

UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI MATEMATICA

Corso di Laurea in INFORMATICA



**Monitoraggio e sicurezza fisica di
Campus Area Network**

Tirocinante: Mirco Cailotto, mat. 1123521

Relatore: Dott. Paolo Baldan

Azienda Ospitante: Wintech Spa

Tutor aziendale: Roberto Pezzile

Anno Accademico 2017/2018

Todo ringraziamenti.

Indice

Sommario

Convenzioni tipografiche

1	Contesto aziendale	1
1.1	Dominio applicativo	1
1.1.1	Com'è cambiata la Cybersecurity negli ultimi anni?	1
1.1.2	La proposta di Wintech	2
1.2	Tipologia di clientela aziendale	2
1.3	Processi aziendali	2
2	Progetto di stage	3
2.1	Pianificazione	3
2.1.1	Fase 1: Analisi	3
2.1.2	Fase 2: Progettazione	3
2.1.3	Fase 3: Implementazione	4
2.1.4	Fase 4: Test in produzione	4
2.1.5	Fase 5: Tuning	5
2.2	Obiettivi	5
2.2.1	Obiettivo aziendale	5
2.2.2	Obiettivo formativo	5
3	Tecnologie	6
3.1	Tecnologie per il monitoraggio	6
3.1.1	PRTG Network Monitor	6
3.1.2	Observium	7
3.1.3	RConfig	7
3.2	Tecnologie per la sicurezza	8
3.2.1	802.1X	8
3.2.2	Extensible Authentication Protocol	9
3.2.3	Windows Network Policy Server	9

3.2.4	Active Directory	9
3.2.5	CAPsMAN	10
3.3	Strumenti di lavoro	11
3.3.1	Microsoft Visio	11
3.3.2	OpenOffice Calc	11
3.3.3	GreaseMonkey	12
3.3.4	Putty	12
3.3.5	Microsoft Telnet	13
3.3.6	MySQL Command-Line Tool	13
3.3.7	Notepad++	13
3.3.8	Vim	14
3.3.9	FileZilla	14
4	Realizzazione	15
4.1	Analisi	15
4.1.1	Lista apparati	15
4.1.2	Analisi sistemi di sicurezza fisica	16
4.1.3	Analisi sistemi di monitoraggio	16
4.1.4	Schema di rete	17
4.2	Progettazione	19
4.2.1	Aggiornamenti configurazioni di rete	19
4.2.2	Nuove politiche di sicurezza fisica	19
4.2.3	Nuove politiche di sicurezza logica basata su 802.1X	19
4.2.4	Progettazione Observium	19
4.2.5	Progettazione rConfig	20
4.2.6	Definizione name-convention	21
4.2.7	Inserimento nomi DNS nella lista degli apparati	22
4.2.8	Lista dei test e risultati previsti	22
4.2.9	Produzione della prima bozza della documentazione progettuale	22
4.3	Implementazione	23
4.3.1	Creazione di un laboratorio con un nuovo switch dove verranno testate le configurazioni prima di andare in produzione	23
4.3.2	Inserimento su DNS interno degli hosts	23
4.3.3	Implementazione Virtual Machine	23
4.3.4	Configurazione di base software RConfig	23
4.3.5	Configurazione di base software monitoraggio Observium . .	24
4.3.6	Predisporre servizio NPS (Radius) sui due Active Directory servers	25
4.3.7	Creazione della configurazione di test per laboratorio con nuove funzionalità di sicurezza	25

4.3.8	Test nuove funzionalità con switch laboratorio	25
4.3.9	Creazione nuove configurazioni per tutti gli switch del Campus	25
4.3.10	Caricamento configurazioni negli switch del Campus	25
4.3.11	Test di base nuove funzionalità di sicurezza implementate . .	25
4.3.12	Scheduling backup delle impostazioni con rConfig	25
4.3.13	Aggiornamento della documentazione progettuale	26
4.4	Test in produzione	27
4.4.1	Monitoraggio eventuali anomalie, censirle, troubleshooting, idenfiticare la soluzione, trovare un workaround, implemen-tare e testare la soluzione	27
4.4.2	Aggiornare la documentazione	27
4.4.3	Upgrade Observium	27
4.5	Tuning	28
4.5.1	In sistema Observium avrà già acquisito dati da oltre un set-timana, verranno quindi configurate tutte le soglie di allarmi con notifica via email e instant message Telegram	28
4.5.2	Completamento della documentazione	28
5	Valutazione retrospettiva	29
5.1	Tempo impiegato	29
5.2	Risultati ottenuti	29
5.3	Vincoli del progetto	29
5.3.1	Vincoli tecnologici	29
5.3.2	Vincoli metodologici e di lavoro	30
5.3.3	Vincoli temporali	30
Appendici		32
Appendice A: Schemi di rete	32	
Appendice B: Script di popolamento rConfig	36	
Glossario		39
Bibliografia		41

Elenco delle figure

1.1	Logo di Wintech	1
3.1	Logo di PRTG	6
3.2	Logo di Observium	7
3.3	Logo di RConfig	7
3.4	Procedura di autenticazione 802.1X	8
3.5	Schema delle tecnologie per l'attualizzazione di 802.1X	9
3.6	Interfaccia di Visio	11
3.7	Interfaccia di Calc	11
3.8	Logo di GreaseMonkey	12
3.9	Schermata iniziale di Putty	12
3.10	Interfaccia di Notepad++	13
3.11	Interfaccia di Vim	14
4.1	Armadio di rete da esterni	16
4.2	Schermata di PRTG Network Monitor	17
4.3	Interfacce visualizzate all'interno di Observium	20
4.4	Attacco SQL injection su rConfig, sulla destra tutte le configurazioni navigabili	21
5.1	Schema Visio della rete datato 2015	33
5.2	Schema Visio della rete a fine stage, prima parte	34
5.3	Schema Visio della rete a fine stage, seconda parte	35

Sommario

Questo documento si prefigge lo scopo di presentare il lavoro svolto durante l'attività di stage, svolta presso Wintech Communications Factory.

Le attività sono state intraprese nell'ambito sistemistico, andando a monitorare e a migliorare la sicurezza di una Campus Area Network di dimensioni riguardevoli.

Gli argomenti trattati riguarderanno il controllo in tempo reale dello stato della rete, individuando colli di bottiglia, problematiche di varia natura e potenziali pericoli, attui a consentire un intervento tempestivo o preventivo.
Ulteriormente verrà trattata anche la sicurezza fisica delle reti, impedendo un accesso non autorizzato a risorse di elevata criticità a coloro che non posseggono dei privilegi sufficientemente elevati.

L'ultima parte di questo documento conterrà una mia valutazione personale retrospettiva sul lavoro svolto, nella quale valuterò i risultati formativi ed aziendali dello stage, evidenziandone i vincoli.

Convenzioni tipografiche

Per favorire la lettura del documento e la sua comprensione è stato introdotto un glossario.

Qualora un termine presente nel glossario comparisse all'interno del testo, in un contesto nel quale si suppone il lettore possa non comprenderlo, verrà evidenziato rispetto al paragrafo presentandolo scritto in corsivo e apponendogli in conclusione una "G" al pedice.

Nel caso si stesse visionando la versione digitale di questo documento è possibile essere reindirizzati direttamente al termine nel glossario semplicemente cliccandoci sopra.

Capitolo 1

Contesto aziendale

Nata nel 1987, Wintech Comumnication Factory SPA è ad oggi uno dei pochi *System Integrator_G* capace di vantare una lunga tradizione e un patrimonio di conoscenze nei diversi ambiti di competenza del settori ICT.

Tra le partnership si possono citare IBM, Symantec, Hewlett Packard, Microsoft, Oracle, VMware e Sophos.



Figura 1.1: Logo di Wintech

1.1 Dominio applicativo

Wintech opera in un dominio molto vasto, che spazia dal Cloud alla *Digital Transformation_G*, per tale motivo in questa sezione verrà analizzato unicamente il dominio relativo allo stage conseguito, cioè quello del monitoraggio e della sicurezza fisica delle reti.

1.1.1 Com'è cambiata la Cybersecurity negli ultimi anni?

Il panorama attuale per tipologia di attacchi e motivazioni, è profondamente mutato rispetto anche solo a qualche anno fa. Tutti gli osservatori sulla tematica Cybersecurity lo confermano con i dati. Non è fare terrorismo psicologico, ma essere realisti, quando si afferma che tutti si è potenzialmente vulnerabili e bersagli del cybercrime e quindi "is not a matter of if, but a matter of when".

Bisogna sfatare l'immaginario collettivo in cui siano solo le grandi società americane, grandi brand, ad essere attaccate per attivismo. Le motivazioni sono notevolmente mutate e hanno come target qualsiasi azienda, anche le realtà della piccole e medie imprese che costituiscono il tessuto delle aziende italiane sono pesantemente bersagliate.

1.1.2 La proposta di Wintech

La proposta per consentire di mantenere un elevato livello di sicurezza all'interno delle proprie reti proposto da Wintech si compone di svariate tecnologie, che vanno ad integrarsi per permettere una protezione completa su tutti i possibili fronti di attacco.

Le tecnologie illustrate in questo documento saranno una parte di quelle utilizzate all'interno dell'azienda, mirate al monitoraggio della rete, al controllo della configurazione degli apparati ed al port-based Network Access Control.

1.2 Tipologia di clientela aziendale

TODO mettere o no?

1.3 Processi aziendali

TODO chiedere a Lisa

Capitolo 2

Progetto di stage

Lo scopo dell'attività di stage è l'analisi, la progettazione e l'implementazione di un sistema di monitoraggio della sicurezza fisica di una LAN Campus.

Le conoscenze apprese durante lo svolgimento dell'attività consistono nella capacità di progettare ed implementare una soluzione per raggiungere gli obiettivi prefissati, oltre che ad effettuare attività di tuning per perfezionarla.

2.1 Pianificazione

Le attività sono state suddivise in cinque fasi principali, le quali andranno a coprire tutta la durata del percorso formativo stabilito.

2.1.1 Fase 1: Analisi

- **Periodo:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore:** 40h.

L'obiettivo di questa prima fase del percorso è familiarizzare con l'infrastruttura amministrata da Wintech e con i supporti hardware e software da utilizzare per la realizzazione del progetto.

Verranno analizzati lo schema di rete dell'infrastruttura, la lista degli apparati e delle loro caratteristiche, il sistema di sicurezza fisica attivi e il sistema di monitoraggio presenti.

2.1.2 Fase 2: Progettazione

- **Periodo:** dal 11/06/2018 al 22/06/2018;

- **Numero di ore:** 40h.

Nella seconda fase si procederà alla configurazione del software di monitoraggio Observium e del software di gestione della versione RConfig.

Per facilitare le attività verrà definita la nomenclatura da dare ai dispositivi.

Ulteriormente si procederà alla definizione delle logiche di sicurezza che verranno implementate basate sul protocollo 802.11X.

Durante questa fase verrà anche prodotta la prima bozza della documentazione progettuale.

2.1.3 Fase 3: Implementazione

- **Periodo:** dal 25/06/2018 al 06/07/2018;
- **Numero di ore:** 80h.

In questa fase è stata implementata la nuova infrastruttura e si sono resi operativi i software precedentemente configurati.

È stato creato un laboratorio con uno nuovo switch sul quale sono state testate le politiche precedentemente scelte per valutarne l'efficacia.

Una volta completata questa fase si procederà alla creazione delle nuove configurazioni per tutti gli switch comprendenti la nuova politica di sicurezza e la loro installazione.

Oltre a questo i dispositivi verranno inseriti all'interno del DNS e verranno resi operativi i software Observium e RConfig.

Durante questo periodo la documentazione progettuale verrà aggiornata di conseguenza alle attività svolte.

2.1.4 Fase 4: Test in produzione

- **Periodo:** dal 09/06/2018 al 13/07/2018;
- **Numero di ore:** 40h.

La fase di test in produzione è la più importante perché verrà messo alla prova l'intero sistema con il picco dell'utenza.

L'attività che verrà svolta è il monitoraggio di eventuali anomalie, per poi procedere con il censirle, cercare la fonte del problema, identificare una soluzione ed implementarla.

Durante questo periodo la documentazione progettuale verrà nuovamente aggiornata di conseguenza alle attività svolte.

2.1.5 Fase 5: Tuning

- **Periodo:** dal 16/07/2018 al 27/07/2018;
- **Numero di ore:** 80h.

Nella fase finale del progetto sono stati eseguiti tuning su tutta la rete, ove possibili, sia sugli apparati che nelle configurazioni dei software.

Questa attività sarà supportata dal software Observium, che nel frattempo avrà raccolto una mole di dati tale da permettere uno studio dei miglioramenti effettuabili.

Un'altra attività derivante dallo studio dei dati raccolti sarà la configurazione delle soglie di alarmi automatici, che verranno comunicati tramite messaggio e-mail e Telegram.

In questa ultima fase si procederà anche a completare la documentazione.

2.2 Obiettivi

2.2.1 Obiettivo aziendale

L'obiettivo a fine stage è aumentare la sicurezza fisica di una LAN Campus dove accedono migliaia di persone, impedendo l'uso illecito e non controllato dei servizi di rete, sabotaggi e furto di dati.

Questo comprende l'implementazione di software di monitoring e lo sfruttamento dei servizi avanzati che offrono per ottenere le migliori performance ed il miglior controllo possibile.

2.2.2 Obiettivo formativo

L'obiettivo per il tirocinante è acquisire competenze in ambito networking e security in un contesto reale quale una LAN Campus estesa, variegata e con un numero di utenti elevato.

Questo al fine di permettergli di mettere in pratica le conoscenze acquisiti durante lo svolgimento dei corsi universitari e fornirgli un forte stimolo ad approfondire ancora di più queste tematiche.

Capitolo 3

Tecnologie

Questa sezione illustra le principali tecnologie utilizzate nel corso dello stage per il controllo, il monitoraggio e la sicurezza delle reti di loro competenza.

Essendo la sicurezza informatica un settore nel quale gli standard, le leggi e le tipologie di attacco evolvono molto in fretta, le tecnologie utilizzate devono adeguarsi di conseguenza. Questo porta i tool ed i programmi utilizzati a diventare obsoleti oppure variare con il passare del tempo.

3.1 Tecnologie per il monitoraggio

3.1.1 PRTG Network Monitor

PRTG è un sistema di monitoraggio della rete, era utilizzato nella rete analizzata durante lo stage prima di Observium per rilevare eventuali anomalie, ma a causa delle limitazioni della versione gratuita e del suo elevato costo si è scelto di sostituirlo.

Il software consiste in un servizio al quale ci si collega mediante il client fornito oppure attraverso una interfaccia web e permette di tenere sotto controllo anche siti web e servizi di varia natura.



Figura 3.1: Logo di PRTG

3.1.2 Observium

Observium è un sistema di monitoraggio della rete compatibile con i dispositivi delle principali aziende produttrici di apparati di rete.

Tra i dispositivi supportati si possono citare Cisco, Dell, HP, Huawei, Lenovo, MikroTik, Netgear e ZTE.

Il software dispone anche di una ricerca automatica dei dispositivi presente all'interno della rete, utile per reti di piccola-media dimensione.

Le funzionalità che fornisce sono il monitoraggio del *Quality Of Service*, il raggruppamento dei dispositivi mediante regole definite dall'utente e l'alert automatico nel caso vengano superate determinate soglie.



Figura 3.2: Logo di Observium

3.1.3 RConfig

Il tool RConfig è un configuration management mirato ai dispositivi di rete che permette in modo veloce ed automatizzato di effettuare una copia delle configurazione degli apparati di rete.

È completamente open source, protetto da licenza GNU v3.0, ed è scritto in linguaggio PHP, questo gli consente di essere installato facilmente su molti sistemi.



Figura 3.3: Logo di RConfig

3.2 Tecnologie per la sicurezza

3.2.1 802.1X

Il 802.1X è uno standard IEEE per il controllo di accesso alla rete port-based, parte della famiglia di protocolli IEEE 802.1. Fornisce un meccanismo di autenticazione mediante una combinazione username/password oppure un certificato digitale. Questa protezione va ad ampliare la *sicurezza fisica*_G delle risorse connesse alla rete, pur essendo di per sè una *sicurezza logica*_G, impedendone il raggiungimento ai dispositivi non autorizzati.

Lo standard viene implementato all'interno del firmware o del sistema operativo degli apparati di rete e dei dispositivi degli utenti.

Funziona sia su connessioni wired che wireless, anche se viene raramente utilizzato nelle connessioni cablate in quanto, erroneamente, una protezione fisica perimetrale viene considerata sufficiente.

Il 802.1X determina unicamente la procedura di autenticazione che deve essere svolta, mentre la definizione degli standard dei messaggi e del trasporto viene definita da altri standard.

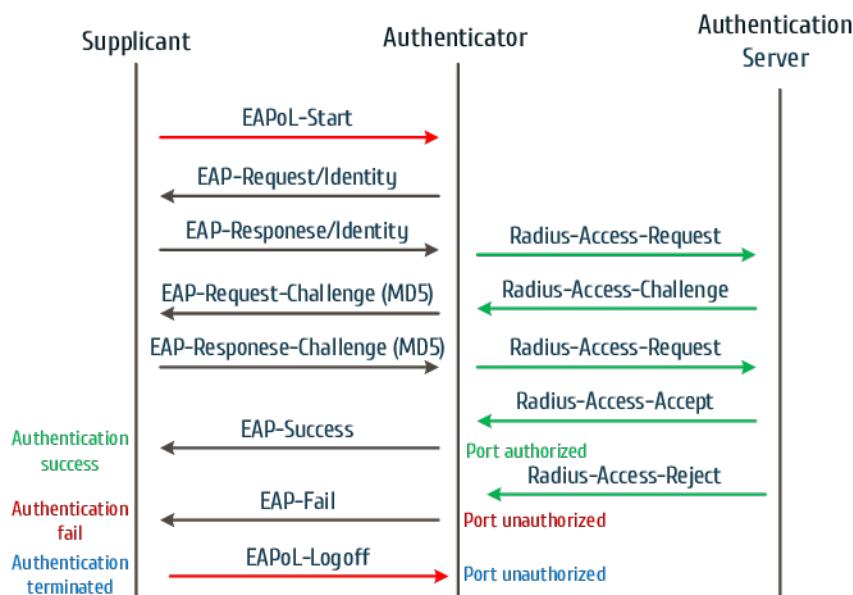


Figura 3.4: Procedura di autenticazione 802.1X

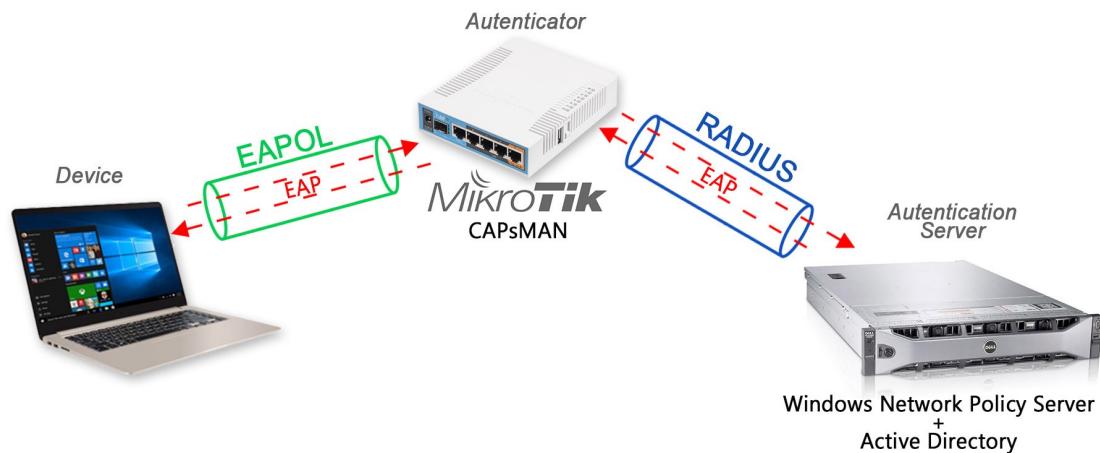


Figura 3.5: Schema delle tecnologie per l'attualizzazione di 802.1X

3.2.2 Extensible Authentication Protocol

Extensible Authentication Protocol, usualmente chiamato semplicemente EAP, è un framework di autenticazione che definisce la struttura dei messaggi. Lo standard include svariate tipologie di messaggio, in modo tale da poter fornire molteplici metodologie di login, come ad esempio combinazioni username e password, utilizzo di certificati o mediante un segreto condiviso. Non essendo un protocollo di rete ha la necessità di essere incapsulato in un messaggio per poter essere inviato, ad esempio all'interno del protocollo $RADIUS_G$ oppure nel protocollo di rete dedicato $EAPoL_G$.

3.2.3 Windows Network Policy Server

Network Policy Server, spesso abbreviato in NPS, in italiano "Server dei criteri di rete", è una tecnologia per il controllo dell'accesso alla rete.

Decreta chi può accedere alla rete ponendo delle restrizioni ed utilizzare il protocollo $RADIUS_G$ per comunicare.

Un server che lo implementa può decretare indipendentemente l'accesso o meno dei vari dispositivi, costituendo quindi un RADIUS server, oppure può inoltrare la richiesta ad un altro server NPS, quindi coprendo il ruolo di RADIUS proxy.

3.2.4 Active Directory

Active Directory è un insieme di servizi di rete adottati dai sistemi operativi Microsoft.

Sono gestiti da un $Domain Controller_G$ e gestisce le modalità di accesso alle risorse

da parte degli utenti.

Le risorse possono essere account utente, account relativi a un computer, cartelle condivise, stampanti e servizi di varia natura. I privilegi di accesso alle varie risorse sono determinati mediante dei criteri di gruppo.

3.2.5 CAPsMAN

CAPsMAN, per esteso Controlled Access Point system Manager, traducibile in "sistema di gestione di access point controllati", è una funzionalità per la gestione degli accessi fornita da MikroTik assieme ai suoi access point.

Permette di identificare i client che si connettono comunicando con un server RADIUS, per poi reindirizzarli automaticamente verso una VLAN adeguata al loro ruolo.

Consente anche la configurazione automatica degli SSID e dei canali di comunicazione secondo indicazioni di altri dispositivi CAPsMAN.

TODO FORSE - PHP, MySql e Javascript per pagina di login

3.3 Strumenti di lavoro

3.3.1 Microsoft Visio

Microsoft Visio è uno strumento dedito alla creazione di grafici ed organigrammi. Nell'abito dello stage si è rivelato utile per la creazione della mappa della rete, in quanto facilmente utilizzabile e mantenibile anche da persone senza una elevata conoscenza dell'informatica o di linguaggi dediti allo scopo.

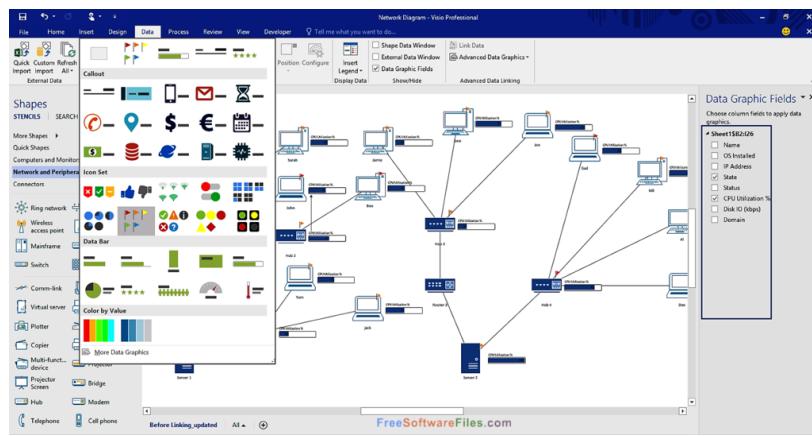


Figura 3.6: Interfaccia di Visio

3.3.2 OpenOffice Calc

OpenOffice Calc è un software per la gestione di fogli elettronici, che consente anche di aprire i formati gestiti da LibreOffice Calc e Microsoft Excel.

È stato impiegato per la realizzazione della lista dei dispositivi, in quanto consente una consultazione veloce e l'esportazione in svariati formati.

	A	B	C	D	E	F	G	H	I	J
1	Country	Population (per 1k)	Downloads Wikipedia	Internet Users per 1k	AOO per 1K population	AOO per 1K internet users	(AOO per Population) Users	Rank (AOO per Internet)		
188	San Marino	1.067	32,457	15,781	32,674	68	13	4		
189	Netherlands	568.068	16,751,323	15,371,298	39,912	37	12	14		
190	Malta	100	100	93	9,908	3017	34	11	18	
191	Finland	212.462	5,387,000	4,700,192	48,362	45	10	10		
192	Switzerland	333.002	8,000,000	6,688,285	41,626	50	9	9		
193	Estonia	56,256	1,294,000	981,467	42,701	56	8	7		
194	Germany	3,602,587	81,799,900	67,621,622	44,042	53	7	8		
195	Belgium	529,150	11,041,266	8,136,552	47,925	65	6	6		
196	Ukraine	224,151	4,570,610	13,811,224	49,042	16	5	44		
197	Italy	3,160,660	60,813,326	34,657,545	51,973	91	4	2		
198	Luxembourg	29,768	517,000	457,451	57,617	65	3	5		
199	Monaco	2,346	35,000	22,940	67,086	102	2	1		
200	Portugal	1,040,000	41,982,832	38,896	994	2	1	1		

Figura 3.7: Interfaccia di Calc

3.3.3 GreaseMonkey

GreaseMonkey è un plugin disponibile per il browser Mozilla Firefox che consente l'esecuzione di script in linguaggio JavaScript.

Permette anche lo store di variabili, il caricamento di librerie esterne e l'esecuzione con permessi privilegiati.

È stato utilizzato durante le attività di stage per automatizzare operazioni ripetitive, consentendo di impiegarci meno tempo, da dedicare ad altre attività.



Figura 3.8: Logo di GreaseMonkey

3.3.4 Putty

Putty è un client SSH, Telnet e seriale combinato con un emulatore di terminale per consentire una iterazione con dispositivi remoti.

È stato ampiamente utilizzato per le connessioni SSH e seriale per la configurazione e il controllo dei dispositivi di rete.

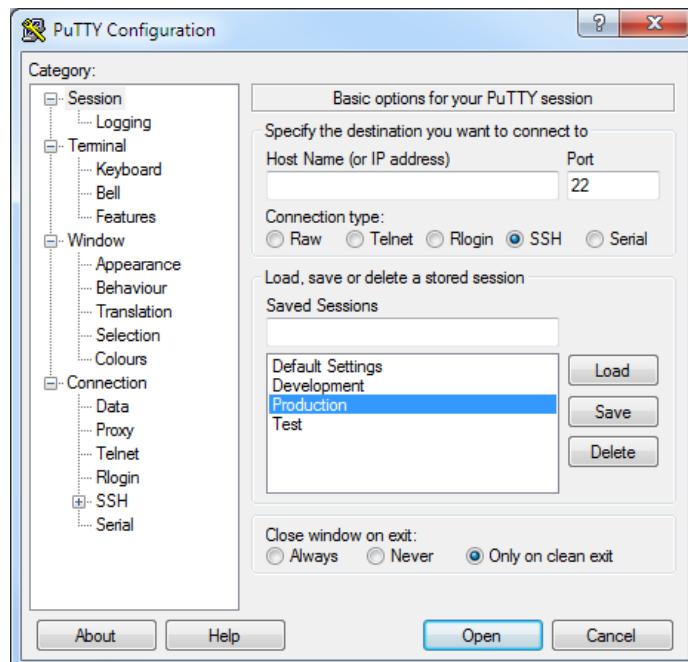


Figura 3.9: Schermata iniziale di Putty

3.3.5 Microsoft Telnet

Il client Telnet fornito assieme al sistema operativo Microsoft Windows permette di collegarsi a dispositivi remoti tramite protocollo Telnet mediante un qualsiasi terminale.

È stato preferito a Putty per il fatto che risulta più veloce ed immediato da utilizzare, in quanto accessibile direttamente dalla console del sistema.

3.3.6 MySQL Command-Line Tool

La shell MySQL è in interfacciamento a linea testuale al database MySQL, che permette una iterazione con la struttura ed i dati in esso contenuto.

Nell'ambito del progetto è stato impiegato principalmente in concomitanza con rConfig, in quanto l'incompletezza del programma ha richiesto svariate volte una modifica manuale alla base di dati dalla quale attingeva le informazioni.

3.3.7 Notepad++

Notepad++ è un editor di file testuali disponibile per sistemi operativi Microsoft Windows.

La sua utilità nell'ambito del progetto è stata l'esecuzione di espressioni regolari per permettere una rapida conversione del formato dei dati, consentendo di convertire file CSV in matrici JavaScript.

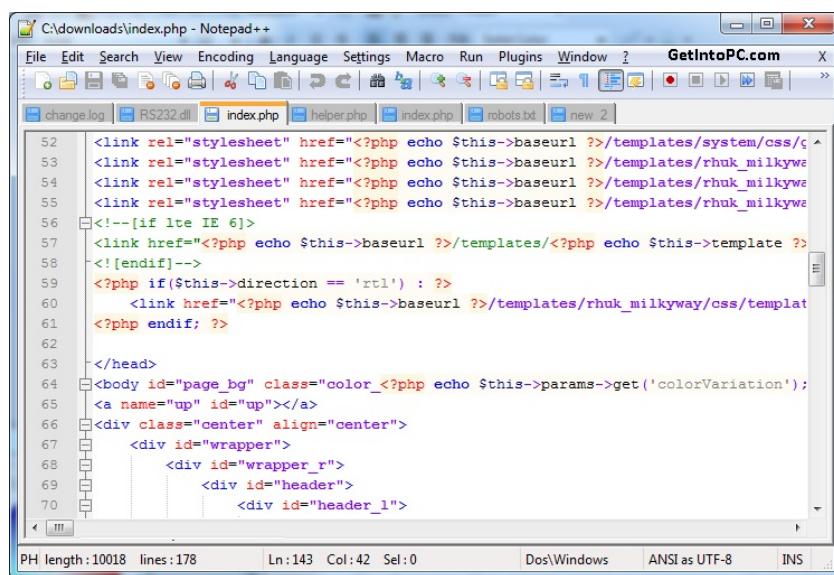


Figura 3.10: Interfaccia di Notepad++

3.3.8 Vim

Vim è un editor di file testuali disponibili su molteplici piattaforme, di storica rilevanza nel mondo Unix.

Essendo spesso preinstallato, disponibile per un numero elevato di sistemi ed eseguibile da terminale si è rivelato comodo per la modifica dei file di configurazione sulle macchine virtuali, grazie anche alle sue modalità di iterazione con il testo.

Figura 3.11: Interfaccia di Vim

3.3.9 FileZilla

Gestire i file su MikroTik - per il login?

Capitolo 4

Realizzazione

4.1 Analisi

- **Periodo previsto:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore previste:** 40h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

Una delle prime attività svolte è stata la raccolta della documentazione preesistente e la sua analisi.

Sono subito emerse svariate incongruenze tra i vari documenti in quanto alcuni erano datati, per questo motivo si è dovuto confrontarli, individuare l'informazione corretta ed aggiornare gli altri.

4.1.1 Lista apparati

Come base di questa attività si sono utilizzati alcuni documenti Excel con riportate informazioni sparpagliate sui dispositivi, le quali sono state integrate tra di loro. Da questa attività è emerso che c'erano informazioni assenti per alcuni devices, che sono state recuperate e documentate.

Successivamente si è andato ad aggiungere la posizione GPS di ogni dispositivo, utilizzando i dati presenti nel software di monitoraggio PRTG e individuando, con l'aiuto di Google Maps, le coordinate mancanti.

I dispositivi possedevano già dei nominativi che ne indicavano la locazione all'interno del contesto, che sono stati mantenuti.

4.1.2 Analisi sistemi di sicurezza fisica

La sicurezza fisica era perseguita prevalentemente controllando l'accesso fisico ai dispositivi di rete. Gli switch sono chiusi a chiave negli appositi armadi e, ove possibile, mantenuti all'interno di strutture dove l'accesso è consentito solo al personale.

Esiste una struttura di VLAN attua a impedire l'accesso alle risorse a coloro che non ne possiedono i permessi, ma da sola non era sufficiente a garantire la sicurezza.

Un possibile attacco che si poteva praticare era forzare un armadietto di rete, costruiti in plastica, ed utilizzare una porta Ethernet untagged per poter connettersi ai dispositivi di quella VLAN. Questo risulta molto pericoloso considerando che la VLAN di manutenzione, presente in quasi tutti gli switch, permette l'accesso a tutti gli altri apparati di rete.

Analogo discorso per le reti wifi dedicate al personale, nelle quali spesso si connettono dispositivi personali o si forniscono le chiavi di autenticazioni ad amici e parenti, mettendo a rischio le risorse raggiungibili.

In questo contesto si è andati ad operare sul controllo d'accesso, impedendo ad un dispositivo non riconosciuto di entrare in una VLAN semplicemente connettendosi ad una rete, ma richiedendogli informazioni aggiuntive e certificate mediante lo standard 802.1X.



Figura 4.1: Armadio di rete da esterni

4.1.3 Analisi sistemi di monitoraggio

La rete analizzata presentava già un software per il monitoraggio, denominato PRTG Network Monitor.

Il suo compito era quello di controllare che tutti i sensori in esso inseriti appartenenti ai devices funzionassero correttamente, avvisando qualora ci fossero dei problemi.

Una delle problematiche fondamentali di questo software era la difficoltà nel tracciare grafici relativi alla connessione e alla qualità del servizio, impedendo di identificare eventuali colli di bottiglia, pacchetti persi o errori di trasmissione.

Questo software veniva utilizzato in versione gratuita e quindi presentava alcune limitazioni, la più problematica è la quantità di sensori che può monitorare, limitata a 1000, che non consentiva di controllare in modo soddisfacente tutti gli apparati di rete presenti.

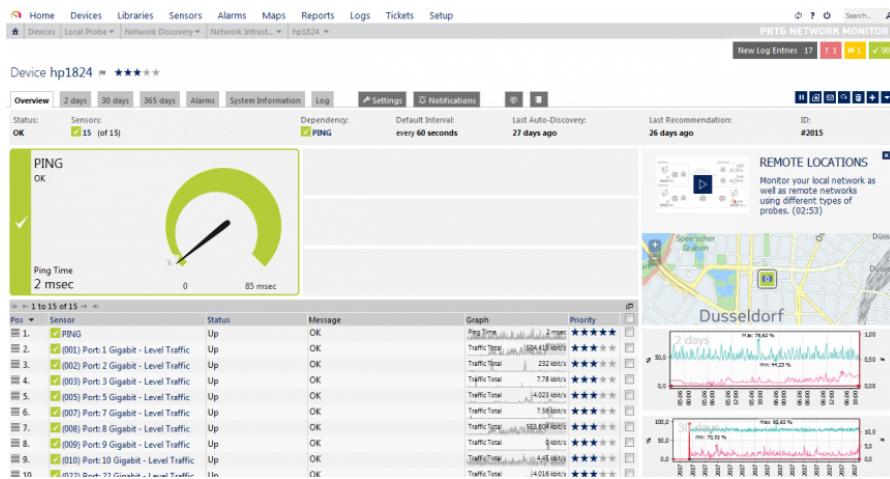


Figura 4.2: Schermata di PRTG Network Monitor

4.1.4 Schema di rete

Per facilitare tutte le attività successive di configurazione e monitoraggio si è proceduto alla redazione di uno schema di rete.

Essendo già disponibile uno schema datato 2015 della rete realizzato dal cliente in Microsoft Visio si è scelto di procedere con lo stesso software.

A supporto di questo lavoro si sono utilizzate svariate mappe prodotte in tempi e per fini diversi tra di loro, la cui integrazione ha evidenziato degli errori che sono stati segnalati.

La posizione degli apparati è stata modificata in modo da seguire più fedelmente la loro collocazione reale, favorendone una identificazione più veloce.

Lo schema di rete di partenza e quello realizzato, presentanti il nome, il modello di dispositivo e l'indirizzo ip, sono presenti in Appendice A.

Si può notare come nella prima versione c'erano molte incongruenze nella forma

nella quale sono stati riportati i dati, in quanto è stata prevalentemente scritta ed utilizzata da una singola persona e quindi non c'è stata attenzione rivolta alla chiarezza espositiva.

Alcune informazioni riportate sugli schemi sono state alterate o omesse per motivi di sicurezza e di privacy.

4.2 Progettazione

- **Periodo previsto:** dal 11/06/2018 al 22/06/2018;
- **Numero di ore previste:** 40h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

Una volta terminata la fase di analisi della rete si è proceduto a progettare le modifiche che saranno implementate.

4.2.1 Aggiornamenti configurazioni di rete

4.2.2 Nuove politiche di sicurezza fisica

4.2.3 Nuove politiche di sicurezza logica basata su 802.1X

4.2.4 Progettazione Observium

Prima di installare e mettere in funzione Observium lo si è provato localmente, andando ad individuare pregi e difetti del programma e comprendendo quindi quale fosse il miglior modo di utilizzarlo.

Inizialmente è stato istanziato inserendo al suo interno 5 apparati di rete, sui quali si sono testate svariate configurazioni per comprendere gli aspetti che potessero ritornare utili al monitoraggio della rete e quelli che, invece, non erano efficaci per il contesto.

Si è notato che la posizione GPS rilevata automaticamente del software era troppo imprecisa, ma la funzionalità era di elevata importanza visto l'estensione della rete. Si è dunque deciso di inserirle manualmente, sovrascrivendo il dato presente. Un'altra opzione che si è rilevata fondamentale era la disabilitazione delle interfacce non in uso, che altrimenti avrebbero generato avvertimenti inutili.



Figura 4.3: Interfacce visualizzate all'interno di Observium

Ulteriormente il software visualizzava anche l'area di appartenenza dei devices prelevandola dalla loro configurazione, ma risultava poco indicativa, quindi si è scelto di sovrascriverla indicando la locazione con più precisione.

4.2.5 Progettazione rConfig

Analogamente a quanto effettuato con Observium, anche per rConfig si è proceduto ad un suo test per comprenderne le potenzialità e la migliore modalità di utilizzo.

Sono stati inseriti anche per esso 6 dispositivi, in modo tale da avere almeno un dispositivo per ogni modello di apparato in utilizzo.

Si sono notati alcuni problemi, sia di utilizzo che di sicurezza, e di conseguenza si è dovuto fare particolare attenzione nella progettazione, in modo da impedire malfunzionamenti ed accessi non autorizzati.

Uno dei problemi di sicurezza riscontrati, che si è scoperto essere presente anche nelle altre istanze utilizzate dall'azienda, è una vulnerabilità *SQL injection*_G che permetteva di ottenere una lista completa dei report effettuati, compresi quelli rimossi o non accessibili per l'account in uso.

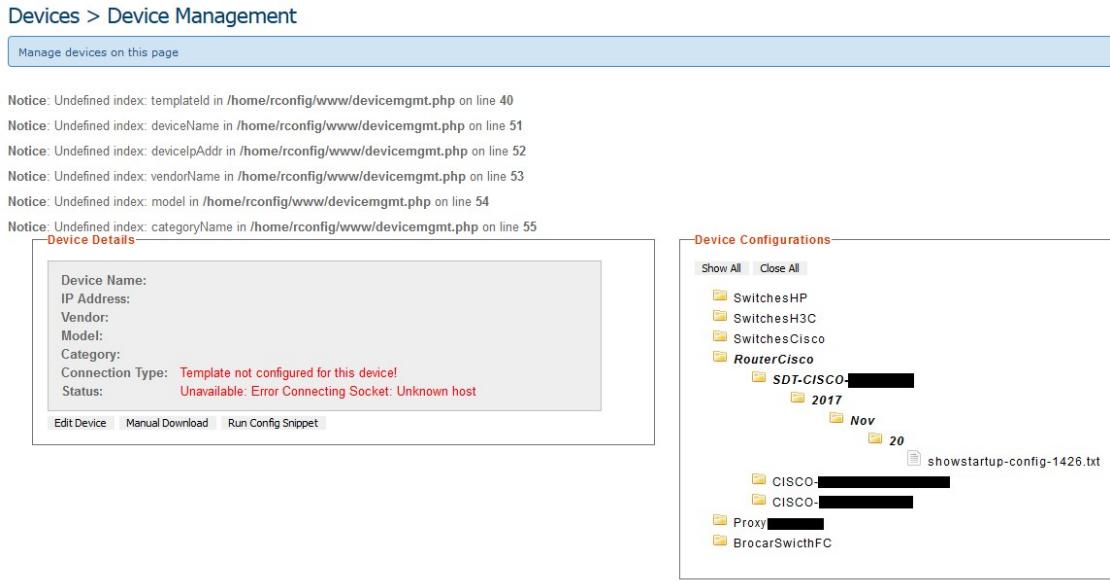


Figura 4.4: Attacco SQL injection su rConfig, sulla destra tutte le configurazioni navigabili

4.2.6 Definizione name-convention

La name-convention scelta per la denominazione degli apparati è la seguente:

DEVICE-ZONA [-LOCAZIONE] [-NUMERO_INC]

Nella quale i campi presenti indicano:

- **DEVICE:** Il modello del dispositivo installato, ad esempio "HP-2520-8-PoE";
- **ZONA:** La zona di appartenenza del dispositivo, ad esempio "ZONA-A", "EDIFICI" o "AMMINISTRAZIONE";
- **LOCAZIONE:** La locazione geografica utilizzata per identificare il dispositivo, opzionale nel caso basti la zona per l'identificazione univoca dell'armadio;
- **NUMERO_INC:** Numero incrementale, da utilizzare nel caso siano presenti più apparati nello stesso armadio di rete.

Questa convenzione è stata scelta in accordo con il cliente per permettere una identificazione veloce dell'apparato di rete anche ai manutentori, in linea con le denominazioni utilizzate internamente.

La presenza del modello di dispositivo è contrario alla best-practice da seguire,

in quanto la sostituzione di un apparato con un modello successivo richiede la sostituzione della voce all'interno del DNS e di conseguenza la riconfigurazione dei software di monitoraggio. Ciò è stato richiesto in quanto si favorisce l'immediatezza dell'identificazione del dispositivo a discapito della manutenibilità, tenendo in considerazione che gli upgrade non sono frequenti.

4.2.7 Inserimento nomi DNS nella lista degli apparati

Dopo aver definito la name-convention da utilizzare ed avere avuto l'approvazione dal cliente si è proseguito applicandola a tutti gli apparati.

È quindi stato individuato il nome DNS per ogni dispositivo ed è stato riportato all'interno del documento contenente la lista degli apparati.

4.2.8 Lista dei test e risultati previsti

TODO - cosa ci scrivo?

4.2.9 Produzione della prima bozza della documentazione progettuale

Durante questo periodo è stata scritta la prima bozza della documentazione. Si è proceduto ad inserire al suo interno la lista degli apparati, lo schema della rete e tutte le informazioni utilizzate durante queste prime settimane.

4.3 Implementazione

- **Periodo previsto:** dal 25/06/2018 al 06/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

4.3.1 Creazione di un laboratorio con un nuovo switch dove verranno testate le configurazioni prima di andare in produzione

4.3.2 Inserimento su DNS interno degli hosts

Per consentire una adeguata implementazione di Observium e rConfig era richiesto l'utilizzo dei nomi DNS degli apparati e non dell'indirizzo IP.

Si è dunque proceduto a comunicare la lista dei nomi e dei relativi IP dei dispositivi al responsabile affinché vengano inseriti nel sistema, in quanto non c'era la disponibilità di accedere direttamente alle impostazioni del DNS.

4.3.3 Implementazione Virtual Machine

Per consentire l'esecuzione continua dei software sono state create due Virtual Machine, o macchine virtuali.

Il server utilizzato per tale fine è quello del cliente, utilizzante le tecnologie prodotte da VMware per la virtualizzazione.

Le due macchine virtuali sono state entrambe create con Linux, in quanto gratuito e già conosciuto nel contesto aziendale.

4.3.4 Configurazione di base software RConfig

Per la configurazione di rConfig si è proceduto ad automatizzare l'inserimento dei dati, che altrimenti avrebbe consumato una ingente quantità di tempo visto il numero di dispositivi presenti.

Come base di riferimento per l'inserimento dei dati si è attinto dalla tabella dei dispositivi precedentemente realizzata, che è stata esportata in formato *csvG*.

Successivamente si è proceduto a modificare il formato dei dati esportati, operando per mezzo di una *espressione regolareG*, al fine di convertirlo in una matrice in linguaggio JavaScript per il suo utilizzo all'interno del browser.

Si è proceduto con lo sviluppo di uno script JavaScript, visionabile in Appendice B, che mediante il plug-in GreaseMonkey consentiva il caricamento automatico dei dati precedentemente posti in forma corretta.

Per terminare è stato eseguito lo script, che ha proceduto all'inserimento degli apparati.

4.3.5 Configurazione di base software monitoraggio Observium

Analogamente con quanto effettuato con RConfig si è proceduto all'inserimento di tutti i dispositivi e alla loro configurazione in Observium.

Questa operazione è stata più complessa rispetto all'altro software, in quanto richiedeva una aggiunta iniziale di ogni dispositivo, seguito dall'attesa della sua identificazioni per poi terminare con l'aggiunta delle informazioni aggiuntive. Seguendo quanto deciso nella fase di progettazione si è andato ad inserire, sempre mediante l'aiuto di GreaseMonkey, la sua locazione e le sue coordinate GPS.

Per completare l'attività si è anche dovuto segnalare al software tutte le interfacce non utilizzate, in modo tale che non venissero generati avvisi a causa della loro inoperatività.

Al termine dell'operazione gli elementi inseriti all'interno del software erano i seguenti:

- 85 switch;
- 2832 interfacce;
- 395 sensori;
- 264 componenti aggiuntivi.

I sensori presenti sono principalmente relativi all'alimentazione ed in alcuni casi alla temperatura del dispositivo, mentre i componenti aggiuntivi sono ventole di raffreddamento ed alimentazione.

Questi numeri dimostrano l'impossibilità di mantenere un controllo soddisfacente della rete utilizzando la versione gratuita di PRTG Netowrk Monitor, che consentiva in totale il monitoraggio di 1000 elementi.

4.3.6 Predisporre servizio NPS (Radius) sui due Active Directory servers

asd

4.3.7 Creazione della configurazione di test per laboratorio con nuove funzionalità di sicurezza

asd

4.3.8 Test nuove funzionalità con switch laboratorio

asd

4.3.9 Creazione nuove configurazioni per tutti gli switch del Campus

asd

4.3.10 Caricamento configurazioni negli switch del Campus

asd

4.3.11 Test di base nuove funzionalità di sicurezza implementate

asd

4.3.12 Scheduling backup delle impostazioni con rConfig

Per completare la messa in funzione di rConfig si è proceduto alla suddivisione dei dispositivi in gruppi secondo la loro locazione ed alla predisposizione di backup periodici.

Per non sovraccaricare la rete si è scelto di svolgere il backup a cadenza settimanale durante la notte, facendo attenzione a non sovrapporsi al backup giornaliero degli altri apparati. Gli orari stati scelti in modo tale che i task non si sovrappongano tra di loro, in modo di evitare eventuali problemi.

Questa attività si è rilevata più ostica del previsto a causa di molte problematiche di rConfig, rimaste per ora irrisolte anche nella versione in sviluppo.

Inizialmente si sono notati un numero di backup superiori a quanto schedulato. Questo avveniva perché le attività inserite e poi rimosse non risultavano più presenti dall’interfaccia web, ma rimanevano in esecuzione. Per arginare questo problema si è dovuto accedere direttamente al database dell’applicazione mediante MySql e correggere le informazioni in esso contenute.

Durante la correzione del problema precedente si sono rilevate altre anomalie all’interno del database, soprattutto dovute a una scarsa normalizzazione dei dati e a una strutturazione non adatta ad un database di tipo SQL. Pertanto si è dovuto controllare eventuali incongruenze e correggerle, in modo da evitare comportamenti inaspettati in futuro.

4.3.13 Aggiornamento della documentazione progettuale

Durante questa fase si è proceduto all’aggiornamento della documentazione, andando a descrivere le funzionalità dei programmi e delle tecnologie utilizzate, il loro utilizzo e tutti i problemi riscontrati, correlati dalla soluzione applicata per correggerli.

4.4 Test in produzione

- **Periodo previsto:** dal 09/06/2018 al 13/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

4.4.1 Monitoraggio eventuali anomalie, censirle, trubleshoo- ting, idenfiticare la soluzione, trovare un workaround, implementare e testare la soluzione

4.4.2 Aggiornare la documentazione

4.4.3 Upgrade Observium

Observium si è subito reso molto utile al monitoraggio della rete, questo ha portato alla decisione di acquistarne la versione professionale.

Le principali funzionalità offerte rispetto alla versione gratuita, definita Community, sono le seguenti:

- Update e fix costanti e non a cadenza di 6 mesi;
- Accesso alla repository SVN;
- Accesso alla versione beta;
- Raggruppamento dei dispositivi e delle interfacce in base alle loro caratteristiche;
- Metriche sulla qualità del servizio;
- Raggruppamento delle statistiche;
- Indicazione della tipologia degli errori di trasmissione;
- Ricerca di un dispositivo tramite IP o MAC address;
- Supporto da parte del team di sviluppo.

4.5 Tuning

- Periodo previsto: dal 16/07/2018 al 27/07/2018;
- Numero di ore previste: 80h;
- Periodo effettivo: ;
- Numero di ore effettive: .

4.5.1 In sistema Observium avrà già acquisito dati da oltre un settimana, verranno quindi configurate tutte le soglie di allarmi con notifica via email e instant message Telegram

4.5.2 Completamento della documentazione

Capitolo 5

Valutazione retrospettiva

5.1 Tempo impiegato

Descrizione dell'attività	Durata prevista	Durata effettiva
Analisi	40h	
Progettazione	80h	
Implementazione	80h	
Test in produzione	40h	
Tuning	80h	

5.2 Risultati ottenuti

5.3 Vincoli del progetto

5.3.1 Vincoli tecnologici

Statistiche VLAN

Una limitazione tecnologica attualmente presente in Observium è la sua incapacità di raggruppare le porte secondo la VLAN untagged che possiede.

Questo fatto, in concomitanza agli switch utilizzati che non permettevano la raccolta di statistiche dalle interfacce virtuali, comprendenti le VLAN, ha impedito di ottenere statistiche sull'utilizzo della rete suddivise per rete virtuale.

La limitazione non si sarebbe presentata con l'adozione di switch Cisco, in quanto essi raccolgono informazioni suddividendoli anche per VLAN, che possono poi essere raggruppati con facilità su Observium.

L'informazione che si sarebbe dovuta utilizzare per il raggruppamento delle porte

fisiche è già presente all'interno del database dell'applicazione, ed è già possibile utilizzarla per il filtraggio degli avvisi, ma non è ancora presente il filtro di raggruppamento.

5.3.2 Vincoli metodologici e di lavoro

5.3.3 Vincoli temporali

Appendici

Appendice A: Schemi di rete

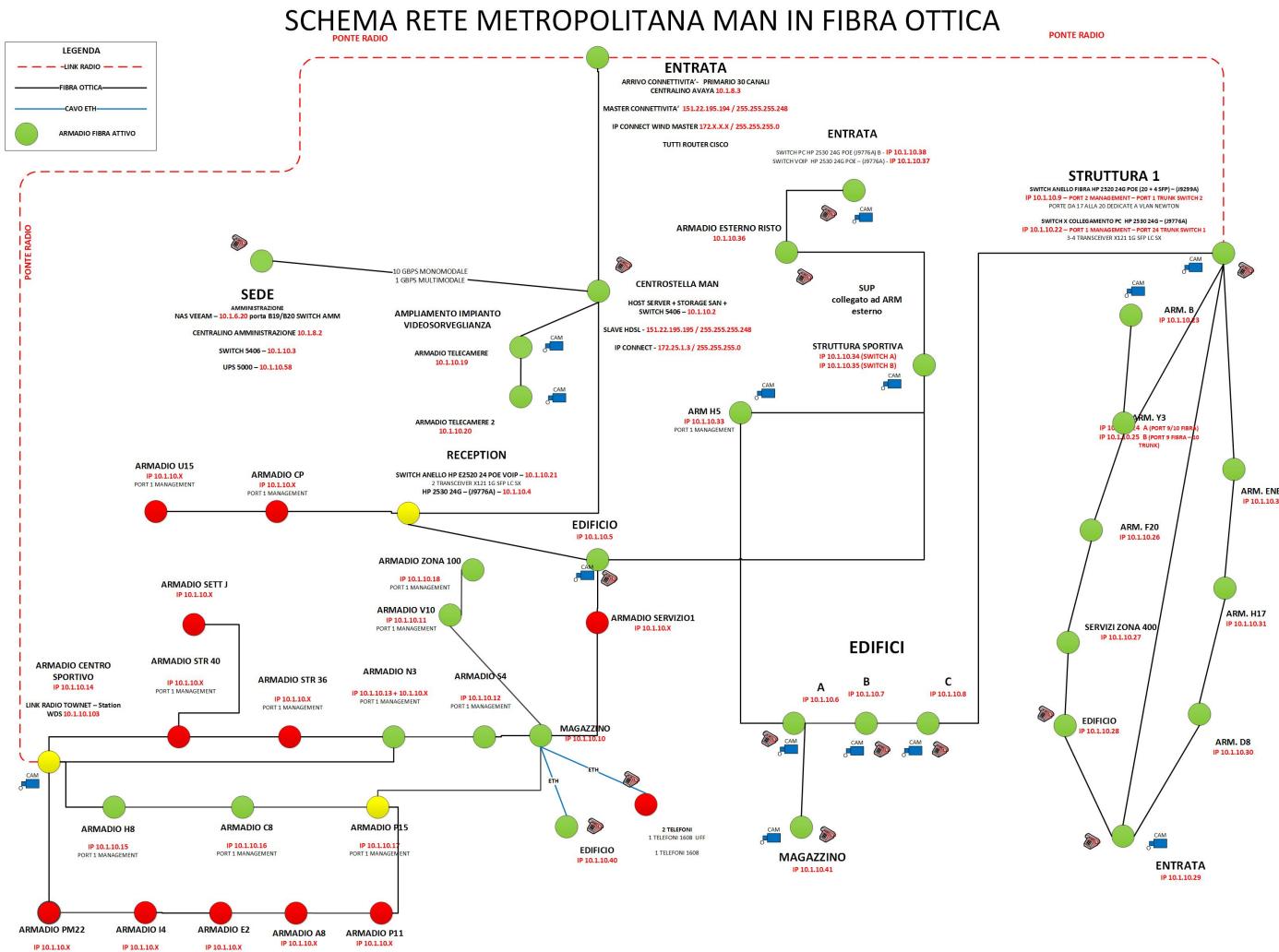


Figura 5.1: Schema Visio della rete datato 2015

SCHEMA RETE METROPO

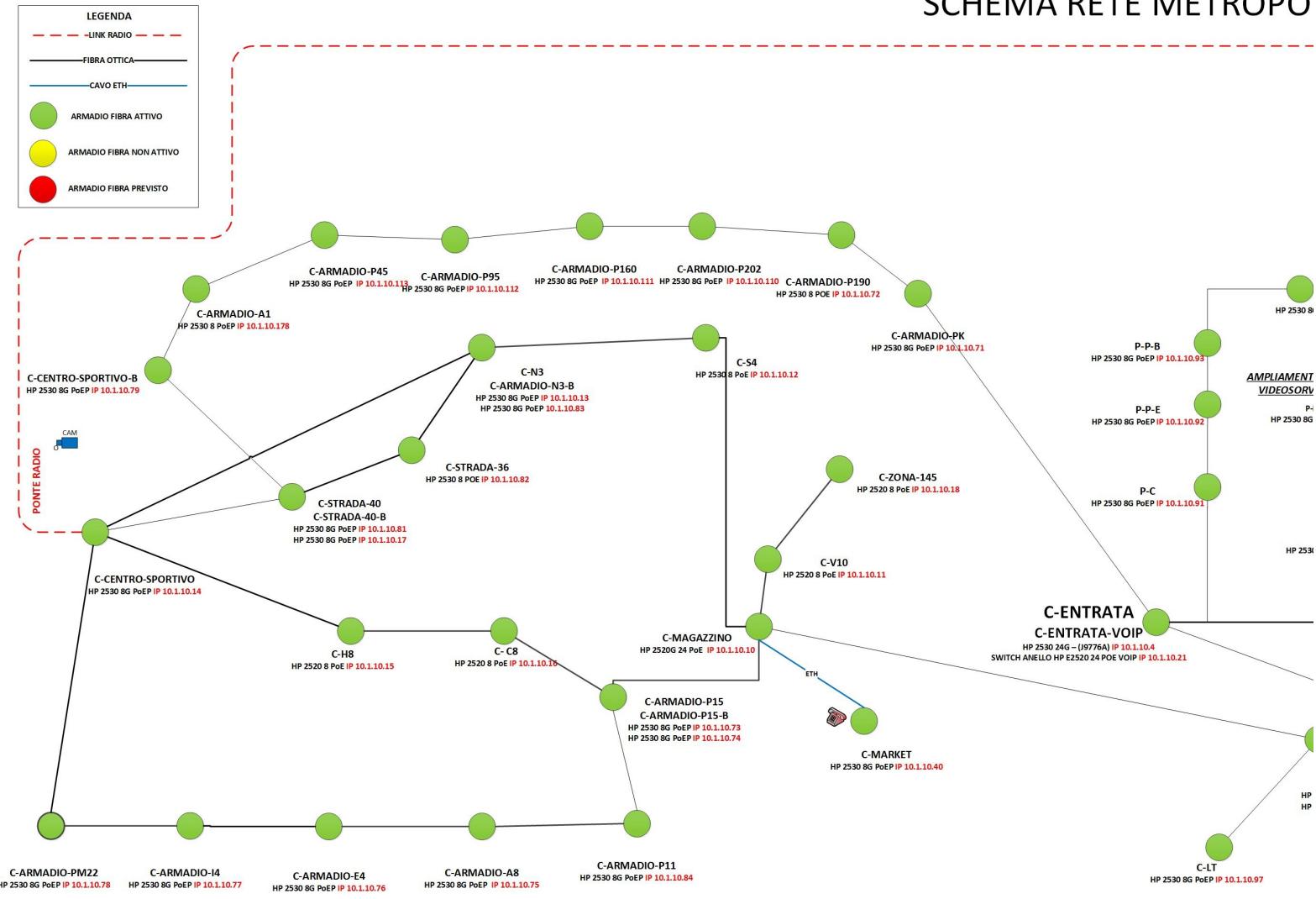


Figura 5.2: Schema Visio della rete a fine stage, prima parte

LITANA MAN IN FIBRA OTTICA

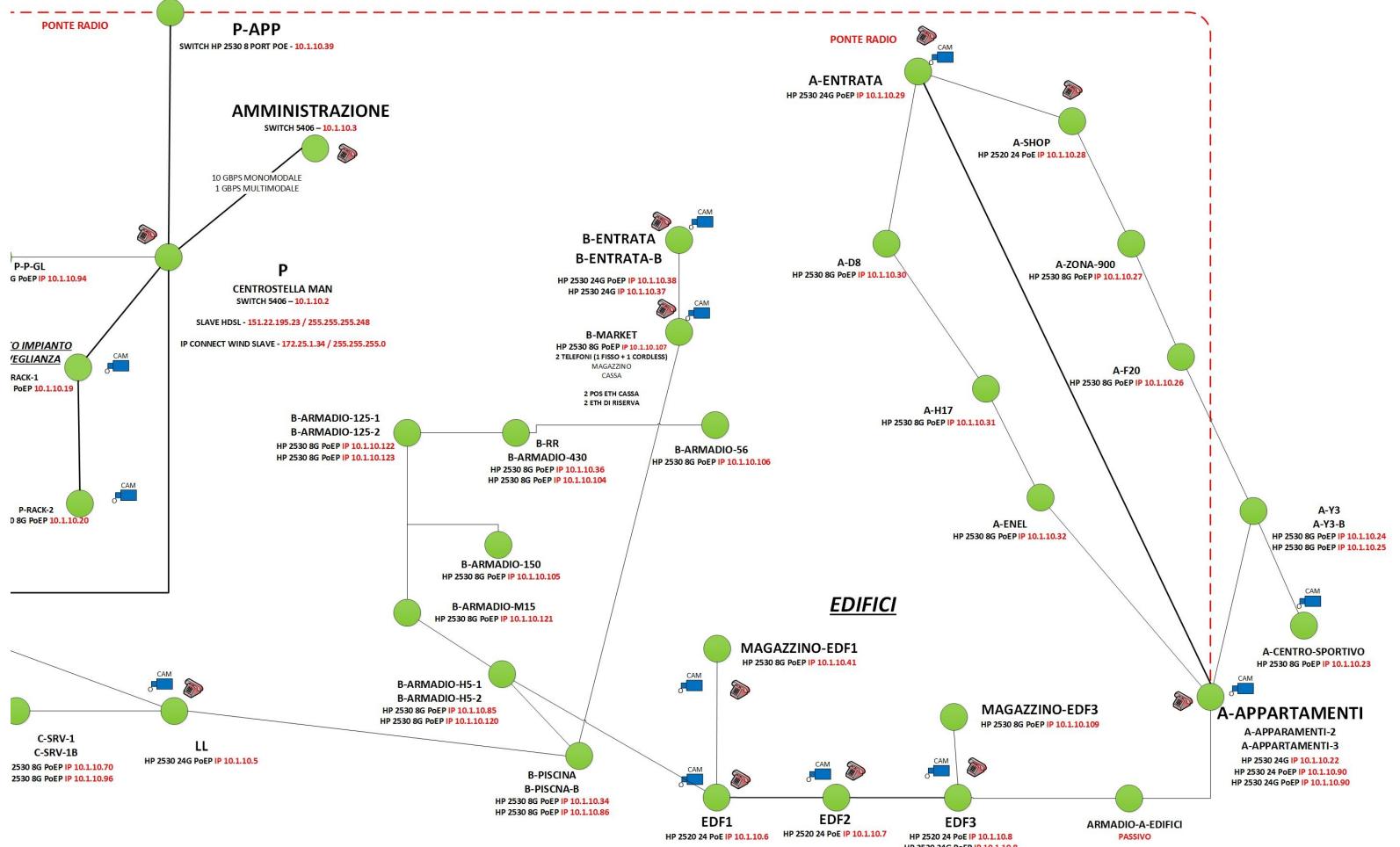


Figura 5.3: Schema Visio della rete a fine stage, seconda parte

Appendice B: Script di popolamento rConfig

Il codice sotto riportato è uno script in linguaggio JavaScript per il popolamento automatico, una volta inseriti i dati, di rConfig.

Lo script può essere utilizzato mediante il plug-in GreaseMonkey versione 4.0 o successive, in quanto richiede l'archiviazione di un valore nella memoria dell'estensione per funzionare.

```

1 // ==UserScript==
2 // @name      auto-insert-devices-rConfig
3 // @namespace MircoCailottoWintech
4 // @include   https://INDIRIZZO_RCONFIG/devices.php
5 // @version   1
6 // @grant     GM.setValue
7 // @grant     GM.getValue
8 // ==/UserScript==
9
10 // DATA
11
12 const data = [
13 ["INDIRIZZO-DISPOSITIVO-IN-DNS", "", "ENABLE-PROMPT#", "MARCA", "",
14   "MODELLO", "GRUPPO", "LOCAZIONE", "TEMPLATE_DI_RECUPERO_DATI"],
15 ["HP3850-24G-POE-C-ARMADIO-S123", "", "ARMADIO-S123#", "HP", "",
16   "HP3850-24G-POE", "SwitchesHP", "ClienteA", "HP Procurve SSH no
17   enable - HP-Procurve-SSH-no-enable.yml"],
18 ["HP3850-24G-POE-C-ARMADIO-C23", "", "C-ARMADIO-C23#", "HP", "",
19   "HP3850-24G-POE", "SwitchesHP", "ClienteA", "HP Procurve SSH no
20   enable - HP-Procurve-SSH-no-enable.yml"],
21 ];
22
23 function insertData(index) {
24   document.getElementById('deviceName').value = data[index][0];
25   document.getElementById('deviceEnablePrompt').value = data[index]
26     [1];
27   document.getElementById('devicePrompt').value = data[index][2];
28
29   var select = document.getElementById('vendorId');
30   for (var i = 0; i < select.options.length; i++) {
31     if (select.options[i].text === data[index][3]) {
32       select.selectedIndex = i;
33       break;
34     }
35   }
36
37   document.getElementById('deviceModel').value = data[index][4];
38 }
```

```

34     select = document.getElementById('catId');
35     for (var i = 0; i < select.options.length; i++) {
36       if (select.options[i].text === data[index][5]) {
37         select.selectedIndex = i;
38         break;
39     }
40   }
41
42   document.getElementById('custom_Location').value = data[index]
43     [6];
44
45   select = document.getElementById('templateId');
46   for (var i = 0; i < select.options.length; i++) {
47     if (select.options[i].text === data[index][7]) {
48       select.selectedIndex = i;
49       break;
50     }
51
52 //LOGIN
53   document.getElementById('defaultCreds').checked = true;
54 // document.getElementById('deviceUsername').value = "username";
55 // document.getElementById('devicePassword').value = "password";
56 // document.getElementById('deviceEnablePassword').value =
57   "passwordroot";
58 };
59
60 function clickOkButton() {
61   setTimeout(function(){
62     unsafeWindow.resolveDevice(document.getElementById('deviceName'
63       ).value);
64     setTimeout(function(){
65       document.getElementById("submit").click();
66     }, 500);
67   }, 500);
68 }
69
70 window.addEventListener('load', function() {
71   // once loaded
72   (async () => {
73     console.log("Async call");
74
75     // ----- RESET THE SCRIPT -----
76     var reset = false;
77
78     if(reset) {
79       GM.setValue('count', 0);
80     } else {
81       var index = await GM.getValue('count', 0);
82     }
83   });
84 }

```

```

80     if(index < data.length) {
81         //insert
82         console.log("Adding item number:");
83         console.log(index);
84         insertData(index);
85         GM.setValue('count', index + 1);
86         clickOkButton();
87     } else {
88         //done, do nothing
89         console.log("Already done");
90     }
91 }
92 }
93 })();
94 }, false);

```

Listing 5.1: Script GreaseMonkey di popolamento rConfig

Le linee 13, 14 e 15 sono 3 apparati che saranno inseriti alla esecuzione dello script, i campi sono:

1. Indirizzo DNS del dispositivo
2. Prompt del dispositivo in modalità non privilegiata, opzionale
3. Prompt del dispositivo in modalità privilegiata
4. Marca del dispositivo
5. Modello del dispositivo
6. Gruppo rConfig di appartenenza del dispositivo, utilizzabile per il filtraggio
7. Locazione del dispositivo, utilizzabile per il filtraggio
8. Template rConfig relativo alla configurazione da utilizzare per il recupero dei dati

Le linee 54, 55 e 56 presentano la possibilità di specificare i parametri per effettuare il login ai dispositivi, attualmente non utilizzati in quanto si utilizza le credenziali impostate come di default.

La linea 74 presenta un variabile "reset" che se impostata a true, invece che eseguire lo script, va ad azzerare i valori utilizzati dal plugin, permettendone una seconda esecuzione.

Glossario

CSV

Il formato CSV, ovvero Comma-Separated Values, è basato su file di testo composti da righe presentanti valori separati da una virgola. Non esiste uno standard formale che lo definisca, ma solamente alcune prassi più o meno consolidate.

Digital Transformation

La Digital Transformation, o trasformazione digitale, è quell'insieme di cambiamenti nei comportamenti aziendali e di business collegato e veicolato dalla tecnologia digitale, tramite il quale è possibile traguardare una maggiore competitività di mercato.

Domain Controller

Un Domain Controller (DC) è un server che, nell'ambito di un dominio, attraverso Active Directory (AD), gestisce le richieste di autenticazione per la sicurezza e organizza la struttura del dominio in termini di utenti, gruppi e risorse di rete fornendo dunque un servizio di directory service.

EAPoL

EAP over Lan, abbreviato in EAPoL, è un protocollo di rete generico che permette di incapsulare il protocollo EAP per essere trasmesso.

Espressione regolare

Una espressione regolare, in inglese Regular Expression, Regex o RE, è una sequenza di simboli che identifica un insieme di stringhe. Essa costituisce una funzione che prende in ingresso una stringa e ne restituisce una seconda.

Quality Of Service

La qualità del servizio, documentata mediante *Request For Comments*_G, è la descrizione o la misurazione delle performance di un servizio di rete, secon-

do la visione da parte dell'utente a seconda della possibile attività che sta svolgendo.

RADIUS

Il protocollo di rete RADIUS fornisce una autenticazione centralizzata ed opera sulla porta 1812. Viene spesso utilizzato con 802.1X. Con il termine RADIUS si può indicare anche il server che fornisce il servizio di autenticazione mediante questo protocollo.

Request For Comments

Una "richiesta di commenti", usualmente indicata utilizzando unicamente la sigla RFC, è un documento pubblicato dalla Internet Engineering Task Force, che riporta informazioni riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico.

Sicurezza fisica

Per sicurezza fisica si intendono il complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, dispositivi, apparati, informazioni e dati di natura riservata.

Sicurezza logica

Per sicurezza logica si intendono il complesso di soluzioni che impediscono ad utenti non autorizzati di compiere azioni che richiedono dei privilegi più elevati rispetto a quelli in loro possesso.

SQL injection

SQL injection è una tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input. .

System Integrator

Con il termine System Integrator viene indicata una azienda che si occupa di far dialogare impianti diversi tra di loro allo scopo di creare una nuova struttura funzionale che possa utilizzare le potenzialità di impianti d'origine e creare quindi funzionalità originariamente non presenti.

Bibliografia

- Manuale Observium - in lingua inglese
<http://docs.observium.org>
- Documentazione Microsoft relativa a Active Directory - in lingua inglese
<https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access>
- Presentazione MikroTik - WiFi Enterprise con CAPsMAN e Windows NPS - in lingua inglese
www.youtube.com/watch?v=RXkoAimlcM8
- Slide MikroTik - WiFi Enterprise con CAPsMAN e Windows NPS - in lingua inglese
https://mum.mikrotik.com/presentations/EU18/presentation_5159_1523293520.pdf