

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	2
1.1.1	Digital Transformation	2
1.1.2	Applicazioni gestionali	2
1.1.3	Cloud	2
1.1.4	eLearning	2
1.1.5	Security	3
2	Progetto di stage	4
2.1	Pianificazione	4
2.1.1	Fase 1: Analisi	4
2.1.2	Fase 2: Progettazione	4
2.1.3	Fase 3: Implementazione	5
2.1.4	Fase 4: Test in produzione	5
2.1.5	Fase 5: Tuning	6
2.2	Obiettivi	6
2.2.1	Obiettivo aziendale	6
2.2.2	Obiettivo formativo	6
3	Tecnologie	7
3.1	Tecnologie per il monitoraggio	7
3.1.1	PRTG Network Monitor	7
3.1.2	Observium	8
3.1.3	RConfig	8
3.2	Tecnologie per la sicurezza	9
3.2.1	802.1X	9
3.2.2	Extensible Authentication Protocol	10

3.2.3	Windows Network Policy Server	10
3.2.4	Active Directory	11
3.2.5	CAPsMAN	11
3.3	Strumenti di lavoro	12
3.3.1	Microsoft Visio	12
3.3.2	OpenOffice Calc	12
3.3.3	GreaseMonkey	13
3.3.4	Putty	13
3.3.5	Microsoft Telnet	14
3.3.6	MySQL Command-Line Tool	14
3.3.7	Notepad++	14
3.3.8	Vim	15
3.3.9	FileZilla	15
4	Realizzazione	16
4.1	Analisi	16
4.1.1	Lista apparati	16
4.1.2	Analisi sistemi di sicurezza fisica	17
4.1.3	Analisi sistemi di monitoraggio	18
4.1.4	Schema di rete	18
4.2	Progettazione	20
4.2.1	Progettazione Observium	20
4.2.2	Progettazione rConfig	21
4.2.3	Configurazioni degli apparati Access Point	22
4.2.4	Politiche di sicurezza	23
4.2.5	Captive portal	23
4.2.6	Definizione name-convention	24
4.2.7	Inserimento nomi DNS nella lista degli apparati	25
4.2.8	Lista dei test e risultati previsti	25
4.2.9	Produzione della prima bozza della documentazione progettuale	25
4.3	Implementazione	26
4.3.1	Inserimento dei dispositivi sul DNS interno	26
4.3.2	Implementazione Virtual Machine di monitoraggio	26
4.3.3	Configurazione del versioning con RConfig	26
4.3.4	Configurazione del monitoraggio con Observium	27
4.3.5	Laboratorio per lo sviluppo	27
4.3.6	Configurazione della rete	28
4.3.7	Predisporre servizio NPS (Radius) sui due Active Directory servers	29
4.3.8	Creazione del Captive Portal	29

4.3.9	Test delle configurazioni in laboratorio	32
4.3.10	Test delle funzionalità di sicurezza in laboratorio	33
4.3.11	Creazione nuove configurazioni per tutti gli switch del Campus	34
4.3.12	Caricamento configurazioni negli switch del Campus	35
4.3.13	Scheduling backup delle impostazioni con rConfig	35
4.3.14	Backup configurazioni MikroTik	36
4.3.15	Aggiornamento della documentazione progettuale	37
4.4	Test in produzione	38
4.4.1	Monitoraggio eventuali anomalie, censirle, troubleshooting, identificare la soluzione, trovare un workaround, implementare e testare la soluzione	38
4.4.2	Aggiornare la documentazione	38
4.4.3	Upgrade Observium	38
4.5	Tuning	39
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	39
4.5.2	Completamento della documentazione	39
5	Valutazione retrospettiva	40
5.1	Tempo impiegato	40
5.2	Risultati ottenuti	40
5.3	Vincoli del progetto	40
5.3.1	Vincoli tecnologici	40
5.3.2	Vincoli metodologici e di lavoro	41
5.3.3	Vincoli temporali	41
Appendici	43	
Appendice A: Schemi di rete	43	
Appendice B: Script di popolamento rConfig	47	
Appendice C: Script di backup Mikrotik	50	
Glossario	52	
Bibliografia	55	
Documenti in lingua italiana	55	
Documenti in lingua inglese	55	

Elenco delle figure

1.1	Logo di Wintech	1
3.1	Logo di PRTG	7
3.2	Logo di Observium	8
3.3	Logo di RConfig	8
3.4	Procedura di autenticazione 802.1X	9
3.5	Schema delle tecnologie per l'attualizzazione di 802.1X	10
3.6	Interfaccia di Visio	12
3.7	Interfaccia di Calc	12
3.8	Logo di GreaseMonkey	13
3.9	Schermata iniziale di Putty	13
3.10	Interfaccia di Notepad++	14
3.11	Interfaccia di Vim	15
3.12	Logo di FileZilla	15
4.1	Armadio di rete da esterni	17
4.2	Schermata di PRTG Network Monitor	18
4.3	Interfacce visualizzate all'interno di Observium	21
4.4	Attacco SQL injection su rConfig, sulla destra tutte le configurazioni navigabili	22
4.5	HP 2530-8G PoE+	28
4.6	MikroTik cAP ac	28
4.7	Router MikroTik	28
4.8	Configurazione della rete	29
4.9	Sequenza per effettuare il login	31
4.10	Sequenza per effettuare la registrazione	32
4.11	Risultato ottenuto dalla analisi di VEGA	33
4.12	Risultati ottenuti con NetCut	34
4.13	Esempio della scarsa normalizzazione dei dati in rConfig	36
4.14	Lista delle cartelle con i backup in Directory Lister	37

ELENCO DELLE FIGURE

5.1	Schema Visio della rete datato 2015	44
5.2	Schema Visio della rete a fine stage, prima parte	45
5.3	Schema Visio della rete a fine stage, seconda parte	46

Elenco delle tabelle

4.1	Servizi per l'implementazione del Captive Portal	30
5.1	Tempo previsto ed impiegato	40

Sommario

Questo documento si prefigge lo scopo di presentare il lavoro svolto durante l'attività di stage, 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 elevata complessità.

Gli argomenti trattati riguarderanno il controllo in tempo reale dello stato della rete, individuando colli di bottiglia, problematiche di varia natura e potenziali pericoli, al fine di 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 possiedono dei privilegi sufficientemente elevati.

L'ultima parte di questo documento conterrà una mia valutazione personale retrospettiva sul lavoro svolto, nella quale evidenzierò 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* capace di vantare una lunga tradizione e un patrimonio di conoscenze nei diversi ambiti di competenza del settori ICT.

WinTech Spa svolge la propria attività in qualità di System Integrator che, grazie alla propria esperienza, competenza e creatività, trasforma le tecnologie IT di mercato in soluzioni informatiche innovative, efficienti e dal facile utilizzo.



Figura 1.1: Logo di Wintech

La società conta su una struttura di circa 80 risorse che svolgono la propria attività nelle Sedi di Padova, Milano, Bassano del Grappa e Pordenone; una precisa strategia di valorizzazione di partnership nazionali ed internazionali, le consente di superare i confini delle proprie dimensioni fruendo di collaborazioni di valore riconosciuto.

1.1 Dominio applicativo

Wintech opera in un dominio molto vasto, per tale motivo in questa sezione verrà trattato con maggiore dettaglio il dominio relativo allo stage conseguito, cioè quello del monitoraggio e della sicurezza fisica delle reti.

1.1.1 Digital Transformation

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

Wintech si impegna in questo settore favorendo la digitalizzazione delle aziende, andando ad integrare sistemi che consentano una archiviazione elettronica dei documenti, certificati mediante firme digitali.

Ulteriormente si impegna anche a fornire soluzioni di Business Process Management e di Case Management, permettendo quindi una gestione evoluta di tutti i processi aziendali.

1.1.2 Applicazioni gestionali

Per consentire la gestione delle risorse aziendali Wintech propone soluzioni dedicate di Enterprise Resource Planning, Business Intelligence e di tesoriere.

Questi software, complementare tra di loro, permettono di monitorare, analizzare e accedere alle risorse disponibili in modo efficace ed efficiente, portando quindi enormi benefici alle aziende che ne fanno uso.

1.1.3 Cloud

Wintech offre servizi cloud mirati alle aziende e certificati secondo lo standard ISO 27001.

I vantaggi offerti da questa esternalizzazione è un supporto professionale e continuo dei propri sistemi, affiancato da una riduzione del downtime grazie al servizio ridondante ad alta affidabilità ed a una sicurezza elevata che protegge le risorse da intrusioni esterne.

1.1.4 eLearning

Wintech desidera migliorare anche la fruizione dei corsi aziendali, operando nello sviluppo di nuove tecnologie che ne consentano un utilizzo da remoto mantenendone la validità legale e assicurando la presenza fisica dell'interessato al terminale

durante le lezioni.

Questo viene effettuato mediante piattaforme di eLearning e di Live Streaming, integrate con software avanzati che consentono funzionalità non presente nella concorrenza.

1.1.5 Security

Evoluzione della Cybersecurity

L'ambito della Cybersecurity è sicuramente uno degli ambiti più dinamici all'interno del mondo informatico, con tipologie di attacchi che variano continuamente nel tempo. Questo può essere riscontrato analizzando i vettori di attacco, chiaramente descritti anche annualmente all'interno del rapporto Clusit.

Oramai è inutile chiedersi se si verrà attaccati, ma ci si deve chiedere solamente quando succederà e se si è pronti a difendersi ed a riparare ai possibili danni. Praticamente qualsiasi ente è un potenziale bersaglio ed, a volte, espone delle vulnerabilità delle quali non si preoccupa, in quanto suppone erroneamente di non essere appetibile per un eventuale attaccante.

A sostegno di quanto appena affermato viene utilizzato, nel mondo anglosassone, il seguente motto:

Is not a matter of "if", but a matter of "when".

La quale può essere tradotta in italiano nel seguente modo:

Non è una questione di "se", ma di "quando".

In conclusione 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.

La proposta di Wintech in ambito Cybersecurity

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 sono 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.

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 previsto:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore previste:** 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 e il sistema di monitoraggio presenti.

2.1.2 Fase 2: Progettazione

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

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

In questa fase verrà implementata la nuova infrastruttura e saranno resi operativi i software precedentemente configurati.

Verrà creato un laboratorio con uno nuovo switch sul quale verranno testate le politiche precedentemente scelte per valutarne l'efficacia.

Una volta accertata la validità del nuovo sistema si procederà alla creazione delle configurazioni per tutti gli switch comprendenti la nuova politica di sicurezza e la loro installazione.

Successivamente i dispositivi saranno 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 previsto:** dal 09/06/2018 al 13/07/2018;
- **Numero di ore previste:** 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 sarà il monitoraggio di eventuali anomalie, per poi censirle, cercare la fonte del problema, identificare una soluzione ed implementarla.

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

2.1.5 Fase 5: Tuning

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

Nella fase finale del progetto verranno eseguiti tuning su tutta la rete, ove possibile, 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 allarme 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 e consentire il monitoraggio dello stato di una rete Campus Area Network dove accedono migliaia di persone.

La finalità è rilevare eventuali anomalie e colli di bottiglia presenti ed impedire l'uso illecito e non controllato dei servizi di rete, sabotaggi e furto di dati.

Questo comprende l'implementazione e l'utilizzo di servizi e protocolli avanzati per ottenere e mantenere le migliori performance possibili garantendo anche una sicurezza elevata.

2.2.2 Obiettivo formativo

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

Questo al fine di permettere di mettere in pratica le conoscenze acquisite durante lo svolgimento dei corsi universitari e fornire uno stimolo ad approfondire ancora di più queste tematiche.

Capitolo 3

Tecnologie

Questa sezione illustra le principali tecnologie incontrate ed 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 velocemente obsoleti oppure a 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 utilizzato nella rete analizzata durante lo stage. Il suo fine è la rilevazione delle 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.

La sua implementazione durante l'attività formativa è stata effettuata per superare ai limiti posti da PRTG e migliorare quindi la qualità dei servizi.

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 configurazioni degli apparati di rete.

È completamente open source, protetto da licenza GNU v3.0, ed è scritto in linguaggio PHP. Per eseguire automaticamente i task fa uso del demone Unix crontab, quindi non risulta utilizzabile su sistemi Windows, ma unicamente Linux e BSD. Le connessioni verso i dispositivi non sono effettuate tramite lo standard Simple Network Management Protocol, o SNMP, ma Telnet e SSH. Questo gli permette di supportare, con la giusta configurazione, molti dispositivi, però complica notevolmente la fase di setup e può generare problemi in alcuni brand.



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 supportato ed utilizzato nelle connessioni cablate in quanto, spesso, 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.

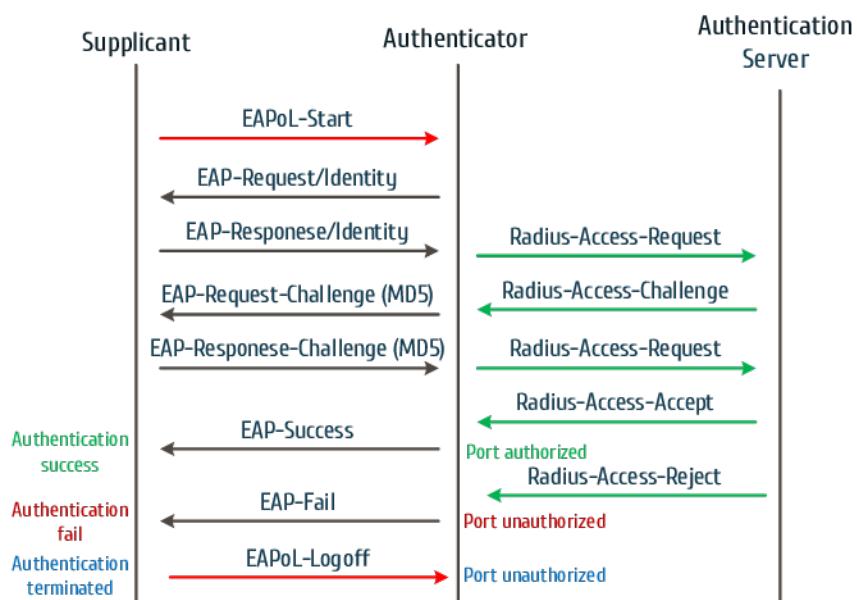


Figura 3.4: Procedura di autenticazione 802.1X

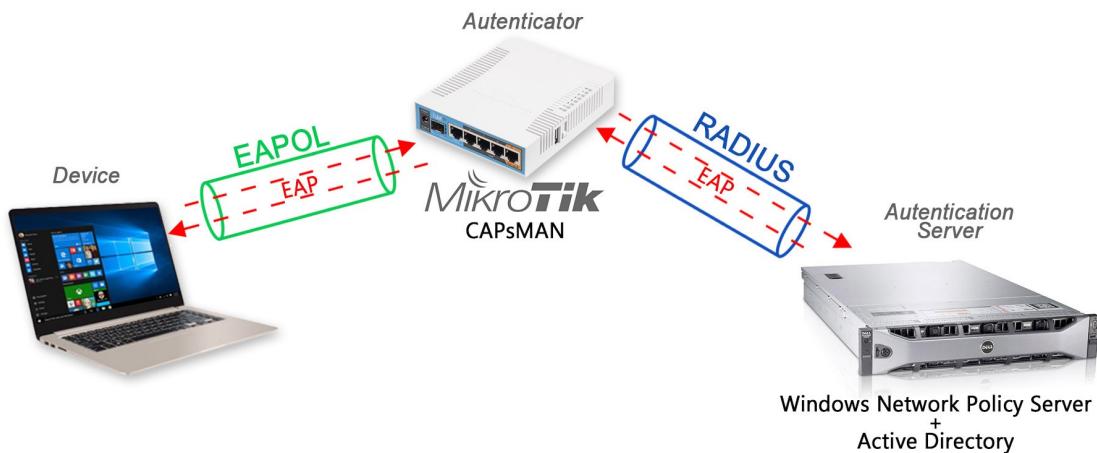


Figura 3.5: Schema delle tecnologie per l'attualizzazione di 802.1X

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 definisce 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.

La sua funzionalità principale è la propagazione di una configurazione comune per l'accesso Wireless a tutti gli apparati presenti nella rete.

Consente l'identificazione dei client che si connettono mediante un server RADIUS e permette anche di reindirizzare dinamicamente gli utenti su VLAN diverse.

Risulta molto utile in caso di estensione della rete, in quanto riduce notevolmente la configurazione iniziale di ogni access point, diminuendo a sua volta il rischio di commettere errori di configurazione.

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 gestibile anche da persone senza una elevata conoscenza dell'informatica o di linguaggi dediti allo scopo.

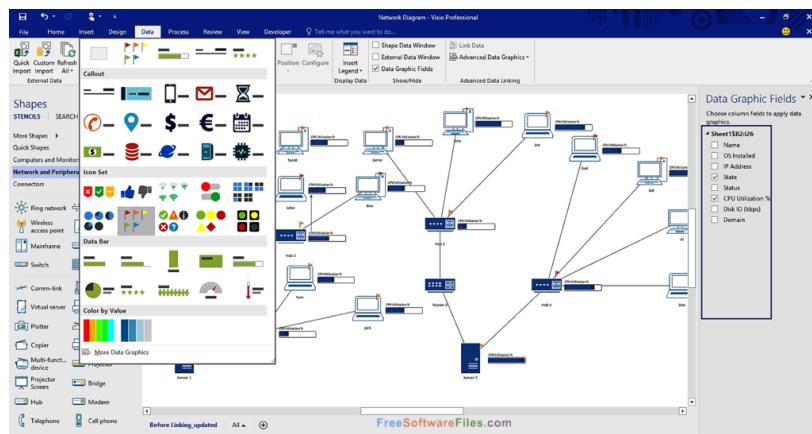


Figura 3.6: Interfaccia di Visio

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	Rank (AOO per internet users)	(AOO per Population) Users			
188	San Marino	1.067	32.457	15.781	32.674	68	13	4		
189	Netherlands	568.068	16.751.323	15.371.000	39.912	37	12	14		
190	Malta	100	1.535	1.938	30.117	34	11	18		
191	Finland	212.062	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	60.813.306	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	1.042.000	1.042.000	64.982.632	68.896	984	2	2		

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 avere più tempo libero 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.

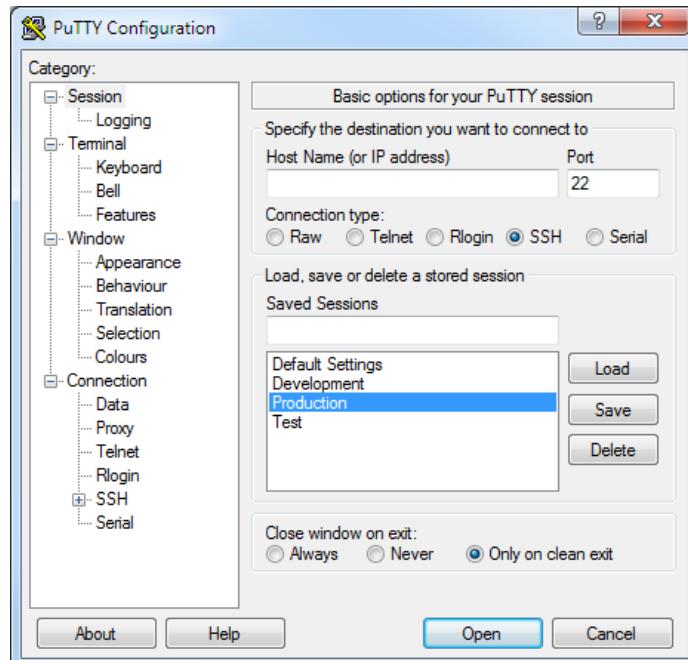


Figura 3.9: Schermata iniziale di Putty

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.

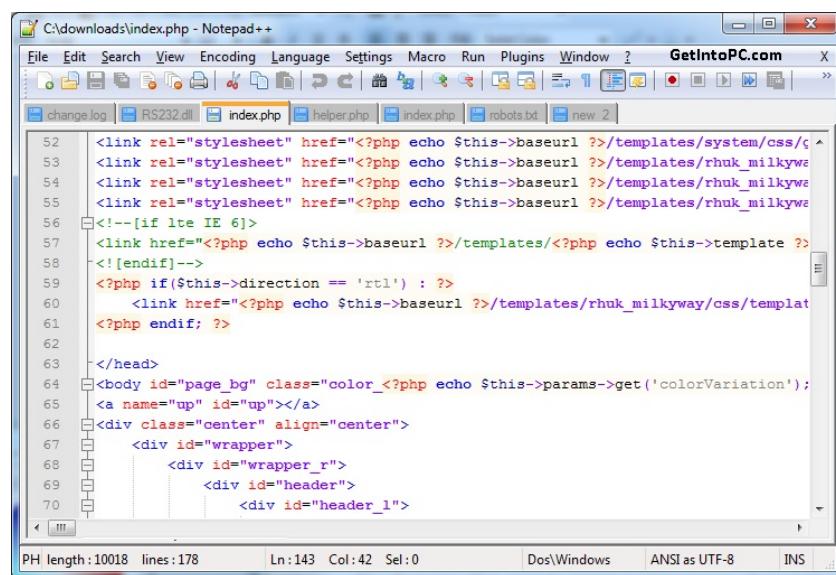


Figura 3.10: Interfaccia di Notepad++

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

FileZilla Client è un software che permette il trasferimento di file in Rete attraverso il protocollo FTP.

Si è rilevato utile per la gestione dei file sulle macchine virtuali e sui dispositivi MikroTik, permettendo un facile trasferimento delle configurazioni e delle pagine web che si sono utilizzate durante tutto lo stage.



Figura 3.12: Logo di FileZilla

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 che riportano informazioni parziali che sono state integrate tra 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 dedicato.

Era già presente una suddivisione in 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.

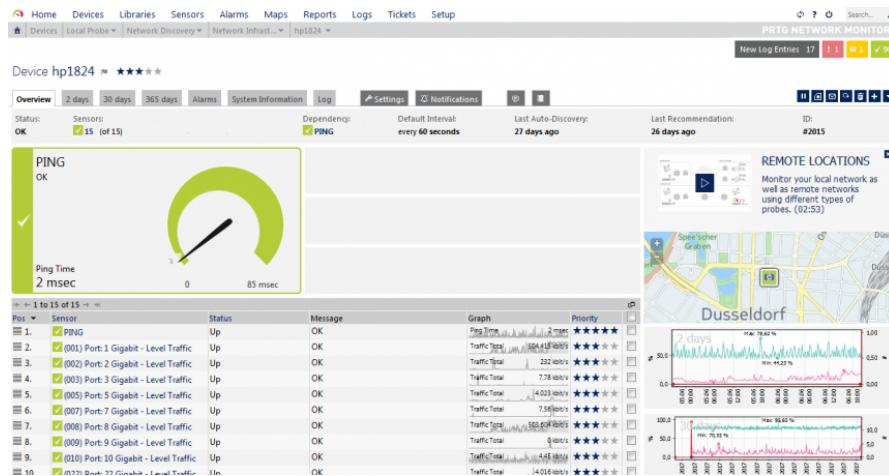


Figura 4.2: Schermata di PRTG Network Monitor

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 tem-

pi 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 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 è 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 è la disabilitazione delle interfacce non in uso, che avrebbero generato avvertimenti inutili.

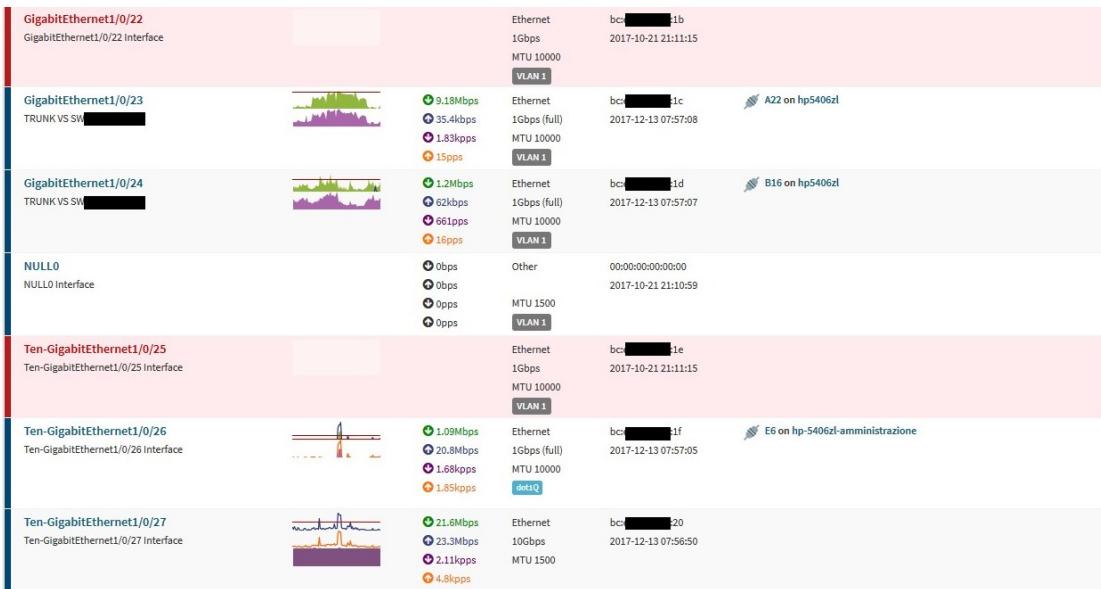


Figura 4.3: Interfacce visualizzate all'interno di Observium

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.

4.2.2 Progettazione rConfig

Analogamente a quanto effettuato con Observium, anche per rConfig si è eseguito un 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 da subito 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* che permetteva di ottenere una lista completa dei report effettuati, compresi quelli rimossi o non accessibili per l'account in uso.

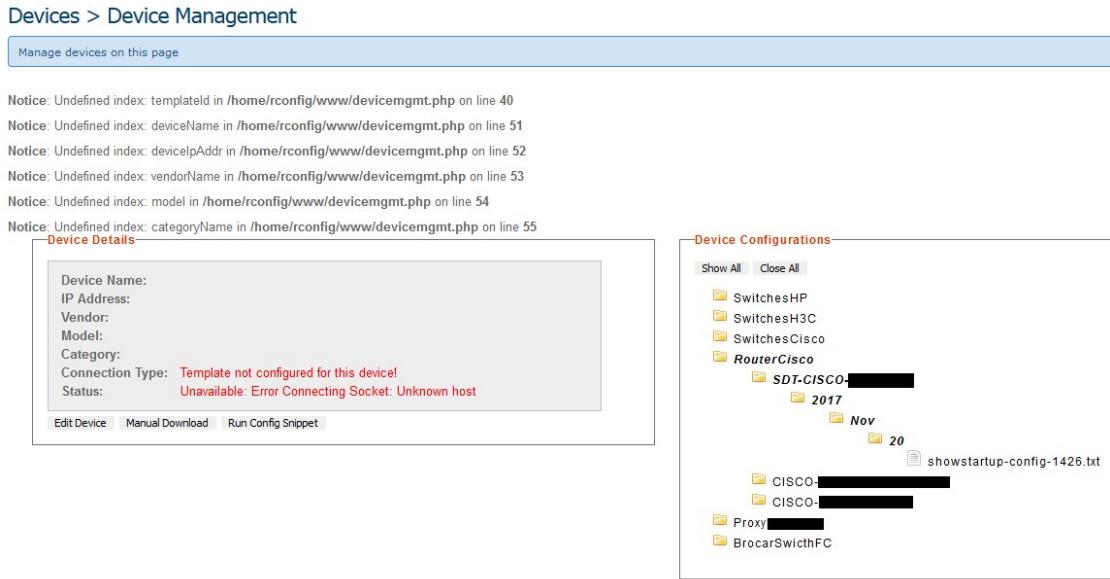


Figura 4.4: Attacco SQL injection su rConfig, sulla destra tutte le configurazioni navigabili

4.2.3 Configurazioni degli apparati Access Point

Per permettere una estensibilità della rete senza l'intervento di un tecnico per la sua configurazione si è scelto di utilizzare CAPsMAN.

La struttura della tecnologia CAPsMAN si basa su un router centrale, prodotto da MikroTik, che gestisce e fornisce le configurazioni. Su questo router vengono collegati, mediante la VLAN a lui dedicata, gli Access Point, che provvederanno autonomamente a recuperare ed applicare le impostazioni corrette.

Questa metodologia permette, in caso di estensione della rete, di evitare una configurazione manuale dei dispositivi, che potrebbe presentare errori di distrazione e compromettere la sicurezza.

Un'altra caratteristica di estrema importanza è che le impostazioni, essendo centralizzate, possono essere modificate unicamente nel router e le modifiche vengono poi trasmesse automaticamente a tutti i dispositivi.

Il sistema così organizzato però introduce un potenziale pericolo, in quanto il router che gestisce CAPsMAN è unico e rappresenta un single point of failure.

4.2.4 Politiche di sicurezza

Durante la progettazione si è decretato anche il numero di SSID wireless da impiegare e le loro modalità di accesso.

L'attenzione è stata posta sulle reti utilizzate dal personale, in quanto consentono l'accesso a risorse di elevata importanza e per tale ragione devono essere protette. Per tali motivazioni si è scelto di creare 3 reti wireless, così definite:

- **Corporate:** rete dedita alla connessione dei computer dediti ad attività lavorative, consente l'accesso alle risorse;
- **Mobile:** rete dedita alla connessione dei dispositivi personali e/o lavorativi dei dipendenti, come smartphone e tablet, che non richiedono l'accesso a risorse;
- **Guest:** rete dedita a fornire una connettività internet agli ospiti degli uffici.

Le misure di autenticazioni sono le seguenti:

- **Corporate:** l'accesso è consentito previa autenticazione mediante EAP utilizzando le proprie credenziali Active Directory e possedendo il relativo certificato digitale;
- **Mobile:** l'accesso è consentito previa autenticazione mediante EAP utilizzando le proprie credenziali Active Directory, senza la necessità di possedere il certificato digitale;
- **Guest:** l'accesso è consentito mediante l'inserimento di una password di bassa complessità e la registrazione su un *captive portal_G*.

4.2.5 Captive portal

Per la progettazione del *captive portal_G* si è scelto di utilizzare come modello uno già in utilizzo in alcune soluzioni sviluppate da Wintech, in modo tale da dedicare meno tempo alla progettazione e porre l'attenzione sugli aspetti di networking e di sicurezza.

La schermata di login si presenta con alcune form dediti all'inserimento della propria e-mail, della selezione di uno sponsor e della durata dell'account.

La registrazione viene effettuata inserendo la propria e-mail ed indicando uno "sponsor" scelto da un elenco di possibili persone, che avrà il compito di confermare o rifiutare la richiesta.

Una volta effettuata la richiesta di registrazione verrà inviata una e-mail allo sponsor, ed in caso di approvazione verrà comunicata la password di accesso al richiedente.

Gli sponsor sono gestibili in un pannello di configurazione solamente da parte dell'amministratore, che può anche amministrare le richieste.

L'account utilizzabile per l'accesso avrà anche una durata temporale prefissata, selezionabile durante la fase di registrazione. Questa caratteristica serve per scoraggiare eventuali dipendenti a farne uso e per impedire la presenza di vecchi account registrati ma non più utilizzati.

La password della rete, di bassa complessità, è stata inserita in modo tale da evitare un possibile spam, o flooding, di e-mail verso gli sponsor.

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 Inserimento dei dispositivi sul DNS interno

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.

4.3.2 Implementazione Virtual Machine di monitoraggio

Per consentire l'esecuzione continua dei software di monitoraggio 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 CentOS Linux, in quanto gratuito e già conosciuto nel contesto aziendale.

4.3.3 Configurazione del versioning con 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 csv_G .

Successivamente si è proceduto a modificare il formato dei dati esportati, operando per mezzo di una *espressione regolare_G*, 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.

4.3.4 Configurazione del monitoraggio con 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:

- 88 switch;
- 7 apparati wireless;
- 2930 interfacce;
- 398 sensori;
- 271 periferiche.

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.

4.3.5 Laboratorio per lo sviluppo

Prima di procedere alla produzione si è ovviamente testato le configurazioni in un laboratorio.

Per tale fine sono stati utilizzati uno switch HP 2530-8G PoE+ e svariati access point MikroTik cAP ac RBcAPGi-5acD2nD, collegati a un router MikroTik CCR1009-7G-1C-1S+.



Figura 4.5: HP 2530-8G PoE+



Figura 4.6: MikroTik cAP ac



Figura 4.7: Router MikroTik

4.3.6 Configurazione della rete

Per il collegamento tra gli access point e il router si è andati ad utilizzare una VLAN ad essi dedicati.

Sopra di essa è stato creato un datapath costituito da un bridge che consenta la comunicazione dei dispositivi connessi alle reti wifi.

Per motivi di sicurezza si è scelto di creare tre tunnel Ethernet over IP (EoIP) per incanalare i tre flussi di dati provenienti dai tre SSID wifi.

Così facendo si è ottenuta una elevata sicurezza, unita alla facilità di installazione di un nuovo dispositivo, in quanto è necessario solamente trasportargli la VLAN che utilizza, nell'immagine denominata "VLAN AP", e non quelle presenti nel tunnel, denominato "BRIDGE DATA".

Lo svantaggio di questa modalità è l'aver aggiunto un piccolo overhead ai pacchetti, che risulta trascurabile a fronte della semplicità di estensione e della elevata sicurezza che offre.

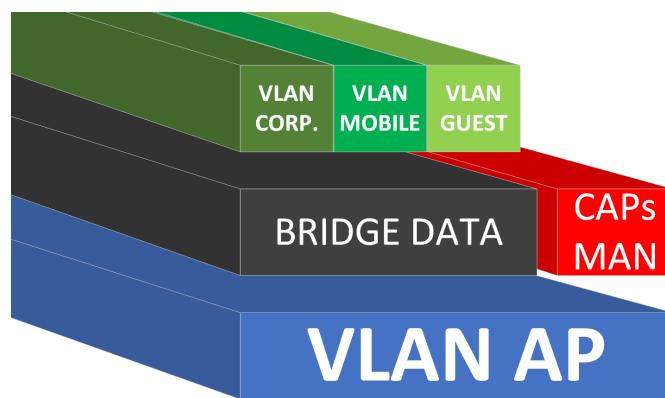


Figura 4.8: Configurazione della rete

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

asd

4.3.8 Creazione del Captive Portal

La creazione del Captive Portal è stata effettuata su una macchina virtuale nuova, in modo tale da garantirne una segregazione nel sistema e delle regole nel firewall specifiche alla sua funzionalità.

Innanzitutto si è proceduto con l'installazione del sistema operativo CentOS 7, che è stato scelto perché già conosciuto ed ampliamente utilizzato nell'ambito aziendale. Successivamente si sono andati ad installare tutti i servizi, o "demoni" nello slang UNIX, in modo da offrire tutte le funzionalità richieste, brevemente riportati nella tabella sottostante.

Demone	Funzionalità	Utilizzo
HttpD	Server web, dedito alla gestione delle richieste http, risoluzione del codice PHP mediante apposito modulo ed invio di pagine web.	Gestione ed interazione dell'interfaccia del Captive Portal.
MySQLD	Database, dedito al mantenimento e alla organizzazione dei dati, assieme al controllo d'accesso.	Gestione delle informazioni relative alla registrazione degli utenti, agli account abilitati e raccoglitore di informazioni per RadD.
CronD	Scheduler, dedito alla pianificazione dell'esecuzione dei comandi.	Controllo periodico degli account scaduti, che dovranno essere rimossi.
RadD	Radius, accede a una serie di direttive legate agli accessi e risponde in modo affermativo o negativo a delle richieste di autenticazione.	Utilizzato per determinare la validità degli account con i quali si effettua l'accesso nella rete.
FirewallD	Firewall, determina quali connessioni sono permesse e quali invece devono essere bloccate.	Preinstallato con CentOS, è stato configurato per permettere un accesso esterno alle risorse che lo richiedevano, mantenendo le altre ad utilizzo esclusivamente locale.
Sendmail	Server email, dedito al trasferimento di messaggi mediante SMTP.	Consente di inviare l'e-mail con la richiesta di approvazione allo sponsor e, in caso di accettazione, avvisa l'utente comunicandogli le informazioni necessarie all'accesso.

Tabella 4.1: Servizi per l'implementazione del Captive Portal

Il compito del login è stato delegato al router MikroTik per evitare complicazioni inutili, il quale andrà a controllare la validità dell'account comunicando con il servizio Radius, RadD, presente nella macchina virtuale.

La registrazione e la parte di amministrazione invece avvengono in autonomia sulla VM, che ha il compito di far interagire il database con l'interfaccia web in modo tale da aggiornare le informazioni contenute nel Radius e di avvisare gli interessati delle iterazioni tramite e-mail.

Il dispositivo MikroTik presentava un Captive Portal di default, che è stato personalizzato modificandone le grafica ed inserendo tutti i collegamenti verso le pagine di registrazione ed amministrazione presenti sulla macchina virtuale.

Di seguito sono riportate alcuni diagrammi per meglio comprendere l'iterazione delle varie parti tra di loro.

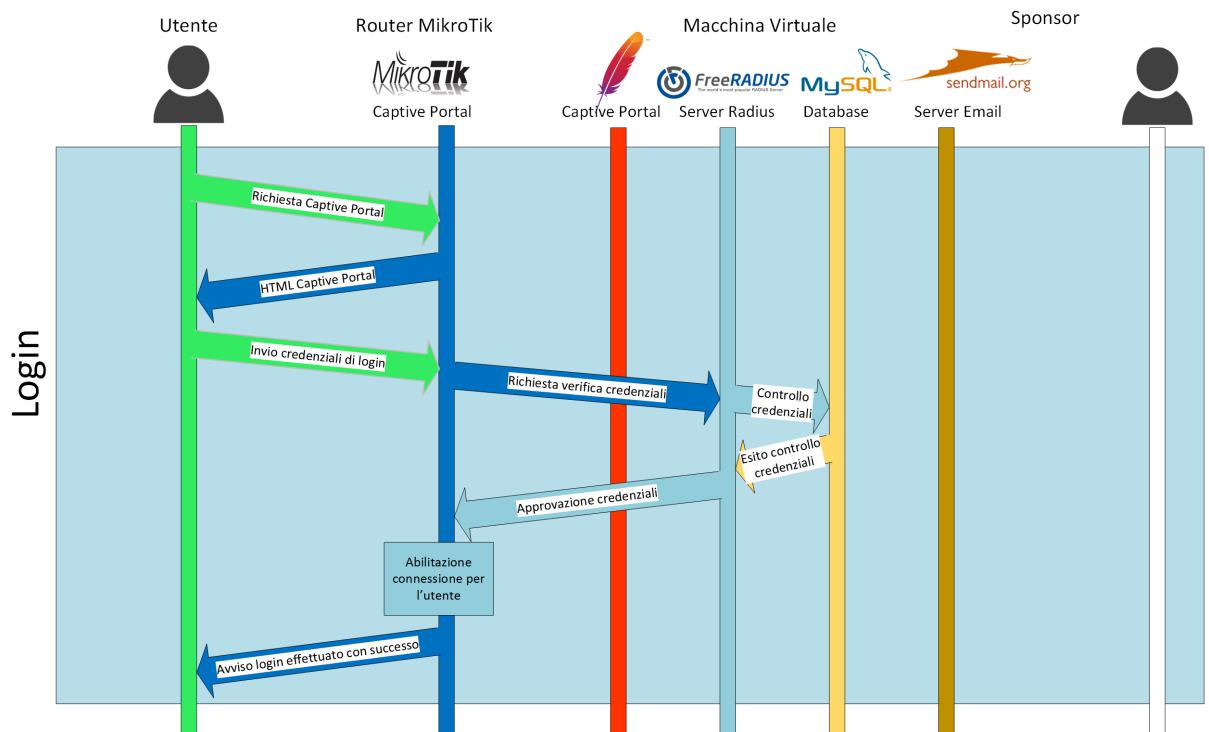


Figura 4.9: Sequenza per effettuare il login

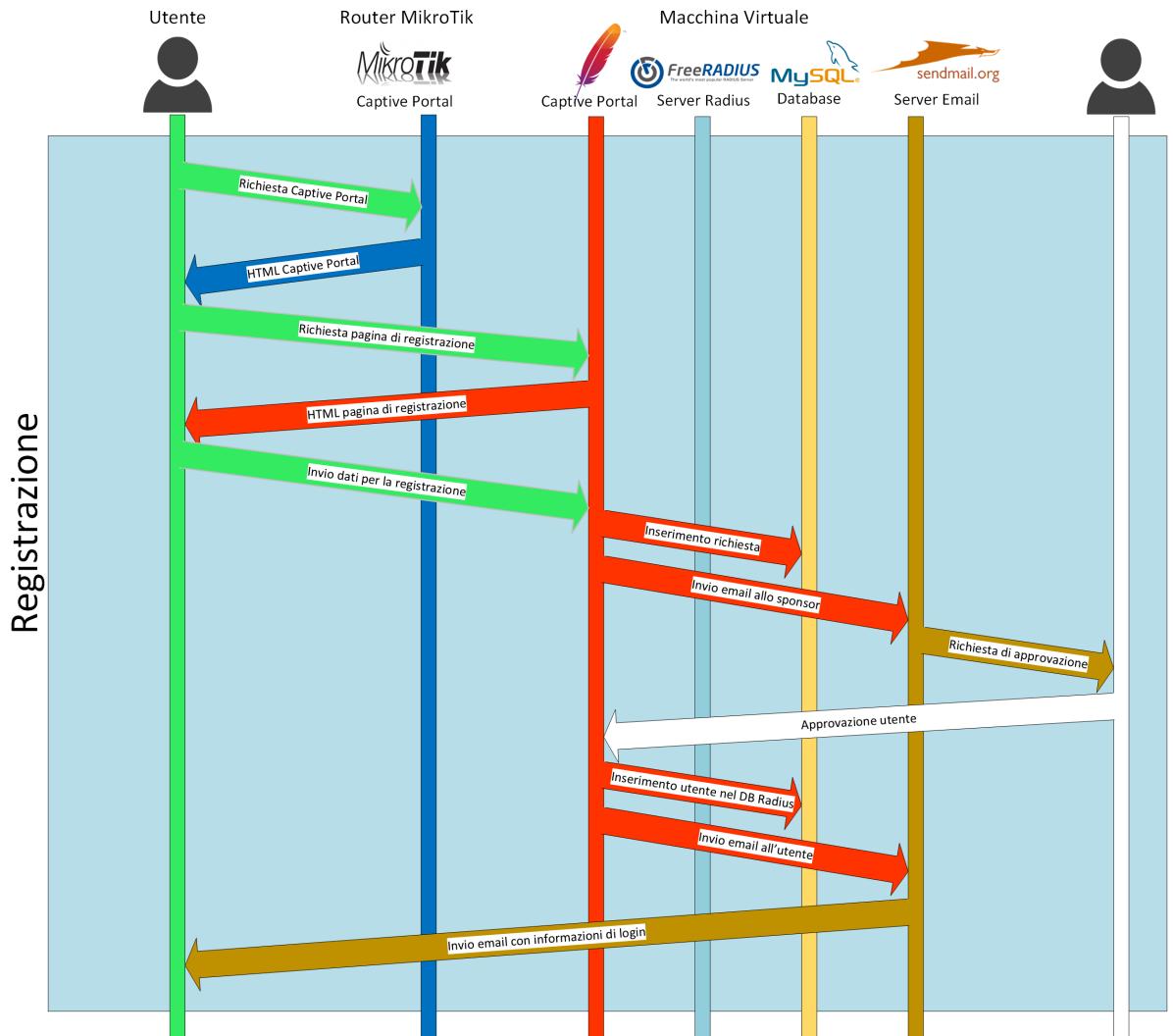


Figura 4.10: Sequenza per effettuare la registrazione

4.3.9 Test delle configurazioni in laboratorio

Prima di inserire il sistema in produzione si è andato a testare il funzionamento e la sua estensibilità.

Innanzitutto si è proceduto ad aumentare il numero di Access Point connessi in contemporanea, passando da 1 a 4, in modo tale da verificare la complessità della configurazione iniziale.

Per ogni nuovo dispositivo è stato sufficiente abilitare CAPsMAN sulle interfacce wireless perché divenga operativo con tutte le misure di sicurezza abilitate.

Si è anche definita una password di accesso alla configurazione, che comunque non

sarebbe stata raggiungibile da parte degli utilizzatori della connettività grazie al tunnel EoIP.

L'accesso ad internet si è rivelato funzionante e tutti i dispositivi venivano inseriti all'interno della VLAN con le corrispettive configurazioni fornite dal DHCP.

4.3.10 Test delle funzionalità di sicurezza in laboratorio

Un altro aspetto di elevata importanza è stata la sicurezza fornita dal nuovo sistema.

Innanzitutto si è verificata la stabilità del captive portal, cercando di forzare il login mediante attacchi *SQL injection* utilizzando SQLmap e VEGA.

I risultati ottenuti sono stati soddisfacenti, in quanto un preciso controllo dei valori inseriti all'interno dei campi di testo impediva di aggirare l'autenticazione.



Scan Alert Summary

! High	(None found)
! Medium	(1 found)
HTTP Trace Support Detected	1
! Low	(None found)
i Info	(None found)

Figura 4.11: Risultato ottenuto dalla analisi di VEGA

Successivamente si è andata a verificare la protezione ad eventuali attacchi eseguiti una volta già autenticati, come ad esempio il *Man In The Middle*.

Non sono state rilevate vulnerabilità, in quanto gli altri dispositivi presenti nella rete risultavano irraggiungibili, e di conseguenza anche software come Wireshark e Arcai's NetCut non riuscivano a rilevare gli altri utenti.

Una vulnerabilità隐式 nel protocollo WiFi, impossibile da risolvere per la sua

natura, è la cattura in monitor mode dei pacchetti che transitano sulla rete, permettendo quindi di identificare i dispositivi che usufruiscono della rete. Però anche questa vulnerabilità implicita risulta di scarsa utilità per un attaccante, in quanto non ha comunque la possibilità di interagire con i dispositivi e manometterli.

Nella immagine sottostante si può notare a sinistra una analisi effettuata in una rete del cliente prima della installazione del nuovo sistema, con rilevati 29 dispositivi connessi, mentre a destra l'analisi effettuata nella nuova configurazione, senza nessun utente connesso visibile.

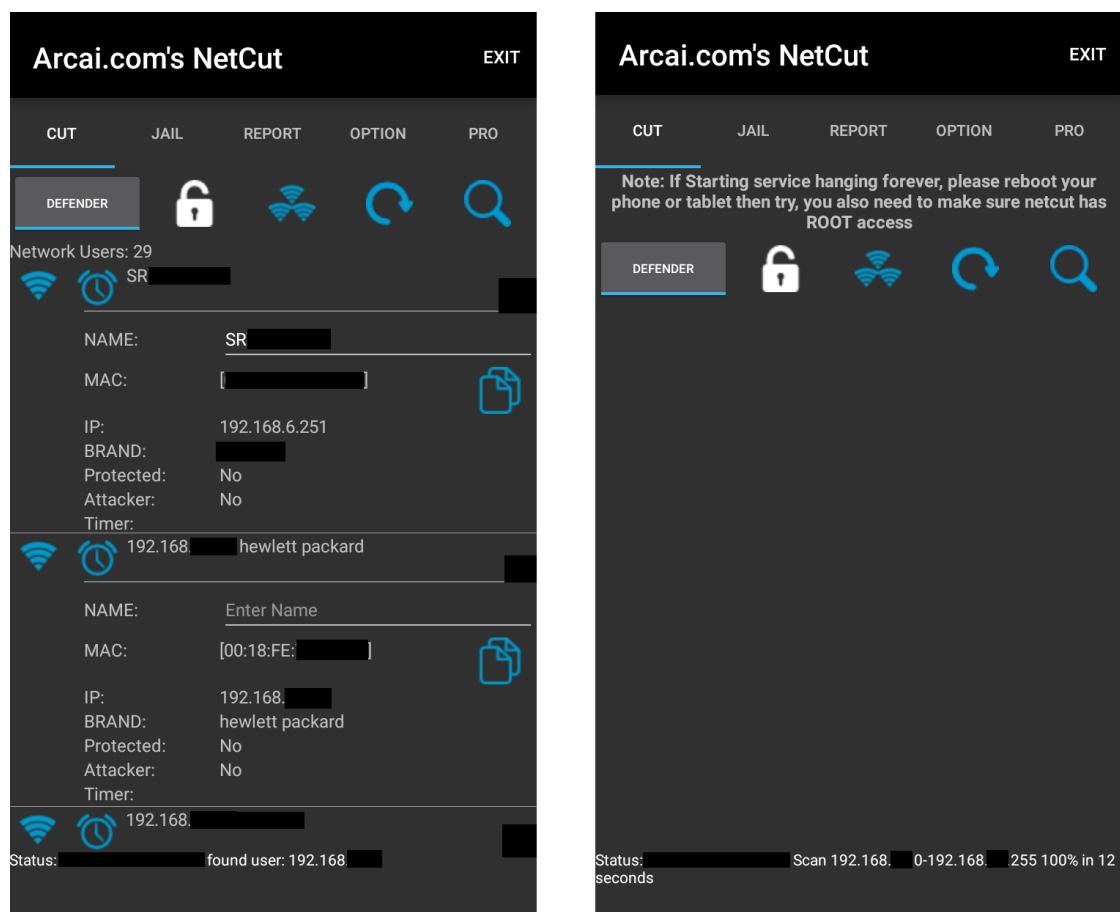


Figura 4.12: Risultati ottenuti con NetCut

4.3.11 Creazione nuove configurazioni per tutti gli switch del Campus

asd

4.3.12 Caricamento configurazioni negli switch del Campus

asd

4.3.13 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 più recente.

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.

Nell’immagine sottostante si può notare un esempio di quanto affermato. I dispositivi, chiamati nodi, non hanno una relazione molti a molti con i task, ma bensì contengono delle colonne con il nome riferito all’id del tast, il cui valore è un enumeratore che ne indica l’abilitazione.

rConfig nodes	
id : int(10)	
taskId556251 : varchar(20)	
taskId450655 : varchar(20)	
taskId637140 : varchar(20)	
taskId842385 : varchar(20)	
taskId164891 : varchar(20)	
taskId687418 : varchar(20)	
taskId669000 : varchar(20)	
deviceName : varchar(255)	
deviceUsername : varchar(255)	
devicePassword : varchar(255)	
deviceEnablePassword : varchar(255)	
deviceIpAddr : varchar(255)	
devicePrompt : varchar(255)	
deviceEnablePrompt : varchar(255)	
# nodeCatId : int(10)	
# templateId : int(10)	
vendorId : varchar(255)	
model : varchar(255)	
nodeVersion : varchar(255)	
nodeAddedBy : varchar(255)	
# defaultCreds : int(1)	
defaultUsername : varchar(255)	
defaultPassword : varchar(255)	
defaultEnablePassword : varchar(255)	
deviceDateAdded : date	
deviceLastUpdated : date	
# status : int(10)	
custom_Location : varchar(255)	

rConfig tasks	
id : int(6)	
# taskType : int(3)	
taskname : varchar(255)	
taskDescription : varchar(255)	
# snipld : int(10)	
crontime : varchar(255)	
croncmd : varchar(255)	
addedBy : varchar(255)	
dateAdded : date	
catId : varchar(255)	
catCommand : varchar(255)	
# status : int(2)	
# mailConnectionReport : int(10)	
# mailErrorsOnly : int(10)	
# complianceId : int(10)	

Figura 4.13: Esempio della scarsa normalizzazione dei dati in rConfig

4.3.14 Backup configurazioni MikroTik

Una volta avuto a disposizione i device MikroTik è emerso un problema inaspettato con rConfig, che non riusciva a completare il backup delle configurazioni su tali dispositivi.

Il problema era causato da una serie di caratteri non stampati a schermo utilizzati dai dispositivi, che rConfig non sapeva rilevare correttamente, impedendogli di compiere i passaggi di login necessari.

Per risolvere tale problema in modo veloce, efficiente e duraturo nel tempo si è scelto di incaricare il dispositivo stesso dell'effettuazione del backup. Per raggiungere tale scopo è stato creato uno script, visibile in Appendice C, che permette il salvataggio automatico delle proprie configurazioni su un server FTP.

Una volta verificato il corretto funzionamento dello script è stato schedulato in modo tale avvenga automaticamente ad intervalli prefissati.

Ulteriormente il server FTP è stato dotato di un demone HTTP Apache, in modo

da consentire la navigazione dei backup effettuati. Per migliorare la fruizione del sito si è utilizzato Directory Lister, il quale è stato modificato per richiedere l'inserimento di una password.

File	Size	Last Modified
AP01	-	2018-07-11 13:04:03
AP02	-	2018-07-11 10:22:51
AP03	-	2018-07-11 10:22:51
AP04	-	2018-07-11 10:22:51
AP05	-	2018-07-11 10:22:51
AP06	-	2018-07-11 10:22:51
Router	-	2018-07-11 10:48:39

Figura 4.14: Lista delle cartelle con i backup in Directory Lister

4.3.15 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 attività	Durata prevista	Durata effettiva
Analisi	40h	
Progettazione	80h	
Implementazione	80h	
Test in produzione	40h	
Tuning	80h	

Tabella 5.1: Tempo previsto ed impiegato

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 creare un filtro sugli avvisi, ma non è ancora presente per il raggruppamento.

Supporto MikroTik in rConfig

Una problematica emersa durante la configurazione dei backup automatici dei dispositivi è stata l'impossibilità di utilizzare rConfig per i dispositivi MikroTik. Questa problematica deriva probabilmente dal fatto che il sistema di MikroTik, denominato RouteOS, invia sui terminali anche caratteri speciali per il colore del testo, i quali sono male interpretati da rConfig. Questo impedisce al programma di svolgere la sua funzionalità, in quanto non riesce a comprendere le risposte che gli vengono fornite dall'apparato.

Infine il log generato dall'applicazione era poco verboso, che in accoppiata ad una progettazione non di elevato livello andava ad aumentare la difficoltà nella individuazione di una eventuale patch. Per tale motivo si è scelto di proseguire per una via alternativa, delegando i singoli dispositivi ad effettuare autonomamente un backup ed a salvarlo in remoto, piuttosto che mettere mano al codice sorgente del programma.

5.3.2 Vincoli metodologici e di lavoro

5.3.3 Vincoli temporali

Appendici

Appendice A: Schemi di rete

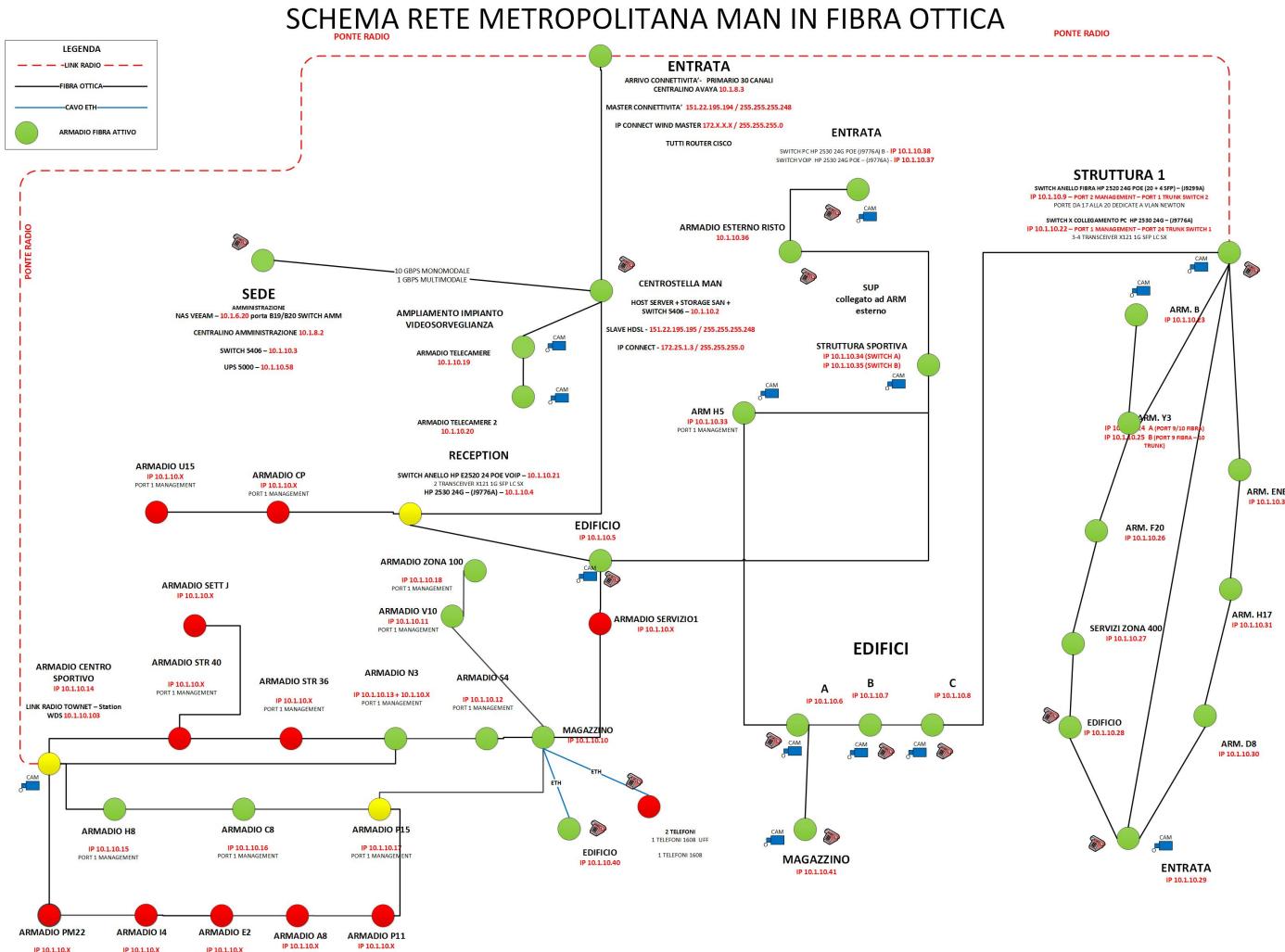


Figura 5.1: Schema Visio della rete datato 2015

SCHEMA RETE METROPO

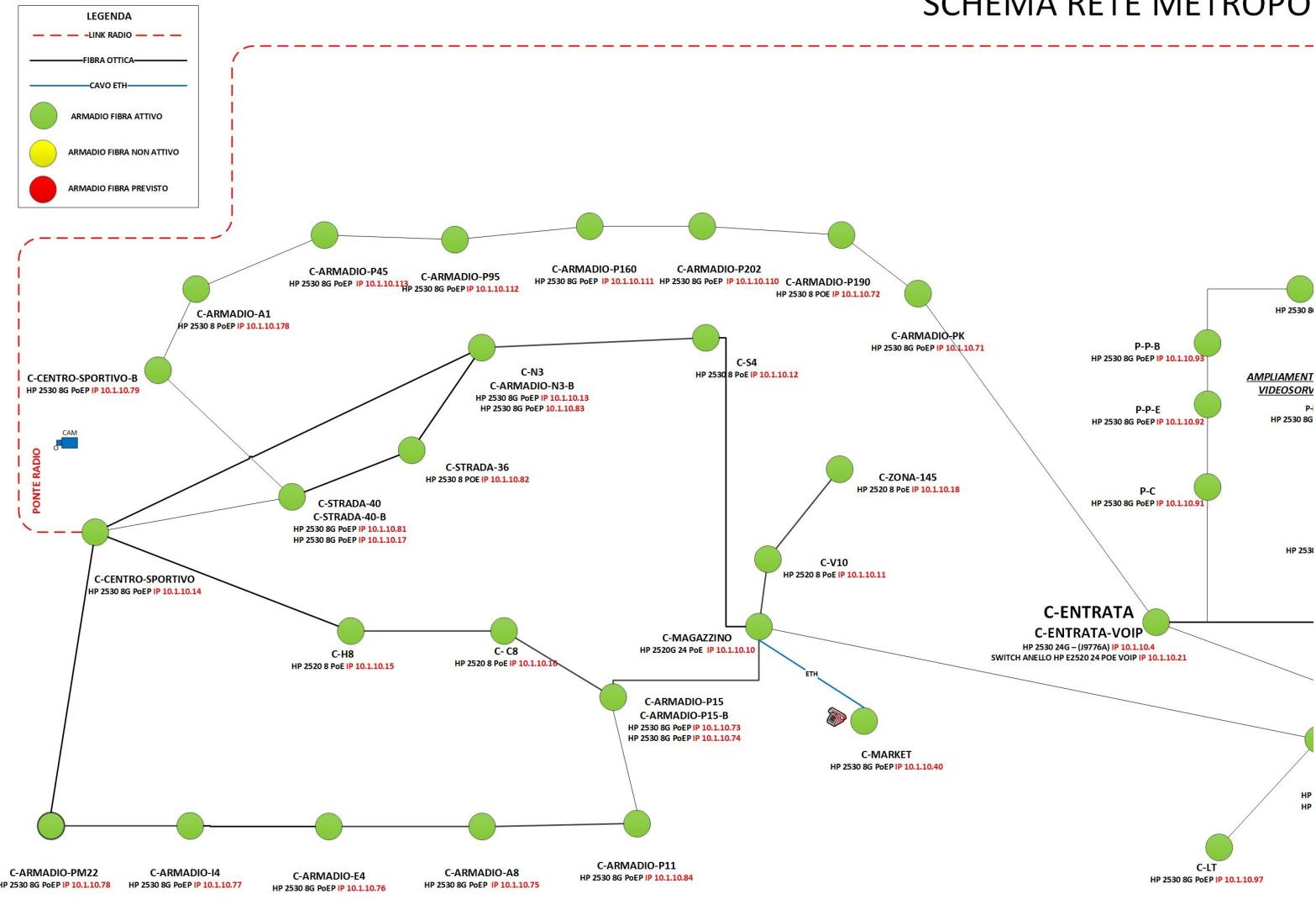


Figura 5.2: Schema Visio della rete a fine stage, prima parte

LITANA MAN IN FIBRA OTTICA

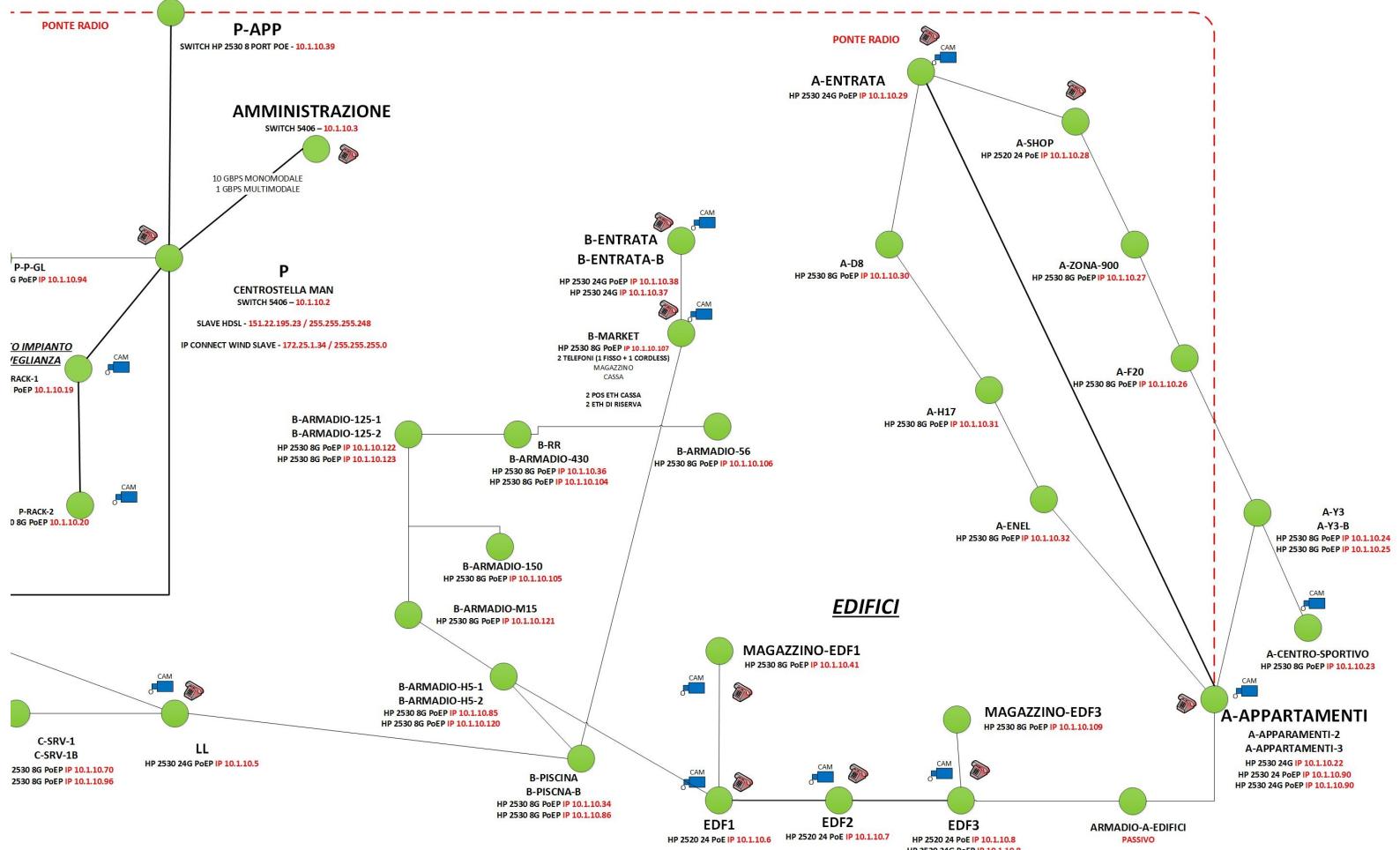


Figura 5.3: Schema Visio della rete a fine stage, seconda parte

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       if(index > 0) {
84         GM.setValue('count', 0);
85       } else {
86         GM.setValue('count', 1);
87       }
88     }
89   })();
90 }

```

```

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.

Appendice C: Script di backup Mikrotik

Di seguito è riportato lo script eseguito e schedulato sui dispositivi MikroTik, sia di tipologia router che access point. La sua esecuzione consiste nella generazione automatica di un file di backup delle impostazioni e il suo salvataggio su server *FTP_G* remoto.

```

1 # ----- Configuration -----
2 # FTP server address
3 :local ftp_server_address backupmikrotik.ftpserver.local
4 # FTP username
5 :local ftp_username ftp_username
6 # FTP password
7 :local ftp_password ftp_password
8 # remote directory
9 :local remote_directory /backupMikroTik/Router/
10 # name of the file, without the date
11 :local file_name ExportMikrotikSettingsController
12 # -----
13
14 # Get the date
15 :local ts [/system clock get time]
16 :set ts ([:pick $ts 0 2]."-".[:pick $ts 3 5]."-".[:pick $ts 6 8])
17 :local months {"jan"=1;"feb"=2;"mar"=3;"apr"=4;"may"=5;"jun"=6;
18     "jul"=7;"aug"=8;"sep"=9;"oct"=10;"nov"=11;"dec"=12}
19 :local ds [/system clock get date]
20 :local mm (:$months->[:pick $date 0 3])
21 :set ds ([:pick $ds 7 11]()."mm-".[:pick $ds 4 6])
22
23 # Compose the filename
24 :local backupFileName "$file_name-$ds-$ts"
25
26 # Export the configuration
27 /export file=$backupFileName
28
29 # Add the automatic extension to the filename
30 :set backupFileName "$backupFileName.rsc"
31 # Compose the remote path
32 :set remoteBackupFileName "$remote_directory$backupFileName.rsc"
33
34 # Upload the file to the ftp server
35 /tool fetch mode=ftp address=$ftp_server_address port=21 user=
36     $ftp_username password=$ftp_password src-path=$backupFileName
37     dst-path=$remoteBackupFileName upload=yes
38
39 # Remove the file from the device
40 /file remove $backupFileName

```

Listing 5.2: Script per il backup dei device MikroTik

Alla riga 3, 5 e 7 sono dichiarate le informazioni di accesso FTP al server dedito al mantenimento dei backup, mentre nella riga 9 viene indicata la cartella remota sulla quale inserire il file.

Alla riga 11 viene definito il nome che assumerà il file di backup, con omesse le informazioni sulla data, che saranno aggiunte automaticamente.

Lo script, che si suppone sia stato nominato "script_backup_ftp", può essere aggiunto alla schedulazione automatica mediante il seguente comando.

```
1 /system scheduler
2 add
3   name=scheduler_backup_ftp \
4     interval=1w \
5     start-date=jan/01/2018 \
6     start-time=03:00:00 \
7     on-event="/system script run script_backup_ftp" \
8     policy=ftp,read,write,policy,password,sensitive
```

Listing 5.3: Comando per la schedulazione del backup

In questo modo lo script verrà eseguito ogni lunedì alle 3:00 del mattino, in quanto il 1 gennaio 2018 è un lunedì e la cadenza sarà settimanale.

Glossario

Captive portal

Un Captive portal è una pagina web che viene mostrata agli utenti di una rete di telecomunicazioni quando tentano di connettersi ad Internet mediante una richiesta http del loro browser.

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.

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.

FTP

Il protocollo FTP, per esteso File Transfer Protocol, permette la trasmissione di dati tra host. Funziona sul protocollo TCP ed utilizza una architettura client-server, anche se è possibile trasferire dati anche tra server.

Man In The Middle

L'attacco Man In The Middle, spesso indicato con "MITM", consiste nella modifica delle tabelle ARP degli apparati di rete al fine di inserirsi in una comunicazione. Questo consente all'attaccante di analizzare il traffico del dispositivo ed eventualmente manometterlo.

Quality Of Service

La qualità del servizio, documentata mediante *RFC_G*, è la descrizione o la misurazione delle performance di un servizio di rete, secondo 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.

RFC

Un RFC o Request For Comments, in italiano "richiesta di commenti", 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

Documenti in lingua italiana

- Portale di Clusit, associazione per la sicurezza informatica
<https://clusit.it>
- Introduzione a CentOS 7
<http://www.html.it/articoli/centos-7-una-distro-enterprise-gratuita>

Documenti in lingua inglese

- Documentazione Observium
<http://docs.observium.org>
- Documentazione Microsoft relativa a Active Directory
<https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access>
- Presentazione MikroTik - WiFi Enterprise con CAPsMAN e Windows NPS
www.youtube.com/watch?v=RXkoAimlcM8
- Slide MikroTik - WiFi Enterprise con CAPsMAN e Windows NPS
https://mum.mikrotik.com/presentations/EU18/presentation_5159_1523293520.pdf
- Manuale per lo scripting su dispositivi MikroTik
<https://wiki.mikrotik.com/wiki/Manual:Scripting>
- Documentazione FreeRADIUS
<https://freeradius.org/documentation>
- Introduzione e guida a Directory Lister
<https://www.directorylister.com>