Appendix 1

About the Fictional Scenarios

Scenario 1

Scenario 1 – Story

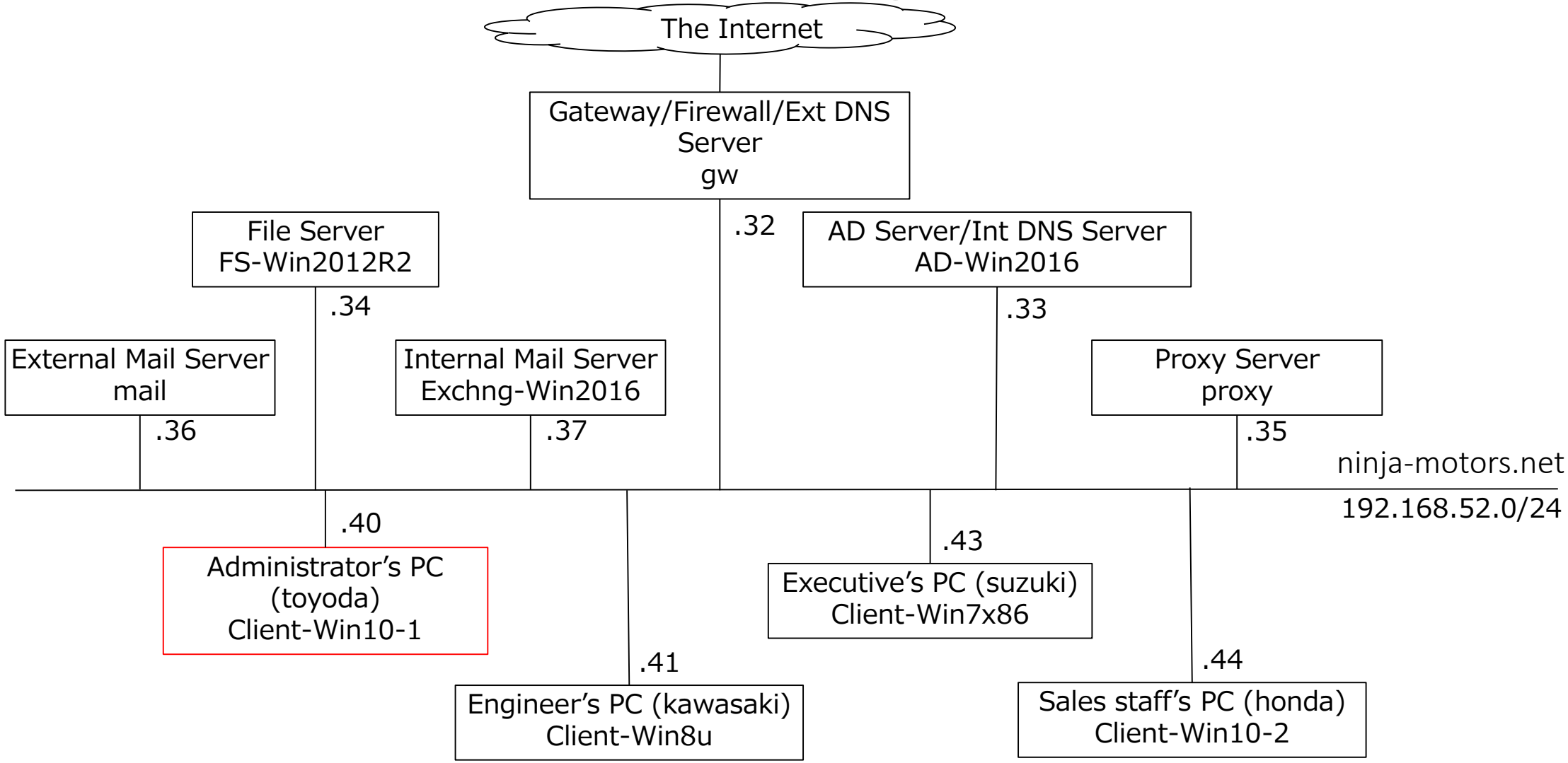
- You are an incident responder working for a certain security company.
- One day, you received a request from a customer that is located in Japan. They said, “Our confidential document has been leaked to the Internet. We’d like you to investigate the cause".
  - Time Zone : JST (+9:00)
- The document was stored in a directory on the file server that only the executive can access.
- First, you acquired the executive’s PC and investigated it. However, you could not find any suspicious evidence.
- Therefore, you decided to investigate the system administrator's PC, which may operate as the authority of all users.
- Any administrator rights (including the local administrator rights) are not given to all users except for the system administrator in the customer’s network.
- The leakage of the file on the Internet was confirmed around the end of March 2018.
- It is estimated that it was stolen in March 2018 from the file creation date.

Scenario 1 – Background Information

- The domain name of the customer: ninja-motors.net
- The saved path of confidential documents: \\fs-win2012r2\executive
- The information of main characters and their PCs

Name	Position	Account name	Groups	Host name	Note
Suzuki	Executive	suzuki	Executives, Domain Users	Client-Win7x86	We have already investigated it and nothing was found.
Toyoda	System Administrator	toyoda	Domain Users	Client-Win10-1	Initial investigation target. * ninja-rdp is used to log on to other computers with RDP for support and maintenance.
		ninja-master	Domain Admins		
		ninja-rdp*	Domain Users		
Honda	General Employee (Sales staff)	honda	Domain Users	Client-Win10-2	
Kawasaki	General Employee (Engineer)	kawasaki	Domain Users	Client-Win8u	

Scenario 1 – Network Diagrams



Scenario 1 – Investigation Strategy

- We suspect that the administrator’s PC (Client-Win10-1) was involved to this incident because the owner of this PC has a privilege.

- We investigate the PC while considering the following two possibilities.
  - Assumption 1: toyoda intentionally stole information.
  - Assumption 2: this PC was infected with malware.