UW i310 IAC

Red Team, Blue Team Exercise

The Activity

We are going to launch a logical attack in minutes and see how effective your rules and mechanisms would be in protecting Enterprise Corp

The Objective

Distributed in class were papers indicating if your role is :

a) **Blue Team (Protectors of Enterprise) infrastructure, servers, IT security, s/w assurance, setting security policies**

b) **Red Team - is a group that attacks an organization's digital infrastructure to test the organization's defenses (often known as penetration testing/PEN testing)**

Blue/teams - You will be given an architecture illlustration and requirements (assume you protect everything you see end to end). Blue team has 10 min to come up with security policies, Blue team (based on those policies – what security mechanisms (not configs – just mechanism and how it protects against specific threats).

The Exercise

Red Team has 10 minutes to prioritize the attacks (order you want to execute that attack (of threats you have or have added). You will get bonus points for added threats.

Blue Team has 5 minutes to prioritize the protection. You will get three mechanisms on wave 1 (before Red launches first attack on policies and mechanisms)

Red launches attack.

Based on attack vector, protection mechanism (protection must deal with specific threat levels spec's in attack)

Red 10 pts successful penetation/attack

Blues 10 pts successful protection (must be CLEAR policies and DETAILED protection mechanisms.

***Each wave – blue can add two more protection mechanisms (in ≤1 minute, red can re-prioritize attacks ≤1 minute**

End of attacks – points tallied to recognize winning team

The Environment - Company ABC

Company has ZERO computing security policies/mechanisms (You are building it !)

4 Large Multi-building campsus – approx 350 people per building

Co Intranet (connects all campus and internal sites (20 in all)

Data Center (20 physical servers 100 virtual), onsite access contractors, suppliers and vendors.

Wireless (seamless) around campus facilties is required

Suppliers access CAD drawings from

Employees (esp remote offices) can bring laptop home, use for personal use

Telecommuting is permitted (and shall be permitted), remote access (VPN) for employee laptops OK

Laptops are company owned and maintained

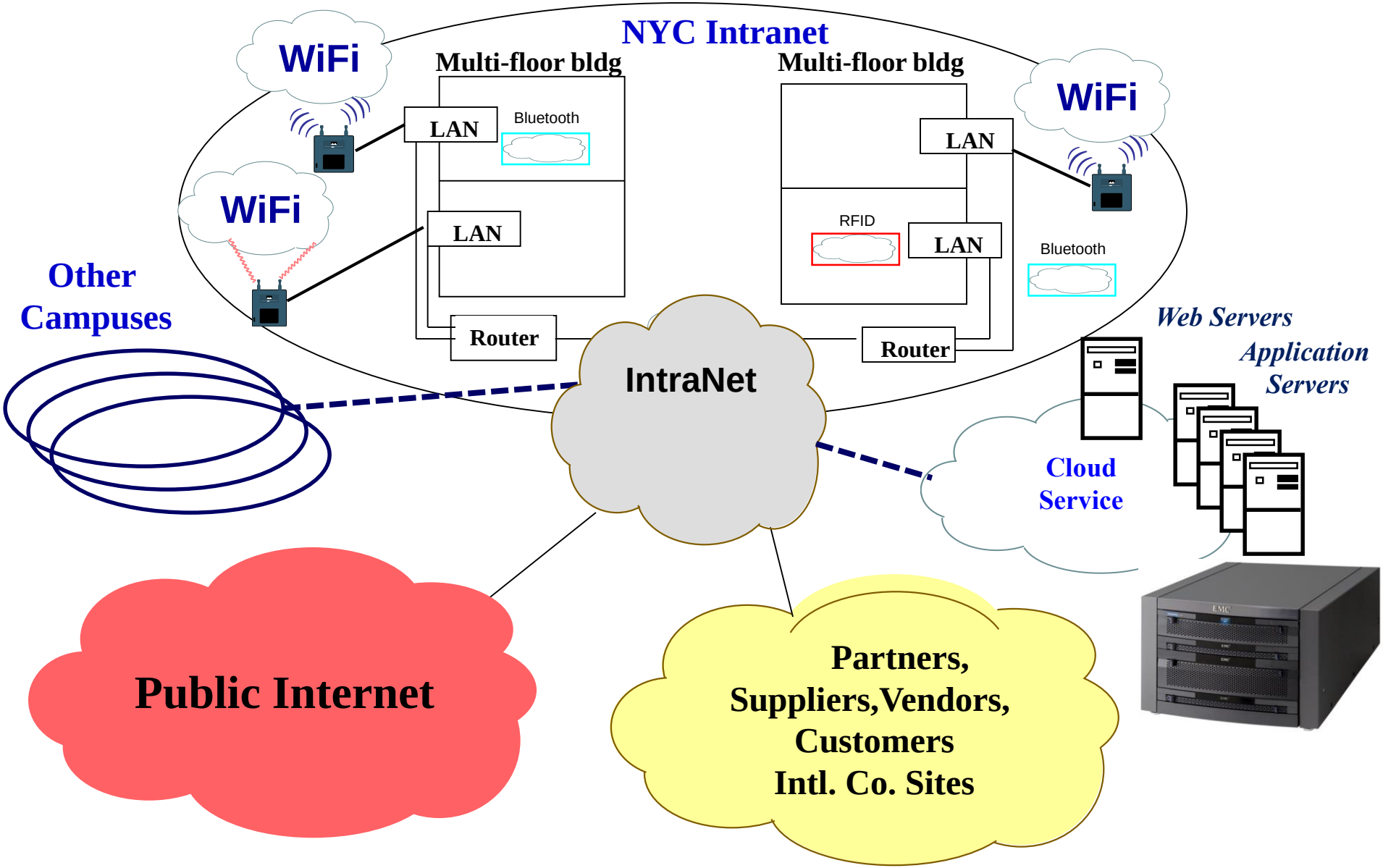
Considering MiFi in workplace policy (allowing)

Design data (used to build products) on nearly everyone's laptops considered competition sensitive.

Application and Web Servers moved offsite to Amazon Cloud Service

Data Management about to generate PO on 100 handheld readers for factory and office RFID testing

4 Multi Bldg Campuses (LA, NYC, Sea, Wash DC)



Threats

Onsite visitor, contractor, supplier BYOD

Snooping

password attack

USB (w/malware) ,

Threats

Contractor, supplier machines, complaining passwords are impacting productivity

Threats

Visited infected Website – browser (infected w/malware)

Threats

System and App Admins allowed remote access for support, troubleshooting.

Threats

Need to change trust rights on application server on Cloud Services data center

Threats

Users can install any software on work computers including malicious as currently all users have elevated rights

Threats

Compromised Wifi/RF Environment

Starbucks builds café on bottom floor of your corp headquaters

Bonus attack – remote sharing/access, Bluetooth, adhoc wireless attack

Threats

Compromise Fiber Optic Cable

(or telecommunications carrier infrastructure)

Fiber should be terminated into locked/alarmed patch panels

Threats

Malware installed when user took laptop home and company policy still permits elevated privileges and installing s/w by end user

Threats

Snooping (LAN)

Threats

Snooping (WLAN/WiFi)

Threats

Unauthorized Device on Network

Threats

Passwords Stolen/Copied

Threats

Trojan (inside email)

Threats

Trojan (inside email)

Threats

ISP (Internet Service Provider)

compromised

Denial of Service attack - You have backup ISP ?

Threats

Wireless Man in Middle (Eavesdropping)

Threats

Unauthorized device

(night janitor plugs into internal - LAN active port and adds sensor, monitor or camera)

Threats

Employees going to “bad” websites

Threats

Accounting Employee purchased WiFi Access Point at Frys, bought to work to enable wireless/mobility for his workgroup – IT told him 3-5 weeks to get Cisco ordered/delivered AP was affecting Acct productivity

Threats

Insider Attack – PII Stolen (Employee records and SSN), HR Dir lost laptop that had copy of records

Disgruntled Employee

Threats

Employees storing Engineering data on laptops (as opposed to engineering computing servers)

Threats

Family member borrows your laptop at home (just few minutes) to print & browse www to look up movie review

Now laptop has malware/virus

Threats

Able to copy files and data from storage area network (SAN) in data center environment. Doesn't authenticate sources (that are writing)