ЭЛЕМЕНТЫ АВТОМАТИЗАЦИИ ТЕХНИЧЕСКОГО АУДИТА ИБ

Пряников Андрей
Заместитель директора по безопасности
по защите информации
ООО «ТД «УНКОМТЕХ»
andpryanik@gmail.com

УНКОМТЕХ
www.uncomtech.ru

С ЧЕГО НАЧАТЬ ПОСТРОЕНИЕ ИБ?

- pentest
- Настройки СЗИ
- Разбор документации
- Инвентаризация
- Текущие проекты
- Сотрудники

ТЕХНИЧЕСКИЙ АУДИТ ИБ

Составление опросных листов	• Список серверов и ПК • Список подсетей и сетевого оборудования. Схемы сети. • Список бизнес-систем и их описание • Список СЗИ • ***
Сбор и анализ технических данных	• **Политики и настройки MS AD, ПК, Серверов** • Настройки сетевого оборудования • Настройки СЗИ • Настройки безопасности бизнес-систем • ***
pentest	• Получение прав на сетевом оборудование • Получение привилегий в домене • Получение прав в СЗИ • Получение прав в бизнес-системах • ***

САМЫЕ ПРОСТЫЕ СЦЕНАРИИ «ВЗЛОМА»? ПРИМЕРЫ.

Подобрать пароль старой забытой УЗ	Получить список всех УЗ	Подобрать множество паролей и повысить привилегии
Найти общую открытую шару с множеством данных	Закинуть туда кейлоггер или найти там чей то пароль.	Повысить привилегии
Подобрать пароль по данным из интернета	У УЗ есть доступ через VPN, а не должно быть.	Удаленный взлом и повышение привилегий
MS 17-010 или другая суперпопулярная уязвимость	Получение прав админа на забытом тестовом ПК	Полный контроль ИТ инфраструктуры
Тривиальный фишинг или социальная инженерия.	У пользователя есть права локального администратора	Повышение привилегий в ИТ инфраструктуре

POWERSHELL. ПОЛЬЗОВАТЕЛИ AD - ОБЩЕЕ.

```
$OrgUnit=Read-Host "Введите OU AD"
$user = Get-ADUser -Filter * -SearchBase $OrgUnit -Properties displayName, sAMAccountName, company, department, distinguishedName, whenCreated, pwdLastSet,
lastLogon, lastLogonTimestamp, logonCount |
    Select-Object displayName, sAMAccountName, company, department, distinguishedName, whenCreated, `
    ***
Export-Excel -Path c:\temp\$OrgUnit.Users.xlsx
```

1) Есть ли те, кто давно не подключался к домену?
2) Кто давно не менял пароль?
3) У кого выставлен Password never expires?
4) Есть ли в OU disabled включенные УЗ?
5) Аномально высокий logonCount?

displayNa	sAMAccou	company	departme	distinguis	whenCreated	pwdLastSetDT	lastLogonDT	lastLogonTimestampDT	Password	logonCou	enabled
					30.10.2012 9:35	01.11.2012 3:14	##########	##########	ИСТИНА		ИСТИНА
					##########	05.02.2013 6:22	##########	##########	ИСТИНА		ИСТИНА
					##########	07.05.2013 4:46	##########	##########	ИСТИНА		ИСТИНА
					12.11.2012 6:32	07.05.2013 5:44	##########	##########	ИСТИНА		ИСТИНА
					30.10.2012 9:35	07.05.2013 5:47	##########	##########	ИСТИНА		ИСТИНА
					##########	23.05.2013 6:02	##########	##########	ИСТИНА	0	ИСТИНА
					##########	17.04.2013 8:45	##########	##########	ИСТИНА		ИСТИНА
					14.04.2015 4:22	24.08.2015 4:59	##########	##########	ИСТИНА	0	ИСТИНА
					30.10.2012 9:35	03.12.2012 0:39	##########	02.12.2012 18:59	ИСТИНА		ИСТИНА
					13.03.2013 8:47	13.03.2013 8:47	##########	13.03.2013 8:48	ИСТИНА		ИСТИНА
					12.11.2012 6:26	21.05.2013 8:24	##########	13.06.2013 3:01	ИСТИНА		ИСТИНА
					12.11.2012 6:32	03.03.2013 6:14	07.10.2013 3:37	04.10.2013 8:14	ИСТИНА	135	ИСТИНА
					08.02.2013 8:08	08.02.2013 8:08	##########	18.10.2013 3:09	ИСТИНА		ИСТИНА
					19.03.2013 5:39	23.09.2013 2:56	19.12.2013 8:15	19.12.2013 8:15	ЛОЖЬ	90	ИСТИНА
					10.09.2012 8:07	23.05.2013 5:20	01.08.2014 6:42	24.07.2014 4:43	ИСТИНА	192	ИСТИНА
					28.11.2013 9:32	29.11.2013 4:11	25.02.2015 13:15	18.02.2015 17:59	ИСТИНА	272	ИСТИНА
					##########	12.03.2013 8:59	05.03.2015 2:23	24.02.2015 3:08	ИСТИНА	525	ИСТИНА
					30.10.2012 9:35	15.01.2013 3:44	30.03.2015 3:01	26.03.2015 9:47	ИСТИНА	251	ИСТИНА
					12.11.2012 6:11	05.03.2013 4:28	23.01.2015 2:28	30.03.2015 1:54	ИСТИНА	559	ИСТИНА
					##########	23.01.2013 11:23	29.04.2015 21:58	29.04.2015 21:58	ИСТИНА	579	ИСТИНА
					26.02.2014 5:11	26.02.2014 5:11	07.05.2015 10:03	07.05.2015 10:03	ИСТИНА	228	ИСТИНА
					12.11.2012 6:26	13.02.2013 9:13	29.04.2015 2:51	18.05.2015 3:23	ИСТИНА	409	ИСТИНА
					31.05.2013 3:55	21.10.2013 5:48	27.05.2015 7:36	18.05.2015 4:15	ИСТИНА	332	ИСТИНА
					12.11.2012 5:47	06.05.2015 5:47	29.06.2015 2:46	19.06.2015 2:35	ЛОЖЬ	565	ИСТИНА
					##########	06.08.2015 11:55	11.08.2015 11:51	06.08.2015 12:00	ИСТИНА	82	ИСТИНА
					02.11.2012 9:23	09.12.2015 3:58	06.11.2015 8:08	09.12.2015 3:58	ЛОЖЬ	437	ИСТИНА
					16.10.2013 6:35	16.10.2013 6:35	11.12.2015 5:45	11.12.2015 5:43	ИСТИНА	181	ИСТИНА
					30.10.2012 9:35	11.01.2013 9:15	18.02.2016 9:40	18.02.2016 9:40	ИСТИНА	309	ИСТИНА
					13.11.2012 3:40	16.04.2013 11:46	11.03.2016 19:53	07.03.2016 14:47	ИСТИНА	319	ИСТИНА
					##########	15.03.2013 10:54	19.03.2016 5:32	19.03.2016 5:32	ИСТИНА	252	ИСТИНА
					13.11.2012 3:40	16.04.2013 11:50	18.04.2016 5:42	18.04.2016 5:42	ИСТИНА	72	ИСТИНА
					13.11.2012 4:07	20.05.2013 5:40	07.10.2016 5:10	07.10.2016 5:10	ИСТИНА	172	ИСТИНА
					##########	07.05.2013 3:55	25.08.2016 17:12	15.10.2016 17:18	ИСТИНА	1032	ИСТИНА
					03.04.2014 3:29	15.11.2016 4:20	29.11.2016 6:28	28.11.2016 5:31	ЛОЖЬ	691	ИСТИНА
					02.09.2015 4:17	02.09.2015 4:17	10.08.2016 7:37	04.05.2017 2:58	ИСТИНА	100	ИСТИНА
					13.11.2012 4:12	22.05.2017 10:30	31.01.2017 10:56	22.05.2017 10:30	ЛОЖЬ	696	ИСТИНА
					10.07.2017 5:09	10.07.2017 5:09	21.09.2017 11:43	21.09.2017 11:43	ИСТИНА	37	ИСТИНА

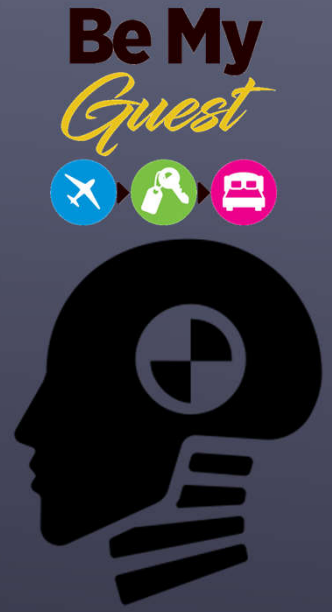
Давно не подключались | Давно не менялся пароль | Прочее | Disabled

POWERSHELL. ПОЛЬЗОВАТЕЛИ AD – ШАБЛОНЫ ИМЕНИ.

```
$username=Read-Host "Введите шаблон имени пользователя"
$user = Get-ADUser -LDAPFilter "(sAMAccountName=*$username*)"  -Properties displayName, sAMAccountName, company, department, distinguishedName, whenCreated, pwdLastSet, lastLogon, lastLogonTimestamp, logonCount |
    Select-Object displayName, sAMAccountName, company, department, distinguishedName, whenCreated, `
```

Цель – проверить какие из типовых названий технических учетных записей есть в AD.

Гостевые	• *guest* • *user* • ***
Тестовые	• *temp* • *test* • ***
Сервисные	• *service* • *svc* • ***



POWERSHELL. SECURITY ГРУППЫ AD.

```
$adgroups = "test", "adm","vpn","remote","test","1C"
foreach ($adgroup in $adgroups)
{
$adgroup_masked="*$adgroup*"
$Groups = Get-ADGroup -Filter {name -like $adgroup_masked}
ForEach ($Group In $Groups)
{
   "Group: " + $Group.Name | Out-File c:\temp\$adgroup.group.users.txt -append
   Get-ADGroupMember -Identity $Group -Recursive | Get-ADUser | select name, samaccountname, enabled | Out-File c:\temp\$adgroup.group.users.txt -append
}
}
```

Цель – проверить какие типовые security группы имеются (по шаблону имени) и кто в них включён.

Удаленный доступ	• *VPN* • *REMOTE* • ***
Тестовые	• *temp* • *test* • ***
Административные	• *adm* • *1C* • ***

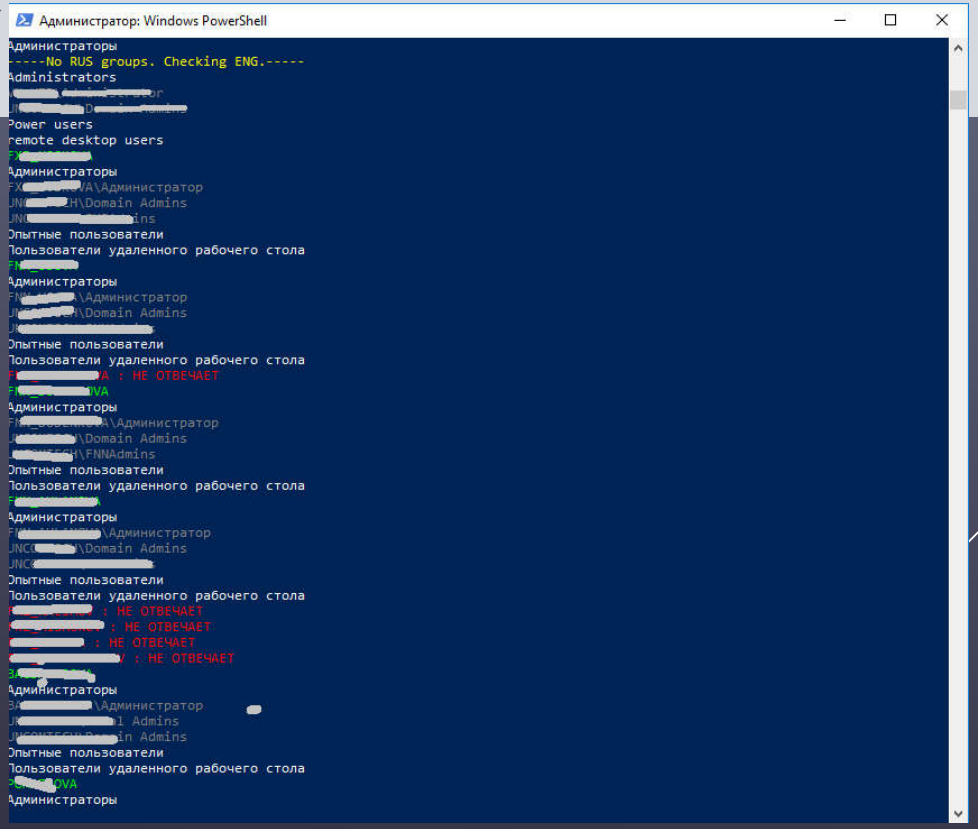
adm.group.users.txt — Блокнот

Файл Правка Формат Вид Справка

```
Group: Enterprise Admins

name           samaccountname enabled
----           -------------- -------
                                 True
                 strator         True
                 min             True


Group: Administrators

name           samaccountname enabled
----           -------------- -------
A                strator         True
Ф                                True
S                                True
A                                True
i                vice            True
D                                True
c                oint            True
K                                True
D                                True


Group: DnsAdmins
Group: DHCP Administrators
Group: DeviceLock Administrators

name                   samaccountname enabled
----                   -------------- -------
Ad                       istrator     True
Фр                                    True
Па                       vl           True
```

POWERSHELL. ПРИВЕЛИГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ ПК.

```
***
$PC_group_all_rus | %{
        $PC_group = $_
          "$PC_group :"
          write-host $PC_group -ForegroundColor White
          $ADSI_WinNT = [ADSI]"WinNT://$PC_name/$PC_group,group"
          $ADSI_WinNT.Members() | foreach {
             $memberDomain = $_.GetType().InvokeMember("AdsPath","GetProperty",$null,$_,$null).split("/")[-2]
             $member = $_.GetType().InvokeMember("AdsPath","GetProperty",$null,$_,$null).split("/")[-1]
             $Domainmember=$memberDomain+"\"+$member
write-host $Domainmember -ForegroundColor DarkGray
***
```



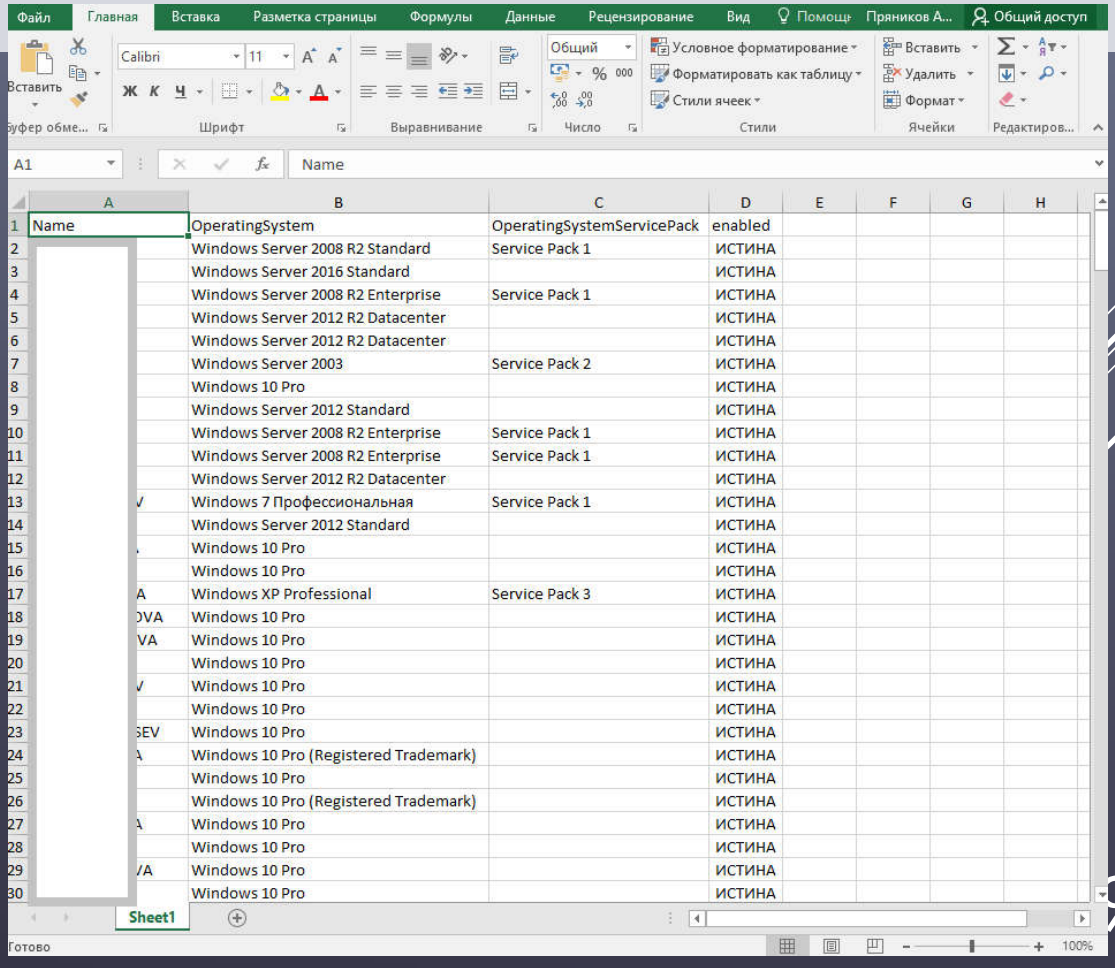
Цель – Собрать список всех локальных администраторов на всех ПК домена. Собрать всех RDP пользователей и Power users.

POWERSHELL. СПИСОК ПК И СЕРВЕРОВ.

```
$OrgUnit=Read-Host "Введите OU AD"
$PC = Get-ADComputer -SearchBase $OrgUnit -Filter * -Property * | Select-Object
Name,OperatingSystem,OperatingSystemServicePack,enabled |
Export-Excel -Path c:\temp\$OrgUnit.PC_OS.xlsx
```

Цель – Собрать список всех ПК и серверов.
Найти:

1) Старые ОС.
2) Что не указали ИТ в опросном листе?
3) ПК УЗ которых должны быть отключены, но значение enabled = истина.



Name	OperatingSystem	OperatingSystemServicePack	enabled
	Windows Server 2008 R2 Standard	Service Pack 1	ИСТИНА
	Windows Server 2016 Standard		ИСТИНА
	Windows Server 2008 R2 Enterprise	Service Pack 1	ИСТИНА
	Windows Server 2012 R2 Datacenter		ИСТИНА
	Windows Server 2012 R2 Datacenter		ИСТИНА
	Windows Server 2003	Service Pack 2	ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows Server 2012 Standard		ИСТИНА
	Windows Server 2008 R2 Enterprise	Service Pack 1	ИСТИНА
	Windows Server 2008 R2 Enterprise	Service Pack 1	ИСТИНА
	Windows Server 2012 R2 Datacenter		ИСТИНА
	Windows 7 Профессиональная	Service Pack 1	ИСТИНА
	Windows Server 2012 Standard		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows XP Professional	Service Pack 3	ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro (Registered Trademark)		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro (Registered Trademark)		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА
	Windows 10 Pro		ИСТИНА

POWERSHELL. СПИСОК СТАРЫХ ПК И КОНТРОЛЛЕРОВ ДОМЕНА.

```
$DaysInactive = 90
$time = (Get-Date).Adddays(-($DaysInactive))
  $PC=Get-ADComputer -Filter {LastLogonTimeStamp -lt $time} -Properties LastLogonTimeStamp |
select-object Name,@{Name="Stamp";
Expression={[DateTime]::FromFileTime($_.lastLogonTimestamp)}},enabled |
Export-Excel -Path c:\temp\Incative_PC.xlsx
```

Цель – Вывести список неактивных более 90 дней ПК. Понять почему они давно не подключались, и не «мусорные» ли они?

```
(Get-ADForest).Domains | % { Get-ADDomainController -Discover -DomainName $_ } | % { Get-ADDomainController -server $_.Name
-filter *} |
select hostname, site, operatingsystem, OperatingSystemServicePack, @{name="vendor";expression={(gwmi Win32_ComputerSystem
-ComputerName $_.hostname).Manufacturer}}, @{name="model";expression={(gwmi Win32_ComputerSystem -ComputerName
$_.hostname).model}}, @{name="CPU, count";expression={(gwmi Win32_ComputerSystem -ComputerName
$_.hostname).NumberOfLogicalProcessors}}, @{name="RAM/GB";expression={[math]::round((gwmi Win32_ComputerSystem -
ComputerName $_.hostname).Totalphysicalmemory/1GB)}} |
sort hostname |
Export-Excel -Path c:\temp\dc_forest_list.xlsx
```

Цель – Получить весь лес с контроллерами домена.

NMAP. СПИСОК ОТКРЫТЫХ ШАР.

nmap -p 445,139 --script **smb-enum-shares** --script-args smbuser=test,smbpassword=test,smbdomain=domain.com 192.168.1.0/24 192.168.2.0/24

Цель – Получить все шары с минимальными правами пользователя (а можно для начала и без них).

```
Host is up (0.0079s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: [redacted]01 (Hewlett Packard)

Host script results:
| smb-enum-shares:
|   account_used: k[redacted]m\test
|   \\[redacted]\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\[redacted]\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1\x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1\xD1\x89\xD0\
|     Anonymous access: <none>
|     Current user access: <none>
|   \\[redacted]\D$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1\x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1\xD1\x89\xD0\
|     Anonymous access: <none>
|     Current user access: <none>
|   \\[redacted]\E$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1\x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1\xD1\x89\xD0\
|     Anonymous access: <none>
|     Current user access: <none>
|   \\[redacted]\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: \xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 IPC
|     Anonymous access: READ
|     Current user access: READ/WRITE
|   \\[redacted]\Share:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ
|   \\[redacted]\Spam:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|_    Current user access: READ
```

NMAP. БЫСТРЫЙ ПОИСК УЯЗВИМЫХ ХОСТОВ.

nmap -p 445,139 **--script smb-vuln-ms17-010** 192.168.1.0/24 192.168.2.0/24
nmap -p 445,139 **--script smb-vuln-ms08-067** 192.168.1.0/24 192.168.2.0/24
***

Цель – Оперативно получить список уязвимых ПК без использования платных сканеров


```
Nmap scan report for i[redacted]com ([redacted])
Host is up (0.00044s latency).

PORT    STATE  SERVICE
139/tcp open   netbios-ssn
445/tcp closed microsoft-ds
MAC Address: 00:02:55:DF:9C:D4 (IBM)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

ПОСЛЕ ИНВЕНТАРИЗАЦИИ И ТЕХНИЧЕСКОГО АУДИТА ИБ

Наведение порядка

- Удалить весь «мусор» из AD и других систем. Установить обновления.
- Ограничить все найденные «шары»
- Ограничить доступ в интернет
- Ограничить доступ к внешним портам (USB и пр.)

Контроль аутентификации и привилегий

- Парольная политика и памятки сотрудникам
- Двухфакторка для привилегированных УЗ
- Изолированные ПК для ИТ администраторов
- Контроль локальных администраторов (LAPS + Powershell)

Настройки ИБ

- Настройка безопасности бизнес-систем
- Настройка безопасности имеющихся СЗИ
- Настройка безопасности отдельных серверов и ПК
- Настройка безопасности сетевого оборудования

Новые проекты

- Написание или актуализация ОРД по ИБ
- SIEM
- IDM
- ***

Если у вас жуткий бардак в квартире – поможет ли робот-пылесос?

*Нет – он захлебнется первым носком

ВОПРОСЫ?

Пряников Андрей
Заместитель директора по безопасности
по защите информации
ООО «ТД «УНКОМТЕХ»
andpryanik@gmail.com

УНКОМТЕХ
www.uncomtech.ru