Action Plan

Guylian De Wit
R0716728
3ITF | CCS

LID VAN ASSOCIATIE KU LEUVEN
EY
THOMAS MORE

1 Company Presentation

1.1 EY (Ernst & Young)

Is an internationally operating company active in the fields of accounting, tax and business consulting.

Until June 2013 the company was known as Ernst & Young. EY is an international partnership of local member firms. EY Global Limited is based in London and ensures the unity of policy of all member firms. EY Global does not provide services to clients, that is done by the member firms such as EY Belgium.

The company employs around 230,000 people worldwide and is based in 150 countries.

Besides accountancy services EY also provides IT/Cyber and Privacy related services, the cybersecurity team is divided into two parts; the financial sector and the business and government sectors.

The services that EY provides regarding the cybersecurity domain include but are not limited to:

- Data Protection (DP)
- Threat Detection and Response (TDR)
- Cyber Risk Management (CTM)
    - Identifying the security needs of customers.
    - Improving the cybersecurity posture.
- Cybersecurity Transformation (CT)
    - Provide services to customers to help withstand the many security “challenges”.

2 Added Value

2.1 Project Description

My project is based around the various weaknesses within a Windows Active Directory environment. During my internship, I am conducting research on the most common vulnerabilities within an Active Directory environment, how an attacker can exploit them and how to prevent and mitigate these problems.

My research is intended to provide the reader with a better understanding of what exactly Active Directory is, what it is used for, which function Active Directory has within a network, and where the weaknesses lie within an Active Directory environment, as well as how these weaknesses can be exploited by people with bad intentions, also known as hackers, and how these weaknesses can be remedied.

It is also my intention to work with the weaknesses I research and abuse them myself in a controlled lab environment to gain hands on experience within the various domains and document my findings.

2.2 Research Question

Together with my internship superiors, we came up with a formal research question that gives a good idea of my research topic and what the research entails.

The research question goes as follows:

"What are the most common vulnerabilities exploited by malicious actors within an Active Directory environment and how can these be mitigated?”

2.3 Conclusion

The added value for the company lies in the fact that annual data breaches cost companies on average $4 million, and 60 percent of these hacks could be avoided by patches issued by a manufacturer such as Microsoft.

My internship company also reported that they themselves don't have too much knowledge about kerberos and kerberoasting attacks, kerberos is

an authentication protocol used within Active Directory and is one of the building blocks to authenticate user accounts and service accounts. Therefore, I thought it would be very interesting to cover this topic. Which is also why it is the first vulnerability I cover in my research.

3 Planning

3.1 Feedback Moments

I have been assigned a mentor from the internship company out, I can contact this mentor at all times in case of questions.

He also follows up on me, there are 2 meetings a week on Monday and Wednesday to discuss the progress and to make any adjustments, input remarks or ask questions.

Furthermore, we have a weekly status meeting with all interns within the consulting department of the company together with Matthias who is the main internship coordinator.

Every two weeks we also have a meeting with the whole consulting department to address progress with clients and other issues.

3.2 Milestones

1) Write the About EY section in the thesis document.
2) Elaborate the Research Question section in the thesis document.
3) Introduce the reader to Active Directory.
4) Explain the reader what Kerberos is.
    a. Write about the three Kerberos vulnerabilities:
        i. Kerberoasting
        ii. Silver Ticket Attack
        iii. Golden Ticket Attack
5) Explain Group Policy Misconfigurations.
6) Explain the Domain Controller Synchronization attack.
7) Explain the Token Impersonation Attack.
8) Explain the Zerologon attack.

3.3 Planning

Below you can find a detailed logbook of my journey as an intern at EY.

1/mrt.	8:45-10:30	Kick off at EY office in Diegem.
1/mrt.	11:00-11:30	Virtual kick off with Internship mentors.
1/mrt.	14:00-15:00	Meeting about research question with mentor.
1/mrt.	15:00-18:00	Creation of PvA and Research Questions document.
2/mrt.	8:45-9:55	Continue working on PvA and Research Questions.
2/mrt.	10:00-10:45	Coffee Break: Meeting Yannick Scheelen & Interns.
2/mrt.	10:45-12:30	Research with regards to Windows Pentesting Tools.
2/mrt.	12:30-12:45	Quick cup of instant noodles for lunch.
2/mrt.	12:45-13:39	Continue research with regards to Windows Pentesting Tools.
2/mrt.	13:39-14:00	Call with mentor with regards to project definition.
2/mrt.	14:00-17:00	Project definition changed -> Research about a more technical project with regards to Windows pentesting.
2/mrt.	17:00-18:00	HR onboarding meeting.
3/mrt.	8:30-10:00	Check mails, schedule & continue researching new project ideas.

3/mrt.	10:00-12:00	Reseach regarding Active Directory Lab environments.
3/mrt.	12:00-13:00	Lab environment master VM installation & documentation.
3/mrt.	13:00-13:15	Lunch break.
3/mrt.	13:15-13:25	Continue working on the lab environment.
3/mrt.	13:30-14:00	Meeting with mentor regarding project subject and research question.
3/mrt.	14:00-14:45	Writing and sending introduction e-mail to the team.
3/mrt.	14:45-17:30	Determining project subject.
4/mrt.	8:30-9:30	Check mails, schedule & continue researching new project ideas.
4/mrt.	9:30-10:00	Productive chat with mentor, new project subject has been established.
4/mrt.	10:00-17:16	Creating list of AD attack vectors.
4/mrt.	17:17-18:00	Creating personal favorites list.

5/mrt.	**8:00-9:00**	Meeting with mentor regarding top threats within active directory.
5/mrt.	**9:30-10:15**	Weekly status meeting
5/mrt.	**10:15-11:00**	Meeting with mentor to finalize tasks and submit timesheet
5/mrt.	**11:00-11:45**	Sending mails
5/mrt.	**11:45-14:00**	Creating structure in thesis Word document.
8/mrt.	**8:30-9:55**	Creating structure in thesis Word document and begin researching further.
8/mrt.	**10:00-11:00**	Call with mentor with regards to thesis document.
8/mrt.	**11:00-12:30**	Documentation with regards to Kerberos in thesis document.
8/mrt.	**12:30-12:45**	Lunch break.
8/mrt.	**12:45-17:30**	Documentation with regards to Kerberos in thesis document.
9/mrt.	**N/A**	Cyber Security Challenge Belgium.

10/mrt.	N/A	Cyber Security Challenge Belgium.
11/mrt.	8:30-10:00	Creation of introduction PowerPoint Slide + Rehearsal.
11/mrt.	10:00-10:35	Mid-week sync with mentor.
11/mrt.	10:35-12:30	Documentation with regards to Kerberoasting in thesis document.
11/mrt.	12:30-12:45	Lunch break.
11/mrt.	12:45-16:00	Documentation with regards to Kerberoasting in thesis document.
11/mrt.	16:00-17:30	Creating PowerPoint Presentation PvA (School).
11/mrt.	17:30-18:00	Bi-Weekly meeting with consultancy.
12/mrt.	8:30-9:30	Documentation with regards to Kerberoasting in thesis document.
12/mrt.	9:30-10:00	Weekly status meeting

12/mrt.	**10:00-11:00**	Documentation with regards to Kerberoasting in thesis document.
12/mrt.	**11:00-12:00**	Documentation with regards to Silver Ticket in thesis document.
12/mrt.	**12:00-12:15**	Lunch break.
12/mrt.	**12:15-14:00**	Documentation with regards to Silver Ticket in thesis document.
15/mrt.	**8:30-11:30**	Documentation with regards to Silver Ticket in thesis document.
15/mrt.	**11:30-12:00**	Meeting with mentor regarding progeress on thesis document.
15/mrt.	**12:00-12:15**	Lunch break.
15/mrt.	**12:15-15:00**	Documentation with regards to Silver Ticket in thesis document.
15/mrt.	**15:00-16:40**	Documentation with regards to Silver Ticket detection in thesis document.
15/mrt.	**16:40-18:00**	Documentation with regards to Golden Ticket in thesis document.
16/mrt.	**8:30-10:00**	Documentation with regards to Golden Ticket in thesis document.

16/mrt.	**10:00-10:30**	Coffee break with Erik Aerts.
16/mrt.	**10:30-12:00**	Documentation with regards to Golden Ticket detection in thesis document.
16/mrt.	**12:00-12:15**	Lunch break.
16/mrt.	**12:15-14:30**	Documentation with regards to Golden ticket detection & mitigation in thesis document.
16/mrt.	**14:30-15:00**	Finalizing and proof reading. Kerberos thesis document.
16/mrt.	**15:00-18:00**	Research regarding next topic GPO Misconfigurations.
17/mrt.	**8:30-10:00**	Research regarding next topic GPO Misconfigurations.
17/mrt.	**10:00-10:30**	Mid-week sync with mentor.
17/mrt.	**10:30-12:00**	Research regarding next topic GPO Misconfigurations.
17/mrt.	**12:00-12:15**	Lunch break.
17/mrt.	**12:15-14:30**	Documentation regarding getting familiar with GPOs
17/mrt.	**14:30-15:00**	First meeting with school mentor.

17/mrt.	15:00-18:00	Documentation Action Plan (School)
18/mrt.	8:30-12:00	Documentation with regards to Getting Familiar With GPO's in Thesis Document.
18/mrt.	12:00-12:15	Lunch break.
18/mrt.	12:15-16:00	Documentation with regards to getting Familiar With GPO's in Thesis Document.
18/mrt.	16:00-17:00	Creating PPT with progress for Weekly Intern meeting.
18/mrt.	17:00-17:45	Documentation with regards to Getting Familiar With GPO's in Thesis Document.
18/mrt.	17:45-18:00	Update logbook file.
19/mrt.	8:30-9:30	Adjusting powerpoint slide for progress report.
19/mrt.	9:30-10:30	Weekly internship sync/progress report
19/mrt.	10:30-12:00	Proofreading an markup of GPO subject in thesis document.
19/mrt.	12:00-12:30	Feedback call with mentor.

19/mrt.	12:30-12:45	Lunch break.
19/mrt.	12:45-14:00	Proofreading an markup of GPO subject in thesis document.
22/mrt.	8:30-12:000	Research regarding Enumerating Group Policies for thesis document.
22/mrt.	12:00-12:15	Lunch break.
22/mrt.	12:15-13:30	Documentation regarding Enumerating Group Policies for thesis document.
22/mrt.	13:30-14:00	Call with mentor.
22/mrt.	14:00-14:30	Writing mail to peers.
22/mrt.	14:30-18:00	Documentation regarding Enumerating Group Policies for thesis document.
23/mrt.	8:30-10:30	Documentation regarding Enumerating Group Policies for thesis document.
23/mrt.	10:30-11:00	Coffee talk.
23/mrt.	11:00-12:30	Research regarding BloodHound for thesis document.

23/mrt.	**12:30-12:45**	Lunch break.
23/mrt.	**12:45-18:00**	Documentation regarding BloodHound for thesis document.
24/mrt.	**8:30-11:00**	Documentation regarding BloodHound for thesis document.
24/mrt.	**11:00-12:00**	Meeting with mentor.
24/mrt.	**12:00-12:15**	Lunch break.
24/mrt.	**12:15-13:00**	Create Glossary in thesis document.
24/mrt.	**13:00-13:30**	Meeting with mentor and supervisor from school.
24/mrt.	**13:30-18:00**	Working on glossary and footnotes thesis document. - completed till page 21.
25/mrt.	**8:30-12:00**	Completing glossary for thesis document
25/mrt.	**12:00-12:15**	Lunch break.
25/mrt.	**12:15-17:00**	Completing footnotes and glossary for thesis document.

25/mrt.	17:00-18:00	Proofreading and changing "I" to "We" form in thesis document.
29/mrt.	8:30-10:00	Document writing for GPO Exploitation chapter thesis.
29/mrt.	10:00-10:30	Call with mentor.
29/mrt.	10:30-12:00	Document writing & Research leveraging schedulded tasks.
29/mrt.	12:00-12:15	Lunch break.
29/mrt.	12:15-18:00	Document writing leveraging schedulded tasks for thesis.
30/mrt.	8:30-10:00	Document writing best practices GPO for thesis document.
30/mrt.	10:00-10:30	Coffee break meeting.
30/mrt.	10:30-12:00	Document writing best practices GPO for thesis document.
30/mrt.	12:00-12:15	Lunch break.
30/mrt.	12:15-18:00	Document writing best practices GPO for thesis document.

31/mrt.	8:30-12:00	Document writing best practices GPO for thesis document.
31/mrt.	12:00-12:15	lunch break.
31/mrt.	12:15-14:00	Kerberos Practical Try Hack Me
31/mrt.	14:00-16:30	kerberos practical Try Hack Me Documentation
31/mrt.	16:30-16:40	Call with Timon.
31/mrt.	16:40-18:00	Kerberos practical Try Hack Me
1/apr.	8:30-10:00	Kerberos practical Try Hack Me
1/apr.	10:00-10:30	Coffee break meeting.
1/apr.	10:30-12:00	Kerberos practical Try Hack Me
1/apr.	12:00-12:15	lunch break.
1/apr.	12:15-17:00	kerberos practical Try Hack Me Documentation

1/apr.	17:00-19:00	Cyber Meeting with WEM.
2/apr.	8:30-9:30	Powerpoint slide meeting
2/apr.	9:30-12:00	kerberos practical Try Hack Me
2/apr.	12:00-12:15	Lunch break.
2/apr.	12:15-13:00	kerberos practical Try Hack Me Documentation
2/apr.	13:00-13:30	Sync meeting with mentor
2/apr.	13:30-14:00	Kerberos practical Try Hack Me Documentation
6/apr.	8:30-10:00	TryHackMe Kerberos Room for thesis document
6/apr.	10:00-10:40	Coffee break meeting.
6/apr.	10:40-12:00	TryHackMe Kerberos Room for thesis document
6/apr.	12:00-12:15	Lunch break.

6/apr.	**12:15-18:00**	TryHackMe Kerberos Room for thesis document
7/apr.	**8:30-12:00**	TryHackMe Kerberos Room for thesis document
7/apr.	**12:00-12:15**	Lunch break.
7/apr.	**12:15-14:00**	TryHackMe Kerberos Room for thesis document
7/apr.	**14:00-14:30**	Sync meeting with mentor
7/apr.	**14:30-18:00**	DCSync research
8/apr.	**8:30-12:00**	DCSync research and documentation
8/apr.	**12:00-12:15**	Lunch break.
8/apr.	**12:15-18:30**	DCSync research and documentation
9/apr.	**8:30-9:30**	Creating PowerPoint

9/apr.	**9:30-10:00**	Weekly sync meeting
9/apr.	**10:00-12:00**	DCSync research and documentation
9/apr.	**12:00-12:15**	Lunch break.
9/apr.	**12:15-14:00**	DCSync research and documentation
12/apr.	**8:30-11:30**	DCSync research and documentation
12/apr.	**11:30-12:00**	Meeting with mentor
12/apr.	**12:00-12:15**	Lunch break.
12/apr.	**12:15-16:00**	DCSync research and documentation
12/apr.	**16:00-18:00**	Editing thesis based on Mentor comments
13/apr.	**8:30-10:00**	Editing thesis based on Mentor comments
13/apr.	**10:00-10:30**	Coffee break meeting.

13/apr.	**10:30-12:00**	Editing thesis based on Mentor comments
13/apr.	**12:00-12:15**	Lunch break.
13/apr.	**12:15-14:00**	Editing thesis based on Mentor comments
13/apr.	**14:00-18:00**	Token Impersonation research and documentation
14/apr.	**08:00-12:00**	Token Impersonation research and documentation
14/apr.	**12:00-12:15**	Lunch break.
14/apr.	**12:15-13:00**	Token Impersonation research and documentation
14/apr.	**13:00-13:30**	Meeting with mentor
14/apr.	**13:30-18:00**	Token Impersonation research and documentation
15/apr.	**8:30-12:00**	Token Impersonation research and documentation
15/apr.	**12:00-12:15**	lunch break.

15/apr.	12:15-18:00	Token Impersonation research and documentation
16/apr.	8:30-9:30	PPT maken voor meeting
16/apr.	9:30-10:00	weekly sync meeting
16/apr.	10:00-12:00	Token Impersonation research and documentation
16/apr.	12:00-12:15	Lunch break.
16/apr.	12:15-14:00	Token Impersonation research and documentation
19/apr.	8:30-9:30	Creating PowerPoint
19/apr.	9:30:11:00	Meeting with teacher
19/apr.	11:00-11:30	Meeting with mentor
19/apr.	11:30-11:45	Lunch break.
19/apr.	11:45-18:00	Token Impersonation research and documentation

20/apr.	8:30-10:00	Token Impersonation research and documentation
20/apr.	10:00-10:30	Coffee break meeting
20/apr.	10:30-12:00	Token Impersonation research and documentation
20/apr.	12:00-12:15	lunch break.
20/apr.	12:15-18:00	PowerPoint Thesis
21/apr.	8:30-12:00	PowerPoint Thesis
21/apr.	12:00-12:15	lunch break.
21/apr.	12:15-18:00	PowerPoint Thesis
22/apr.	8:30-12:00	PowerPoint Thesis
22/apr.	12:00-12:15	lunch break.

22/apr.	**12:15-17:00**	PowerPoint Thesis
22/apr.	**17:00-18:00**	Bi-weekly meeting
23/apr.	**8:30-9:30**	PowerPoint meeting
23/apr.	**9:30-10:00**	Weekly sync meeting
23/apr.	**10:00-11:30**	End-week sync & evaluatie met mentor
23/apr.	**11:30-14:00**	PowerPoint Thesis
26/apr.	**8:30-10:30**	PowerPoint bachelorproef
26/apr.	**10:30-11:00**	Meeting with mentor
26/apr.	**11:00-12:15**	Powerpoint bachelorproef
26/apr.	**12:15-12:30**	Lunch break.
26/apr.	**12:30-18:00**	Zerologon thesis

27/apr.	**8:30-10:00**	Thesis Document Zerologon
27/apr.	**10:00-10:30**	Coffee break meeting
27/apr.	**10:30-12:15**	Thesis Document Zerologon
27/apr.	**12:15-12:30**	Lunch break.
27/apr.	**12:30-17:30**	Thesis Document Zerologon
28/apr.	**8:30-10:00**	Thesis Document Zerologon
28/apr.	**10:00-10:30**	Mid-week sync
28/apr.	**10:30-12:15**	Thesis Document Zerologon
28/apr.	**12:15-12:30**	Lunch break.
28/apr.	**12:30-17:30**	Thesis Document Zerologon

29/apr.	**8:30-12:15**	Thesis Document Zerologon
29/apr.	**12:15-12:30**	Lunch break.
29/apr.	**12:30-17:30**	Powerpoint bachelorproef
30/apr.	**8:30-9:30**	Powerpoint weekly sync
30/apr.	**9:30-10:00**	Weekly sync meeting
30/apr.	**10:00-10:30**	Meeting with mentor
30/apr.	**10:30-14:00**	Powerpoint bachelorproef
3/mei	**8:30-12:15**	Powerpoint bachelorproef
3/mei	**12:15-12:30**	lunch break.
3/mei	**12:30-14:00**	EY PowerPoint
3/mei	**14:00-14:30**	Weekly sync meeting

3/mei	14:30-17:30	EY PowerPoint & rehearsal
4/mei	8:30-10:00	Powerpoint EY proef
4/mei	10:00-11:00	EY Presentation practice round with interns
4/mei	11:00-12:00	Adjusting EY Powerpoint
4/mei	12:00-12:15	Lunch break.
4/mei	12:15-14:00	EY PowerPoint & rehearsal
4/mei	14:00-17:30	Adjusting PvA (school)
5/mei	8:30-11:30	Powerpoint EY proef
5/mei	11:30-12:00	Mid-week sync
5/mei	12:00-12:15	Lunch break.
5/mei	12:15-17:00	EY PowerPoint & rehearsal

5/mei	17:00-18:30	EY Powerpoint presentation
6/mei	8:30-12:15	Plan Van Aanpak adjustments
6/mei	12:15-12:30	Lunch break.
6/mei	12:30-13:30	TryHackMe Zerologon room
6/mei	13:30-14:00	Coffee Break Steven
6/mei	14:00-17:00	TryHackMe Zerologon room
6/mei	17:00-18:00	Bi-weekly meeting
7/mei	8:30-9:30	Powerpoint Friday Meeting
7/mei	9:30-10:00	Friday Meeting
7/mei	10:00-12:15	TryHackMe Zerologon room
7/mei	12:15-12:30	Lunch break.

7/mei	12:30-14:00	TryHackMe Zerologon room
10/mei	8:30-11:30	TryHackMe Zerologon room
10/mei	11:30-12:00	Meeting with mentor
10/mei	12:00-12:15	Lunch break.
10/mei	12:15-18:00	TryHackMe Zerologon room
11/mei	8:30-12:00	Adjusting comments
11/mei	12:00-12:15	Lunch break.
11/mei	12:15-18:00	Adjusting comments
12/mei	8:30-10:00	Writing Foreword
12/mei	10:00-10:30	Midweek sync

12/mei	10:30-12:00	Writing Foreword
12/mei	12:00-12:15	Lunch break.
12/mei	12:15-18:00	Writing Active Directory explanation
13/mei	N/A	FESTIVE DAY
14/mei	8:30-12:15	Writing Active Directory explanation
14/mei	12:00-12:15	Lunch break.
14/mei	12:15-14:00	Writing Active Directory explanation
17/mei	8:30-10:00	Finishing AD explanation
17/mei	10:00-10:30	Sync meeting with mentor
17/mei	10:30-12:15	Listing screenshot sources

17/mei	12:15-12:30	Lunch break.
17/mei	12:30-18:00	Lunch break.
18/mei	8:30 - 12:15	Listing screenshot sources
18/mei	12:15-12:30	Lunch break.
18/mei	12:30-18:00	Listing screenshot sources
19/mei	8:30 - 11:00	Listing screenshot sources
19/mei	11:00-11:30	Meeting with mentor
19/mei	11:30-12:15	Modifying thesis based on comments provided by mentor
19/mei	12:15-12:30	Lunch break.
19/mei	12:30-17:00	Modifying thesis based on comments provided by mentor & changing screenshot references
19/mei	17:00-18:00	Writing summary

20/mei	**8:30-12:15**	Writing summary
20/mei	**12:15-12:30**	Lunch break.
20/mei	**12:30-17:30**	Writing summary & About EY
21/mei	**8:30-9:30**	Weekly powerpoint
21/mei	**9:30-10:00**	Weekly meeting
21/mei	**10:00-13:30**	About EY
25/mei	**8:30-12:15**	Writing About EY
25/mei	**12:15-12:30**	Lunch break.
25/mei	**12:30-14:30**	Completing thesis document
25/mei	**14:30-17:30**	Working on portfolio

26/mei	**8:30-10:30**	Working on portfolio
26/mei	**10:30-11:00**	Meeting with mentor
26/mei	**11:00-12:15**	Working on Attacktive directory lab
26/mei	**12:15-12:30**	Lunch break.
26/mei	**12:30-14:30**	Working on Attacktive directory lab
26/mei	**14:30-17:30**	Working on Attacktive directory lab
27/mei	**8:30-12:15**	Working on attacktive directory lab
27/mei	**12:15-12:30**	Lunch break.
27/mei	**12:30-17:30**	Working on Attacktive directory lab
28/mei	**8:30-9:30**	Powerpoint weekly meeting

28/mei	**9:30-10:00**	Weekly meeting
28/mei	**10:00-10:30**	Final meeting with mentor
28/mei	**11:00-15:00**	Handing in badge & hardware in Diegem