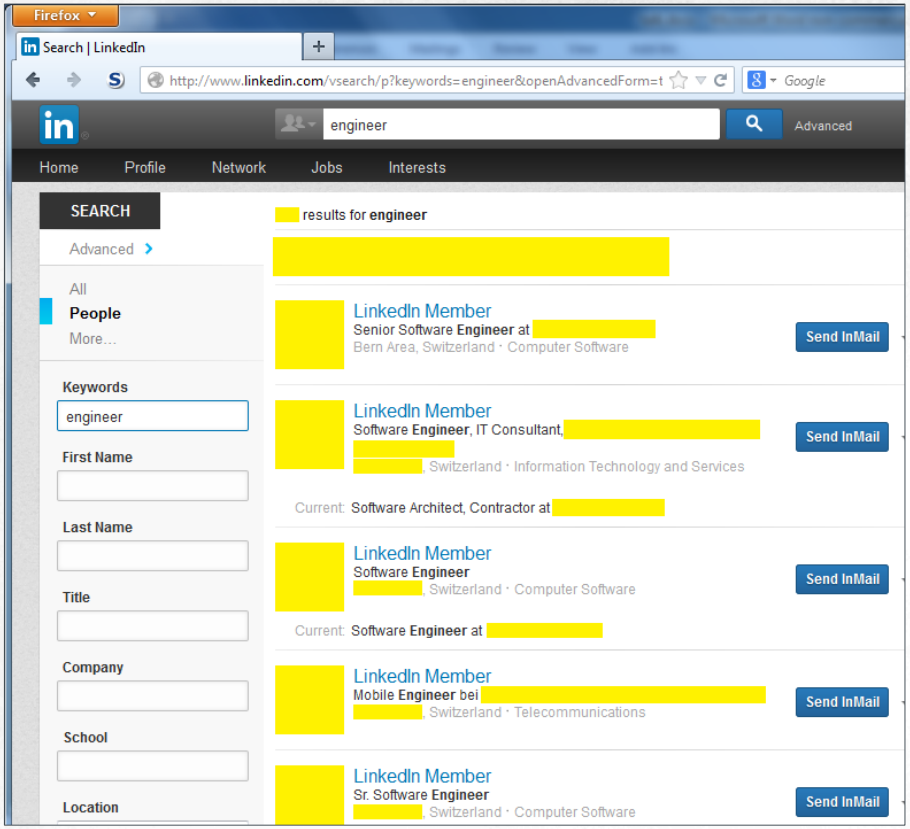


Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

List the employees

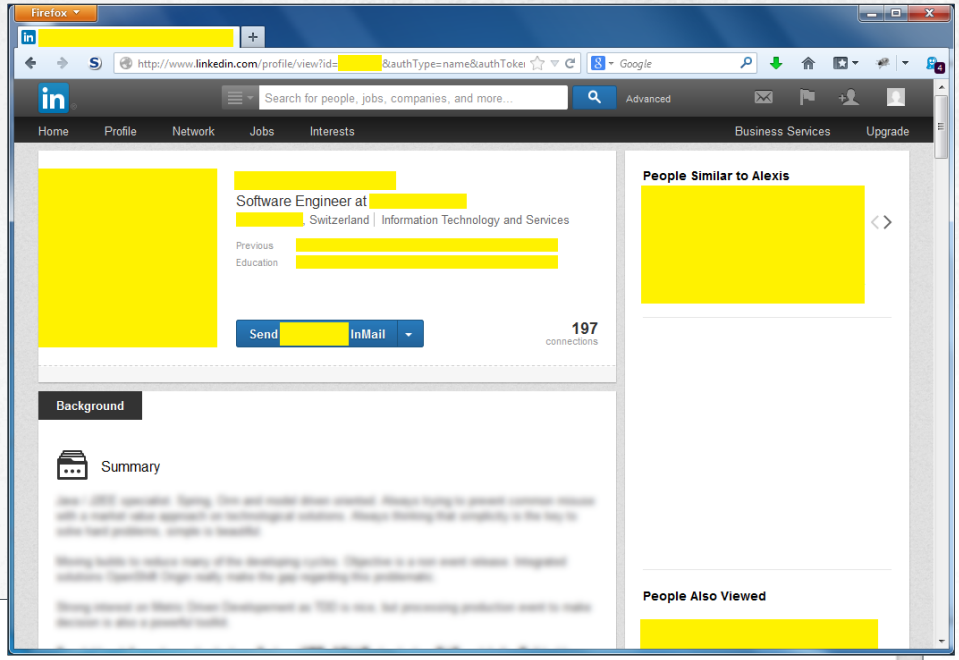
- Get an idea of the company's workforce.
- Find out the roles and responsibilities of each employee
- The target has X software engineers, Y system admins, Z network admins, etc.



Case 0x01 – Inaccessible system

Additional information

- LinkedIn users like to share information about their current job



- Most of this information is extremely helpful to get a good idea of your target's IT infrastructure.

Junior Platform Engineer

SBB

December 2012 – Present (10 months) | Bern Area, Switzerland

Deploy and manage database changes, support development teams with Oracle know-how, performance tuning of new and existing applications, conduct internal training of developers in Oracle basics, Partitioning, Oracle statistics, operating and management of Oracle databases

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Additional information (part 2)

Firmware engineer

ERA electronic systems

October 2007 – February 2008 (5 months)

Design and implementation of Firmware(under DO-178B) for a freescale 56800E DSC in C language under RTXC Quadros real time operative system.

Consultant

DL Groupe GMG

2008 – August 2010 (2 years)

- Install, plan and design of VMware ESX 3.5, VSphere infrastructures and Hyper-V infrastructures.
- Migration of VMware 2.5 to VMware 3.5.
- P2V of physical servers with VMware Converter.
- SAN infrastructure installation.
- Data protection with System Center Data Protection Manager, Avamar, Symantec Backup Exec.
- Implementation, migration and administration on Exchange 2007 (physical or virtual infrastructures).
- Implementation of archiving solutions with Symantec Enterprise Vault.
- Administration of the DNS and Active Directory services, advance scripting on powershell.

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Additional information (part 3)

System Engineer

BCP Bank, Geneva

October 2010 – Present (3 years) | Geneva Area, Switzerland

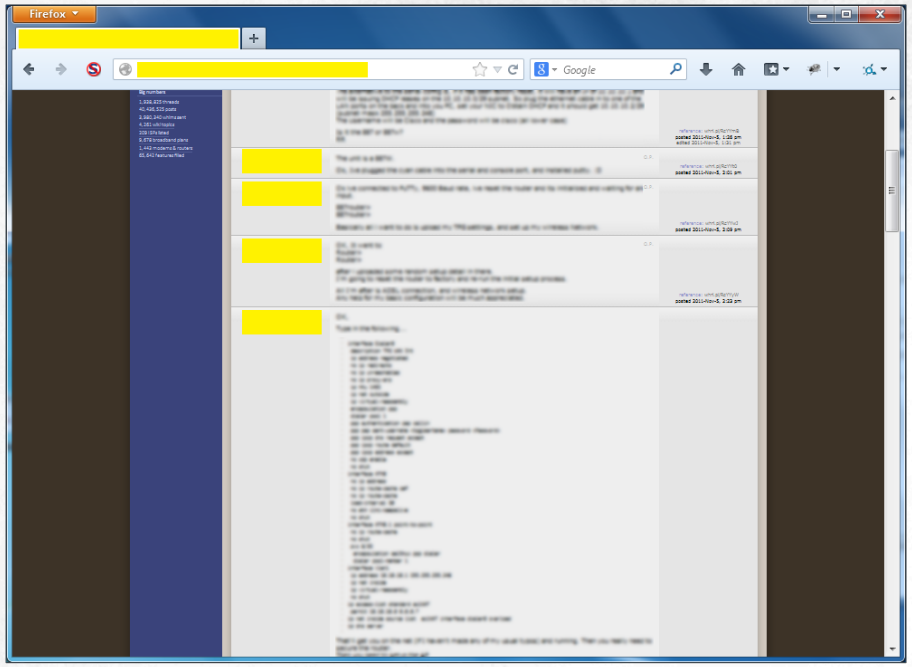
- Servers 2008 (print server, cluster, NLB, DFS).
- Servers 2003/2008 (migration DNS & Active Directory).
- Exchange 2010 (migration 2003/2010)
- BlackBerry 5.0
- Emterprise Vault 9.0
- Citrix Metaframe XenApp 6
- VmWare ESX 4.1 (vSphere).
- VmView Client 4.6
- NEXThink 4.0
- Backup/restore (Net Backup & Backup Exec).
- Patch deployment (WSUS).
- Anti-Virus deployment (McAfee - ePo)
- Second level Windows support team.

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Did he really post his router config on a public forum??

- A network admin working at the target company had a problem with a network device and posted sensitive info on a public forum.



- IT forums are full of people sharing their system and/or network configurations .

- Most of them are unaware of the risks or simply have to get a service up and running by Monday!

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Information about the target

- OS used: Debian and Windows 7

- Applications: Several custom Web apps, PmWiki, phpMyAdmin, Apache, Oracle, MySQL, Kerberos, …

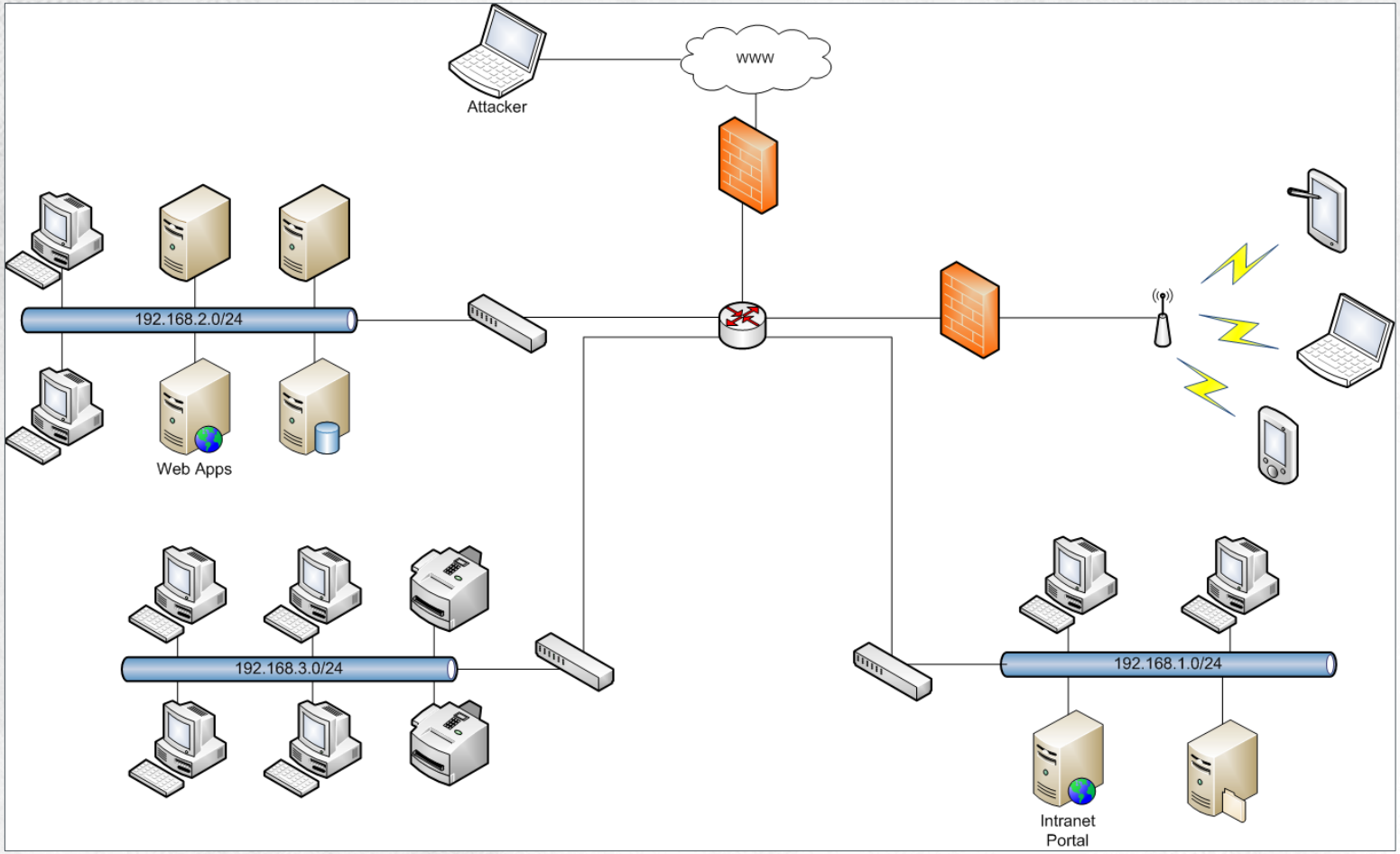
- Network topology: 4 networks (WLAN, servers, IT, users). Users cannot reach IT. WLAN cannot reach IT or Users.

- Wireless: Only registered devices are allowed to connect to the WLAN which is separated from the intranet by a firewall/packet filter.

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

The target's network



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

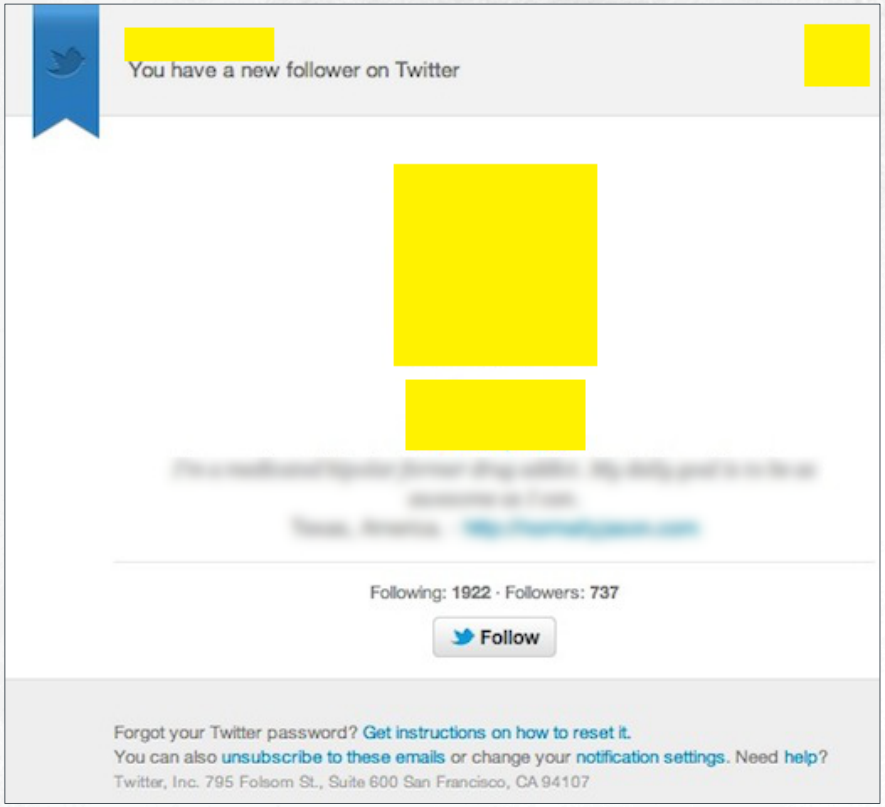
Case 0x01 – Inaccessible system

Initial Entry

- Within a group of hundreds of employees is not that difficult to find a good target for a phishing attack.

- Employees addicted to social networks are good targets cause they will often check their new followers or friends.

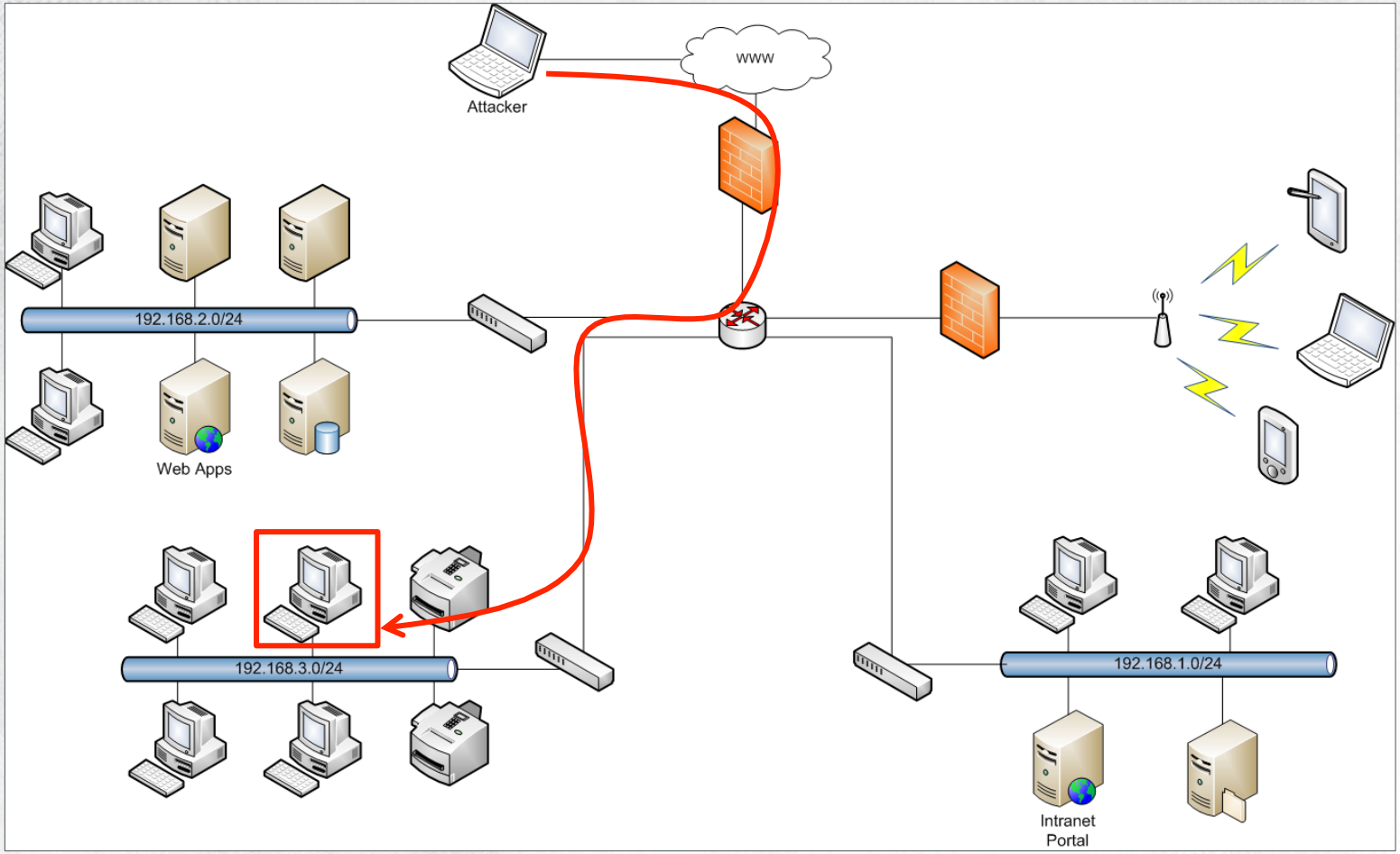
- The victim opened our e-mail and clicked on one of the links. Too easy!



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

The target's network



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

The Next Move

- Through our extensive information gathering, we found out that one of **the network admin was using PmWiki to store HOWTOs**.

- The installed version of PmWiki was unknown, but based on the time of a forum discussion among the network admin and other users of the forum, we estimated that **the version used had to be between 2.2.22 and 2.2.30**.

- **Versions prior to 2.2.34 are vulnerable** to a PHP code injection!

- Unfortunately, hosts in the User network segment cannot directly access those ones in the IT segment!

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Web technologies are very handy sometimes

- **The target is going through some important changes** in their infrastructure and now users have several RIA applications to perform their daily tasks from their computer, laptops or tablets.

- A rich Internet application (RIA) is a Web application that has many of the characteristics of desktop application software. (source: Wikipedia)

- **The target's rich internet applications must manage a lot of data from several sources**.

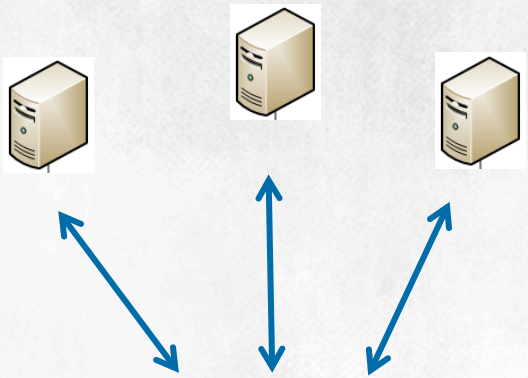
- AJAX cannot access data from multiple sources. It needs a **bridge**!

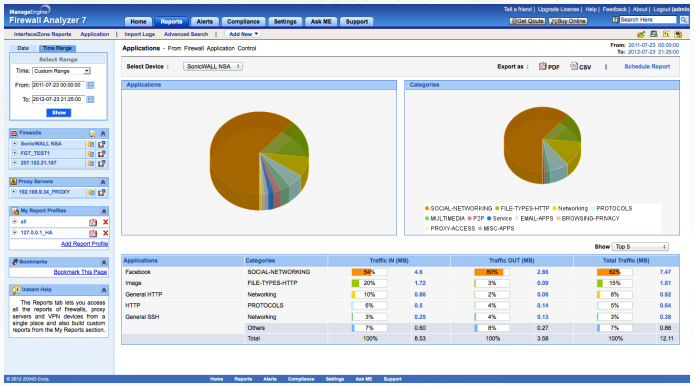
Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

AJAX Bridging

- In order to get the resources needed by a RIA application, the app will send its request to the bridge which will forward them to the right server. The response will then be sent back to the RIA application.



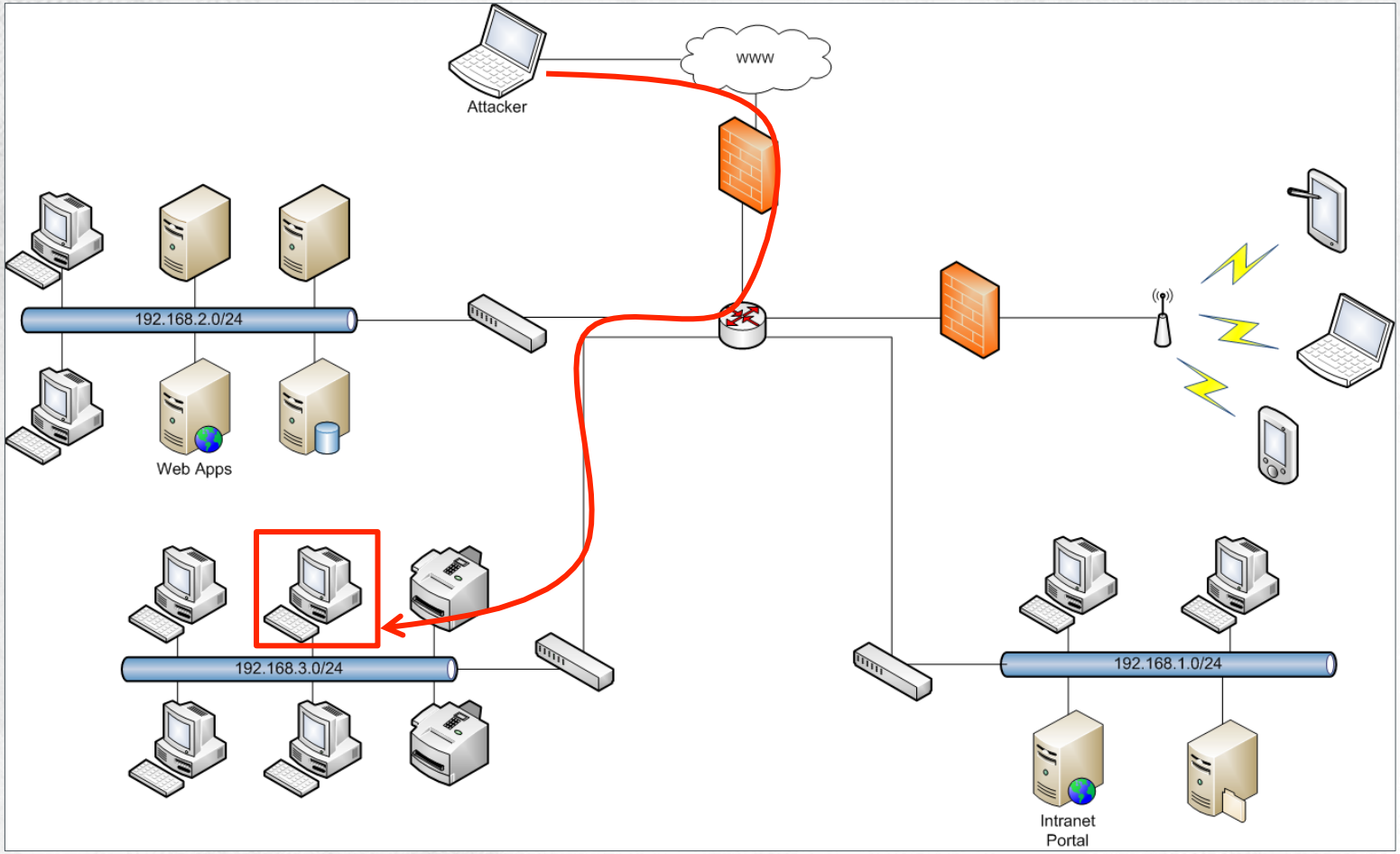


- The use of an AJAX bride opens new interesting scenarios. Note that the servers can access the IT network segment!

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

The current situation

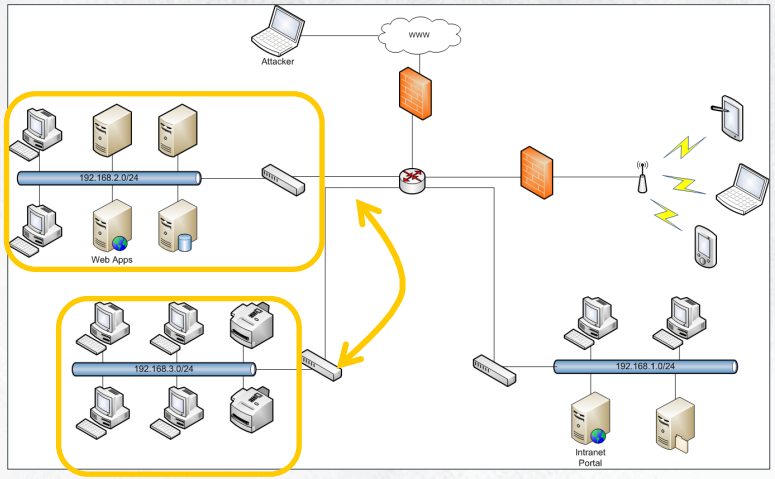


Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

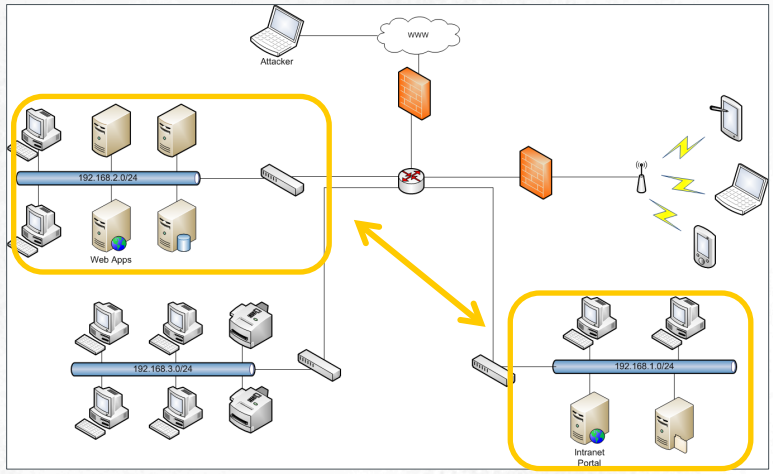
Case 0x01 – Inaccessible system

Trust Relationships

- Ajax Bridge trusts RIA applications.



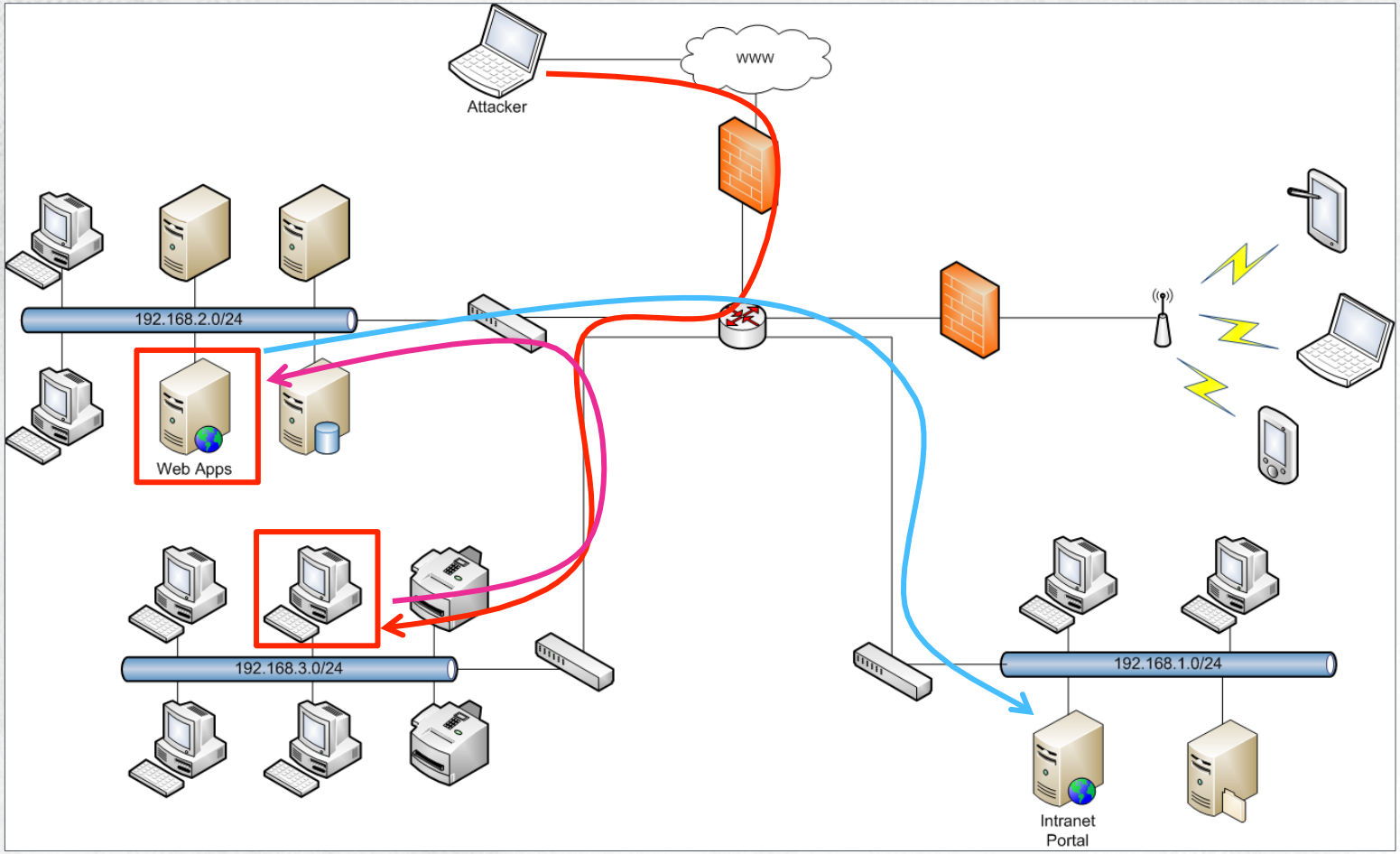
- The IT segment network trusts the server segment network.



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Trust Exploitation



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

It's show time!

DEMO

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x01 – Inaccessible system

Solutions

- Be careful **what you post on the Internet stays there forever**.

- **Security Awareness**. A network administrator should not share sensitive information about his network! Explain to your staff the risks of sharing such information.

- **Document every trust relationship and make sure the proper access control mechanism are in place**. Who should access the Internal Portal?

- **Avoid dangerous solutions** (if possible).

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Presentation

Summary

1. Introduction
    - The State of Exploit Development
    - Unconventional Exploits
2. Trust Relationships
3. Case 0x01 – Inaccessible system
4. **Case 0x02 – Who is who?**
5. Penetration Testing in 2020
6. Conclusion

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x02 – Who is who?

Kerberos 101

- Kerberos is a **sophisticated authentication technology** for securing access to network applications.

- **Kerberos never sends your password** over the network. Instead, it uses cryptographic tokens also known as tickets.

- Kerberos requires **mutual authentication** of both parties (client and server)

- You can find more information on the MIT Kerberos website (http://web.mit.edu/kerberos/).

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x02 – Who is who?

Tickets and ticket cache

- A ticket is created when you login in a Kerberized service

- The ticket cache is usually a file in /tmp with all the information about the tickets issued.

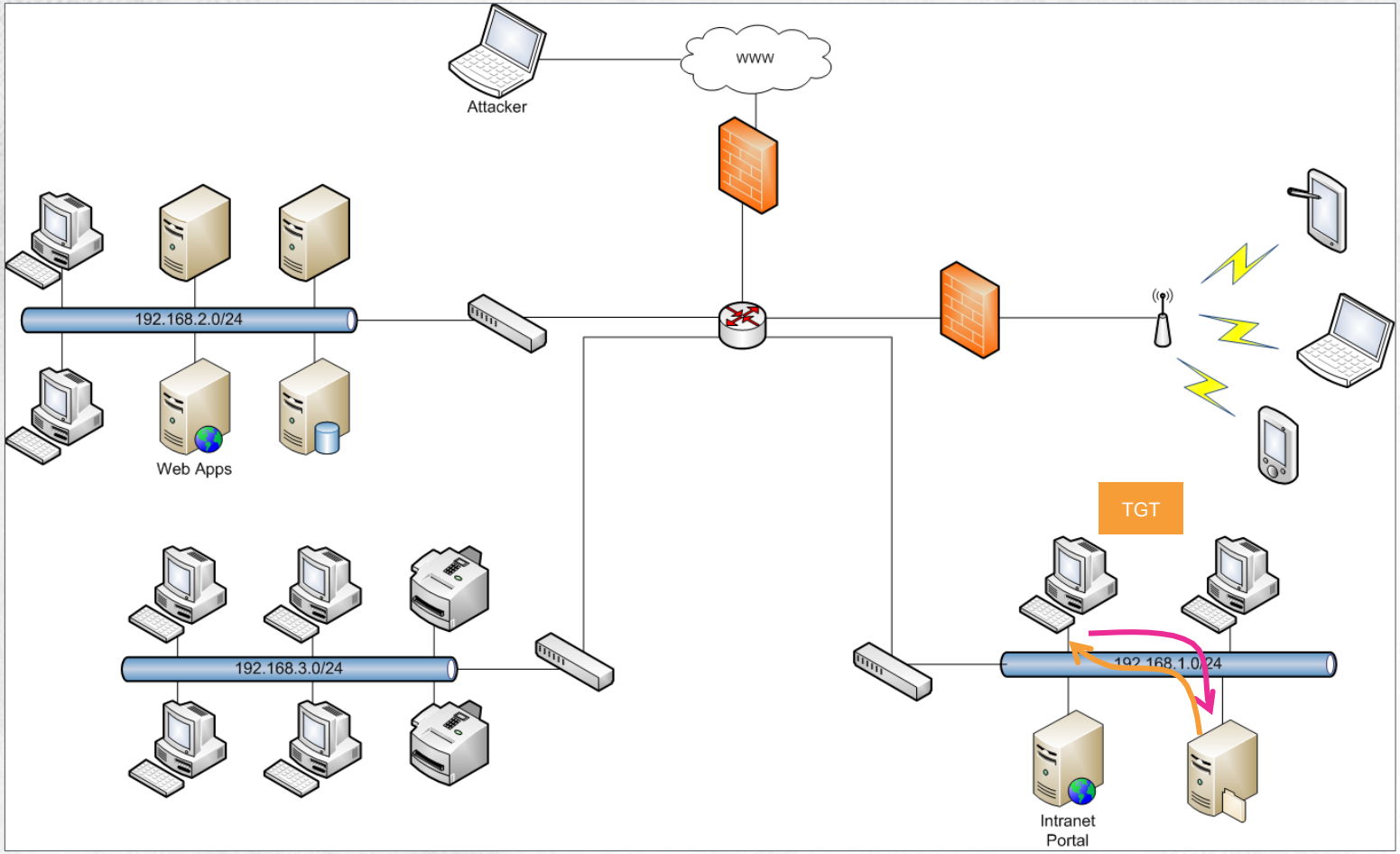
- The exact location of the ticket cache is stored in the KRB5CCNAME environment variable.

- This file is owned by the user but root have access to it!

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x02 – Who is who?

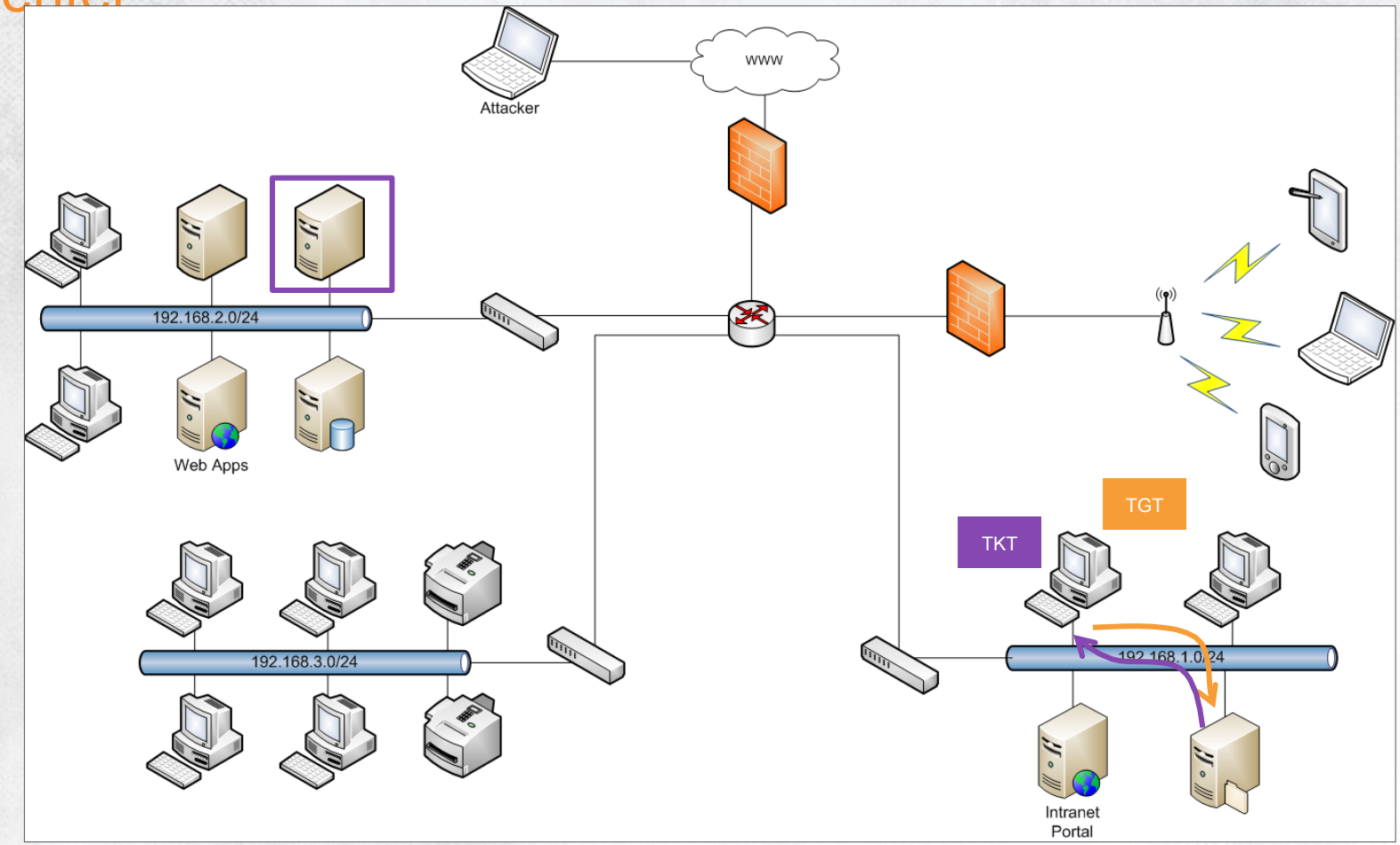
Get Ticket-Granting Ticket (TGT)



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x02 – Who is who?

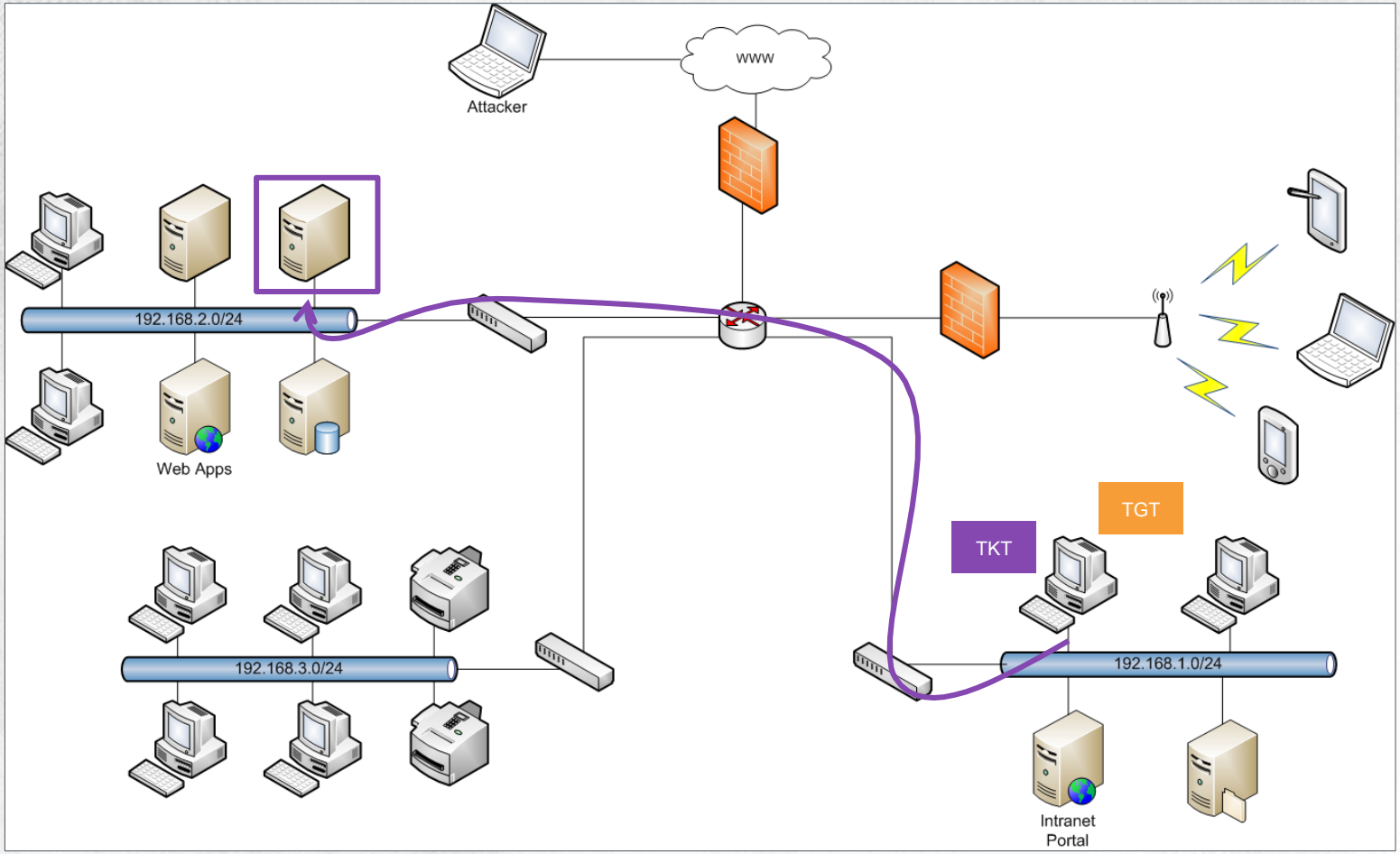
Get ticket to access a server from the Key Distribution Center



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x02 – Who is who?

Access the server without providing a password



Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Case 0x02 – Who is who?

The Attack

- Moving around the target network we found Kerberos server and quickly exploited a vulnerability to get root. As a root user on a Kerberos server, you can read every file on the file system, including the ticket cache of a user.

- Scanning the .ssh/known_hosts file of the users in the system we found several unexplored machines. So, we decided to exploit the trust relationship between the kerberos and those unexplored machines.

- **We access those machines using the tickets in the kerberos server**. No password required and no alarms triggered.

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Presentation

Summary

1. Introduction
    - The State of Exploit Development
    - Unconventional Exploits
2. Trust Relationships
3. Case 0x01 – Inaccessible system
4. Case 0x02 – Who is who?
5. **Penetration Testing in 2020**
6. Conclusion

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Penetration Testing in 2020

or maybe 2030

- Vulnerability scanners will detect numerous vulnerabilities, but most of them will require a **very skillful exploit developer** to be exploited.

- Penetration testing frameworks will have to face the fact that a single new **security feature of Microsoft could potentially "kill" all their exploits**.

- Hackers will start looking for **alternative ways to get from UID X to UID 0**, perhaps using unconventional exploits.

- IDS/IPS's and SIEM solutions will have a hard time to detect **unconventional exploits** because most of them **appear as normal activity**.

Presentation

Summary

1. Introduction
    - The State of Exploit Development
    - Unconventional Exploits
2. Trust Relationships
3. Case 0x01 – Inaccessible system
4. Case 0x02 – Who is who?
5. Penetration Testing in 2020
6. **Conclusion**

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Conclusion

and final thoughts

- In the future, the **cost of exploit development will increase** because of the countless security countermeasures exploit writers have to bypass.

- A higher cost of exploits will most likely promote the use of unconventional exploits which are often very difficult to spot because they target trust relationships and they are not so noisy as the traditional exploits.

- **Think out of the box**!

Email: research@ptrace-security.com | Website: www.ptrace-security.com
Address: Untermüli 9, 6300 Zug, Switzerland

Thank you

research@ptrace-security.com

www.ptrace-security.com

@ptracesecurity